Guiding Behavior in Organizational Cybersecurity

Dissertation | Tobias Reittinger



Guiding Behavior in Organizational Cybersecurity

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft eingereicht an der Fakultät für Informatik und Data Science der Universität Regensburg

vorgelegt von

Tobias Reittinger, M.Sc.

Berichterstatterin und Berichterstatter:

Prof. Dr. Günther Pernul

Prof. Dr. Susanne Leist

Prof. Dr. Sokratis Katsikas

Tag der mündlichen Prüfung: 22. Oktober 2026



Universität Regensburg
Fakultät für Informatik und Data Science
Lehrstuhl für Wirtschaftsinformatik I – Informationssysteme

Regensburg, 2026

To my loving wife Lisa,
and my parents, Petra and Markus.

Acknowledgement

I would like to express my deepest gratitude to those who supported me throughout these wonderful three years. To my supervisor, Günther Pernul, for this research opportunity, for the supportive mentorship, for encouraging me to pursue my ideas, and for granting the flexibility that sustained my unconventional daily rhythm. To my second supervisor, Susanne Leist, for the insightful perspective and for demonstrating how to translate research into practical applications within our university.

I have been fortunate to collaborate with an extraordinary group of colleagues who became dear friends. To Manfred, for showing me how exciting research can be. To Daniel, for the feedback during the early days and the discussions about the Tour de France. To Lena, for the support on research challenges, the company on trips to project meetings, and every day in the office, you have been a role model. To Thomas, for our debates over every sentence that pushed our work to its best possible form. I'll never forget our conference adventure in San José, and the lesson that each drive back across the Golden Gate Bridge carries its own toll. To Johannes, for our endless conversations about life, and occasionally research, and for the fun we shared on project-meeting trips and while watching football. We've grown together as researchers, and I'm grateful for your shared passion. To Sabrina, Sascha, and Raphael, for integrating a new perspective into our research. To Philip, Markus, Mathis, Daniel, Marietheres, and Robin, the coffee breaks and lunches wouldn't have been the same without you. To Vahiny, for your engaging visits. To Petra, for guiding me through the bureaucratic labyrinth. To Eric, Christoph, and Werner for helping me with every technical challenge.

My journey has also been supported by the unwavering support of friends and family. To my wife Lisa, for making every day a joy, supporting me through difficult times, and for our unforgettable travels and road bike tours. You remind me that there is more to life than work, and you inspire me to become the very best version of myself. To my parents, Petra and Markus, for encouraging my curiosity, for your unwavering support, and for our incredible mountain-biking adventures. To my brother Fabian, for letting me stay at your Regensburg apartment, for our gaming sessions, and for showing me that helping others is one of life's greatest rewards. To my grandparents Heinrich, Irmgard, and Gerti, for teaching me to savor the present and to recognize what truly matters in life. To my friends Michael, Sebastian, and Tobias, for our trips and gaming sessions. To the squirrels on our balcony, who always put a smile on my face and remind me that a snack can turn any day around.

Cybersecurity is a sociotechnical challenge: outcomes arise from the interaction of technical controls and people navigating everyday work demands, usability constraints, and bounded attention. This dissertation examines how behavior can be guided so that secure action becomes well-integrated into everyday work. Across four research areas, it (i) relates organizational motivational practices to behavioral theory, (ii) identifies barriers and effective interventions for passkey adoption, (iii) investigates how digital nudges shape decisions in access reviews, and (iv) develops incentive mechanisms to support inter-organizational cyber threat intelligence sharing.

Contents

Acknowledgement **i**

Abstract **ii**

I Dissertation Outline **1**

1 Introduction . . . 2
2 Background and Related Work . . . 4
2.1 Motivation: Self Determination Theory (SDT) . . . 4
2.2 Decision-Making: Choice Architecture and Digital Nudges . . . 5
3 Research Areas . . . 7
3.1 Selection of Research Areas . . . 7
3.2 Research Areas and Research Questions . . . 9
3.3 Research Environment . . . 12
4 Results . . . 14
4.1 Overview of Publications . . . 14
4.2 Research Area 1: Foundations . . . 15
4.3 Research Area 2: Passkeys . . . 17
4.4 Research Area 3: Access Reviews . . . 20
4.5 Research Area 4: Cyber Threat Intelligence (CTI) Sharing . . . 22
4.6 Complementary Publications . . . 25
5 Discussion . . . 28
5.1 Implications for Research and Industry . . . 28
5.2 Ethical Aspects of Guiding Human Behavior . . . 28
5.3 Future Work: AI and Human Behavior in Cybersecurity . . . 30
5.4 Limitations . . . 31
6 Conclusion . . . 32

Bibliography **34**

II Research Papers **48**

P1 Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice . . . 49

P2 No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage 66
P3 Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption. 87
P4 Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations. 105
P5 Share and Benefit: Incentives for Cyber Threat Intelligence Sharing 127

Part I

Dissertation Outline

1 Introduction

Cyberattacks have become a persistent risk in organizations: incidents continue to increase in frequency and sophistication, and their consequences reach beyond immediate financial loss to include operational disruption, legal consequences, and long-term reputational harm [57, 117]. As organizations extend business processes across cloud services and AI-enabled tools, the attack surface continues to expand [31, 80]. In response, organizations invest heavily in security technologies and compliance programs [32, 41, 91]. However, the effectiveness of many of these measures depends on employees correctly enacting them in daily work, and breach evidence indicates that compromises often begin with the human element [117].

This reflects a recurring paradox in organizational cybersecurity: attackers often succeed by exploiting human behavior around technical systems rather than defeating the systems themselves [1,53]. Phishing, social engineering, and credential compromise remain common initial access vectors across incidents of varying scale [47, 117]. Authentication illustrates this gap particularly well. Password-based authentication can be technically robust when correctly implemented, yet real-world security is frequently undermined by the cognitive burden passwords place on users [1, 35]. Individuals are expected to create long, hard-to-guess passwords, follow complex password policies, and remember a unique secret for each service [35, 65, 78]. In practice, many adopt coping strategies such as predictable password choices, minor variations of existing passwords, and credential reuse [24,35,123]. In other words, security mechanisms that are robust in principle can become fragile in use when everyday practices diverge from their design assumptions. From a socio-technical perspective, this should not be framed as a moral failure of users, as employees are integral components of organizational defense [1, 103]. Instead, it underscores that secure behavior is inherently demanding, and that security outcomes depend on how controls and requirements align with human capabilities and everyday workflows [11, 53].

Organizations have responded to these human-dependent risks, often driven by regulatory and compliance expectations, by investing in security awareness and training programs [29, 88]. However, evidence suggests that awareness efforts alone frequently struggle to translate knowledge into sustained behavior change [67, 88]. A recent meta-analysis reports stronger effects of training on knowledge than on observed security behavior [88], and a large-scale study indicates that embedded phishing training may be less effective than assumed and can even produce unintended side effects [67]. This highlights that improving security outcomes requires complementing knowledge with measures that make secure action easier in day-to-day work.

Taken together, this points to a broader implication: even when organizations deploy strong technologies and invest in awareness, security outcomes can remain fragile if secure action is opaque, effortful, or poorly integrated into everyday workflows [11, 53]. Security tasks compete with primary work goals, and employees operate under

bounded attention, deadline pressure, and increasing tool complexity [11, 53]. When policies are complicated, interfaces unclear, or the consequences of choices are hard to anticipate, people may postpone, circumvent, or superficially complete security tasks, resulting in nominal compliance without commensurate risk reduction [53, 93]. Organizational cybersecurity, therefore, depends on making secure behavior usable and actionable in the context of real work [93, 103].

Accordingly, this dissertation argues that improving organizational cybersecurity requires systematic behavior guidance by shaping environments, processes, and interfaces so that secure action becomes easier to choose, execute, and sustain. Such guidance can draw on complementary behavioral lenses. Self-Determination Theory (SDT) explains how motivation can be supported by fostering autonomy, competence, and relatedness, with extrinsic mechanisms such as incentives playing a supporting role [26]. In parallel, digital nudges are interventions that modify digital choice architectures (e.g., defaults, salience cues, and reminders) to shape behavior while maintaining freedom of choice and upholding ethical principles [98, 109, 124]. Together, these perspectives motivate a behavioral approach to organizational cybersecurity. Thus, the following research question is posed for this dissertation:

How to guide behavior in organizational cybersecurity?

The dissertation addresses this research question through four research areas, each examining a distinct leverage point for guiding security behavior in organizations. Research Area 1 *Foundations* examines how organizations motivate members toward secure behavior and evaluates these practices against theory-based recommendations [93]. Research Area 2 *Passkeys* investigates why passkey use remains low despite security and usability benefits, focusing on usage barriers and interventions that increase adoption [94, 97]. Research Area 3 *Access Reviews* evaluates whether digital nudges can improve regulatory-driven access reviews and support revocation of excessive authorizations [10]. Research Area 4 *CTI Sharing* addresses the limited sharing of cyber threat intelligence between organizations by designing incentive mechanisms, integrating them into a CTI sharing platform, and evaluating their effects on organizations' willingness to share and participate [95].

The dissertation is organized as follows. Chapter 2 establishes the conceptual foundations by introducing SDT and digital nudges, and situates them in related work. Chapter 3 presents the research areas by motivating their selection, formulating the corresponding research questions, and describing the research environment. Chapter 4 presents the dissertation's contributions through five publications spanning these research areas. Chapter 5 synthesizes the findings and discusses implications, ethical considerations, future work, and limitations, and Chapter 6 concludes the dissertation.

2 Background and Related Work

Organizational cybersecurity is a sociotechnical challenge: security outcomes emerge from the interplay of technical controls, work practices, and the decision-making of people who must implement security measures under real-world constraints [1, 93]. This chapter introduces two behavioral perspectives and situates them in related work, providing the conceptual foundation for the dissertation papers and informing the design of the dissertation's applied interventions. Specifically, it draws on motivation through SDT and on decision-making through choice architecture and digital nudges.

2.1 Motivation: Self Determination Theory (SDT)

Self Determination Theory (SDT) explains why people initiate, sustain, or disengage from behaviors by focusing on the quality of motivation, particularly whether it is experienced as *autonomous* (self-endorsed) or *controlled* (pressure-driven) [39, 100]. Rather than viewing motivation as fixed, SDT conceptualizes it as a continuum of internalization in which externally prompted behaviors can become more self-determined as individuals come to accept the underlying goals as their own [26]. This distinction is especially relevant in organizational cybersecurity because many security behaviors (e.g., authentication practices) are formally required, yet their effectiveness depends on employees enacting them reliably and repeatedly in day-to-day work [1, 53]. In the following, motivational reasons are discussed in terms of *intrinsic* motivation, where people act because the activity itself is enjoyable or satisfying, and *extrinsic* motivation, where people act to achieve a separable outcome such as compliance, rewards, or a valued goal [100]. Importantly, intrinsic motivation is inherently autonomous, whereas extrinsic motivation can be experienced as autonomous or controlled depending on whether the goal is personally endorsed or primarily driven by external pressure [26, 100].

Intrinsic motivation. Intrinsic motivation refers to engaging in an activity because it is inherently enjoyable or satisfying [100]. SDT further proposes that intrinsic motivation is supported when three basic psychological needs are satisfied: *autonomy* (experiencing choice and volition), *competence* (feeling capable and effective), and *relatedness* (feeling socially connected and valued) [100]. In cybersecurity, organizations often try to support these needs through training and user support, for example, by providing clear guidance, timely feedback, and help with secure workflows [50]. However, these needs are frequently undermined by friction, unclear rationales, and policies users perceive as misaligned with their job goals [1, 11]. For example, credential management increasingly relies on password managers and Multi-Factor Authentication (MFA), yet users may avoid these practices when setup feels imposed, interfaces or recovery steps are confusing, or security is perceived as policing rather than shared responsibility [15, 68]. SDT suggests that such behaviors are more likely to be maintained when designs support autonomy, competence, and relatedness, for example, by

offering meaningful options within approved methods (e.g., choosing a second factor type), providing actionable feedback that helps users succeed, and using positive social messaging that reinforces collective responsibility [1, 106, 115].

Extrinsic motivation. By contrast, extrinsic motivation covers behaviors that are prompted by external demands or incentives, as well as behaviors people pursue because they personally value the underlying goal [100]. In cybersecurity, organizations frequently use deterrence and structured incentives to raise policy compliance [22, 61, 93]. Similarly, training and awareness programs often incorporate gamified elements such as points, challenges, and feedback loops to increase engagement and learning, with evidence of improvements in security-related attitudes and self-reported behavior in some settings [6, 28, 116]. While these approaches can be effective, SDT cautions that rewards or sanctions perceived as controlling may backfire by reducing people's sense of choice and, in turn, undermining intrinsic motivation [25]. Sustained effects are therefore more likely when incentives and gamified features are designed to feel supportive rather than coercive, for example by emphasizing progress and skill building, offering meaningful choice in participation, and framing security as a shared responsibility [39, 100].

2.2 Decision-Making: Choice Architecture and Digital Nudges

People make thousands of small decisions every day [36], for example, when prioritizing emails, deciding which tasks to delegate, or choosing when to double-check details. Security-relevant choices are embedded in this stream of routine activity, such as judging whether a message is legitimate or deciding whether to enroll in MFA for an account. As a result, security decisions compete with day-to-day work goals and are frequently handled under the same practical pressures as other workplace choices [11, 53]. Accordingly, decision makers operate under constraints such as limited attention, time pressure, and incomplete information [62, 107]. When many choices accumulate over the course of a day, sustained deliberation can become harder, a phenomenon often discussed as *decision fatigue* [21, 87]. This state is associated with an increased tendency to simplify decisions and to rely more on default or low-effort responses [86, 119].

A central mechanism for coping with these constraints is the use of *heuristics*: simple decision strategies that reduce cognitive effort by simplifying the problem and focusing on cues that are quick to evaluate [112]. In security contexts, trust judgments often function as a heuristic, shaped by contextual cues such as apparent authority, familiarity of a sender identity, or urgency framing, because these cues are salient and easy to process [59, 118, 125]. In many situations, such shortcuts are efficient, however, in adversarial settings, they can be systematically exploited [43, 108]. Phishing research shows that users frequently attend to these persuasive cues while overlooking or misinterpreting more diagnostic indicators, which helps explain why well-crafted phishing messages succeed even when technical signals (e.g., fraudulent look-alike URLs) are available [27, 118].

Heuristic processing can therefore be prone to *cognitive biases*, which are systematic and predictable deviations from normative judgment under uncertainty [62, 112]. A prominent example is the *status quo bias*: when choices are complicated, or consequences are uncertain, individuals tend to prefer maintaining the current state or accepting a default [102]. In organizational security, status quo bias can be amplified by enrollment effort and uncertainty, discouraging protective actions such as adopting stronger authentication and installing security updates promptly [18, 102, 110].

Nudges address such patterns by deliberately shaping *choice architecture*, the way options are presented, to guide behavior toward beneficial actions while preserving freedom of choice [109]. Many nudges work by accounting for predictable decision tendencies, including cognitive biases, and redesigning the choice architecture so that users are less likely to remain in a suboptimal status quo and more likely to follow through on intentions they already endorse [109]. A particularly prominent nudge is the *choice default*: by pre-selecting an option or presenting it as the standard, defaults harness the same inertia described by status quo bias and can shift behavior without restricting alternatives [60, 102]. A well-known example is automatic enrollment in retirement savings plans, which substantially increases participation by changing the default while maintaining opt-out [69]. In digital systems, nudging translates to *digital nudging*, i.e., interface- and process-level interventions such as defaults, salience, timely prompts, friction adjustments, and guided steps [16, 74–76, 124]. Because nudges intentionally influence behavior, their use requires particular care regarding transparency, user welfare, and legitimacy [98]. Importantly, nudges can be misused as *dark patterns*, design elements that coerce, steer, or deceive users into unintended and potentially harmful decisions [70], so the ethical dimension of guiding behavior is discussed in Section 5.2. In cybersecurity contexts, evidence from phishing-warning banners in email clients, MFA enrollment prompts, and software-update messaging suggests that calibrated salience nudges can measurably increase protective actions [33, 46, 85].

3 Research Areas

This dissertation addresses the overarching question of *how to guide behavior in organizational cybersecurity* through four research areas, as visualized in Figure 1. The areas structure the dissertation's five publications (P1–P5) and reflect distinct, complementary leverage points for behavior guidance: (i) individual motivation and organizational practices that shape security behavior (*Foundations*), (ii) secure adoption and use of passkeys for authentication (*Passkeys*), (iii) secure decision-making in organizational access review processes (*Access Reviews*), and (iv) inter-organizational cooperation as a prerequisite for collective defense (*CTI Sharing*). Together, these areas cover complementary points at which behavior can be guided, through individual actions, organizational processes, and cross-organizational collaboration, providing a coherent view of behavior guidance across the cybersecurity lifecycle.



Figure 1: This dissertation focuses on four research areas: *Foundations*, *Passkeys*, *Access Reviews*, and *CTI Sharing*.

3.1 Selection of Research Areas

The selection of the four research areas follows three criteria aligned with the dissertation's overall research question and socio-technical premise:

1. *Behavioral criticality.* The security outcome depends considerably on human action or decision-making.
2. *Practical relevance and impact.* The topic corresponds to persistent, frequent risk patterns in organizational practice.
3. *Actionability.* There exists design space to guide behavior through motivational support, choice architecture, or incentives.

In the following, the selection per research area is explained in detail.

Foundations. Security behavior is not a pure knowledge problem: humans commonly make trade-offs between primary work goals and security tasks, responding to perceived costs, benefits, and organizational signals [11, 19, 53]. Policy-compliance research likewise shows that motivation, attitudes, and perceived organizational support

strongly shape intended and actual compliance [13, 90]. Because secure behavior in this domain is behavior-critical, practically relevant in everyday work, and actionable through motivational support and choice architecture, Research Area 1 establishes a theory-informed baseline of current motivational practices as a foundation for subsequent behavior guidance.

Passkeys. Authentication is a frequent entry point for attacks, with incident reports repeatedly implicating credential abuse and phishing/social engineering [117]. At the same time, the ecosystem is shifting from passwords to phishing-resistant, public-key-based methods [42, 126]. Passkeys can mitigate credential reuse, weak passwords, and phishing susceptibility, but their benefits depend on correct adoption and use in everyday practice amid heterogeneous devices, platforms, and recovery flows [97, 126]. This makes passkeys behavior-critical because security outcomes depend on user adoption, practically relevant given the prevalence of credential attacks, and actionable because the user authentication interface offers clear design levers for guidance during this high-impact transition.

Access Reviews. Over-privileged identities amplify the impact of compromise and insider misuse, and permissions accumulate over time [56, 82]. Accordingly, many regulations require organizations to conduct periodic access reviews, aiming to limit excess privileges [14, 49, 54, 113, 114]. In practice, access reviews are recurring, time-constrained decisions in which humans must interpret opaque authorizations, making them prone to superficial completion [58]. Given persistent authorization weaknesses in application security [81], access reviews are practically relevant because they recur frequently, behavior-critical because reviewers' decisions directly shape authorization risk, and actionable because the user interface offers design opportunities to shift revocation decisions at scale.

CTI Sharing. Cyber threats span organizations, supply chains, and infrastructures, making CTI valuable for preparedness and response [30]. Yet sharing remains limited due to coordination costs, confidentiality concerns, legal and reputational risk, and free-rider dynamics [4, 12, 111, 121]. Prior work and guidance therefore emphasize that effective sharing requires governance and participation mechanisms that align incentives and build trust, in addition to standards and platforms [73, 120, 121]. Research Area 4 targets CTI sharing because it is behavior-critical, as participation hinges on organizations' sharing decisions, practically relevant because barriers recur across initiatives, and actionable because incentive and mechanism design provides concrete intervention points for building sustainable CTI-sharing ecosystems.

Synthesis. Together, the four areas capture complementary, high-leverage use cases where security outcomes depend considerably on human decisions, the risks are persistent in practice, and there is clear design space to guide behavior: motivating secure work practices (Area 1), supporting secure authentication behavior (Area 2), improving authorization decisions for risk reduction (Area 3), and enabling cooperation for collective defense (Area 4). This scope supports both explanatory insight into why behavior

diverges from security intent and prescriptive knowledge on how processes, interfaces, and incentives can better guide behavior.

3.2 Research Areas and Research Questions

The dissertation's five publications are organized into four research areas, each paired with a corresponding research question. The following introduces each area by outlining its central problem and behavioral leverage point, then states the research question and identifies the publications (P1–P5) that address it. Section 4 subsequently presents the results on a per-area basis and summarizes the individual papers.

Research Area 1: Foundations. Organizations increasingly recognize that cybersecurity outcomes are shaped not only by technical controls, but also by whether employees can effectively enact these controls in daily work under time pressure, competing priorities, and usability constraints [1, 53, 117]. In response, organizations commonly invest in formal compliance measures such as security policies, awareness training, and monitoring or sanctioning mechanisms, yet these approaches often fail to produce sustained secure behavior and may encourage superficial compliance [7, 23, 52]. When security demands exceed employees' available time, attention, or practical ability to comply, employees may instead adopt coping strategies and "good-enough" behavior that preserves primary work goals [11, 53]. Behavioral research therefore points to complementary strategies for fostering secure behavior, for example, by supporting autonomy, competence, and relatedness, and by designing choice architecture through digital nudges [26, 109, 124]. However, existing studies have often evaluated individual interventions in isolation (e.g., training, phishing simulations, interface warnings), leaving limited insight into the broader portfolio of behavioral measures organizations implement and how employees perceive and respond to these measures in practice [67, 85, 88, 93]. To address this gap, Research Area 1 examines how organizations currently motivate secure behavior, how employees perceive these measures, and how organizational practice aligns with theory-based recommendations. Accordingly, it tackles the following research question:

RQ1. *How do organizations motivate employees toward secure behavior?*

Publication **P1** addresses RQ1 by examining motivational strategies used in organizational practice and analyzing how these strategies relate to intrinsic support (autonomy, competence, relatedness), extrinsic approaches (incentives), and choice-environment interventions (nudges), deriving implications for theory-informed guidance [93].

Research Area 2: Passkeys. Credential abuse and phishing remain persistent drivers of security incidents [117]. A key underlying contributor is continued reliance on passwords: while password-based authentication can be technically robust when correctly implemented, its real-world security is often constrained by the cognitive effort it demands from users [1, 35]. In practice, users must create long, random passwords, comply with password policies, and manage numerous secrets across multiple

accounts [35, 65, 78]. Unsurprisingly, they often fall back to coping strategies such as password reuse, predictable modifications, or weak and easily guessable passwords, which introduce systemic risk into the authentication schemes [24, 35, 123].

One common approach to mitigate these challenges is the use of password managers, which reduce memory burden by storing (and often generating) unique passwords [83]. However, they introduce adoption hurdles (setup, onboarding, and trust decisions) and still expose users to phishing and account-takeover attempts at the point of login [5, 71, 83]. Complementarily, multi-factor authentication (MFA) aims to limit the impact of password compromise by requiring an additional factor (e.g., SMS/OTP or push approvals) [18]. Yet widely deployed MFA variants have low usage rates, often add usability friction, and remain vulnerable to phishing and social engineering (e.g., real-time relay or approval fatigue), leaving substantial residual risk in password-centric authentications [2, 18].

To address both the usability challenges and the phishing surface inherent in passwords and their compensating controls, passkeys have been introduced as phishing-resistant, public-key credentials based on WebAuthn/FIDO2 [34, 55]. In a passkey flow, the private key remains on (or is protected by) the user's device and authentication is completed by unlocking the credential with user verification, typically a built-in biometric or, as a fallback, the device PIN, so no shared secret needs to be typed or remembered [34, 55]. However, empirical work shows that moving to passwordless authentication does not automatically yield a seamless experience: users report confusion and concerns around device dependence, portability across heterogeneous ecosystems, and especially account recovery when a device or authenticator is lost [42, 126]. Consequently, the technical promise of passkeys does not automatically translate into broad real-world uptake, leaving a gap between capability and everyday adoption. This research area therefore investigates which barriers impede passkey use and evaluates interventions that increase adoption across key user-journey touchpoints. Thus, this area addresses the following research question:

RQ2. *Which barriers impede passkey use, and how to increase adoption?*

Publications **P2** and **P3** address RQ2. **P2** reports a large-scale field study of passkey adoption and longitudinal use, identifying barriers encountered in practice, including challenges related to synchronization [97]. Building on these insights, **P3** designs and evaluates digital nudges across multiple touchpoints in the passkey journey (e.g., registration, login, recovery) to increase adoption in the field [94].

Research Area 3: Access Reviews. Over-privileged identities amplify the impact of compromise and insider misuse, and authorizations tend to accumulate over time as responsibilities change and exceptions persist [56, 82]. To counter excessive authorizations, organizations rely on the foundational principle of least privilege [101], which is commonly operationalized through periodic access reviews [49]. In access reviews, domain experts such as department heads are tasked with validating that permissions

in their area of responsibility remain appropriate [58]. In practice, access reviews are primarily driven through regulatory requirements, for example, under Basel III [9], SOX [114], or HIPAA [113].

However, the effectiveness of such reviews is often limited in practice [49]. Access review campaigns require human deciders to assess very large authorization sets (potentially up to six figures of individual authorizations) under time pressure, while simultaneously interpreting opaque authorization labels and organizational structures with little context about actual need, usage, or criticality [49, 58, 63, 89]. This environment encourages superficial completion and a tendency to confirm the status quo: revoking access can trigger immediate operational disruption, whereas the security risk of retained excess privilege is delayed, probabilistic, and therefore easy to discount [10, 63]. Consistent with this, empirical studies report revocation rates that fall well below expert expectations of how much access is excessive, indicating substantial unrealized potential of access reviews [10, 49].

One response to address these challenges might be through *technical* and *process* improvements, such as reducing scale by remodelling access control policies or using attribute-based policies [63, 66]. While promising, such approaches depend on high-quality data and deep integration across heterogeneous systems, and still typically require human exception handling in many organizations [58, 63, 89]. Consequently, improving the choice architecture of access reviews remains a key approach for closing the gap between compliance-driven completion and meaningful privilege reduction. This research area therefore evaluates how digital nudges can improve access review outcomes and decision efficiency while maintaining deciders' autonomy. Therefore, the following research question is explored:

RQ3. *How do digital nudges benefit access reviews?*

Publication **P4** addresses RQ3 by formalizing the access-review problem, mapping suitable digital nudges for access reviews by interviewing industry experts, and empirically evaluating their effects on revocation behavior [10].

Research Area 4: CTI Sharing. CTI captures indicators of compromise (e.g., IP addresses, domains, file hashes), adversaries' tactics, techniques, and procedures, and contextual insights that help organizations anticipate attacks, prioritize defenses, and accelerate response [111, 121]. Because no single defender observes the full threat landscape, organizations can benefit substantially from external CTI: it broadens coverage beyond local visibility, helps surface rare adversary behaviors, and reduces duplicated investigative effort across defenders [111, 121]. Since commercial CTI can be prohibitively expensive for many organizations, cross-organizational sharing is an attractive complement to obtain external CTI [12]. Yet in practice, organizational CTI sharing remains insufficient. Producing shareable intelligence requires upfront effort (e.g., validation and often sanitization), while the benefits from contributing are uncertain, delayed, or accrue primarily to other participants [40, 64]. This creates a classic

participation imbalance in which many actors primarily consume shared intelligence rather than contribute to it, reducing coverage and limiting the ecosystem's overall value [40, 48].

Beyond effort, organizations face confidentiality, trust, and compliance constraints when exchanging CTI, which can further suppress participation [4, 12]. Prior work and practice therefore emphasize measures that lower friction and risk, for example via interoperability standards, automation, and purpose-built sharing infrastructures (e.g., STIX and platforms such as MISP) [8, 120]. While these measures improve *how* CTI can be exchanged, they do not by themselves resolve *why* organizations should contribute consistently, nor how a platform can sustain participation and high-quality contributions in the presence of free-riding and risk perceptions [40, 64, 95].

Accordingly, incentive mechanisms have been proposed as a means to motivate contribution and provide more predictable returns for participating organizations [73]. However, critical design questions remain open regarding which incentives are effective under organizational constraints and how such incentives should be integrated into CTI-sharing platforms [95]. This research area therefore investigates incentive-centered platform design and integration strategies to make organizational CTI sharing sustainable in practice. Thus, the following research question is posed:

RQ4. *How to design and integrate incentives into a CTI sharing platform?*

Publication **P5** addresses RQ4 by deriving incentive requirements from security professionals, translating them into incentive mechanisms implemented in a platform prototype, and evaluating their effects on willingness to share and participate [95].

3.3 Research Environment

During this dissertation, I was employed by the Chair of Information Systems I (Professor Pernul) at the University of Regensburg. This environment enabled close collaboration with fellow researchers, provided access to state-of-the-art research infrastructure, and facilitated the acquisition of study participants through incentives across the publication set. The dissertation was partially conducted in the context of two collaborative projects, DEFENSIVE and CONTAIN, which also provided the main funding basis for this work. Both projects were funded by the German Federal Ministry of Education and Research (BMBF), which has been renamed to the Federal Ministry of Research, Technology and Space (BMFTR).

The dissertation initially took shape around incentives and cybersecurity information sharing. DEFENSIVE and prior work on decentralized incentives for threat intelligence reporting (e.g., Menges et al. [73]) provided an early conceptual and practical foundation for investigating how incentives can be designed and embedded into a CTI sharing platform. Building on this starting point, the idea for P5 emerged to explore incentive integration for organizational CTI sharing in more depth [95]. In parallel,

the work on access reviews was enabled through the chair's close ties to the company Nexis, a spin-off that develops commercial software for access control and contributes to research activities at the chair. This collaboration made it possible to study access reviews in a software-realistic setting, which directly supported P4 and the complementary study C7. Through P4, digital nudging was integrated as an additional mechanism for guiding behavior within the dissertation's overall framing.

A second strand emerged from developments around FIDO2 and passkeys, which have introduced passwordless authentication as a practical option with both security and usability benefits [42, 97, 126], shaping Research Area 2 and underpinning the studies reported in P2 and P3. A key enabler for these studies was a field cooperation connected to earlier work on a digital healthcare platform, where passkeys had been implemented as an authentication option. This created an opportunity to recruit participants in a real-world usage context and to evaluate barriers and interventions under realistic conditions [94, 97].

Research Project DEFENSIVE. DEFENSIVE is based on the problem that organizations often hesitate to share cybersecurity incidents and CTI because disclosure can create reputational and legal risk, even when sharing would improve collective defense [4, 12, 48, 121]. The project's goal is to enable trustworthy information exchange through a decentralized data trustee concept that supports pseudonymity and data protection while still providing integrity for shared reports. The consortium included two industry partners with an extensive background in cybersecurity. For the dissertation, DEFENSIVE was especially important for grounding the *CTI sharing* perspective (Research Area 4) and for recruiting expert interview partners. The papers P5 and C2 resulted from this project context.

Research Project CONTAIN. CONTAIN is motivated by the growing impact of ransomware and complex cross-organizational incidents, where response quality depends on coordinated actions across organizations and value chains [3, 17, 30]. The project aims to improve incident-response effectiveness and efficiency by developing a framework with reference scenarios, policies, processes, and playbooks, complemented by training-oriented artifacts such as serious games and simulation models. The consortium combined research and industry partners, enabling continuous requirements-oriented exchange. In the dissertation, this environment supported the *Foundations* perspective (Research Area 1) by providing organizational contexts and practitioner access for investigating motivational mechanisms and competence building. The papers P1, C1, C3, and C4 resulted from CONTAIN.

4 Results

This chapter first provides an overview of the dissertation's publications, then summarizes the papers grouped by research area. Finally, it outlines complementary publications that are not included in the dissertation but extend its core contributions to related application contexts.

4.1 Overview of Publications

This dissertation comprises five publications that address the research questions of the four research areas. All publications have been accepted for publication in international, peer-reviewed conference proceedings or journals. Table 1 summarizes the publications and reports venue quality using the **ICORE 2026 conference ranking**[1] together with the corresponding **acceptance rate (AR)** for conference publications and the 2024 five-year **impact factor (IF)** for journal publications.

Table 1: Overview of publications and corresponding ranking.

Publication		Ranking
Research Area: Foundations		
P1	Reittinger, T., Glas, M., Aminzada, S., & Pernul, G. (2025). Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice. *Information and Computer Security*. **Invited extended version**. (in press).	**2.2** IF
Research Area: Passkeys		
P2	Reittinger, T., & Pernul, G. (2026). No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage. In *Proceedings of the 2026 IEEE Symposium on Security and Privacy (SP)*. (accepted for publication).	**A*** ICORE 13% AR
P3	Reittinger, T., Glas, M., & Pernul, G. (2026). Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. (accepted for publication).	**A*** ICORE 25% AR
Research Area: Access Reviews		
P4	Baumer, T., Reittinger, T., Kern, S., & Pernul, G. (2024). Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, pp. 239–258.	**A** ICORE 21% AR
Research Area: CTI Sharing		
P5	Reittinger, T., Grill, J., & Pernul, G. (2026). Share and Benefit: Incentives for Cyber Threat Intelligence Sharing. *International Journal of Information Security*, *25*, Article 37.	**3.1** IF

[1] https://portal.core.edu.au/conf-ranks/

In the remainder of this chapter, each research area is briefly outlined, followed by an overview of the papers in that area. An in-depth introduction to the research areas is provided in Section 3.2.

4.2 Research Area 1: Foundations

Security outcomes in organizations depend not only on technical controls, but also on whether employees enact security behaviors under everyday constraints [1, 53]. Prior work shows that security demands are often perceived as effortful and misaligned with work goals, which can lead to coping strategies and superficial compliance [11,53]. This research area therefore aims to establish a baseline of how organizations currently motivate secure behavior and how employees experience these measures, and to assess how these practices align with theory-based recommendations from the behavioral literature. Accordingly, P1 addresses the following research question:

RQ1. *How do organizations motivate employees toward secure behavior?*

P1 – Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice

Source. This subsection summarizes P1 [93].

Publication context. P1 is an invited extended version of an earlier conference publication [92, 93]. The extended version expands the theoretical and empirical account of how motivational mechanisms are implemented in organizational cybersecurity [93].

Motivation. The paper is motivated by the observation that many organizations invest in awareness and compliance programs, yet employees may experience security requirements as burdensome, unclear, or misaligned with day-to-day work [93]. This gap is commonly discussed as a mismatch between security requirements and human constraints, where employees adopt coping strategies when demands exceed time, attention, or usability limits [11, 53]. Building on this misalignment, the study examines how organizations attempt to motivate secure behavior, how these measures are experienced by employees, and whether these attempts match recommendations from prior work [93].

Method. The study reports a qualitative interview design capturing motivational practices and experiences from three organizational perspectives: executive management, security specialists, and regular employees [93]. In total, 18 participants from organizations in Germany were interviewed using a semi-structured protocol designed to elicit concrete practices without explicitly priming theoretical terminology. The analysis applies deductive coding informed by Self-Determination Theory (competence, relatedness, autonomy) and extends it with extrinsic motivators (incentives and nudges) to classify observed organizational approaches [26, 93, 109]. The resulting coding scheme is then used to identify recurring implementation patterns and frictions that affect perceived effectiveness [93].

Results. The results indicate that organizations deploy a heterogeneous set of measures, but reported motivational effects depend strongly on perceived relevance, effort, organizational responsiveness, and the degree to which measures support intrinsic needs [93]. In the interviews, perceived effectiveness was described as eroding when interventions were experienced as generic, overly mandatory, or not paired with feedback and visible leadership commitment.

Autonomy. The study finds that autonomy is often described to be constrained by mandatory formats and rigid rules, which can shift attention from meaningful engagement toward merely satisfying requirements [93]. Participants report that highly prescriptive controls can foster superficial compliance and workarounds, especially when requirements are perceived as unreasonable under workload pressure. Prior work similarly argues that overly demanding security requirements may lead to circumvention when costs outweigh perceived benefits [53]. Consistent with this logic, the paper reports that security specialists observed better outcomes when employees were given flexibility, e.g., choosing their own password-management approach within guardrails, because this added autonomy made requirements feel less arbitrary, reduced frustration, and encouraged more proactive, sustained security compliance [93].

Competence. The paper reports that competence is primarily addressed through awareness training, phishing simulations, and security policies [93]. Participants frequently described training as generic and difficult to translate into role-specific action, which reduces engagement and encourages a completion mindset. Interviewees also reported policies as lengthy, hard to interpret, or hard to locate, leaving employees uncertain about expected behavior in concrete situations. By contrast, the paper notes that phishing simulations were described as comparatively compatible with daily work because they are lightweight and can help employees build routines for identifying and reporting suspicious messages.

Relatedness. The results suggest that relatedness is supported when cybersecurity is framed as a shared responsibility and when employees experience a cooperative security culture [93]. Participants described stronger motivation when colleagues discuss security issues openly and when reporting is socially normalized rather than treated as exceptional. The interviews further highlight visible leadership commitment as pivotal: when managers signaled that security efforts were secondary, employees interpreted initiatives as low priority and disengaged.

Incentives. In the study, interviewees connected incentive effects to organizational error culture, particularly whether mistakes were treated as learning opportunities or as grounds for punishment [93]. A non-punitive approach was described as supporting willingness to report incidents and ask for help, whereas punitive responses were described as discouraging reporting and increasing fear of security functions. The paper also reports that some organizations used positive rewards (e.g., small vouchers) to stimulate reporting. Participants noted that increased reporting volume required sufficient operational capacity to process and respond. Across roles, timely feedback on

reports was described as a key reinforcer because employees felt more motivated when they saw that their reports were valued and led to visible action.

Nudges. In P1, interviewees reported widespread use of attention cues in email clients (e.g., external-sender banners) to increase vigilance [93]. Participants described a boundary condition when warnings were ubiquitous and not risk-differentiated: habituation and reduced salience were reported, with some interviewees explicitly describing a fatigue-like effect from constant alerts. This pattern is consistent with broader concerns that repeated security demands can exceed employees' compliance capacity and reduce engagement over time [11]. In addition, the paper also describes social reference nudges (e.g., making reporting norms visible) that can normalize desired behavior and increase reporting engagement when implemented carefully [93].

Contribution to RQ1 derived from P1 [93]

- Provides a theory-grounded empirical account of how organizations motivate secure behavior, structured along competence, relatedness, autonomy, incentives, and nudges.
- Identifies recurring motivational frictions, including low perceived relevance of generic training, complexity and poor discoverability of policies, autonomy-reducing mandatory measures that foster workarounds, and habituation effects from non-differentiated cues.
- Derives improvement directions aligned with motivational theory, emphasizing leadership signaling, role-relevant learning opportunities, autonomy-supportive guardrails, and positive and feedback-driven reporting cultures.

4.3 Research Area 2: Passkeys

Password requirements often conflict with everyday work constraints, prompting coping strategies such as reuse, weak secrets, and insecure storage that undermine security and contribute to a common entry point for attackers [1, 11, 117]. Passkeys offer a phishing-resistant alternative, yet adoption remains limited despite their security and usability benefits [42, 97, 104, 126]. This research area examines barriers that impede passkey adoption and sustained use, and evaluates strategies to increase uptake at scale. Building on this, P2 and P3 examine the following research question:

RQ2. *Which barriers impede passkey use, and how to increase adoption?*

P2 – No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage

Source. This subsection summarizes P2 [97].

Motivation. The study addresses two gaps in understanding passkeys in practice: why users decline passkeys or fail setup during real-world registration, and which usability issues emerge during repeated logins and multi-device use, especially around synchronization [97]. To close these gaps, the work examines both the initial authentication-method decision and the sustained-use experience over a multi-month period.

Method. The study uses a two-phase field design on a production healthcare platform, comparing passkeys against passwords with SMS-based 2FA [97]. In Phase 1 (n=5,057), users chose during registration between creating an account with a passkey or with a password, and the interface provided brief, general information about passkeys following recommendations of prior work. The paper outlines that a post-flow survey captured users' reasons for their choice and, where applicable, reasons for canceling or failing adoption, alongside relevant background variables (e.g., prior passkey experience and technology affinity). In Phase 2 (n=2,716), participants who successfully adopted their selected method were observed for six months via authentication telemetry and brief post-attempt surveys that captured perceived issues, second-factor choices, and synchronization context (including cross-platform cases), complemented by usability and acceptance measures.

Results. The results show high passkey interest but substantial early friction: a majority selected passkeys during registration, yet passkey setup succeeded less often than the password baseline, with the largest gaps among inexperienced users [97]. The paper reports that survey results associate passkey refusal primarily with established password habits and limited passkey experience, whereas setup failures are often attributed to misconceptions, perceived complexity, and manual activation requirements on some operating systems. Over time, the study notes that repeated logins shift the picture: passkey success rates surpass the declining success of password sessions, and reported usability and acceptance continue to improve. Longitudinal feedback also surfaces ecosystem-level obstacles, especially cross-platform synchronization difficulties, passkey sharing hurdles, and friction when relying on third-party password managers. Building on these observations, the paper recommends improving onboarding so that users better understand passkeys during setup, and reducing friction in activation and cross-device management to support reliable use beyond first-time adoption.

Contribution to RQ2 derived from P2 [97]

- Provides field evidence on passkey choice and setup success in a real registration flow by comparing passkeys to a password with SMS-based 2FA as a baseline.
- Characterizes why users do not adopt passkeys by distinguishing refusal drivers

(e.g., password habit and limited experience) from setup barriers (e.g., misconceptions and OS-dependent activation requirements).

- Extends the analysis to sustained use over six months, showing that passkey success and acceptance improve with repeated logins while surfacing ecosystem frictions (e.g., cross-platform synchronization) that can hinder reliable use beyond initial adoption.
- Derives practical directions for improving adoption and long-term reliability, emphasizing clearer onboarding and reduced friction in activation and cross-device management.

P3 – Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption

Source. This subsection summarizes P3 [94].

Motivation. The paper is motivated by the observation that passkeys offer security and usability advantages, yet many users continue to rely on passwords [94]. The study reports that this gap is commonly attributed to adoption frictions along the user journey, where users face uncertainty about what passkeys are, limited perceived benefit at the moment of choice, and effortful setup that make sticking with passwords feel easier. Building on this misalignment between passkeys' promised benefits and users' real-world decision context, the study examines how digital nudges can be embedded at different touchpoints of the user journey to increase passkey adoption and whether these nudges measurably change adoption behavior in practice.

Method. The study adopts a mixed-methods design that combines expert interviews with a randomized controlled field experiment [94]. First, semi-structured expert interviews (n=15) are conducted to identify promising digital nudges and derive touchpoint-appropriate design principles. Second, the selected nudges are evaluated on a commercial healthcare platform across five journey touchpoints (registration, login, account recovery, the settings menu, and in-app activity) with a total sample of N=3,680 users. The publication outlines that at each touchpoint, users faced an authentication choice between passkeys and passwords, and the embedded nudges intended to guide users toward the passkey option. The paper implements nudges from multiple categories, including salience, visibility, and choice defaults, complemented (depending on the touchpoint) by effort reduction, social reference, or reminder mechanisms. The study measured outcomes as (i) interaction rate (engagement with the passkey option), (ii) adoption rate (completed passkey setup), and (iii) success rate (adoption conditional on interaction), enabling the analysis to separate attention effects from completion effects.

Results. The results show that digital nudges significantly increase interaction and overall adoption at most touchpoints, suggesting that nudges primarily work by increasing attention, while the conditional success does not considerably change once

users engage [94]. The study further reports that choice defaults yield the highest adoption rates across stages, with salience and visibility often performing similarly depending on context. The analysis highlights registration and account recovery as particularly receptive moments, as users are more likely to interact with prompts at these stages. Touchpoint-specific comparisons in the paper suggest that salience is particularly effective for driving interaction during registration, whereas visibility is especially effective at recovery, reinforcing the value of stage-specific nudge selection. In addition, the study derives practical design guidance from expert input, including avoiding negative framing that could undermine users' trust and ensuring transparent fallbacks when defaults are used.

Contribution to RQ2 derived from P3 [94]

- Shows that digital nudges primarily increase passkey adoption by raising engagement with the passkey option, while conditional success remains largely stable once users interact. It further demonstrates that effectiveness varies by touchpoint and nudge type, with choice defaults generally strongest, with salience and visibility performing differently across stages.
- Identifies high-opportunity moments in the user journey for passkey adoption, highlighting registration and account recovery as particularly receptive stages for prompting adoption.
- Derives practical design guidance for deploying adoption nudges without undermining trust, including avoiding negative framing of passwords and ensuring transparent fallbacks when defaults are used.

4.4 Research Area 3: Access Reviews

Access reviews are a recurring, primarily compliance-driven IAM control intended to reduce excessive authorizations before they become exploitable attack surface [9, 14, 58, 81]. In practice, reviews are frequent and large-scale, and decision makers often lack time and context, which can lead to superficial confirmations rather than meaningful revocations [58]. This research area examines whether digital nudges can improve review outcomes and reduce decision burden by shaping the interface-level choice architecture without constraining reviewers' choices. Building on this, P4 explores the following research question:

RQ3. *How do digital nudges benefit access reviews?*

P4 – Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations

Source. This subsection summarizes P4 [10].

Motivation. The paper is driven by the observed gap between the intended purpose of access reviews of revoking unnecessary authorizations and the limited revocation observed in practice [10]. The publication links this gap to the scale and complexity of enterprise authorization landscapes, and that deciders often prioritize operational continuity over security. Building on this problem framing, the study investigates how access reviews can be formalized, how access-review challenges map to digital nudges, and whether a concrete nudge implementation measurably improves outcomes.

Method. The paper adopts a mixed-methods design that combines formal modeling, expert interviews, and a user-study evaluation [10]. First, it formalizes the Access Review Problem (ARP) as a transition between authorization states using a confusion-matrix representation, which grounds the subsequent hypotheses and evaluation metrics. Second, it conducts semi-structured expert interviews ($n = 10$) with experienced IAM professionals to connect observed access-review challenges to candidate digital nudges. Third, it evaluates the *Choice Defaults* nudge in a between-subjects user study ($n = 102$) with three conditions: default accept, default reject, and control. The study measures decision outcomes and decision time, and complements these behavioral measures with participants' self-reported workload.

Results. The paper indicates that digital nudges can steer revocation behavior and reduce perceived burden in access reviews [10]. In the experimental study, *Choice Defaults* reduced review time and perceived stress compared to the neutral condition and shifted revocation behavior, while overall quality metrics did not differ significantly between default configurations, suggesting that improving decision quality may require support beyond simple defaults.

Formalization of the ARP. The study introduces the ARP as a transition between authorization states and formalizes review quality as reducing excessive authorizations while limiting erroneous revocations [10]. The formalization yields explicit evaluation metrics that can be used to benchmark review designs and compare interventions.

Expert-based nudge mapping. The expert interviews map literature-based access-review challenges (e.g., scale, lack of knowledge) to an established taxonomy of digital nudges and discuss expected benefits and risks [10]. Overall, experts view nudges as a promising mechanism to make reviews more manageable and to steer attention toward risk-relevant decisions, while cautioning that poorly designed nudges can undermine reflection and lead to superficial, low-effort reviewing. In particular, experts highlight that defaults can reduce effort but may reduce reflection if deciders over-trust preselection, motivating careful deployment.

Choice Defaults user study. The user study shows that *Choice Defaults* influenced revocation behavior and reduced perceived workload, while overall quality metrics did

not differ significantly between configurations in the experimental setup [10]. Compared to the neutral condition, the paper reports that default-accept reduced average review time by 24.3%, while default-reject reduced average review time by 16%. At the same time, default-reject increased revocations but also increased erroneous revocations, illustrating that shifting decisions is not automatically equivalent to improving review quality. The paper therefore discusses safeguards against low-effort reviewing and highlights smart defaults and complementary nudges as promising directions for improving quality in practice.

Contribution to RQ3 derived from P4 [10]

- Provides a formal model of access reviews (ARP) that makes review quality measurable and supports comparative evaluation of review designs.
- Maps access review challenges to digital nudge categories through expert interviews, highlighting both expected benefits and risks.
- Demonstrates that *Choice Defaults* can measurably shift revocation behavior and reduce perceived burden (e.g., time, stress), while also showing that improving review quality likely requires more comprehensive design beyond defaults.

4.5 Research Area 4: Cyber Threat Intelligence (CTI) Sharing

CTI can strengthen organizations' detection and mitigation capabilities against cyberattacks by providing indicators of compromise, adversary TTPs, and contextual insights about campaigns [111, 121]. However, organizational CTI sharing often stalls because contributing requires preparation and coordination, returns are uncertain, and organizations face trust, confidentiality, and data-protection concerns [4, 12, 111]. This research area focuses on incentive-centered platform design to increase willingness to participate and to make CTI sharing sustainable in practice. Therefore, P5 examines the following research question:

RQ4. *How to design and integrate incentives into a CTI sharing platform?*

P5 – Share and Benefit: Incentives for Cyber Threat Intelligence Sharing

Source. This subsection summarizes P5 [95].

Motivation. The study starts from the observation that inter-organizational CTI sharing could strengthen collaborative defense, yet participation remains limited in practice [95]. The paper attributes this to recurring barriers: producing shareable CTI requires effort, sensitive details create trust and confidentiality concerns, and expected benefits are often uncertain. To address these barriers, the study examines which incentives can increase willingness to share and how such incentives can be embedded into a CTI-sharing platform that organizations are willing to adopt.

Method. The paper follows a three-phase approach that moves from understanding practitioner needs to prototyping and evaluation [95]. First, 15 semi-structured interviews with security professionals identified impediments to CTI sharing and derived incentive-related requirements and design options. Second, the selected incentive mechanisms were implemented in a novel open-source platform prototype. Third, the prototype was examined in 14 hands-on evaluation sessions with security specialists to assess feasibility and to explore how the implemented incentives influence participants' willingness to share.

Results. The findings indicate that effective CTI-sharing incentives must address three recurring concerns: CTI should be shareable only with trusted recipients, it should entail minimal coordination overhead, and contributors should be able to realize clearer returns for the effort of preparing and providing CTI [95]. The paper organizes its outcomes into three *incentivizing features (IF)*, platform elements that support initial adoption, and two *incentive mechanisms (IM)* designed to stimulate active participation.

Community-based sharing (IF). The paper emphasizes that organizations prefer sharing CTI within closed, member-restricted communities to reduce distrust of unknown parties and to better align exchange with data-protection expectations [95]. The platform design therefore foregrounds community membership and access control, allowing organizations to decide with whom CTI is shared.

Reputation system (IF). The study describes a reputation system as a way to reduce uncertainty about CTI quality and to support prioritization of analyst time [95]. The design relies on member ratings and short feedback signals and discusses participation requirements intended to keep the reputation signal informative.

Price guidance (IF). The paper identifies CTI pricing as a practical barrier, particularly because value varies by type and context and external validation is often infeasible [95]. To lower this burden, the platform provides automated price suggestions based on similarity to previously traded CTI records while preserving the contributor's final control over the offered price.

Financial payments (IM). The results highlight that payments can make the benefits of sharing more tangible by compensating the effort required to create CTI and by offsetting potential cybersecurity losses, thereby providing explicit returns for contributors [95]. The proposed integration uses recurring deposits to ensure liquidity for purchases and to reduce friction during incident response, while still allowing withdrawals and revenue collection.

Marketing label (IM). The paper introduces a marketing label as an external incentive that signals proactive cybersecurity participation to partners and customers [95]. To keep the label meaningful and reduce gaming risks, the design ties it to community-defined requirements and limited validity periods.

Platform integration. The paper implements the proposed incentives in an open-source prototype that combines controlled membership with platform-wide visibility of marketplace metadata (e.g., offers, ratings, and transactions), while handling CTI

data in a confidentiality-preserving manner [95]. As an example architecture, the prototype employs a private permissioned blockchain to support pseudonymous transactions within a vetted community and to provide an auditable basis for incentive mechanisms; sensitive CTI content is stored and exchanged off-chain to avoid exposing exchange data on the ledger.

Contribution to RQ4 derived from P5 [95]

- Characterizes key impediments to organizational CTI sharing, such as distrust of unknown recipients or unclear net benefits; derives incentive requirements grounded in expert input.
- Specifies incentive mechanisms for CTI sharing platforms that address trust, coordination costs, and returns for contributors, including community-based sharing, reputation information, price guidance, financial compensation, and a marketing label.
- Demonstrates how these incentives can be embedded into a feasible platform design and evaluates the resulting prototype in expert hands-on sessions, reporting increased willingness to share under the proposed incentive configuration.

4.6 Complementary Publications

These complementary publications, summarized in Table 2, extend the dissertation's core contributions by providing additional theoretical grounding, methodological building blocks, and related application contexts beyond the main publication set.

Table 2: Outline of the dissertations' complementary publications.

Complementary Publications	
C1	Reittinger, T., Glas, M., Aminzada, S., Pernul, G. (2025). Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality. In: Proceedings of the 2024 Symposium on Human Aspects of Information Security and Assurance. HAISA 2024. IFIP Advances in Information and Communication Technology, vol 721. **Best Student Paper Award**.
C2	Reittinger, T., Pernul, G. (2025). A Taxonomy of Positive Incentives to Motivate Cybersecurity Behaviors. In: Proceedings of the 58th Hawaii International Conference on System Sciences. HICSS-58 2025, pp. 4542–4551.
C3	Friedl, S., Reittinger, T., Pernul, G. (2024). From Play to Profession: A Serious Game to Raise Awareness on Digital Forensics. In: Ferrara, A. L., Krishnan, R. (eds.) Data and Applications Security and Privacy XXXVIII. DBSec 2024. Lecture Notes in Computer Science, vol. 14901, pp. 269–289.
C4	Friedl, S., Reittinger, T., Pernul, G. (2024). Digital Detectives: A Serious Point-and-Click Game for Digital Forensics. In: Drevin, L., Leung, W. S., von Solms, S. (eds.) Information Security Education - Challenges in the Digital Age. WISE 2024. IFIP Advances in Information and Communication Technology, vol. 707, pp. 129–145.
C5	Glas, M., Vielberth, M., Reittinger, T., Böhm, F., Pernul, G. (2022). Visual Programming in Cyber Range Training to Improve Skill Development. In: Clarke, N., Furnell, S. (eds.) Human Aspects of Information Security and Assurance. HAISA 2022. IFIP Advances in Information and Communication Technology, vol. 658, pp. 3–13.
C6	Glas, M., Vielberth, M., Reittinger, T., Böhm, F., Pernul, G. (2023). Improving Cybersecurity Skill Development through Visual Programming. In: Information and Computer Security, 31(3), pp. 316–330.
C7	Neudert, R., Baumer, T., Reittinger, T., & Pernul, G. (2026). Digital Nudges in Access Reviews: Guiding Deciders with Range and Composition. *Submitted for publication.*

The complementary publications are summarized as follows.

C1 reports the initial conference version of the motivational study that P1 later extends, establishing the empirical basis for the dissertation's behavioral foundation [92]. This paper was recognized with the Best Student Paper Award. In the dissertation, it can be classified to Research Area 1 (Foundations) as it directly informs RQ1 by showing how organizations attempt to motivate secure behavior and where employees experience friction (e.g., generic training, rigid requirements, and limited feedback).

C2 responds to the lack of a shared structure for positive cybersecurity incentives by developing a taxonomy through a staged taxonomy-development approach that begins with a systematic literature review and uses 15 expert interviews to refine the emerging dimensions [96]. The taxonomy is then iterated again against the literature and consolidated into a final set of incentive dimensions that is presented as the paper's main artifact. The publication evaluates this final taxonomy in a second round of 15 expert interviews, indicating that experts can apply it consistently in practice. Based on the evaluation, an interactive version of the taxonomy is published as an open-source artifact to support practical use. In the dissertation, it can be classified within Research Area 1 (Foundations) because it strengthens the incentive-oriented part of RQ1 with a reusable conceptual lens. As a complementary publication, it extends the dissertation's core contributions by providing terminology and design parameters that support systematic selection, tailoring, and transparent comparison of incentive designs across settings.

C3 addresses the cybersecurity workforce and skills shortage by using a serious game to raise awareness of the digital forensics profession [38]. The paper presents the design of the serious game and evaluates it in a pre/post study with students, reporting significant improvements in learning outcomes and awareness of digital forensics. The publication additionally reports that learning outcomes and the quality of the game experience are strongly related to increases in professional awareness, suggesting that effectiveness depends on how the intervention is experienced. The paper extends the dissertation's core contributions by providing evidence that capability building and engagement, supported through gamification and serious game design, can serve as mechanisms for guiding security-relevant behavior.

C4 is motivated by the scarcity of cybersecurity professionals and the lack of digital forensics knowledge in organizations, and therefore introduces a point-and-click serious game intended to educate students and raise awareness among non-specialist employees [37]. The publication follows an instructional design process to align learning objectives with game mechanics and evaluates the resulting artifact with pre/post measurement. The results indicate substantial improvements across multiple knowledge areas after gameplay, providing additional evidence that interactive learning artifacts can shift security-relevant understanding. Within the dissertation framing, the publication shows that gamified interventions can increase digital forensics competence and awareness, extending the methodological toolkit for competence-oriented behavioral guidance.

C5 examines whether reducing programming overhead in cyber range exercises can support learning in security training [44]. The paper integrates a visual programming approach based on Blockly[2] into a cyber range for SIEM rule creation and compares it to a text-based baseline in a randomized controlled study. The findings of the publication show comparable learning outcomes across conditions and indicate a more favorable perceived learning experience for the visual approach, while time-related effects are less clear. Regarding the dissertation, C5 extends the dissertation's core contributions by demonstrating guidance through usability, showing how tool design can lower friction and support sustained skill development that many organizational security behaviors implicitly depend on.

C6 is an extended journal version of C5 that expands the description and analysis of the training and its evaluation, including a more detailed assessment of learner engagement and a refined integration concept for future Blockly-based SIEM rule training [45]. In the dissertation, it complements the core work by showing how tool and training design can support competence-oriented guidance beyond the main areas.

C7 is motivated by the observation that regulatory-driven access reviews often struggle to achieve effective least-privilege outcomes at scale and therefore tests if a *range and composition* nudge can improve review decisions [79]. The nudge is realized through an identity-grid interface that clusters similar access patterns against a conventional list-based interface in a large user study. The paper reports higher decision accuracy and improved identification of anomalous access patterns with the identity-grid approach, while also showing increased time and cognitive demand. Within the dissertation, it can be classified within Research Area 3 (Access Reviews) as it directly advances RQ3 by providing evidence on how digital nudges can guide review behavior in governance workflows. As a complementary publication, it refines the dissertation's design implications by making the benefits and operational trade-offs of nudge-based decision support explicit.

[2]https://developers.google.com/blockly

5 Discussion

This discussion synthesizes the dissertation's findings and derives implications for research and practice, ethical considerations, and promising directions for future work, before outlining key limitations.

5.1 Implications for Research and Industry

The results across this dissertation suggest that behavior guidance is most effective when security measures are designed for real work constraints and evaluated at the points where people actually decide and act.

Implications for research. Across the four research areas, three implications for research stand out. (1) *Study guidance as bundles:* examine how motivation, choice architecture, and incentives work together to shape behavior, rather than evaluating each mechanism in isolation. *Identify mechanisms and boundary conditions:* explain *why* guidance works or fails, including habituation, reduced reflection under time pressure, and unintended responses such as gaming or low-quality contributions. (3) *Develop stronger evaluation designs and measures:* move beyond adoption and efficiency metrics by using metrics that capture security impact, error costs, and distributional effects across heterogeneous users and organizations.

Implications for industry. For practice, three lessons stand out. (1) *Make secure action workable:* translate policies and training into role-relevant, actionable guidance and provide timely feedback. (2) *Reach users at the right moment:* for passkeys, focus adoption efforts on moments where users already face authentication choices (e.g., registration and recovery), pair nudges with brief explanations, and treat fallback and recovery as core requirements. (3) *Guide without undermining accountability:* in access reviews, defaults and other nudges should remain easy to override and be designed to preserve reviewer reflection and responsibility; for CTI sharing, incentives should be complemented by mechanisms that support quality and fair participation, rather than merely maximizing contribution volume.

Overall, the dissertation highlights that organizations can improve cybersecurity by shaping the conditions under which security decisions are made, so that secure behavior is easier to carry out and more reliably sustained.

5.2 Ethical Aspects of Guiding Human Behavior

The dissertation shows that incentives and digital nudges can substantially shape behavior in cybersecurity. This raises a central ethical question: when is it legitimate to guide behavior, and how can such guidance remain aligned with user welfare, autonomy, and accountability? A helpful baseline is provided by established ethics principles (respect for persons, beneficence, and justice [77]) and their security-focused operationalization for nudging [98]. For this dissertation, three requirements are especially

important: (i) *transparency*, users should be able to recognize guidance and understand what is being encouraged; (ii) *reversibility*, a viable alternative must remain available, opting out should be straightforward, and decisions should be reversible when circumstances change; and (iii) *proportionality*, expected benefits should outweigh foreseeable downsides and should not systematically disadvantage users with constraints.

In the following, these requirements are applied to papers that **practically implement** digital nudges and incentives.

P3: Passkey Nudges. P3 increases passkey adoption by embedding digital nudges across several stages of the user journey [94]. For *transparency*, users should understand what passkeys are and anticipate their practical implications. As in the study setup, nudges should therefore include a brief informational text explaining the passkey concept and what adoption entails. With respect to *reversibility*, passkey guidance remains defensible when users retain a viable alternative and can opt out or switch back without disproportionate friction. Regarding *proportionality*, nudges are most appropriate when they are placed at moments where users are already making authentication decisions (e.g., registration or recovery), while explicitly accepting non-adoption for all users, especially those constrained by devices, ecosystems, or accessibility. Finally, proportionality also requires monitoring for adverse outcomes (e.g., increased failed logins or lockouts) and adjusting the intervention if such downsides emerge [94].

P4: Access Review Nudges. P4 shows that choice defaults can shift revocation decisions and reduce burden in access reviews [10]. For *transparency*, defaults should be clearly recognizable as recommendations, and the interface should make it explicit that reviewers retain full control. With respect to *reversibility*, reviewers must be able to override the preselection with minimal effort; in addition, because revocations affect third parties, deployments should provide fast restoration and clear exception handling so that mistaken revocations can be reversed promptly. Regarding *proportionality*, defaults should balance the security value of reducing excessive authorizations with the risk of erroneous revocations and their operational impact.

P5: CTI Sharing Incentives. P5 embeds incentives into a CTI-sharing platform to increase participation [95]. For *transparency*, incentive mechanisms should have rules that are understandable and predictable so organizations can anticipate how contributions translate into benefits. With respect to *reversibility*, participation must remain voluntary: organizations should be able to refrain from sharing, limit sharing to trusted recipients, and adjust or withdraw offers as circumstances and risk assessments change. Regarding *proportionality*, incentives are ethically defensible when they increase contributions without introducing undue side effects such as low-quality CTI records, or systematic disadvantage smaller organizations; this implies coupling incentives with feedback and safeguards.

5.3 Future Work: AI and Human Behavior in Cybersecurity

Building on the dissertation's results, a particularly promising direction is to examine how the rapid rise of AI reshapes human-centered cybersecurity. Recent guidance and empirical work suggest that AI can amplify social-engineering threats by lowering the effort required to craft persuasive, personalized content at scale, thereby changing both the frequency and the quality of attacks that target human decision-making [20, 51, 72]. This development raises a fundamental question for usable security: how do AI-enabled attacks alter users' perceptions, coping strategies, and the effectiveness of established interventions (e.g., training, nudges)?

Two complementary opportunity areas emerge. First, AI may partially *replace* human work in security-critical workflows by automating routine work. In access reviews, where scale and time pressure are persistent barriers [58], AI-based decision support could pre-handle low-risk or non-security-critical authorizations and present a reduced, risk-focused set of authorizations for accountable human verification. Similarly, in CTI sharing, AI could reduce preparation costs by automatically sanitizing sensitive information and generating structured narrative reports from event data (e.g., log-derived indicators), thereby making contributions easier to produce and consume [84]. These automation directions are attractive, but they also introduce new questions about accountability, transparency, and how to keep humans meaningfully "in the loop" when AI becomes the primary producer of decisions and artifacts.

Second, AI can *support* human behavior by improving both preventive and in-situation interventions. On the preventive side, AI-enabled personalization could make training more relevant to an employee's role, current proficiency, and work context, which is a recurring requirement [93, 105]. On the in-situation side, AI can help generate context-rich, individualized warnings and explanations at the moment of risk (e.g., explaining why a website looks suspicious rather than issuing generic alerts), which may strengthen users' mental models and decision quality [99]. In the dissertation's application contexts, similar support could be explored for (i) passkeys, where an AI assistant could provide device- and OS-specific guidance during setup or recovery, and (ii) access reviews, where AI could explain opaque authorization labels and highlight potentially critical authorizations based on context.

Overall, AI has the potential to both automate selected security tasks and augment human decisions where friction and uncertainty currently undermine outcomes; realizing these benefits will require careful design and evaluation that accounts for trust, transparency, and failure modes in real organizational settings [72].

5.4 Limitations

The limitations of this dissertation are described as follows.

Generalizability. Several studies are grounded in specific contexts and regions, which may limit generalizability. For example, P1 draws on interviews in Germany, P2/P3 on a European healthcare platform in a field setting, P4 on a university-recruited sample in a simulated review setting, and P5 on largely European organizations. Still, these diverse contexts provide a broad starting point for testing transferability across domains and regions in future work.

Methodological Trade-Offs. The dissertation combines qualitative interviews, controlled experiments, and field studies, each with inherent trade-offs. Field studies reflect real-world behavior but offer less control (as in P2/P3), interviews may be influenced by recall and social desirability biases (as in P1/P3/P4/P5), and prototype-based evaluations demonstrate feasibility without capturing long-term ecosystem dynamics (as in P5). Taken together, these methods still provide complementary evidence that balances realism, control, and actionable design insight.

Observation Horizon. Except for P2, which uses a six-month timeline, most evaluations capture behavior at specific points in time and focus on immediate or near-term outcomes, providing limited insight into the durability of effects and how interventions perform under long-run use and organizational change. However, the results establish an initial baseline of short-term effectiveness and boundary conditions that future longitudinal studies can build on to assess sustained impact.

6 Conclusion

This dissertation addresses the central research question: *"How to guide behavior in organizational cybersecurity?"*. Its contributions are developed across four research areas, *Foundations*, *Passkeys*, *Access Reviews*, and *CTI Sharing*, each articulated through a dedicated research question (RQ1–RQ4) and examined in the publication set P1–P5. The areas speak to different audiences within organizational security: *Passkeys* center on novices (end users), *Access Reviews* on domain experts, and *CTI Sharing* on security experts, while *Foundations* offers a unifying perspective that spans all three groups. Table 3 summarizes this orientation. In sum, the dissertation integrates complementary research areas and target groups.

Table 3: Research areas across primary target-groups.

Research Area	Novices	Domain Experts	Security Experts
Passkeys	●	○	○
Access Reviews	○	●	○
CTI Sharing	○	○	●
Foundations	●	●	●

Foundations. The first research area establishes a behavioral baseline for organizational cybersecurity by examining how organizations motivate employees toward secure behavior (RQ1). P1 relates observed measures to theory by mapping organizational practices onto established behavioral perspectives and contrasting intended interventions with how employees perceive and enact them [93]. The results highlight recurring points where practice loses traction: requirements that collide with everyday work demands, guidance that remains hard to translate into concrete action, and insufficient feedback and visible support to sustain engagement. Beyond its direct contribution to RQ1, this area provides the conceptual foundation linking the remaining research areas by outlining how real-world constraints shape security-relevant actions and which interventions can narrow that gap across organizational settings.

Passkeys. The second research area examines why passkey authentication has yet to achieve broad uptake and identifies how adoption can be increased (RQ2). P2 reports field evidence that distinguishes adoption obstacles from setup barriers and shows that sustained passkey use is strongly influenced by multi-device use, synchronization, and recovery expectations [97]. Building on these insights, P3 embeds digital nudges along key journey touchpoints and evaluates which interventions increase engagement and completed setup in practice [94]. Taken together, the passkey contributions indicate that adoption increases when users are approached at receptive moments in the journey (e.g., registration and recovery), and that once successfully onboarded, passkeys can become more dependable over time than password-based authentication.

Access Reviews. The third research area focuses on authorization governance and asks how digital nudges affect access reviews (RQ3). P4 formalizes access reviews as a measurable decision problem, uses expert input to connect review frictions to suitable nudge categories, and evaluates a concrete nudge implementation that steers revocation behavior while reducing perceived burden [10]. At the same time, the results underline a central boundary condition for behavior guidance: mechanisms that accelerate decisions can also reduce reflection if deployed without safeguards. This area therefore highlights that effective guidance must balance efficiency with decision quality under accountability and operational risk.

CTI Sharing. The fourth research area moves to the inter-organizational level and examines how incentives can be designed and integrated into a CTI sharing platform (RQ4). P5 derives incentive requirements from practitioners, implements mechanisms that address trust boundaries, coordination overhead, and contributor returns, and evaluates how these mechanisms influence willingness to share and participate [95]. The work emphasizes that sustainable sharing requires more than technical interoperability: it depends on participation logic that organizations perceive as legitimate, worthwhile, and compatible with confidentiality constraints.

Final remarks. Cybersecurity in organizations will likely remain inseparable from human action. The core message of this dissertation is that security outcomes improve when measures are designed around real constraints rather than assumed ideal behavior: novices need clarity and low-friction paths for secure adoption, domain experts need decision environments that support careful revocation under pressure, and security experts need incentive-compatible mechanisms that make cooperation viable. By aligning motivational support, choice architecture, and incentives with ethical principles and operational realities, organizations can strengthen cybersecurity by creating conditions in which secure behavior is well-integrated into everyday work.

Bibliography

[1] Anne Adams and M. Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999. doi:10.1145/322796.322806.

[2] Elham Al Qahtani, Lipsarani Sahoo, Yousra Javed, and Mohamed Shehab. "why would someone hack me out of thousands of students": Video presenter's impact on motivating users to adopt 2fa. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, SACMAT '22, page 139–150, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3532105.3535013.

[3] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74:144–166, 2018. URL: https://www.sciencedirect.com/science/article/pii/S016740481830004X, doi:10.1016/j.cose.2018.01.001.

[4] Adham Albakri, Eerke Boiten, and Rogério De Lemos. Sharing cyber threat intelligence under the general data protection regulation. In Maurizio Naldi, Giuseppe F. Italiano, Kai Rannenberg, Manel Medina, and Athena Bourka, editors, *Privacy Technologies and Policy*, pages 28–41, Cham, 2019. Springer International Publishing.

[5] Claudio Anliker, Daniele Lain, and Srdjan Čapkun. Phishing attacks against password manager browser extensions. In *Proceedings of the 34th USENIX Conference on Security Symposium*, SEC '25, USA, 2025. USENIX Association.

[6] Nalin Asanka Gamagedara Arachchilage and Steve Love. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706–714, 2013. URL: https://www.sciencedirect.com/science/article/pii/S0747563212003585, doi:10.1016/j.chb.2012.12.018.

[7] Maria Bada, M. Angela Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *CoRR*, abs/1901.02672, 2019. URL: http://arxiv.org/abs/1901.02672, arXiv:1901.02672.

[8] Sean Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, 11(2012):1–22, 2012.

[9] Basel Committee on Banking Supervision. Basel III: A global regulatory framework for more resilient banks and banking systems. BCBS 189, Bank for International Settlements, Basel, Switzerland, June 2011. December 2010 (rev. June 2011). URL: https://www.bis.org/publ/bcbs189.pdf.

[10] Thomas Baumer, Tobias Reittinger, Sascha Kern, and Günther Pernul. Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 239–258, Philadelphia, PA, August 2024. USENIX Association. URL: https://www.usenix.org/conference/soups2024/presentation/baumer.

[11] Adam Beautement, M. Angela Sasse, and Mike Wonham. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the New Security Paradigms Workshop (NSPW '08)*, pages 47–58. ACM, 2008. doi: 10.1145/1595676.1595684.

[12] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. A different cup of TI? the added value of commercial threat intelligence. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 433–450. USENIX Association, August 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman.

[13] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Q.*, 34(3):523–548, September 2010.

[14] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Rundschreiben 05/2023 (ba): Mindestanforderungen an das risikomanagement – MaRisk, June 2023. Dated 29 June 2023. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html.

[15] Patricia Arias Cabarcos and Peter Mayer. 'the more accounts i use, the less i have to think': a longitudinal study on the usability of password managers for novice users. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security*, SOUPS '25, USA, 2025. USENIX Association.

[16] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–15, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3290605.3300733.

[17] Anna Cartwright and Edward Cartwright. The economics of ransomware attacks on integrated supply chain networks. *Digital Threats*, 4(4), October 2023. doi: 10.1145/3579647.

[18] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–11, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3173574.3174030.

[19] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, USA, 2008. USENIX Association.

[20] Stefan Czybik, Anne Josiane Kouam, Peter Heubl, Jan Magnus Nold, and Konrad Rieck. A Large-Scale Study of Personalized Phishing using Large Language Models. In *USENIX 2026 - 35th USENIX Security Symposium*, Baltimore (MD), United States, August 2026. URL: https://hal.science/hal-05457471.

[21] Shai Danziger, Jonathan Levav, and Liora Avnaim-Pesso. Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences*, 108(17):6889–6892, 2011. doi:10.1073/pnas.1018033108.

[22] John D'Arcy and Anat Hovav. Does one size fit all? examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89(1):59–71, May 2009. doi:10.1007/s10551-008-9909-7.

[23] John D'Arcy, Anat Hovav, and Dennis F. Galletta. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1):79–98, 2009. doi:10.1287/isre.1070.0160.

[24] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2014. URL: https://www.ndss-symposium.org/ndss2014/the-tangled-web-of-password-reuse/.

[25] Edward L. Deci, Richard Koestner, and Richard M. Ryan. A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, 125(6):627–700, 1999. doi:10.1037/0033-2909.125.6.627.

[26] Edward L. Deci and Richard M. Ryan. The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, 11(4):227–268, 2000. doi:10.1207/S15327965PLI1104_01.

[27] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, page 581–590, New York, NY, USA, 2006. Association for Computing Machinery. doi:10.1145/1124772.1124861.

[28] Ersin Dincelli and InduShobha Chengalur-Smith. Choose your own training adventure: designing a gamified seta artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 29(6):669–687, 2020. doi:10.1080/0960085X.2020.1797546.

[29] European Union. Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive). Official Journal of the European Union, December 2022. CELEX: 32022L2555. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[30] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape for Supply Chain Attacks. Technical report, European Union Agency for Cybersecurity (ENISA), July 2021. Accessed 2026-02-16. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf, doi:10.2824/168593.

[31] European Union Agency for Cybersecurity (ENISA). Enisa threat landscape 2025. Technical report, ENISA, 2025. Accessed 2026-02-16. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[32] EY. How organizations are turning risk into resilience: 2025 ey technology risk pulse poll survey results. Web report, October 2025. URL: https://www.ey.com/en_us/insights/technology-risk/2025-ey-technology-risk-pulse-poll-survey-results.

[33] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, 2015. URL: https://www.sciencedirect.com/science/article/pii/S0747563215003854, doi:10.1016/j.chb.2015.04.075.

[34] FIDO Alliance. Replacing password-only authentication with passkeys in the enterprise. White paper (fido enterprise deployment working group), FIDO Alliance, June 2023. June 2023. URL: https://fidoalliance.org/wp-content/uploads/2023/06/FIDO-EDWG-Spring-2023_Paper-2_Replacing-Password-Only-Authentication_FINALv3.docx.pdf.

[35] Dinei Florêncio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW '07)*, pages 657–666. ACM, 2007. doi:10.1145/1242572.1242661.

[36] Birte U. Forstmann, Roger Ratcliff, and Eric-Jan Wagenmakers. Sequential sampling models in cognitive neuroscience: Advantages, applications, and extensions. *Annual Review of Psychology*, 67:641–666, 2016. doi:10.1146/annurev-psych-122414-033645.

[37] Sabrina Friedl, Tobias Reittinger, and Günther Pernul. Digital detectives: A serious point-and-click game for digital forensics. In Lynette Drevin, Wai Sze Leung, and Suné von Solms, editors, *Information Security Education - Challenges in the Digital Age*, pages 129–145, Cham, 2024. Springer Nature Switzerland.

[38] Sabrina Friedl, Tobias Reittinger, and Günther Pernul. From play to profession: A serious game to raise awareness on digital forensics. In Anna Lisa Ferrara and Ram Krishnan, editors, *Data and Applications Security and Privacy XXXVIII*, pages 269–289, Cham, 2024. Springer Nature Switzerland.

[39] Marylène Gagné and Edward L. Deci. Self-determination theory and work motivation. *Journal of Organizational Behavior*, 26(4):331–362, 2005. doi:10.1002/job.322.

[40] Esther Gal-Or and Anindya Ghose. The economic incentives for sharing security information. *Information Systems Research*, 16(2):186–208, 2005. doi:10.1287/isre.1050.0053.

[41] Gartner, Inc. Gartner forecasts worldwide end-user spending on information security to total $213 billion in 2025. Press release, July 2025. URL: https://www.gartner.com/en/newsroom/press-releases/2025-07-29-gartner-forecasts-worldwide-end-user-spending-on-information-security-to-total-213-billion-us-dollars-in-2025.

[42] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285, 2020. doi:10.1109/SP40000.2020.00047.

[43] Gerd Gigerenzer and Wolfgang Gaissmaier. Heuristic decision making. *Annual Review of Psychology*, 62:451–482, 2011. doi:10.1146/annurev-psych-120709-145346.

[44] Magdalena Glas, Manfred Vielberth, Tobias Reittinger, Fabian Böhm, and Günther Pernul. Visual programming in cyber range training to improve skill development. In Nathan Clarke and Steven Furnell, editors, *Human Aspects of Infor-*

mation Security and Assurance, pages 3–13, Cham, 2022. Springer International Publishing.

[45] Magdalena Glas, Manfred Vielberth, Tobias Reittinger, Fabian Böhm, and Günther Pernul. Improving cybersecurity skill development through visual programming. *Information and Computer Security*, 31(3):316–330, 02 2023. doi: 10.1108/ICS-11-2022-0170.

[46] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. Driving 2FA adoption at scale: Optimizing Two-Factor authentication notification design patterns. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 109–126. USENIX Association, August 2021. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/golla.

[47] Google Cloud Security and Mandiant. M-trends 2025 report. Technical report, Google LLC, 2025. Accessed 2026-02-16. URL: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf.

[48] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5):509–519, 2015. URL: https://www.sciencedirect.com/science/article/pii/S0278425415000423, doi:10.1016/j.jaccpubpol.2015.05.001.

[49] Sebastian Groll, Sascha Kern, Ludwig Fuchs, and Günther Pernul. Monitoring access reviews by crowd labelling. In Simone Fischer-Hübner, Costas Lambrinoudakis, Gabriele Kotsis, A. Min Tjoa, and Ismail Khalil, editors, *Trust, Privacy and Security in Digital Business*, pages 3–17, Cham, 2021. Springer International Publishing.

[50] Julie Haney and Wayne Lutters. Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer*, 53(10):91–95, 2020. doi: 10.1109/MC.2020.3001959.

[51] Julian Hazell. Spear phishing with large language models, 2023. URL: https://arxiv.org/abs/2305.06972, arXiv:2305.06972.

[52] Tejaswini Herath and H. R. Rao. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.*, 47(2):154–165, May 2009. doi:10.1016/j.dss.2009.02.005.

[53] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the New Security Paradigms Workshop (NSPW '09)*, pages 133–144. ACM, 2009. doi:10.1145/1719030.1719050.

[54] Linda Hill. How automated access verification can help organizations demonstrate HIPAA compliance: A case study. *J Healthc Inf Manag*, 20(2):116–122, 2006.

[55] Jeff Hodges, J.C. Jones, Michael B. Jones, Akshay Kumar, and Emil Lundberg. Web authentication: An api for accessing public key credentials — level 2. Recommendation, W3C, 2021. W3C Recommendation, 8 April 2021. URL: https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

[56] Matthias Hummer, Michael Kunz, Michael Netter, Ludwig Fuchs, and Günther Pernul. Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security*, 2016:19, 2016. doi:10.1186/s13635-016-0043-2.

[57] IBM Security and Ponemon Institute. Cost of a data breach report 2025. Technical report, IBM, 2025. Accessed 2026-02-16. URL: https://www.ibm.com/reports/data-breach.

[58] Pooya Jaferian, Hootan Rashtian, and Konstantin Beznosov. To authorize or not authorize: helping users review access policies in organizations. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 301–320, USA, 2014. USENIX Association.

[59] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, October 2007. doi:10.1145/1290958.1290968.

[60] Eric J. Johnson and Daniel Goldstein. Do defaults save lives? *Science*, 302(5649):1338–1339, 2003. doi:10.1126/science.1091721.

[61] Allen C. Johnston and Merrill Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS Q.*, 34(3):549–566, September 2010.

[62] Daniel Kahneman. Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review*, 93(5):1449–1475, December 2003. doi:10.1257/000282803322655392.

[63] Sascha Kern, Thomas Baumer, Sebastian Groll, Ludwig Fuchs, and Günther Pernul. Optimization of access control policies. *Journal of Information Security and Applications*, 70:103301, 2022. URL: https://www.sciencedirect.com/science/article/pii/S2214212622001533, doi:10.1016/j.jisa.2022.103301.

[64] Priscilla Koepke. Cybersecurity information sharing incentives and barriers. Technical Report Working Paper CISL# 2017-13, Cybersecurity Interdisciplinary Systems Laboratory (CISL), MIT Sloan School of Management, Massachusetts Institute of Technology, June 2017. Accessed 2026-02-17. URL: https://cams.mit.edu/wp-content/uploads/2017-13.pdf.

[65] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*, pages 2595–2604. ACM, 2011. doi:10.1145/1978942.1979321.

[66] Michael Kunz, Ludwig Fuchs, Michael Netter, and Günther Pernul. How to discover high-quality roles? a survey and dependency analysis of quality criteria in role mining. In Olivier Camp, Edgar Weippl, Christophe Bidan, and Esma Aïmeur, editors, *Information Systems Security and Privacy*, pages 49–67, Cham, 2015. Springer International Publishing.

[67] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859. IEEE, 2022. doi:10.1109/sp46214.2022.9833766.

[68] Sanam Ghorbani Lyastani, Michael Backes, and Sven Bugiel. A systematic study of the consistency of two-factor authentication user journeys on top-ranked websites. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2023)*, San Diego, CA, USA, 2023. Internet Society. URL: https://www.ndss-symposium.org/ndss-paper/a-systematic-study-of-the-consistency-of-two-factor-authentication-user-journeys-on-top-ranked-websites/, doi:10.14722/ndss.2023.23362.

[69] Brigitte C. Madrian and Dennis F. Shea. The power of suggestion: Inertia in 401(k) participation and savings behavior*. *The Quarterly Journal of Economics*, 116(4):1149–1187, 11 2001. doi:10.1162/003355301753265543.

[70] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019. doi:10.1145/3359183.

[71] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. Why users (don't) use password managers at a large educational institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, Boston, MA, August 2022. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/mayer.

[72] Katerina Megas, Barbara Cuthill, Marissa Dotter, Michael Garris, Ishika Khemani, Bronwyn Patrick, Noah Schiro, Julie Nethery Snyder, and Mohammad Zarei. Cybersecurity framework profile for artificial intelligence (nist ir 8596 iprd). Technical report, National Institute of Standards and Technology (NIST),

December 2025. Initial Preliminary Draft, Accessed 2026-02-16. URL: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8596.iprd.pdf.

[73] Florian Menges, Benedikt Putz, and Günther Pernul. DEALER: decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security*, 20(5):741–761, 2021. doi:10.1007/s10207-020-00528-1.

[74] Stephanie Mertens, Mario Herberz, Ulf J. J. Hahnel, and Tobias Brosch. The effectiveness of nudging: A meta-analysis of choice architecture interventions across behavioral domains. *Proceedings of the National Academy of Sciences*, 119(1):e2107346118, 2022. doi:10.1073/pnas.2107346118.

[75] Tobias Mirsch, Christiane Lehrer, and Reinhard Jung. Digital nudging: Altering user behavior in digital environments. In Jan Marco Leimeister and Walter Brenner, editors, *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, pages 634–648, St. Gallen, Switzerland, 2017.

[76] Robert Münscher, Max Vetter, and Thomas Scheuerle. A review and taxonomy of choice architecture techniques. *Journal of Behavioral Decision Making*, 29(5):511–524, 2016. doi:10.1002/bdm.1897.

[77] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The belmont report: Ethical principles and guidelines for the protection of human subjects of research. U.S. Department of Health, Education, and Welfare, 1979. Accessed: 2026-02-18. URL: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html.

[78] National Institute of Standards and Technology (NIST). Digital identity guidelines: Authentication and lifecycle management (sp 800-63b). Technical report, NIST, 2024. Accessed 2026-02-16. URL: https://pages.nist.gov/800-63-4/sp800-63b.html.

[79] R. Neudert, T. Baumer, T. Reittinger, and G. Pernul. Digital nudges in access reviews: Guiding deciders with range and composition. Submitted for publication, 2026.

[80] OWASP. Owasp top 10 for large language model applications. Project page, 2025. URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/.

[81] OWASP Foundation. OWASP top 10:2025 — A01 broken access control, 2025. Accessed 2026-02-16. URL: https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/.

[82] Simon Parkinson and Shakil Khana. Identifying high-risk over-entitlement in access control policies using fuzzy logic. *Cybersecurity*, 5:6, 2022. doi:10.1186/s42400-022-00112-1.

[83] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, page 319–338, USA, 2019. USENIX Association.

[84] Filippo Perrina, Francesco Marchiori, Mauro Conti, and Nino Vincenzo Verde. AGIR: Automating Cyber Threat Intelligence Reporting with Natural Language Generation . In *2023 IEEE International Conference on Big Data (BigData)*, pages 3053–3062, Los Alamitos, CA, USA, December 2023. IEEE Computer Society. URL: https://doi.ieeecomputersociety.org/10.1109/BigData59044.2023.10386116, doi:10.1109/BigData59044.2023.10386116.

[85] Justin Petelka, Yixin Zou, and Florian Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–15, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3290605.3300748.

[86] Grant A Pignatiello, Richard J Martin, and Ronald L HickmanJr. Decision fatigue: A conceptual analysis. *Journal of Health Psychology*, 25(1):123–135, 2020. doi:10.1177/1359105318763510.

[87] Evan Polman and Kathleen D. Vohs. Decision fatigue, choosing for others, and self-construal. *Social Psychological and Personality Science*, 7(5):471–478, 2016. doi:10.1177/1948550616639648.

[88] Julia Prümmer, Tommy van Steen, and Bibi van den Berg. Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, 150:104206, 2025. doi:10.1016/j.cose.2024.104206.

[89] Alexander Puchta, Sebastian Groll, and Günther Pernul. Leveraging dynamic information for identity and access management: An extension of current enterprise iam architecture. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP*, pages 611–618, Online Streaming, 2021. INSTICC, SciTePress. doi:10.5220/0010315706110618.

[90] Petri Puhakainen and Mikko Siponen. Improving employees' compliance through information systems security training: an action research study. *MIS Q.*, 34(4):757–778, December 2010.

[91] PwC. Global compliance survey 2025. Technical report, PwC, 2025. Accessed 2026-02-16. URL: https://www.pwc.com/gx/en/issues/risk-regulation/pwc-global-compliance-study-2025.pdf.

[92] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Employee motivation in organizational cybersecurity: Matching theory and reality.

In Nathan Clarke and Steven Furnell, editors, *Human Aspects of Information Security and Assurance*, pages 3–16, Cham, 2025. Springer Nature Switzerland.

[93] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Motivational factors in cybersecurity: linking theory to organizational practice. *Information and Computer Security*, 06 2025. Invited extended version. In press. doi:10.1108/ICS-02-2025-0046.

[94] Tobias Reittinger, Magdalena Glas, and Günther Pernul. Moving beyond passwords: Investigating the effect of digital nudges on passkey adoption. In *026 CHI Conference on Human Factors in Computing Systems*. ACM, 2026. Accepted for publication.

[95] Tobias Reittinger, Johannes Grill, and Günther Pernul. Share and benefit: incentives for cyber threat intelligence sharing. *International Journal of Information Security*, 25:37, 2026. Article 37.

[96] Tobias Reittinger and Günther Pernul. A taxonomy of positive incentives to motivate cybersecurity behaviors. In *Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS-58)*, pages 4542–4551, 2025. doi:10.24251/HICSS.2025.545.

[97] Tobias Reittinger and Günther Pernul. No password, no problem? a large-scale field study of passkey adoption and usage. In *2026 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2026. Accepted for publication.

[98] Karen Renaud and Verena Zimmermann. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies*, 120:22–35, 2018. doi:10.1016/j.ijhcs.2018.05.011.

[99] Sayak Saha Roy, Cesar Torres, and Shirin Nilizadeh. "'explain, don't just warn!" – a real-time framework for generating phishing warnings with contextual cues, 2025. URL: https://arxiv.org/abs/2505.06836, arXiv:2505.06836.

[100] Richard M. Ryan and Edward L. Deci. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1):68–78, 2000. doi:10.1037/0003-066X.55.1.68.

[101] J.H. Saltzer and M.D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975. doi:10.1109/PROC.1975.9939.

[102] William Samuelson and Richard Zeckhauser. Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1(1):7–59, 1988. doi:10.1007/BF00055564.

[103] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[104] Ryan Schin. Despite increasing cybersecurity attacks, people still believe antiquated username and passwords are strong enough. Accessed: 02/11/25. URL: https://www.yubico.com/press-releases/despite-increasing-cybersecurity-attacks-people-still-believe-antiquated-username-and-passwords-are-strong-enough/.

[105] Lorin Schöni, Victor Carles, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. You know what? - evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. In *Proceedings of the 2024 European Symposium on Usable Security*, EuroUSEC '24, page 1–14, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3688459.3688460.

[106] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Trans. Inf. Syst. Secur.*, 18(4), May 2016. doi:10.1145/2891411.

[107] Herbert A Simon. A behavioral model of rational choice. *The quarterly journal of economics*, 69:99–118, 1955.

[108] Frank Stajano and Paul Wilson. Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3):70–75, March 2011. doi:10.1145/1897852.1897872.

[109] Richard H. Thaler and Cass R. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, 2008.

[110] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel Von Zezschwitz. Security, availability, and multiple information sources: exploring update behavior of system administrators. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, SOUPS'20, USA, 2020. USENIX Association.

[111] Wiem Tounsi and Helmi Rais. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72:212–233, 2018. doi:10.1016/j.cose.2017.09.001.

[112] Amos Tversky and Daniel Kahneman. Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157):1124–1131, 1974. doi:10.1126/science.185.4157.1124.

[113] United States Congress. Health insurance portability and accountability act of 1996, August 1996. Pub. L. 104–191, 110 Stat. 1936 (Aug. 21, 1996). URL: https://www.govinfo.gov/link/plaw/104/public/191.

[114] United States Congress. Sarbanes–oxley act of 2002, July 2002. Pub. L. 107–204, 116 Stat. 745 (July 30, 2002). URL: https://www.govinfo.gov/link/plaw/107/public/204.

[115] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How does your password measure up? the effect of strength meters on password creation. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 65–80, Bellevue, WA, August 2012. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur.

[116] Tommy van Steen and Julia R. A. Deeleman. Successful gamification of Cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9):593–598, September 2021. doi:10.1089/cyber.2020.0526.

[117] Verizon Business. 2025 data breach investigations report (dbir). Technical report, Verizon Business, 2025. Accessed 2026-02-16. URL: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf.

[118] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576–586, 2011. URL: https://www.sciencedirect.com/science/article/pii/S016792361100090X, doi:10.1016/j.dss.2011.03.002.

[119] Kathleen D. Vohs, Roy F. Baumeister, Brandon J. Schmeichel, Jean M. Twenge, Noelle M. Nelson, and Dianne M. Tice. Making choices impairs subsequent self-control: A limited-resource account of decision making, self-regulation, and active initiative. *Journal of Personality and Social Psychology*, 94(5):883–898, 2008. doi:10.1037/0022-3514.94.5.883.

[120] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. Misp: The design and implementation of a collaborative threat intelligence sharing platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, WISCS '16, page 49–56, New York, NY, USA, 2016. Association for Computing Machinery. doi:10.1145/2994539.2994542.

[121] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87:101589, 2019. doi:10.1016/j.cose.2019.101589.

[122] Jan Philip Wahle, Terry Ruas, Saif M Mohammad, Norman Meuschke, and Bela Gipp. Ai usage cards: Responsibly reporting ai-generated content. In *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, pages 282–284. IEEE, 2023.

[123] Chun Wang, Steve T. K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. The next domino to fall: Empirical analysis of user passwords across online services. In *Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, CODASPY '18, pages 196–203, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3176258.3176332.

[124] Markus Weinmann, Christoph Schneider, and Jan vom Brocke. Digital nudging. *Business & Information Systems Engineering*, 58(6):433–436, 2016. doi:10.1007/s12599-016-0453-1.

[125] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120:1–13, 2018. URL: https://www.sciencedirect.com/science/article/pii/S1071581918303628, doi:10.1016/j.ijhcs.2018.06.004.

[126] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. Fido2 the rescue? platform vs. roaming authentication on smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3544548.3580993.

Declaration of Generative AI Technologies

During the preparation of this work, the author used DeepL, Grammarly, and ChatGPT (version 5.2) to improve the language and readability of the manuscript. After using these tools, the author reviewed and revised the text as necessary and takes full responsibility for the content of the publication. For transparency, we publish AI Usage Cards on GitHub[3] documenting our use of generative AI [122].

[3] https://github.com/ReittingerDissertation/Availability

Part II

Research Papers

P1 Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice

Current status:	Published
Journal:	Information and Computer Security
Ranking:	2.2 Impact Factor
Date of acceptance:	May 28, 2025
Date of publication:	June 26, 2025
Comment:	Invited extended version of C1 [92]
Full citation:	Reittinger, T., Glas, M., Aminzada, S., & Pernul, G. (2025). Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice. *Information & Computer Security*. (in press).

Authors' contributions:		
	Tobias Reittinger	50%
	Magdalena Glas	25%
	Sarah Aminzada	15%
	Günther Pernul	10%

Journal description: The *Information and Computer Security* (peer-reviewed) is an interdisciplinary journal focused on the management and security of information and information systems. It publishes research and case studies on new technologies, methods, empirical studies and practical applications, emphasizing business, organizational and human aspects relevant to academics and practitioners.

The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/2056-4961.htm

Motivational factors in cybersecurity: linking theory to organizational practice

Information & Computer Security

Tobias Reittinger, Magdalena Glas, Sarah Aminzada and Günther Pernul
Department of Information Systems, University of Regensburg, Regensburg, Germany

Received 14 March 2025
Revised 28 May 2025
Accepted 28 May 2025

Abstract

Purpose – This study investigates the application of motivational strategies to encourage security-compliant behavior among employees in organizational cybersecurity, exploring how organizations motivate security-compliant behavior among employees in Germany. This study aims to bridge the gap between theoretical motivational models and practical implementation within organizations.

Design/methodology/approach – This research uses a qualitative approach, conducting semi-structured interviews with 18 participants from organization of different sizes and sectors in Germany, illuminating the topic from three perspectives: executive managers, security specialists and regular employees. A deductive analysis is applied to coding the interview along intrinsic motivators (competence, relatedness and autonomy) and external motivators (incentives and nudges).

Findings – This study found that some motivational factors, such as positive incentives like vouchers, and a healthy error culture effectively lead to employees being motivated to follow security guidelines. Conversely, the authors found several aspects that employees perceive as frustrating and ineffective, such as compulsory e-learnings or overcomplex security policies, hindering their intrinsic motivation to contribute to organizational cybersecurity.

Originality/value – While existing literature offers insights into specific motivational methods applied within organizations, to the best of the authors' knowledge, this paper is the first to adopt a broader perspective by analyzing how organizations' cybersecurity strategies integrate both intrinsic and extrinsic motivational approaches.

Keywords Cybersecurity, Motivation, Incentives, Nudges, Awareness, Compliance, Policy

Paper type Research paper

1. Introduction

As today's digital landscape evolves rapidly, the threat of cybercrime is ever-growing. In 2023, the reported costs of cyberattacks amounted to US$8.15bn, estimated to rise to over US$13bn by 2028 (Statista, 2023). Most of these attacks target employees as entry points to infiltrate organizational systems or extract sensitive information, for example, through phishing or stolen credentials (Verizon, 2023). To this end, organizations must recognize their employees' essential role in maintaining a robust cybersecurity posture, acting as the

This paper is part of the CONTAIN project, funded by the Federal Ministry of Education and Research as part of the German government's "Research for Civil Security" framework program (13N16586).

Use of Generative AI: The authors refined the language and readability of this paper with DeepL, Grammarly and ChatGPT (Version 4), for which they take full responsibility [3].

Information & Computer Security
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2025-0046

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

"last line of defense" against cyberattacks (Eze and Hawker, 2022; Kirsch and Boss, 2007). This makes it vital that employees understand and adhere to cybersecurity policies (von Solms *et al.*, 2023). Hence, exploring ways to motivate employees toward security-compliant behavior emerges as a critical challenge. While existing literature provides theoretical methods for improving individuals' intrinsic and extrinsic motivation in this regard (Fisher *et al.*, 2021; Gangire *et al.*, 2019; Yang *et al.*, 2020), there is a lack of research examining how these strategies are implemented in current organizational settings (Section 2). Thus, we raise the following research question:

RQ. How do organizations motivate employees toward security-compliant behavior?

To address this research question, we conducted a study in Germany, a leading economic country with a diverse landscape of organizations. Through semi-structured interviews with 18 participants drawn from organizations of varying sizes and industry sectors, we capture insights from three organizational perspectives: executive managers, security experts and regular employees. We use a literature-based classification scheme to categorize the identified strategies and examine their efficacy in improving the organizational security posture based on the participants' experiences. Through this analysis, we outline ways for enhancing and complementing existing strategies, aiming to provide organizations with actionable insights on effectively motivating employees toward security-compliant behavior.

The remainder of this paper is structured as follows. In Section 2, we provide the theoretical foundation of this work. Section 3 outlines our methodology for conducting and analyzing the semi-structured interviews, followed by presenting our findings in Section 4. We then discuss the conclusions drawn from these findings in Section 5 and conclude this work in Section 6.

This work represents an extension of the research we presented at the International Symposium on Human Aspects of Information Security and Assurance 2024 and which is published in the corresponding proceedings (Reittinger *et al.*, 2024). As such, we could extend the background and related work section (Section 2), giving the reader a more comprehensive overview of existing theories and literature in the field. Additionally, this extended version allowed us to include more findings drawn from the interviews (Section 4) and extend the recommendations for organizations (Section 5) accordingly.

2. Background and related work

We outline the theoretical background and related work in the following.

2.1 Motivational theory

To categorize motivational strategies, we use Self-Determination Theory (SDT) as proposed by Ryan and Deci (2000). SDT offers a framework for understanding human motivation by distinguishing between *intrinsic motivation* and *extrinsic motivation*. Intrinsic motivation, which arises from an internal interest in an activity, fosters long-term commitment and is enhanced by fulfilling three basic psychological needs: *competence*, *relatedness* and *autonomy*. Specifically, competence entails a sense of mastery in one's actions; relatedness involves forming meaningful interpersonal connections; and autonomy refers to experiencing volition in one's behavior. Although organizations cannot directly shape employees' experience of autonomy, they can modify the work environment to promote intrinsic motivation (Gagné and Deci, 2005). In contrast, extrinsic motivation derives from external rewards and punishments and effectively drives short-term behavior. However, its use should be approached with caution, as overreliance on external incentives may

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

undermine intrinsic motivation. Extrinsic motivation can be reinforced through two primary mechanisms: *incentives* and *nudges* (Ryan and Deci, 2000; Thaler and Sunstein, 2008). Incentives are designed to influence behavior by offering rewards or imposing penalties, whereas nudges are subtle cues that encourage desired decisions without restricting individual choice (Thaler and Sunstein, 2008). Examples include information visibility nudges, which highlight relevant details; choice-default nudges, which preset options to guide users toward specific decisions; messenger reputation nudges, which leverage the credibility of the communicator to underscore the importance of a message; and social reference nudges, which highlight how peers behave and, thus, lowering the perceived barrier to actions (Hummel and Maedche, 2019; Jesse and Jannach, 2021). In the cybersecurity domain, applying SDT enables organizations to cultivate long-term commitment by fostering intrinsic motivation, thereby encouraging employees to adopt security-compliant behaviors based on a personal conviction in the value of these practices (Gangire *et al.*, 2019). Additionally, organizations can strategically use extrinsic motivation to promote short-term security compliance (Golla *et al.*, 2021). Figure 1 illustrates the categorization of these motivational strategies. In this paper, we define *motivators* as the factors that organizations can leverage to enhance employees' motivation toward security-compliant behavior.

2.2 Related work

Several studies have advanced the understanding of employee motivation in organizational cybersecurity. Pham *et al.* (2017), using a methodology similar to ours, found that IT environments often demotivate employees. Two conceptual studies by Gangire *et al.* (2019) and Fisher *et al.* (2021) highlight the potential impact of employees' intrinsic motivation on security-compliant behavior, drawing on existing literature. Empirical research further examines the influence of intrinsic motivation on adherence to security protocols: for instance, Yang *et al.* (2020) showed that intrinsic motivation, as described by SDT, encourages security compliance, though their findings were limited to employees' willingness to adopt password managers. Li *et al.* (2019) investigated how cybersecurity awareness, corresponding to the SDT factor *competence*, shapes cybersecurity behavior, demonstrating that better-informed employees are more likely to act in a security-compliant manner. In contrast, Reeves *et al.* (2021) focused on negative motivators, revealing that excessive security training or forced security measures (e.g. frequent password changes) can lead to "security fatigue" and, consequently, non-compliant behavior. On the other hand, Goel *et al.* (2021) examined extrinsic motivators,

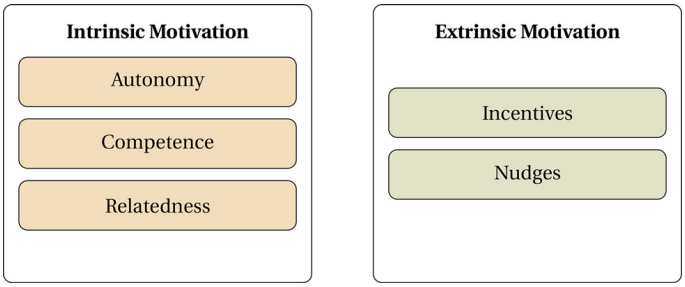


Figure 1. Categorization of motivational strategies based on self-determination theory (Ryan and Deci, 2000) and Thaler and Sunstein (2008)
Source: Authors' own creation

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

finding that financial rewards and penalties increase security compliance. Reittinger and Pernul (2025) proposed a taxonomy of cybersecurity incentives, presenting a range of extrinsic motivators organizations can use. Additionally, Renaud and Zimmermann (2019) found that nudges encourage users to select stronger passwords, and Golla *et al.* (2021) noted a similar effect in increasing the adoption of two-factor authentication. Baumer *et al.* (2024) further demonstrated that digital nudges can significantly alter employees' behaviors during access reviews. Overall, prior research has either taken a purely theoretical approach or zeroed in on specific motivational factors (such as *competence*) or discrete areas of security compliance. By contrast, our study adopts a broader perspective, exploring how diverse organizations implement motivational strategies to encourage security-compliant behavior. We compare our findings to these earlier works to contextualize our results within the larger literature, identify common ground and highlight opportunities for organizations to refine their motivational strategies.

3. Method

In this section, we describe our methodology. We chose semi-structured interviews (Adams, 2015) to engage participants in an open discussion on their experiences with employee motivation in organizational cybersecurity. We explored the topic from three different perspectives: *managers*, who hold leadership positions within organizations; *security specialists*, who are professionals responsible for security measures; and *employees*, who comprise organizations' broader workforce.

3.1 Participant recruitment

To ensure participants are from all three perspectives, we used purposive sampling for the recruitment. Suitable participants were recruited from the authors' professional networks. We aimed to recruit participants from various industrial sectors and organization sizes to capture a broad spectrum of experiences. Participants were not compensated for their participation. We stopped recruiting after the interview findings reached saturation, as described below. The final sample consists of 18 participants with four *managers*, five *security specialists* and nine *employees*, all from Germany. Participants are described in Table 1.

3.2 Interview structure

In the questionnaire development, we deliberately avoided questions about specific types of motivational approaches or SDT so as not to bias their answers. First, participants described their general demographics. Subsequently, participants shared their general perceptions of the security culture within their organizations. This enabled us to establish a foundation for the discussion and provide context for understanding participants' perspectives. Next, an open dialogue was facilitated to explore the strategies used by their respective organizations to enhance employee motivation, as well as areas they identified for potential enhancement. The interview questionnaire is presented on GitHub [1].

3.3 Interview procedure and ethics

The interviews were conducted by two of the authors between October 2023 and March 2024. In all, 14 interviews were held remotely via Zoom or Microsoft Teams, and 4 were conducted in person. For interviews where participants agreed, we conducted audio recordings, which were later transcribed for the analysis. If this was not feasible (M4, S9,

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

Table 1. Summary of our 18 interview participants' demographics

ID	Job title	Sector	Employees	Gender	Experience
M1	CEO	Retail	10–99	M	35
M2	CEO	Consulting	100–999	F	10
M3	Head of department	Construction	1,000–9,999	F	9
M4	Doctor	Healthcare	10–99	M	22
S5	CISO	Financial services	100–999	M	8
S6	Security architect	Infrastructure	1,000–9,999	M	6
S7	Head of department	Metal processing	1,000–9,999	M	6
S8	CISO	Infrastructure	+10,000	M	12
S9	Security consultant	Software development	1–9	M	10
E10	Engineer	Metal processing	1,000–9,999	M	3
E11	Administration	Public administration	100–999	F	5
E12	Graphic designer	Consulting	100–999	M	7
E13	Chemist	Chemical industry	1,000–9,999	M	1
E14	Researcher	Public administration	1,000–9,999	M	2
E15	Administration	Construction	1,000–9,999	M	2
E16	Accountant	Public administration	+10,000	F	9
E17	Financial advisor	Financial services	100–999	F	17
E18	Medical assistant	Healthcare	10–99	F	6

Note(s): IDs beginning with *M* refer to *management*, *S* to *security specialist* and *E* to *employee* positions
Source(s): Authors' own creation

E16), then we manually captured participants' responses during the interviews. The interviews lasted, on average, 40 min.

Before conducting our study, the study design was approved by the *German Association for Experimental Economic Research*, and we obtained an Institutional Review Board certificate [2]. Participants consented to participating and to recording the interviews. After the transcription, we deleted the audio recordings and anonymized participants' affiliations to preserve their privacy.

3.4 Coding and analysis

To analyze the use of strategies to motivate employee motivation in cybersecurity, we used a deductive analysis approach (Bingham and Witkowsky, 2021) to map interview data with the theory-based classification of employee motivation introduced in Section 2. This classification served as an initial codebook. Two authors refined the coding structure through multiple rounds, resolving conflicts with flexible coding (Deterding and Waters, 2021). After 18 interviews, no additional code was created, indicating that the analysis reached saturation and further interviews would likely yield no further insights.

3.5 Limitations

We acknowledge our methodology's limitations. The geographic scope of the interviewees was limited to Germany. While this might restrict the generalizability of the results to other countries, it allowed for a focused exploration of employee motivation for security practices within the German context. Future research could validate our results in different regions. There is also the possibility of self-reporting bias, particularly among managers and specialists, which may affect the data's accuracy. To mitigate this limitation, we interviewed participants from diverse organizations and only stopped as the coding reached saturation.

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

4. Findings

In this section, we present the identified motivators of the interviews. As introduced in Section 2, we distinguish between two types of motivators. First, *intrinsic motivators* are internal factors that engage employees in long-term security-compliant behavior based on personal interest and the activities' inherent satisfaction. In contrast, *extrinsic motivators* are external factors that drive short-term security-compliant behavior based on rewards or encouragement.

4.1 Intrinsic motivators

In the following, we describe intrinsic motivators we identified in the interviews, classified by the three categories *competence*, *relatedness* and *autonomy.*

4.1.1 Competence. Organizations can encourage employees to adhere to security-compliant behaviors by implementing cybersecurity education programs. All the interviewees' organizations offer some sort of cybersecurity awareness training for their employees. Organizations typically test the knowledge gained from a training course in an assessment. Half of the organizations offer training solely when hiring employees. One employee summarizes the experience:

Organizations can encourage employees to adhere to security-compliant behaviors by implementing cybersecurity education programs. All interviewed organizations offer some form of awareness training, and most of them assess employees' newly acquired knowledge after the training. Half of the organizations provide this instruction only when employees are first hired, potentially limiting its effectiveness over time. In addition, making employees aware of real-world security incidents, particularly those at suppliers or within the broader industry, can further enhance motivation by illustrating that this can happen to every organization. Such tangible examples help employees grasp the seriousness of potential threats and reinforce the need for security-compliant behavior. One employee summarizes the training experience:

> I only had one training course at the beginning of my employment. Little of it has stuck […] and a refresher wouldn't hurt. (E17)

In contrast, the other half of the organizations conduct cybersecurity training on an annual basis. While research underscores the importance of periodic sessions for preserving employees' cybersecurity competence (Hatzivasilis *et al.*, 2020), many participants reported difficulties applying the training to their everyday tasks. They struggle to derive benefits for their daily work and often perceive it as an additional burden. Moreover, several participants emphasized that perceived relevance plays a crucial role in motivating engagement. As one employee explained:

> There is often discussion about the usefulness of the training courses, as the relevance is not recognized. This can increasingly be observed among colleagues who are not IT-savvy. (E10)

Additionally, participants noted that much of this training remains overly generic, covering basic cybersecurity best practices with limited relevance to their day-to-day responsibilities. As a result, one participant explained the following:

> […] most people just endure the training and then go back to doing whatever for the rest of the year. (E11)

Some training courses offer gamification and serious games. Through a playful environment, organizations want to engage their employees to gain knowledge in a hands-on environment. Yet, not all employees are fond of gamification and serious games. Interviewees reported that

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

younger employees enjoy playing serious games but noted older employees prefer a more neutral learning environment with fewer distractions. One participant explains the perception of a serious game:

> […] quiz questions and mini-games that older employees comment on with little enthusiasm. (E10)

Managers and security specialists have also recognized the different training requirements of different employee groups. Still, the same training content is typically used for all employees. This has disadvantages for the training's effectiveness, as a manager acknowledges that many employees cannot derive benefits from it for their daily work.

Interviewees of large organizations reported they are regularly exposed to phishing simulations. These simulations have two objectives. First, they want to check employees' knowledge levels to adjust the scope of training accordingly. Second, employees' awareness is raised as they know that they regularly receive phishing emails and develop a routine of reporting emails. Employees recognize the positive effect of increased awareness and are not bothered by phishing simulations, as they take up little time in their day-to-day business.

Furthermore, all the interviewees' organizations have security policies that aim to guide employees toward security-compliant behavior, such as rules for passwords or the use of USB sticks. However, acceptance of these policies is perceived differently across roles: while security specialists view acceptance as high, employees feel it is generally low. As a result, employees report facing practical challenges with those guidelines:

> The security policies are a 10-page document with countless regulations. As a result, I am unsure what I can and cannot do. (E11)

Although employees know that there are security policies, some interviewees reported that they are unaware of where they are stored and how to access them. To summarize, organizations lack personalized training to continuously educate employees and comprehensible security policies.

4.1.2 Relatedness. The interviewees agree that the more employees feel connected to the organization, the more likely they are to protect the organization and, thus, behave in a security-compliant manner:

> A happy employee is more attentive and likely to report […] if something seems strange or if they have clicked on a suspicious link. (M1)

Additionally, organizations encourage relatedness by strengthening cooperation and a sense of belonging among employees, emphasizing that cybersecurity is a collective responsibility. As one participant explained:

> Everyone understands that security risks are also business risks and that we can only manage them together. (S8)

In detail, organizations pass on reported incidents via their intranet, as attackers typically try different places in the same organization. This practice spreads crucial information and initiates open discussions on cybersecurity matters within the workplace. In addition, some employees reported an open information culture among the organizations' workforce, where they openly discuss uncertainties about cybersecurity practices and incidents that have occurred in the organization with their colleagues.

Despite ongoing efforts to promote teamwork and collective responsibility, many employees noted a lack of relatedness in their organizations' cybersecurity initiatives. They stressed that visible commitment from managers is essential for motivating the workforce to take cybersecurity seriously. When senior leadership does not treat cybersecurity as a core

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

business concern, employees' sense of organizational belonging fails to translate into secure behaviors. One interviewee remarked:

> Managers dismiss awareness training as a gimmick and demand that employees clock out. (E10)

According to participants, such an attitude diminishes the perceived importance and value of security training, ultimately undermining employees' motivation to remain vigilant. They called for a reversal of this pattern, emphasizing that executives should model responsible cybersecurity practices. As another participant explained:

> C-Levels are not even aware that they have to take cybersecurity into their own hands. They see it as a task of the security department. (E12)

By actively exemplifying cybersecurity as a shared responsibility, managers can reinforce the importance of secure practices and foster a stronger sense of relatedness across the organization. In sum, relatedness can foster security-compliant behavior, but often, management lacks cybersecurity commitment, diminishing employees' relatedness.

4.1.3 Autonomy. Many employees reported feeling that their autonomy in security-related practices is overly restricted. Training sessions, for instance, are often compulsory and include mandatory assessments. This obligatory format can sap employees' motivation, as it shifts their focus from genuinely learning to merely completing the course:

> The mandatory training is an additional burden in day-to-day business. One colleague even had the training done by an intern. (E10)

While interview participants recognize the importance of mandatory security training, many still find it frustrating:

> People get it, but it still gets on their nerves. (E13)

This frustration also extends to certain security policies – such as mandatory password changes every three months – that aim to enhance security but often yield superficial compliance. By compelling frequent password updates, some organizations inadvertently encourage minimal adjustments rather than meaningful improvements:

> I comply with the mandatory password change by adding a single character or adjusting the capitalization. I think it's doubtful whether the rule makes sense at all, […] but I have no choice. (E12)

In short, a culture of enforced cybersecurity measures could lead to a superficial compliance. Instead of genuinely bolstering security, these rigid rules can undermine it by fostering resentment and habitual workarounds. Notably, several security specialists reported better outcomes when granting employees more flexibility, such as selecting their own password management strategies within certain guardrails. This added autonomy helps employees perceive these requirements not as arbitrary burdens, but as meaningful steps to protect their organization. Striking a balance between firm guidelines and reasonable freedom can alleviate frustration and cultivate a more proactive, security-conscious culture.

4.2 Extrinsic motivators

As outlined above, extrinsic motivators can effectively promote a timely shift in employee behavior. In the following, we describe the identified extrinsic motivators classified by the two categories *incentives* and *nudges*.

4.2.1 Incentives. Most organizations within our study avoid negative incentives, like punishments, for employees who have made a mistake in cybersecurity. Organizations recognize the value of a positive error culture, where mistakes are viewed as an opportunity

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

for improvement. This approach encourages employees to report security incidents without fear of sanctions, as one manager articulated:

> Who clicks is a victim, not a perpetrator. […] We live a healthy error culture. No employee is punished for making unintentional mistakes. Employee reportings help us immensely, so we want to facilitate it. (S8)

Yet, implementing a healthy error culture is not successful in all organizations. In some cases, employees must pass additional mandatory training if they make a mistake, which is perceived as a punishment. Employees stated that sanctions diminish their motivation to act security-compliantly and report security incidents. One employee even reported being scared of the security department.

Regarding positive incentives, some interviewees' organizations have introduced bonus programs to motivate proactive cybersecurity behaviors. These initiatives reward employees for reporting phishing emails or suggesting improvements to cybersecurity practices. The prospect of receiving a voucher for the most submitted reports encourages employee awareness and reporting commitment. An interviewee shared their experience:

> Before [the bonus program], we simply deleted potential phishing emails. Now we report them with the phishing button in Outlook and can win a voucher as a result. (E17)

While incentives can increase reporting and positively shift employee behavior, they also have downsides, including higher processing efforts and costs for IT departments. Yet, managers view these as acceptable trade-offs for enhancing cybersecurity and maintaining an incident-free reputation. A management participant elaborates on this balance:

> The numerous reports cause a higher efforts in our IT department, which results in higher costs. But it's worth the positive reputation. (M2)

Furthermore, employees describe that their motivation to report suspicious activities or emails greatly increases when they know that the organizations use their reports and have value. Interviewees are also uncertain whether their reports are actual incidents or false positives. Thus, feedback would be an incentive for employees and could improve their competence. Yet, employees often lack a response, which can lead to disillusionment, as one noted:

> I often report emails via the phishing button, but nothing happens, which is demotivating. It feels as if […] my efforts are for nothing. (E18)

Timely feedback for reported security incidents not only acknowledges employees' efforts but also can reinforce the learning process:

> Although my reports are processed by IT, it takes several weeks to receive feedback. I can no longer remember what I reported. […] The learning effect would be greater if I received feedback more quickly. (E17)

In summary, establishing a healthy error culture, creating rewards for proactive cybersecurity behavior and leveraging employee commitment were identified as compelling incentives for cybersecurity within the organization.

4.2.2 Nudges. Information visibility nudges are widely used in organizations to heighten employee awareness of potential security threats. For instance, many email programs display prominent warnings, such as a red banner, to indicate when messages originate from outside the organization. As one security specialist explained:

> Employees are often careless and click on links and open attachments from external untrusted senders. We want to increase awareness with a red banner so employees read the message more carefully. (S5)

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

By prompting employees to scrutinize external emails more thoroughly, these nudges can help reduce careless interactions with potential phishing attempts. However, the lack of granularity in how these warnings are applied diminishes their overall effectiveness. According to multiple interviewees, all messages from external senders receive the same alert – regardless of their actual risk level. Our interviewees described that this implementation has inadvertently led to security fatigue, as they feel overwhelmed by constant alerts and start to disregard these warnings. An employee described their experience:

> Every email from a customer has the same warning. Initially, I read every message cautiously, now I hardly see the warning anymore. (E12)

Beyond highlighting potential risks, some organizations have introduced a social reference nudge to encourage reporting of security incidents and suspicious emails. One security specialist (S5) described using a social reference nudge, showing how many colleagues have submitted reports. This approach leverages the human tendency to *follow the herd* (Jesse and Jannach, 2021), signaling that reporting suspicious emails is common among the colleagues. As the specialist noted, reporting rates increased once employees realized many of their peers were also taking action.

Overall, nudges can promote security-compliant behavior of employees, as they guide them toward more secure decisions. Nonetheless, overuse of nudges may cause security fatigue and reduce their effectiveness.

5. Discussion

We now discuss our findings and offer recommendations for organizations to motivate employees toward security-compliant behavior in the long term. We map our recommendations with the different types of motivators in Table 2.

5.1 Management commitment

Organizations need to adapt their security culture to motivate employees to comply with security policies, as outlined by Mwim and Mtsweni (2022). They emphasize that cybersecurity is a collective responsibility, with every employee potentially representing a security vulnerability. The fighter analogy by von Solms *et al.* (2023) offers an effective way to communicate this concept to employees. Inspired by firefighting principles, this approach involves training employees to detect and address security incidents, similar to how firefighters extinguish fires to protect their organization. Within this analogy, every employee becomes a security fighter capable of identifying and mitigating cybersecurity threats. This analogy can help build a culture where all employees recognize themselves as contributors to organizational security, fostering ownership and empowerment.

Table 2. Mapping of our recommendations with the different types of motivators

	Intrinsic motivators			Extrinsic motivators	
Recommendations	Competence	Relatedness	Autonomy	Incentives	Nudges
Management commitment		•			•
Personalized education	•		•		
Comprehensible policy	•		•		•
Using employee reports	•	•	•	•	•

Source(s): Authors' own creation

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

Organizations can further support this cultural shift by using *messenger reputation* nudges to promote the analogy of cybersecurity as a shared responsibility. Jesse and Jannach (2021) emphasize that employees are more inclined to follow the lead of people they respect and trust. By doing so, leaders motivate employees to adopt secure behavior and reinforce their central role in safeguarding the organization. Improving this sense of relatedness can integrate cybersecurity into everyone's job responsibilities.

However, our study, in line with prior research (ISACA, 2023), shows that these approaches often lack support at the management level. When executive leaders are not involved and lack an understanding of cybersecurity, it is frequently perceived as a mere cost rather than a vital part of the organization's IT strategy. This perception may stem from insufficient cybersecurity expertise among executives (Haislip *et al.*, 2021; Olt *et al.*, 2019; Sonnenschein *et al.*, 2017). Therefore, a comprehensive cybersecurity strategy should not only engage executives in decision-making but also enhance their competence through tailored initiatives and awareness programs. Programs such as cyber range exercises offer practical opportunities for executives to experience simulated cybersecurity incidents, enabling them to understand the impact of real-time threats and the importance of proactive security measures (Glas *et al.*, 2025; Glas *et al.*, 2023). Through such initiatives, executives can make better-informed decisions, ensuring that cybersecurity is recognized and prioritized as a critical component of the organization's long-term success.

5.2 Personalized and voluntary education

Li *et al.* (2019) identified that better-educated employees adhere more to security policies and are more aware. However, in the evolving cybersecurity landscape, training methods often fall short, presenting learning material that is too complex and abstract for the diverse needs of employees (Alotaibi *et al.*, 2023). These one-size-fits-all programs often disregard the fact that employees come with varying degrees of technical expertise, perform different roles and operate under diverse workloads, leading to suboptimal learning outcomes. An effective approach could be to tailor the content and difficulty of training materials to employees' current knowledge levels and specific responsibilities, ensuring that instruction remains relevant, accessible and appropriately challenging. In particular, it could be vital to illustrate how small errors can escalate into major security breaches, underscoring the real-world consequences. Sharing examples of actual attacks within the same industry or among suppliers, along with their underlying causes, could further explain the impact that seemingly minor oversights can have.

Additionally, serious games have been shown to significantly enhance cybersecurity knowledge by immersing learners in interactive, problem-solving scenarios (Friedl *et al.*, 2024b; Friedl *et al.*, 2024a). Although younger employees may respond more enthusiastically to these techniques, the immersive format can boost knowledge retention across all age groups. By highlighting tangible risks and everyday relevance, such targeted and engaging training strategies can motivate employees to adopt security-compliant behaviors and ultimately fortify the organization's overall security posture.

However, not all employees encounter the same cybersecurity challenges. Certain *high-risk* groups, such as those with access to highly sensitive data, critical infrastructure or direct influence over organizational security, require specialized awareness strategies beyond standard training. Developers, for instance, regularly handle proprietary source code and other confidential information, making them prime targets for cyberattacks. Conventional training modules often fail to cover application-level vulnerabilities, secure coding practices or the specific social engineering tactics targeting developers (Gasiba *et al.*, 2020;

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

Siadati *et al.*, 2024). Tailored training for these groups could enhance knowledge retention and strengthen their commitment to security-compliant behavior.

Another promising alternative is using cyber range-based security awareness campaigns that offer a hands-on, immersive experience by simulating attacks, such as brute-force password cracking, to demonstrate both the threat and its organizational impact (Glas *et al.*, 2024). This approach helps employees understand the critical importance of cybersecurity practices, improving their ability to identify, prevent and respond to security incidents. Beyond traditional awareness training, microlearning approaches present another promising approach by providing security guidelines at the moment of need, making security education more practical and context-driven (Kävrestad and Nohlberg, 2020).

Fisher *et al.* (2021) advocates for voluntary education programs rather than mandatory training. However, none of the interviewees' organizations currently offer such opportunities. While regulatory requirements may pose challenges, organizations could supplement mandatory programs with voluntary cybersecurity education. Employees eager to deepen their knowledge or specialize in specific cybersecurity areas often lack the opportunity to do so. By providing optional training courses, organizations can bridge this gap, allowing employees to pursue further education out of genuine interest rather than mere compliance. This autonomy fosters intrinsic motivation, which has been shown to substantially enhance both the effectiveness and depth of learning (Vansteenkiste *et al.*, 2004).

Generative AI (GenAI) gives organizations the potential to deliver highly personalized and voluntary cybersecurity training. While many organizations already tailor content to specific departments, such one-size-fits-all grouping may still overlook individual learning needs. By dynamically adapting the depth and complexity of materials based on each learner's progress and interests, GenAI can create more relevant and engaging experiences. However, fully individualizing GenAI-driven training requires considerable effort to account for each employee's background knowledge. As a practical compromise, organizations can develop targeted modules for distinct employee groups, such as trainees, junior developers or senior developers, while still leveraging GenAI's adaptive capabilities to refine content within those modules. This balanced approach ensures that employees receive training suited to their roles and competencies, aiming to foster stronger motivation and more effective security-compliant behavior.

5.3 Comprehensible security policies

Employees in our study have asked for the security policies to be more accessible and understandable. This highlights the need for a centralized repository where the policies are widely known. By streamlining access to security policies, organizations can ensure that every employee, regardless of their technical background, can access crucial information about their role in organizational cybersecurity.

Furthermore, the clarity and comprehension of these guidelines are vital. Often, employees are eager to comply with security measures but find themselves unable to because of the complexity or vagueness of the instructions. A simplified overview of the guidelines could substantially increase competence and, in turn, employees' motivation to comply with the guidelines. Moreover, it is essential to modernize the content of these guidelines to reflect current best practices in cybersecurity. For instance, Reeves *et al.* (2021) suggest moving away from outdated protocols like mandatory periodic password changes to more effective and user-friendly measures. Additionally, Fisher *et al.* (2021) argued that simplified security policies can prevent security fatigue.

Additionally, organizations can simplify employees' security policy implementation by adopting strategies that guide employees toward secure behaviors. An example is the choice

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

default nudge. By suggesting strong passwords or enabling two-factor authentication by default, employees could be nudged into security compliance, as identified by Renaud and Zimmermann (2019) and Golla *et al.* (2021). Such measures of combining the security guidelines with practical, user-friendly solutions can increase the willingness of employees to behave in a security-compliant manner. Simply put, making the secure choice the easiest choice can enhance an organization's security posture.

5.4 Using employee reports effectively

Prior research has encouraged organizations to shift their perspective from viewing employees as a security liability to recognizing them as a key part of the solution (Zimmermann and Renaud, 2019). One practical way to achieve this is by actively incorporating employee-generated security reports into cybersecurity strategies. When organizations acknowledge and act on these reports, employees gain a heightened sense of contribution and relatedness, as they see the tangible impact of their efforts. This recognition also fosters autonomy, empowering employees to continue reporting incidents and to maintain security-conscious behaviors. Moreover, offering timely and constructive feedback on submitted reports further develops employees' competence. As they learn to identify and understand emerging threats, employees become more adept at producing high-quality reports. In turn, both the organization and its workforce benefit from a stronger overall security posture, as improved reporting leads to more effective prevention, mitigation and response to potential incidents.

Adopting a healthy error culture within the organization is crucial to motivating employees toward security-compliant behavior. While Goel *et al.* (2021) suggest that financial punishments can increase security compliance in the short term, our interviewees report that negative incentives lead to lower security efforts among employees in the long term. When organizations do not punish their employees for mistakes, employees are much more willing to report threats and behave in a security-compliant manner. In addition, carefully considered positive incentives can complement employees' motivation. In detail, small but relevant bonus programs are unlikely to diminish intrinsic motivation and can lead to a sustained increase in the quality and quantity of reports. Thus, incentives can provide organizations with valuable insights into potential security threats.

Nudges are a valuable tool to promote security-compliant behavior. Nevertheless, the success hinges on their careful application. Overuse or poorly designed nudges can lead to security fatigue, reducing effectiveness and potentially undermining the desired security behavior. Organizations should adopt a more nuanced approach to mitigate security fatigue and maintain the effectiveness of nudges. For instance, refining email warnings to provide more specific and relevant alerts can greatly reduce the risk of security fatigue. Instead of identical warnings for all external communications, a more differentiated approach can be more effective, such as flagging emails that are likely phishing attempts or exhibit suspicious characteristics. This strategy prevents the overload of warnings and enhances employees' overall security awareness and vigilance. Thus, nudges with a nuanced approach are promising to foster employees' security compliance.

6. Conclusion

This study aimed to analyze the application of different theoretical approaches to employee motivation in organizational cybersecurity. We identified that the organizations in scope focus on raising employees' motivation mainly through educating employees about security-compliant behavior and short-time incentives. Meanwhile, there is substantial untapped potential in using motivational strategies to enhance employees' sense of autonomy and relatedness toward security-compliant behavior, as well as effectively using security-related incentives and nudges. Moving forward, our future research will focus on verifying our

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

suggested improvements. To this end, we intend to conduct studies in organizations to assess to what extent the integration of the suggested strategies can improve employee motivation toward security-compliant behavior.

Notes

1. https://github.com/employee-motivation/questionnaire
2. The Institutional Review Board certificate is available online: https://gfew.de/ethik/MwJFdwPK
3. We outline AI Usage Cards (Wahle *et al.*, 2023): https://ai.uversy.com/employee-motivation

References

Adams, W.C. (2015), "Conducting semi-structured interviews", *Handbook of Practical Program Evaluation*, Wiley, New York, NY, pp. 492-505.

Alotaibi, S., Furnell, S. and He, Y. (2023), "Towards a framework for the personalization of cybersecurity awareness", *Proceedings of the 2023 Conference on Human Aspects of Information Security and Assurance (HAISA)*, *Springer Nature Switzerland*, *Cham*, pp. 143-153.

Baumer, T., Reittinger, T., Kern, S. and Pernul, G. (2024), "Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations", *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, *USENIX Association*, *Philadelphia*, *PA*, pp. 239-258, available at: www.usenix.org/conference/soups2024/presentation/baumer

Bingham, A.J. and Witkowsky, P. (2021), "Deductive and inductive approaches to qualitative data analysis", *Analyzing and Interpreting Qualitative Data: After the Interview*, Vol. 1, pp. 133-146.

Deterding, N.M. and Waters, M.C. (2021), "Flexible coding of in-depth interviews: a twenty-first-century approach", *Sociological Methods and Research*, Vol. 50 No. 2, pp. 708-739.

Eze, T. and Hawker, N. (2022), "Cap: Patching the human vulnerability", in Clarke, N. and Furnell, S. (Eds), *Proceedings of the 2022 Conference on Human Aspects of Information Security and Assurance (HAISA)*, Springer International Publishing, Cham, pp. 106-119.

Fisher, R., Porod, C. and Peterson, S. (2021), "Motivating employees and organizations to adopt a cybersecurity-focused culture", *Journal of Organizational Psychology*, Vol. 21 No. 1, pp. 114-131.

Friedl, S., Reittinger, T. and Pernul, G. (2024b), "Digital detectives: a serious point-and-click game for digital forensics", *IFIP World Conference on Information Security Education*, *Springer*, pp. 129-145.

Friedl, S., Reittinger, T. and Pernul, G. (2024a), "From play to profession: a serious game to raise awareness on digital forensics", *IFIP Annual Conference on Data and Applications Security and Privacy*, *Springer*, pp. 269-289.

Gagné, M. and Deci, E.L. (2005), "Self-determination theory and work motivation", *Journal of Organizational Behavior*, Vol. 26 No. 4, pp. 331-362.

Gangire, Y., Da Veiga, A. and Herselman, M. (2019), "A conceptual model of information security compliant behaviour based on the self-determination theory", *Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS)*, *IEEE*, pp. 1-6.

Gasiba, T., Lechner, U., Pinto-Albuquerque, M. and Zouitni, A. (2020), "Design of secure coding challenges for cybersecurity education in the industry", *International Conference on the Quality of Information and Communications Technology*, *Springer*, pp. 223-237.

Glas, M., Hilmer, C. and Pernul, G. (2025), "Cyber ranges: Five use cases for improving cybersecurity skills development in organizations", *IEEE Security and Privacy*.

Glas, M., Messmann, G. and Pernul, G. (2024), "Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises", *Computers and Security*, Vol. 144, p. 103965, doi: 10.1016/j.cose.2024.103965, available at: www.sciencedirect.com/science/article/pii/S0167404824002700

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

Glas, M., Vielberth, M. and Pernul, G. (2023), "Train as you fight: Evaluating authentic cybersecurity training in cyber ranges", *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*.

Goel, S., Williams, K.J., Huang, J. and Warkentin, M. (2021), "Can financial incentives help with the struggle for security policy compliance? ", *Information and Management*, Vol. 58 No. 4, p. 103447.

Golla, M., Ho, G., Lohmus, M., Pulluri, M. and Redmiles, E.M. (2021), "Driving 2FA adoption at scale: optimizing Two-Factor authentication notification design patterns", *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), USENIX Association*, pp. 109-126.

Haislip, J., Lim, J.H. and Pinsker, R. (2021), "The impact of executives' IT expertise on reported data security breaches", *Information Systems Research*, Vol. 32 No. 2, pp. 318-334, doi: 10.1287/isre.2020.0986.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. and Koshutanski, H. (2020), "Modern aspects of cyber-security training and continuous adaptation of programmes to trainees", *Applied Sciences*, Vol. 10 No. 16, p. app10165702.

Hummel, D. and Maedche, A. (2019), "How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies", *Journal of Behavioral and Experimental Economics*, Vol. 80, pp. 47-58.

ISACA (2023), State of cybersecurity 2023: global update on workforce efforts, resources and cyberoperations", Tech. rep.

Jesse, M. and Jannach, D. (2021), "Digital nudging with recommender systems: survey and future directions", *Computers in Human Behavior Reports*, Vol. 3, p. 100052.

Kävrestad, J. and Nohlberg, M. (2020), "Contextbased microtraining: a framework for information security training", in Clarke, N. and Furnell, S. (Eds), *Human Aspects of Information Security and Assurance*, Springer International Publishing, Cham, pp. 71-81.

Kirsch, L. and Boss, S. (2007), "The last line of Defense: motivating employees to follow corporate security guidelines", *Proceedings of the 2007 ICIS conference*, p. 103.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24.

Mwim, E.N. and Mtsweni, J. (2022), "Systematic review of factors that influence the cybersecurity culture", *Proceedings of the 2022 Conference on Human Aspects of Information Security and Assurance (HAISA), Springer International Publishing, Cham*, pp. 147-172.

Olt, C., Gerlach, J., Sonnenschein, R. and Buxmann, P. (2019), "On the benefits of senior executives' information security awareness", *Proceedings of the 2019 International Conference on Information Systems (ICIS) 25*.

Pham, H.C., Pham, D.D., Brennan, L., Richardson, J., *et al*. (2017), "Information security and people: a conundrum for compliance", *Australasian Journal of Information Systems*, Vol. 21.

Reeves, A., Delfabbro, P. and Calic, D. (2021), "Encouraging employee engagement with cybersecurity: how to tackle cyber fatigue", *Sage Open*, Vol. 11 No. 1, p. 21582440211000049.

Reittinger, T., Glas, M., Aminzada, S. and Pernul, G. (2024), *Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality*, Springer Nature, Cham, pp. 3-16, doi: 10.1007/978-3-031-72559-3_1.

Reittinger, T. and Pernul, G. (2025), "A taxonomy of positive incentives to motivate cybersecurity behaviors", *Proceedings of the 58th HI International Conference on System Sciences (HICSS-58)*.

Renaud, K. and Zimmermann, V. (2019), "Nudging folks towards stronger password choices: providing certainty is the key", *Behavioural Public Policy*, Vol. 3 No. 2, pp. 228-258.

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

ICS

Ryan, R.M. and Deci, E.L. (2000), "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being", *American Psychologist*, Vol. 55 No. 1, p. 68.

Siadati, H., Jafarikhah, S., Sahin, E., Hernandez, T., Tripp, E., Khryashchev, D. and Kharraz, A. (2024), "Devphish: exploring social engineering in software supply chain attacks on developers", *2024 IEEE 15th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE*, pp. 517-523.

Sonnenschein, R., Loske, A. and Buxmann, P. (2017), "The role of top managers' IT security awareness in organizational it security management", *Proceedings of the 2017 International Conference on Information Systems (ICIS)*, p. 13.

Statista (2023), "Estimated cost of cybercrime worldwide 2017-2028", available at: www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (accessed 1 August 2024).

Thaler, R.H. and Sunstein, C.R. (2008), *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press.

Vansteenkiste, M., Simons, J., Lens, W., Sheldon, K.M. and Deci, E.L. (2004), "Motivating learning, performance, and persistence: the synergistic effects of intrinsic goal contents and autonomy-supportive contexts", *Journal of Personality and Social Psychology*, Vol. 87 No. 2, p. 246.

Verizon (2023), "2023 data breach investigations report", Tech. rep.

von Solms, S.H., Du Toit, J. and Kritzinger, E. (2023), "Another look at cybersecurity awareness programs", *Proceedings of the 2023 Conference on Human Aspects of Information Security and Assurance (HAISA), Springer Nature Switzerland, Cham*, pp. 13-23.

Wahle, J.P., Ruas, T., Mohammad, S.M., Meuschke, N. and Gipp, B. (2023), "Ai usage cards: Responsibly reporting AI-generated content", *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL), IEEE*, pp. 282-284.

Yang, N., Singh, T. and Johnston, A. (2020), "A replication study of user motivation in protecting information security using protection motivation theory and self determination theory", *AIS Transactions on Replication Research*, Vol. 6 No. 1, p. 10.

Zimmermann, V. and Renaud, K. (2019), "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset", *International Journal of Human-Computer Studies*, Vol. 131, pp. 169-187.

Corresponding author
Tobias Reittinger can be contacted at: tobias.reittinger@ur.de

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded from http://www.emerald.com/ics/article-pdf/doi/10.1108/ICS-02-2025-0046/9877259/ics-02-2025-0046.pdf by Mr. Reittinger on 29 January 2026

P2 No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage

Current status:	Accepted for publication
Conference:	47th IEEE Symposium on Security and Privacy
Ranking:	A* ICORE 2026, 13% Acceptance Rate
Date of acceptance:	September 09, 2025
Date of publication:	To be determined.
Full citation:	Reittinger, T., & Pernul, G. (2026). No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage. In *Proceedings of the 2026 IEEE Symposium on Security and Privacy (SP)*. (accepted for publication).

Authors' contributions:		
	Tobias Reittinger	90%
	Günther Pernul	10%

Conference description: The *IEEE Symposium on Security and Privacy (S&P)* (peer-reviewed) is a premier annual conference that brings together leading figures from academia and industry to present and discuss the latest advances in computer security and electronic privacy. The 2026 symposium, the 47th annual meeting in the series, will take place in San Francisco, CA on May 18–20, 2026.

No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage

Tobias Reittinger
University of Regensburg
tobias.reittinger@ur.de

Günther Pernul
University of Regensburg
guenther.pernul@ur.de

***Abstract*—Passkeys were introduced to mitigate password-related security risks. However, passwords remain prevalent, and the usability of synchronization, one of the core benefits of passkeys, has not yet been studied. To address this gap, we conducted a large-scale field study examining passkey adoption and usage by partnering with an industrial healthcare service. In Phase 1 (n = 5,057), users chose between a passkey and a password with 2FA during registration. We reveal that (especially inexperienced) users struggle with passkey adoption but still perceive passkeys to offer superior usability and acceptance. Our survey results identified novel reasons why users decline passkeys, notably the habit of using passwords and lack of passkey experience, and pinpointed adoption barriers, including new misconceptions and manual passkey activation. In Phase 2 (n = 2,716), we monitored authentication behavior over six months and captured immediate feedback through surveys. We found that passkey usability and acceptance continued to increase, and success rates surpassed the declining metrics of passwords. Still, we uncovered new issues with cross-platform synchronization, passkey sharing, and interactions with password managers. Finally, we provide recommendations to streamline the adoption and usability of passkeys.**

1. Introduction

Although passwords are technically secure [48], they suffer from poor usability: Users are required to create passwords that are long and random [49], [79], compliant with complex policies [79], unique for each account [33], [68], and memorable for numerous accounts [31], [84]. Moreover, phishing campaigns, now amplified by generative AI [36], pose an escalating threat to password compromise [59]. Consequently, password-based authentication is one of the primary vectors for cyberattacks [60]. Multi-Factor Authentication (MFA) can mitigate these risks, but its adoption rates remain low [3], [15], and attackers often circumvent it through social engineering or sophisticated phishing [59], [60]. Despite these shortcomings, passwords continue to serve as the *de facto* standard for authentication [48], [75].

To address these issues, the Fast IDentity Online (FIDO) Alliance introduced FIDO2 passwordless authentication, which uses public-key cryptography to resist phishing and strengthen security compared to passwords [30], [50]. FIDO2 eliminates password creation and memorization [29] and inherently supports MFA via biometrics or a device passcode, but credentials remain tied to individual devices, limiting portability and recovery options [55], [65], [85]. To overcome these limitations, passkeys extend FIDO2 by offering credential synchronization across devices [25]. While synchronization introduces a tradeoff between security [45] and usability [51], passkeys deliver enhanced security and usability over password-based authentication [25]. However, password authentication still prevails [75]. We identified two research gaps in understanding passkey adoption and use: First, prior work has focused on lab experiments [53], [85] yet fails to capture real-world adoption barriers and longitudinal usage challenges. Second, although passkeys offer synchronization, this core feature has not yet been examined in a user study. We aim to close these gaps by answering the following research questions:

RQ1 *What concerns deter users from choosing passkeys, and what obstacles impede passkey adoption?*

RQ2 *Which challenges do users encounter with passkeys, including synchronization, in a multi-month period?*

We conducted a large-scale field study to examine passkey adoption (n = 5,057) and six-month usage (n = 2,716) by collaborating with a healthcare appointment platform (see Section 3.1). Thereby, we compared passkeys against passwords with two-factor authentication (2FA), collecting both authentication metrics and survey responses. Our contributions are as follows:

- We find that users are interested in passkeys but hesitate due to password habits and inexperience. Adoption success rates were lower than for passwords with 2FA, especially for novices, yet passkeys exhibited superior usability and acceptance. We also identify new barriers, including novel misconceptions and manual activation.
- With repeated logins, passkey success rates surpassed those of passwords with 2FA, while usability and acceptance continued to rise. We conducted the first user study assessing passkey synchronization, uncovering major cross-platform challenges, and also identifying issues with passkey sharing and password managers.
- We offer recommendations to enhance passkey adoption and usability, and publish the source code and statistical analysis to facilitate future work.

The paper is organized as follows. Section 2 reviews background and related work. Section 3 describes the methodology. Section 4 presents the results of passkey adoption. Section 5 reports passkey usage results. Section 6 discusses implications. Section 7 concludes the paper.

2. Background and Related Work

In this section, we describe the functionality of FIDO2 and passkeys and review related studies.

2.1. FIDO2

To mitigate the security risks of password-based authentication, the FIDO Alliance developed FIDO2, a successor to the initial Universal 2nd Factor (U2F) protocol [27], [40], [53]. By leveraging public-key cryptography [29], FIDO2 provides a secure, passwordless authentication supported by major operating systems (OSs) [66] and browsers [12], [58]. FIDO2 offers two modes:

- **Roaming Authentication:** This mode employs external hardware authenticators (e.g., security keys) that can be used across multiple devices via Client to Authenticator Protocol 2 (CTAP2), communicating securely over USB, Bluetooth, or NFC [26]. However, hardware-based tokens require an upfront purchase and can be lost or damaged [76], [85].
- **Platform Authentication:** In this mode, the authenticator is built into a user's device (e.g., smartphone, tablet, or PC) and leverages the W3C Web Authentication (WebAuthn) API for secure authentication [46]. Users verify their identity using **biometrics** (fingerprint or facial recognition, depending on device capability) or the device's **passcode** (PIN, pattern, or password) [46]. However, binding a credential to a single device can limit portability and complicate recovery if the device is lost [65], [85].

In sum, FIDO2 offers passwordless authentication that provides enhanced security compared to passwords [30], as credentials are inherently resistant to phishing attacks [50], but limited portability and recovery options [51], [65], [85].

2.2. Passkeys

Passkeys extend FIDO2's platform authentication by enabling credential synchronization across devices, addressing the limitations of device-specific storage [25]. Although synchronization introduces a security–usability trade-off [45], [51], it enhances portability and recovery options [25], [51].

- **Built-in Cloud Services:** Major vendors like Apple, Google, and Microsoft offer passkey synchronization via proprietary cloud services (e.g., iCloud Keychain, Google Password Manager, Windows Hello) [4], [7], [21]. However, this functionality is typically restricted to the same ecosystem.
- **Manual Device-to-Device Transfer:** Users can manually transfer passkeys cross-platform via a QR code or Bluetooth [30]. However, this requires physical proximity between devices, does not scale well for numerous devices, and may be less intuitive for users.
- **Third-Party Password Managers (PMs):** PMs, such as 1Password, Bitwarden, support cross-platform synchronization, and sharing [1], [8]. However, this functionality typically requires a premium subscription.

Most built-in cloud services and PMs allow users to share passkeys with others [1], [5], [8], [35]. Passkeys also inherently incorporate 2FA [46]: The first factor is the stored cryptographic key on the device (*something you have*). The second factor is either the user's biometrics (*something you are*) or the device's passcode (*something you know*). During passkey setup, users complete two steps, with their order and layout (one or two pages) varying by OS:

- **Storage Selection:** Users choose a passkey storage option: A built-in cloud service, PM, or another device. OSs offer either a default or require active selection.
- **Authentication:** Users authenticate locally with biometrics or the device's passcode to authorize passkey creation or authentication.

On subsequent logins, only the authentication step is required. Overall, passkeys offer a user experience (UX) distinct from FIDO2 security keys by enabling synchronization. Although passkeys deliver security and usability benefits over passwords [25], passwords remain the most common authentication method [75].

2.3. Related Work

Discussing related work, we first look at roaming authentication with security keys. Although these findings do not directly translate to passkeys, they offer insights into potential usability and acceptance challenges. Subsequently, we outline prior works on platform authentication and passkeys.

Roaming Authentication. Initially, security keys served as a second factor via the U2F protocol, a precursor to FIDO2. Das et al. [19], [20] evaluated U2F-based Yubico Security Keys (YubiKeys), demonstrating how clearer setup instructions and the removal of confusing demo features improved usability. However, acceptance remained low due to users' fears of losing access and uncertainty about the technology's benefits. Building on these observations, Reynolds et al. [74] compared setup and long-term usage. They found that while participants initially struggled with configuring their accounts, those who succeeded found YubiKeys both convenient and secure for everyday use. In a related study, Ciolino et al. [13] contrasted security keys with SMS-based one-time passwords (OTPs), reporting longer setup times and interface complexities for security keys. These factors led many users to prefer SMS OTPs. Subsequently, FIDO2 introduced passwordless logins, allowing security keys to function as a first factor [27], [40]. Lyastani et al. [55] found FIDO2 with a YubiKey more usable and acceptable than passwords, though concerns about device loss, trust, and hardware limitations persisted. Farke et al. [23] further explored a four-week deployment of FIDO2 keys in

a small software company. Although employees appreciated the enhanced security and simplicity, many reverted to passwords due to fear of key loss and slower authentication. Collectively, these studies highlight the importance of intuitive setup, clear benefit communication, and user-friendly designs in enhancing adoption rates.

Platform Authentication. In addition to roaming authentication with security keys, FIDO2 supports platform authentication via WebAuthn, allowing users to utilize their own devices, such as smartphones, as authenticators. Oogami et al. [64] highlighted usability barriers to WebAuthn fingerprint authentication on Android devices, noting that many users tapped the on-screen fingerprint icon instead of the physical sensor. Building on these findings, Lassak et al. [53] investigated common misconceptions about FIDO2 biometric WebAuthn. They found that clarifying how and where biometric data are stored significantly improved user perceptions and willingness to adopt biometric WebAuthn over passwords. Similarly, Owens et al. [65] compared smartphone-based FIDO2 authenticators to passwords, observing that, despite enhanced security, participants were deterred by complex setup processes, slow authentication, and limited recovery options. In a quantitative study, Nawrath [63] found platform authentication yielded higher success rates on mobile devices. However, compatibility challenges and concerns about data privacy remained. Würsching et al. [85] later compared platform authentication (using Apple Touch ID) with roaming authentication (using a YubiKey). Their findings showed that platform authentication was rated more favorably for user acceptance. Still, many users expressed concerns about account recovery and multi-device access, specifically noting the inconvenience of carrying an external key for roaming authentication. Overall, these studies demonstrate the potential of FIDO2 passwordless authentication yet emphasize the need to address setup complexities, clarify biometric data handling, and ensure device compatibility.

Passkeys. Subsequently, passkeys evolved from these developments, offering multi-device synchronization [30]. Lassak et al. [54] surveyed organizational hurdles to deploying passkeys, identifying the lack of standardized fallback options, technical constraints, and user resistance to change as key barriers. Security studies map emerging risks: Daffalla et al. [18] introduced a framework for analyzing interpersonal threats and identified abuse vectors across major services. Islam et al. [45] revealed vulnerabilities in cloud-based passkey synchronization and proposed a novel framework to detect the unauthorized use of leaked passkeys. Further, Büttner and Gruschka [10] categorize passkey access levels and show that synced passkeys, while enhancing recoverability, centralize security risk in the provider. Additionally, multiple industry case studies discuss how organizations benefit from passkeys' enhanced UX [16], [37], [38], [61], [77].

Our Differentiation To Prior Work. We distinguish our work from previous studies in content and methodology. While most prior studies centered on roaming authenticators (e.g., security keys) or single-device platform authentication, we investigate passkeys and their unexplored multi-device synchronization features. Given the continued prevalence of passwords [75], we also examine why users might resist or abandon passkeys and identify adoption barriers. Moreover, while earlier research relied on lab experiments and diary studies, our industrial collaboration (Section 3.1) enables continuous monitoring of real-world authentication use and immediate user feedback. To the best of our knowledge, we present the first large-scale field study of passkey adoption and usage, offering actionable insights to improve the adoption and usability.

3. Methodology

From October 2024 to May 2025, we conducted an exploratory user study in two phases (adoption and usage) employing a mixed-methods approach.

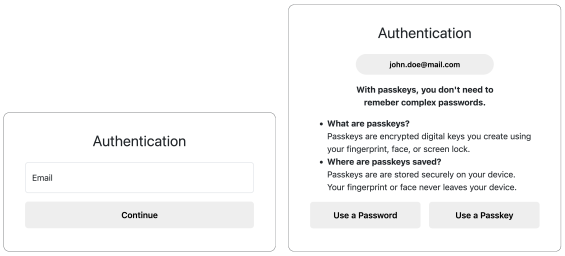
3.1. Study Design

Below, we outline the implementation, study groups, and the design of both between-group phases.

Implementation. We partnered with a European healthcare appointment platform, hereafter referred to as the **platform**, that recently added passkeys. The passkey implementation is available on GitHub. Passkeys are stored on participants' devices via platform authenticators and serve as the primary authentication method. Roaming authenticators (e.g., security keys) were disabled to isolate passkey use. We layered study instructions, measurements, and surveys atop the existing platform infrastructure.

Study Groups. In this study, we compared two user groups based on their self-selected authentication method (Figure 1). Participants who chose passkeys were assigned to **Group K**, which inherently requires 2FA. They can select either biometrics or the device's passcode as the second factor (Section 2.2). In contrast, participants opting for passwords formed **Group W**, which combines a password with 2FA. For Group W, we adopted a common password policy requiring at least eight characters in accordance with NIST recommendations [39]. Passwords also had to include characters from a minimum of two character classes (e.g., uppercase, lowercase, numeric, or special symbols), as seen in practice by services such as PayPal [67]. The second factor for Group W was an SMS-based OTP valid for ten minutes, chosen both for its prevalence in the industry [2], [34], [44], [56] and because the platform already supports it. Consequently, both groups employ forms of MFA commonly seen in real-world applications [55], [62].

Phase 1: Passkey Adoption. Phase 1 aimed to uncover the key motivators and challenges associated with passkey adoption in a realistic setting. In line with current industry practices (e.g., Apple [43], Google [34], Uber [44]), participants first entered their email address (see Figure 1a) and were then offered the choice to create a new account using either a passkey or a password (see Figure 1b). This step divided all participants into two groups: those who chose a passkey (Group K) and those who selected



(a) 1. Enter email (b) 2. Choose authentication

Figure 1: Authentication choice, following recommendations of the FIDO Alliance [28] and Lassak et al. [53].

TABLE 1: Participants during the study by authentication method: Group K (passkey) vs. Group W (password + 2FA).

Study	Step of Study	Group K	Group W	Σ
Phase 1	Authentication Choice	2,950	2,107	5,057
	Successful Adoption	1,664	1,924	3,588
Phase 2	At least one auth. attempt	1,295	1,421	2,716

a password (Group W). In accordance with the FIDO Alliance UX guidelines [28], we provided general information about passkeys and incorporated insights from Lassak et al. [53] addressing common misconceptions about biometrics. Although this information may have influenced decisions, it aligns with the guidance typically provided by vendors during passkey setup (e.g., Adobe [2], Amazon [42], Google [34]). To mitigate potential bias, we randomized the order of the sign-up buttons. All interactions with the authentication methods were monitored, and participants were allowed to cancel their setup at any point, thereby replicating a genuine user experience. After completing or canceling the setup process, participants were directed to a survey designed to capture their reasons for their choice, any difficulties they encountered, and relevant demographic details. Participants who did not successfully adopt their chosen method were surveyed about their reasons for discontinuation, but were subsequently excluded from Phase 2 to prevent bias. Only those who successfully adopted their chosen authentication method advanced to Phase 2.

Phase 2: Passkey Usage. Phase 2 aimed to investigate the experience and potential usability challenges of passkeys during long-term usage and compare their UX to that of 2FA-based passwords as a baseline. We monitored the authentication behavior of participants who successfully adopted their chosen method in Phase 1 for six months, starting from each participant's adoption date. At each login, participants entered their email addresses and were then presented with their previously selected authentication method. Because passkey telemetry does not report storage location, second factor, or synchronization type, we used a brief post-authentication survey after each attempt to capture these attributes and participants' experiences accurately. To ensure robust data collection, only participants who made at least one authentication attempt during the study period were included. Participants retained their initially chosen authentication method throughout the study, aligning with industry practice [47], to prevent password fallback during multi-device use and thereby preserve observable synchronization events. Switching the authentication method was available after completion or upon withdrawal. Further, participants could register multiple passkeys and synchronize them via built-in cloud services, device-to-device transfers, or PMs. For **account recovery**, both groups received a six-digit SMS OTP (valid for 10 minutes) and then registered a new passkey (Group K) or set a new password (Group W). A follow-up survey captured their recovery experiences. OTPs are commonly used for recovery, either via SMS (e.g., Adobe [2], Amazon [42]) or email (e.g., FIDO's passkey prototype [28]). SMS-based OTP recovery is vulnerable to phishing [51], but widely used with passwords in practice [2], [34], [44], and prior research has suggested exploring its use for passkeys [65], [85].

3.2. Recruitment and Participants

Participants were new users signing up for the healthcare production platform. Users with passkey-compatible devices were invited to create a new account. We outlined the study objectives, data collection procedures, expected duration, and incentives (see Section 3.5). Table 1 lists participant numbers during the study.

In Phase 1, 5,057 participants completed the authentication choice, 3,588 successfully adopted it and advanced to Phase 2, and 2,716 made at least one authentication attempt. Attrition was similar (31.8% in Group K and 29.5% in Group W), reflecting typical patterns observed in platform usage and longitudinal research [65]. Participants are from diverse demographics, as detailed in Appendix B.

3.3. Data Collection

We collected measured and self-reported data in both phases. Survey questionnaires are listed in Appendix A and the characteristics of quoted participants in Appendix D.

Phase 1: Passkey Adoption Data. During registration, we monitored participants' interactions with the authentication methods. We distinguished between the initial authentication choice (passkey or password) and the subsequent adoption outcome. This dual-phase data collection enabled us to quantitatively assess both the decision to adopt passkeys and the barriers encountered during adoption.

Additionally, participants provided qualitative feedback via a free-text survey available in both English and German. To control for accidental selections, we asked whether their choice was intentional. They also explained their reasons for choosing or not choosing passkeys, described any difficulties encountered during adoption, and clarified their reasons for canceling the adoption. Additionally, the survey collected background information, including computer science (CS) background, prior use of passkeys and OTPs, scores on the

Affinity for Technology Scale (ATI) [32], privacy concerns (PC) [52], and demographic details. Background data were only collected in Phase 1, as Phase 2 participants are a subset of this sample. On average, the survey took 5 minutes to complete (Mdn = 4 min).

After adoption, participants were asked to complete the usage survey of Phase 2 to investigate the influence on authentication choice or adoption success.

Phase 2: Passkey Usage. During the six-month usage period, we recorded several metrics to assess how participants, those who made at least one authentication attempt, interacted with the authentication methods. We tracked:

- Number of authentication attempts
- Duration of each authentication attempt
- Number and duration of recovery attempts
- Contextual data, such as device type, operating system (OS), and a unique device identifier

After each login attempt, we displayed participants a survey to report their authentication experiences, such as issues encountered and reasons for failures [55], [65]. Since a passkey implementation only reports success or failure, we asked participants of Group K for additional details in the survey, including the used second factor, if and how the passkey was synced from another device, and any associated challenges. Both groups then completed the System Usability Scale (SUS) [9] and the Acceptance Scale [55], [82]. The survey took 4 minutes on average (Mdn = 4 min).

3.4. Data Analysis

For qualitative analysis of free-text survey responses, we employed a flexible coding approach [22]. One researcher conducted the initial coding, which a second researcher co-interpreted. Discrepancies were resolved through joint discussions. The codebook is described in Appendix C, and code frequencies are stated in the results (Sections 4 and 5).

In the quantitative analysis, ordinal variables were analyzed with the Wilcoxon-Mann-Whitney test [57], as the Shapiro-Wilk test [78] indicated non-normality. Nominal variables used Pearson's chi-square test [69] with Cramér's V for effect size [17]. We fit a multivariable logistic regression to estimate adjusted odds ratios while controlling for covariates. Significance was set at $p < 0.001$ for all tests. Medians are reported to minimize outlier effects.

To assess authentication performance, we define an **authentication session** as any sequence of attempts within a ten-minute window. This session-based metric is adapted from earlier research on FIDO2 [65] and reflects real-world behavior in which users may enter multiple credentials in quick succession. A session is considered **successful** if a participant completes the initial adoption process (Phase 1), logs in without invoking account recovery (Phase 2), and registers a new passkey or password (account recovery in Phase 2). Conversely, a session is categorized as **unsuccessful** if the participant cancels the procedure, fails to complete authentication, or allows the session to time out.

Session duration is measured as the elapsed time from the click on one of the authentication options (Phase 1), the click on the "Login" button (Phase 2), and the click on the "Forgot Password" button through to the last interaction of the final attempt in that session. Attempts that are initiated within an existing session window are attributed to that session. Any attempt starting ten minutes or more after the session's start will begin a new session. We flagged outliers with >3 failed sessions in 24h, identifying one outlier (five failures) and no evidence of scripted abuse.

In Phase 2, we classify a synchronization as **platform-specific** when a passkey is synchronized within a vendor ecosystem (e.g., from iOS to macOS or Android to Android) and as **cross-platform** when it spans heterogeneous ecosystems (e.g., from iOS to Windows, or Android to iOS).

3.5. Ethical Considerations

Before conducting the study, the ethics committee of the German Association for Experimental Economic Research e.V. approved our study, and we received an Institutional Review Board (IRB) certificate, which is available online.[1]

User Study. Before the study, we displayed a GDPR-compliant privacy policy. Participation was voluntary, and we limited personal information to demographics. To reduce bias, users were told the study concerned authentication without additional details. Participants were briefed on objectives, data collection, and their right to withdraw at any time, either via a button in the settings tab or, if logged out, via a link in the invitation email, and provided informed consent. Upon completion or withdrawal, they received a debriefing. All surveys ran on a self-hosted LimeSurvey[2] instance to ensure data privacy. To minimize burden from the retained-authentication requirement, we (i) clearly communicated the request, (ii) confirmed with the platform vendor that no participants contacted support about study-related restrictions, and (iii) appointments remained bookable through traditional channels. To encourage participation, we ran a raffle for a €100 gift card. When enrollment exceeded expectations, we added 100 €5 gift cards post-study to increase the number of winners. In retrospect, a raffle that scales proportionally with enrollment would be preferable, as it lets participants know their odds in advance and maintains fairness regardless of final sample size.

Impact on Access to Healthcare. The study did not affect participants' access to healthcare services. Although the platform offers a convenient interface for booking doctor appointments, users can still schedule appointments via traditional methods (e.g., phone or email). The platform also provides public access to doctor information without registration. The passkey feature was thoroughly tested before implementation to ensure no adverse impact on platform access. No participants reported issues with the passkey implementation, aside from the obstacles inherent to passkeys, which are unrelated to the implementation itself.

1. IRB certificate: https://gfew.de/en-ethik/PFMLTKKY
2. https://github.com/LimeSurvey/LimeSurvey

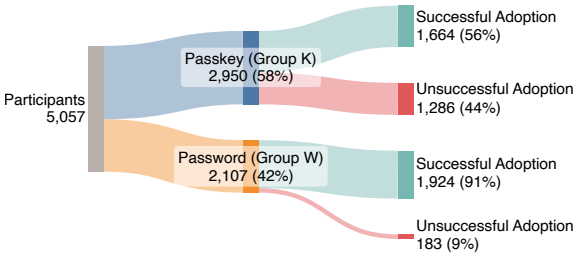


Figure 2: Flow diagram illustrating participants' authentication choices and adoption outcomes.

TABLE 2: Authentication choices and adoption outcomes of participants, segmented by prior passkey experience (Exp.) and no passkey experience (No Exp.).

Category	Exp.	No Exp.	Total
Total Participants	2,396	2,661	5,057
Passkey (Group K)	1,721 (72%)	1,229 (46%)	2,950 (58%)
Successful Adop.	1,235 (72%)	429 (35%)	1,664 (56%)
Unsuccessful Adop.	486 (28%)	800 (65%)	1,286 (44%)
Password (Group W)	675 (28%)	1,432 (54%)	2,107 (42%)
Successful Adop.	613 (91%)	1,311 (92%)	1,924 (91%)
Unsuccessful Adop.	62 (9%)	121 (8%)	183 (9%)

3.6. Pilot Study

Before conducting the main user study, we performed a pilot study (n = 13). The pilot study, which included both Phase 1 and Phase 2 procedures, aimed to detect technical difficulties and identify ambiguities in the survey questions. Based on the feedback, minor adjustments were made to improve the clarity of the questionnaire. As a result of these revisions, pilot data were excluded from analysis.

4. Results: Passkey Adoption (Phase 1)

This section details the findings of Phase 1 on passkey adoption. We begin by presenting the quantitative metrics, followed by qualitative insights into the factors driving adoption decisions and the obstacles encountered during the adoption of both passkey and password with 2FA.

Because prior passkey experience emerged as the strongest predictor of both choice and adoption success across two logistic regression models (see Sections 4.1.4 and 4.1.5), we stratify results by prior experience.

4.1. Passkey Adoption Metrics

This section details our findings on quantitative adoption metrics. Nearly all participants, 4,972 out of 5,057 (98%), indicated that their choice of authentication method was intentional, and all participants reported password experience.

TABLE 3: Adoption outcomes and median duration of authentication sessions of Group K, differentiated by OS.

Category	Mobile		Desktop	
	Android	iOS	macOS	Windows
Group K	1,554	844	191	361
Successful	896 (58%)	539 (64%)	76 (40%)	153 (42%)
Unsuccessful	658 (42%)	305 (36%)	115 (60%)	208 (58%)
Duration	12.9 s	6.2 s	20.4 s	19.2 s

4.1.1. Authentication Choices. Figure 2 shows 58% (2,950 of 5,057) of participants opted for passkeys, whereas 42% (2,107 of 5,057) selected passwords. These findings **indicate a promising level of interest in passkeys.**

4.1.2. Adoption Outcomes. In Group K, 56% (1,664 of 2,950) of participants who attempted passkey adoption achieved successful authentication, compared to 91% (1,924 of 2,107) of participants in Group W using passwords with SMS-based 2FA. Moreover, successful adopters required an average of 1.38 attempts in Group K versus 1.10 attempts in Group W. These findings **suggest that passkey adoption imposes greater friction than passwords with 2FA**.

4.1.3. Durations. The median duration of authentication sessions was 12.6 s for Group K and 52.9 s for Group W. Within Group W, the median time to create and enter a password was 24.8 s, while SMS-based 2FA took a median of 28.1 s. The results **indicate that passkey authentication is faster than passwords and passwords with 2FA**.

Table 3 shows that median authentication times for Group K varied across OSs, Android (12.9 s), iOS (6.2 s), macOS (20.4 s), and Windows (19.2 s), **indicating faster passkey adoption on mobile platforms than on desktops**.

4.1.4. Factors Influencing Authentication Choices. We evaluated the association between a range of variables and participants' authentication choices (see Table 9 in Appendix B). A chi-square test [69] on demographics, CS background, and OS, along with a Wilcoxon–Mann–Whitney test [57] on ATI, indicated no significant influence on the authentication choice.

A Wilcoxon-Mann-Whitney test [57] showed PC scores differed significantly between Group K (Mdn = 5.5) and Group W (Mdn = 5), $U = 2,567,618.0$, $p < .001$, with a small effect size $r = .15$ [14], **indicating participants with higher privacy concerns chose passkeys more frequently**.

Overall, 47% (2,396 of 5,057) of participants reported prior passkey experience, and 53% (2,661 of 5,057) didn't. In detail, 72% (1,721 of 2,396) of participants with prior passkey experience chose passkeys, compared to only 46% (1,229 of 2,661) among those without such experience, as displayed in Table 2. A chi-square test [69] revealed a significant association between prior passkey experience and authentication selection, $\chi^2(1, N = 5,057) = 341.08$, $p < .001$, with a moderate effect size ($V = .26$) [14], **suggesting that participants familiar with passkeys are more likely to select them for authentication**.

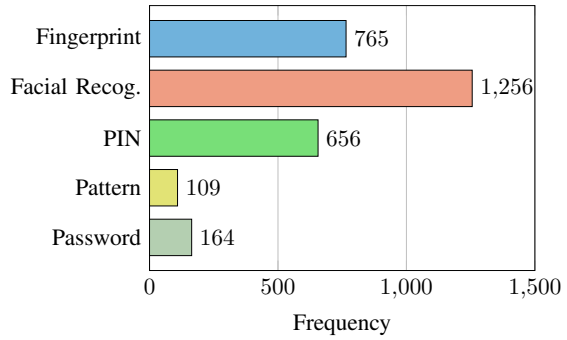


Figure 3: Frequencies of passkey second factors in Phase 1.

A binomial logistic regression substantiated these patterns with a significant model fit, $\chi^2(24) = 608.62$, $p < .001$; Nagelkerke $R^2 = .153$; accuracy = 65.7%. Controlling for demographics and OS, predictors of choosing passkeys were **prior experience** (OR = 2.93, 95% CI $[2.59, 3.30]$, $p < .001$), **privacy concerns** (OR = 1.42, $[1.35, 1.51]$, $p < .001$), **acceptance** (OR = 1.27, $[1.19, 1.36]$, $p < .001$), and **SUS** (OR = 1.01, $[1.007, 1.013]$, $p < .001$). Full coefficients and odds ratios are reported on GitHub.

4.1.5. Factors Influencing Passkey Adoption Outcome. We examined the association between various factors and the successful adoption of passkeys, with detailed results listed in Table 9 in Appendix B. A chi-square test [69] on demographics and CS background along with a Wilcoxon–Mann–Whitney test [57] on ATI and PC indicated no significant influence on passkey adoption success.

Prior passkey experience was significantly associated with successful adoption, $\chi^2(1, N = 2{,}950) = 396.04$, $p < .001$, with a moderate effect size ($V = .37$) [14]. Table 2 shows 72% (1,235 of 1,721) of experienced participants had successful adoptions, versus 35% (429 of 1,229) of inexperienced ones, **indicating that prior passkey experience increases the likelihood of successful adoption**.

Additionally, a chi-square test [69] suggested that the OS significantly influenced passkey adoption outcomes, $\chi^2(3, N = 2{,}950) = 70.39$, $p < .001$, with a small effect size ($V = .15$) [14]. Table 3 details that participants using mobile devices (smartphones and tablets) achieved higher success rates, 58% on Android and 64% on iOS, compared to 40% on macOS and 42% on Windows. These results **indicate that passkey adoption is more successful on mobile devices than on desktop ones**.

The secondary passkey factor significantly influenced outcomes, $\chi^2(4) = 68.71$, $p < .001$, with a small effect ($V = .15$). Figure 3 shows Phase 1 distributions: There were 765 authentications with a fingerprint (60% success rate), 1,256 with facial recognition (62%), 656 with a PIN (45%), 109 with pattern (58%), and 164 with password (42%). The results **suggest that biometric methods are most commonly employed, and biometrics and patterns offer higher passkey adoption rates than PINs and passwords.**

TABLE 4: Survey results on motivating factors influencing the decision to adopt passkeys in Group K, split by prior passkey experience (Exp.) and no prior experience (No Exp).

Motivating Factors	**Exp.** $n = 1{,}721$	**No Exp.** $n = 1{,}229$	**Total** $n = 2{,}950$
No memorization required	33%	54%	42%
Fast authentication	51%	22%	39%
Enhanced security	29%	38%	33%
No password creation	5%	10%	7%
Multifactor ease	6%	1%	4%
No password resets	2%	1%	2%
Other	1%	1%	1%

Note. Numbers are in-group percentages; multiple factors possible. n denotes the number of users in the corresponding group.

Finally, passkey storage location was significantly associated with adoption success, $\chi^2(3, N = 2{,}950) = 21.05$, $p < .001$, with a small effect size ($V = .08$) [14]. Of the 2,950 participants, 1,628 stored passkeys in the built-in cloud service (57% success rate), 244 in a PM (43%), 39 on another device (54%), and 1,039 were unsure of their storage location (58%). These results **suggest built-in cloud storage is the most frequently chosen option, whereas PM-based storage is linked to lower success rates**.

A binomial logistic regression supported these patterns. The model fit was significant $\chi^2(31) = 2332.15$, $p < .001$; Nagelkerke $R^2 = .733$; accuracy = 86.9%. Controlling for all other variables, significant predictors of successful passkey adoption were **prior experience** (OR = 4.51, 95% CI $[3.52, 5.79]$, $p < .001$), **acceptance** (OR = 4.21, $[3.58, 4.95]$, $p < .001$), and **SUS** (OR = 1.116, $[1.105, 1.127]$, $p < .001$). Full coefficients and odds ratios are outlined on GitHub.

4.1.6. Usability and Acceptance. Wilcoxon-Mann-Whitney test [57] showed SUS scores differed significantly between Group K (Mdn = 75) and Group W (Mdn = 67.5), $U = 2{,}640{,}040.5$, $p < .001$, $r = .13$, **indicating passkeys have higher usability than passwords with 2FA**.

Similarly, the acceptance scores differed significantly between Group K (Mdn = 1.11) and Group W (Mdn = 0.67), $U = 2{,}508{,}831.0$, $p < .001$, $r = .17$, **indicating passkeys have higher acceptance than passwords with 2FA**.

4.2. Factors Influencing Decision to Adopt Passkeys

This section outlines the factors influencing the decision to adopt passkeys, detailing motivating factors and concerns.

4.2.1. Motivating Factors. Table 4 summarizes the survey findings on why Group K chose passkeys. Chi-square test [69] revealed motivating factors varied significantly according to participants' prior passkey experience, $\chi^2(6) = 316.91$, $p < .001$, $V = .29$, indicating a moderate effect [14].

- *No Memorization.* Passkeys eliminate the need to remember complex passwords. This reason was cited by 42% overall (33% exp., 54% no exp.).

TABLE 5: Survey results on concerns influencing the decision against passkey adoption in Group W, split by prior passkey experience (Exp.) and no prior experience (No Exp).

Concerns	**Exp.** $n = 675$	**No Exp.** $n = 1{,}432$	**Total** $n = 2{,}107$
Habit of using passwords	44%	48%	47%
Lack of exp. or knowledge	32%	36%	35%
Lack of perceived benefit	18%	26%	23%
Passkey misconceptions	2%	12%	8%
Account recovery concerns	5%	6%	6%
Multiple client concerns	6%	5%	5%
Past negative experiences	13%	0%	4%
Deferred passkey adoption	1%	3%	2%
Security & privacy concerns	2%	1%	2%
Other	1%	1%	1%

Note. Numbers are in-group percentages; multiple concerns possible. n denotes the number of users in the corresponding group.

TABLE 6: Survey results on barriers to passkey adoption among unsuccessful Group K participants, split by prior passkey experience (Exp.) and no experience (No Exp).

Barriers	**Exp.** $n = 486$	**No Exp.** $n = 800$	**Total** $n = 1{,}286$
Passkey misconceptions	19%	28%	25%
Passcode misconceptions	18%	26%	23%
Manual passkey activation	15%	18%	17%
Perceived complexity	10%	12%	11%
Account recovery concerns	10%	8%	9%
Multiple client concerns	9%	8%	8%
Password manager issues	9%	6%	7%
Biometric misconceptions	5%	8%	7%
Technical difficulties	3%	3%	3%
Other	2%	1%	1%

Note. Numbers are in-group percentages; multiple barriers possible. n denotes the number of users in the corresponding group.

- *Fast Authentication.* Passkeys enable fast authentication, written by 39% overall (51% exp., 22% no exp.):

> *"[...] It is a lot quicker than typing out a password as I am able to use my Face ID for this."* (P8, Group K)

- *Enhanced Security.* Passkeys offer enhanced security, named by 33% overall (29% exp., 38% no exp.).
- *No Password Creation and Policy.* By removing the need to create and manage passwords, this factor was selected by 7% overall (5% exp., 10% no exp.).
- *Multifactor Ease.* Passkeys offer convenient MFA (e.g., biometrics), cited by 4% (6% exp., 1% no exp.).
- *No Password Resets.* Avoiding frequent password resets were noted by 2% overall (2% exp., 1% no exp.).
- *Other.* Includes misclicks or ambiguous answers.

4.2.2. Concerns. Table 5 details why Group W opted against passkeys. Chi-square test [69] revealed that concerns varied significantly by prior passkey experience $\chi^2(9) = 265.79$, $p < .001$, $V = .31$, indicating a moderate effect [14].

- *Habit of Using Passwords.* A reliance on familiar passwords was noted by 47% overall (44% exp., 48% no exp.), making it feel easier than switching to passkeys.
- *Lack of Experience or Knowledge.* No passkey exp. or knowledge was cited by 35% (32% exp., 36% no exp.).
- *Lack of Perceived Benefit.* Twenty-three percent overall (18% exp., 26% no exp.) did not perceive a clear advantage in adopting passkeys over passwords.
- *Passkey Misconceptions.* Incorrect passkey assumptions were reported by 8% (2% exp., 12% no exp.), e.g.:

> *"I don't own a physical passkey."* (P3, Group W)

- *Account Recovery Concerns.* Worries about regaining access if a device is lost or damaged were cited by 6% overall (5% exp., 6% no exp.). One respondent noted:

> *"I am terrible at losing or breaking my phone. If I use a passkey, it is a nightmare to log into apps on a new phone. [...]"* (P15, Group W)

- *Multiple Clients.* Doubts about seamless use across devices were cited by 5% (6% exp., 5% no exp.).
- *Past Negative Experiences.* Some participants recalled previous difficulties and therefore refrained from passkeys (4% overall; 13% exp., 0% no exp.), as noted:

> *"I have had trouble with passkeys on a few websites. I didn't want to go through that hassle."* (P1, Group W)

- *Deferred Adoption.* Two percent overall (1% exp., 3% no exp.) delayed the adoption by initially registering with a password and adding a passkey later:

> *"I like to sign up with passwords first and passkeys second. Don't trust them enough."* (P5, Group W)

- *Security and Privacy Concerns.* Few participants (2% overall; 2% exp., 1% no exp.) felt that passwords offered better security. A participant wrote the following remark, overlooking that most smartphones also support alphanumeric passcodes, and passkeys additionally require physical access to the device to be exploited.

> *"I felt more secure using a password because it offers more possible combinations than a passkey PIN does."* (P12, Group W)

- *Other.* Covers misclicks or ambiguous answers.

4.3. Barriers to Successful Passkey Adoption

Table 6 lists barriers for Group K participants who attempted but didn't complete passkey adoption. Chi-square

test [69] showed a significant association between passkey experience and barriers, $\chi^2(9) = 27.70$, $p < .001$, $V = .14$.

- *Passkey Misconceptions.* Misunderstandings about passkeys occurred in 25% of participants (19% exp. and 28% no exp.), primarily due to expecting password-like behavior or confusion about the process:

> *"I kept clicking [on] passkey, but it kept popping up my Face ID."* (P16, Group K)

- *Passcode Misconceptions.* The need to enter the device passcode (PIN, pattern, or password) was misinterpreted as a security risk by 23% (18% exp. and 26% no exp.), fearing it granted the platform excessive access:

> *"I had to enter my device PIN, which I found very suspicious! [...]"* (P7, Group K)

- *Manual Passkey Activation.* Several OSs require manually activating passkeys, e.g., enabling iCloud Keychain on iOS/macOS, or Windows Hello on Windows. 17% (15% exp., 18% no exp.) noted this barrier due to technical difficulty or reluctance to change settings:

> *"It was going to make me change the settings on my PC. I didn't want to do that. [...]"* (P2, Group K)

- *Perceived Complexity.* Overall, 11% (10% exp., 12% no exp.) felt the setup process was overly complicated:

> *"Too many boxes came up, and I didn't understand what was being asked of me."* (P14, Group K)

- *Account Recovery Concerns.* 9% (10% exp., 8% no exp.) feared losing access if their device was lost.
- *Multiple Clients.* 8% (9% exp., 8% no exp.) expressed concern about cross-device passkey use.
- *Password Manager Integration.* 7% (9% exp., 6% no exp.) reported PM integration issues, including no Android browser support [41], needing to adjust settings or install extensions, and failed passkey insertion:

> *"I couldn't save it in my password manager, and I want to have all my accounts there."* (P6, Group K)

- *Biometric Misconceptions.* Although our description of passkeys incorporated prior work [53] to address biometric misconceptions, 7% of participants still voiced these concerns (5% exp., 8% no exp.):

> *"I got nervous about the app storing my fingerprint, even though it said it would store on my device only. Because I do not trust the app yet."* (P11, Group K)

- *Technical Difficulties.* All devices supported passkeys, yet technical errors were reported by 3% overall.
- *Other.* Encompasses misclicks and ambiguous answers.

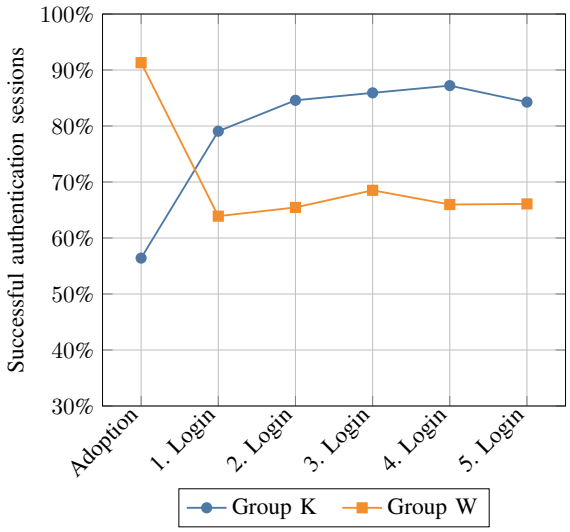


Figure 4: Successful authentication rates of both groups during adoption (Phase 1) and five subsequent logins (Phase 2).

4.4. Barriers to Password with 2FA Adoption

Among 183 participants of Group W who began but didn't finish authentication, 163 (89%) had SMS-OTP problems (e.g., not receiving or finding the message, entering a wrong code, or confusion), 13 (7%) faced password-policy issues, 5 (3%) timed out, and 2 (1%) gave unclear reasons.

5. Results: Passkey Usage (Phase 2)

In this section, we present the findings from Phase 2 on passkey adoption and compare them to Group W, which serves as the baseline to interpret the results. We examine usage telemetry, challenges, synchronizations, and recovery.

5.1. Longitudinal Usage Telemetry

Table 7 presents usage telemetry from the first five login attempts per participant in Phase 2 alongside Phase 1 results, illustrating longitudinal trends from initial passkey enrollment through sustained use. It also reports sample sizes for both measured metrics and self-reported surveys (86% overall completion; 75% in Phase 2). To maintain representative participant numbers, we limited the analysis to up to five login sessions per participant. Nevertheless, of the 6,233 attempted authentication sessions recorded in Phase 2, 6,172 (99%) are included in our analysis.

5.1.1. Success Rates. Figure 4 shows the success rates during participants' first five login attempts. During the adoption phase (Phase 1), Group W had a higher success rate than Group K (91% vs. 56%). At the first login in

TABLE 7: Longitudinal comparison of Groups K and W across initial adoption (Phase 1) and five subsequent login sessions per participant (Phase 2). For each session, authentication metrics include total attempts, successful attempts (with success rate), and median duration. Survey outcomes include completion rates, median SUS scores, and median acceptance ratings.

			Phase 1	Phase 2				
	Category	**Group**	**Adoption**	**1. Login**	**2. Login**	**3. Login**	**4. Login**	**5. Login**
Sessions Measured	**Attempts**	Group K	2,950	1,295	727	490	344	89
		Group W	2,107	1,421	909	432	291	174
	Successful	Group K	1,664 (56%)	1,024 (79%)	615 (85%)	421 (86%)	300 (87%)	75 (84%)
		Group W	1,924 (91%)	908 (64%)	595 (65%)	296 (69%)	192 (66%)	115 (66%)
	Duration	Group K	12.6 s	9.2 s	8.9 s	9.4 s	9.6 s	8.5 s
		Group W	52.9 s	59.1 s	57.3 s	60.0 s	58.3 s	58.5 s
Surveys Self-Reported	**Completed**	Group K	2,950 (100%)	1,012 (78%)	533 (73%)	341 (70%)	232 (67%)	68 (76%)
		Group W	2,107 (100%)	1,088 (77%)	708 (78%)	325 (75%)	214 (74%)	134 (77%)
	SUS	Group K	75.00	81.25	80.00	82.50	85.00	82.50
		Group W	67.50	60.00	57.50	55.00	57.50	55.50
	Acceptance	Group K	1.11	1.33	1.44	1.56	1.50	1.56
		Group W	0.67	0.56	0.67	0.89	0.72	0.67

Phase 2, this trend reversed: Group K jumped to 79% (a 23-point gain), while Group W fell to 64% (a 27-point drop). In subsequent logins, Group K's success rose to 84-87%, whereas Group W plateaued at 65-69%. In total, during Phase 2, Group K recorded 2,945 login attempts, of which 2,435 (83%) succeeded and 510 (17%) failed. By comparison, Group W made 3,227 attempts, yielding 2,106 (65%) successes and 1,121 (35%) failures. On average, Group K required 1.17 attempts per successful login, compared with 1.44 attempts for Group W. These results **indicate that, after initial setup, passkeys deliver higher and more consistent success rates than passwords with 2FA**.

5.1.2. Durations. Median authentication durations for Group K decreased from 12.6 s at initial adoption to between 8.5 s and 9.6 s during subsequent logins. In contrast, Group W's median time rose from 52.9 s at setup to between 57.3 and 60.0 s across login sessions. The accelerating speed of passkey logins likely reflects both a streamlined process since users no longer choose a storage location and growing familiarity with the authentication flow. By comparison, password logins probably remained slow due to repeated entry attempts. These results **demonstrate that passkey authentication continues to speed up over time, whereas password-based login becomes progressively slower**.

5.1.3. Usability and Acceptance. Self-reports align with the measured trends. In Phase 1, Group K had higher median SUS scores (75 vs. 67.5) and acceptance (1.11 vs. 0.67) than Group W. At the first login in Phase 2, Group K's SUS rose to 81.25 and acceptance to 1.33, while Group W's SUS fell to 60 and acceptance to 0.56. Over subsequent logins, Group K sustained SUS scores of 80-85 and acceptance ratings of 1.33-1.56, whereas Group W's SUS declined to 55-57.5 and acceptance plateaued at 0.56-0.89. These results **indicate that passkeys improve in perceived usability and acceptance over time and maintain those gains, whereas passwords with 2FA show stagnation or decline**.

5.2. Encountered Challenges

We now present the challenges participants experienced when using passkeys, as reported in the survey.

5.2.1. Reasons for Unsuccessful Logins. Participants in Group K recorded a total of 510 unsuccessful login attempts, yielding 394 completed surveys. The reported causes are:

Unsuccessful Synchronization. The most common issue, cited by 77% of participants, was unsuccessful passkey synchronization. Specific issues are detailed in Section 5.3.

Device Dependency. Eighteen percent of participants encountered problems due to device dependency. Typical scenarios included lost, broken, or stolen devices. A few participants also lost access after performing a device reset.

Technical Difficulties. Four percent of participants noted encountering technical errors during the login process.

Other. A small fraction (1%) provided unclear reasons.

5.2.2. Passkey Sharing. In 170 login attempts, participants noted three hurdles when trying to share passkeys with others (e.g., family members). First, not all storage solutions support user-to-user sharing. For example, Windows Hello synchronized passkeys across a user's Windows devices but offered no mechanism to share them with other users, leaving a PM as the only option for passkey sharing on Windows. Second, even when a storage location did support sharing, participants were often unaware of this capability or mistakenly searched for the option in the app or device settings. Third, among those who did discover the sharing feature, the workflow was perceived as complex: For iCloud, users must create a "Shared Group" in the "Passwords" app, add existing contacts from their address book, and then assign passkeys to that group. Several participants also noted that the app's name, "Passwords", is misleading given its role in also managing passkeys. These insights **suggest that platform constraints, poor discoverability, and complex procedures hinder users' ability to share passkeys**.

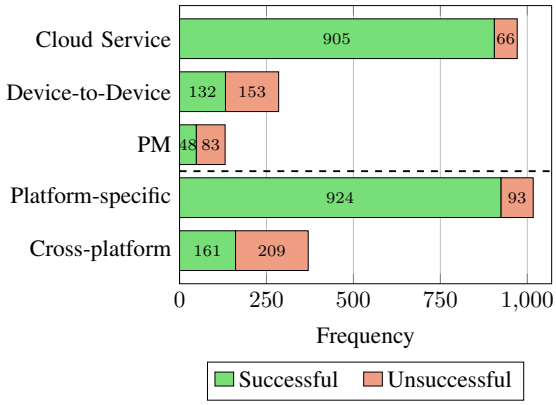


Figure 5: Frequencies and success rates of passkey synchronizations by method (cloud service, device-to-device, and PM) and scope (platform-specific vs. cross-platform).

5.2.3. Immutable Storage Location. In 84 attempts, participants noted a key limitation: once created, a passkey's storage location cannot be changed. If the initial storage lacks sharing or cross-platform synchronizations, users cannot transfer it (e.g., to a PM), without undergoing account recovery to generate a new passkey. As some OSs set a default storage location (e.g., iCloud Keychain on Apple devices), users seldom consider this choice and are unaware of its long-term implications. As one participant noted:

> *"It's trapped in the [iCloud] keychain[.] I can't move it to Bitwarden and sync it to Windows."* (P4, Group K)

This **suggests users may lack accurate mental models of passkeys and expect them to work like passwords.**

5.2.4. Non-uniform Authentication UI. In 67 attempts, participants reported inconsistent authentication interfaces across OSs. On Android, participants were prompted to select a storage location actively, while iOS presented a default choice that could be passively accepted or manually changed. Terminology varied as well, e.g., labels such as "master key" appeared instead of "passkey". These discrepancies caused confusion and fostered uncertainty about whether a passkey had been created and where it was stored, **suggesting that UI and terminology inconsistencies impede users from forming mental models of passkeys**.

5.2.5. Perceived Loss of Control. In 32 attempts, participants expressed concerns about losing control of their credentials, unsure where passkeys were stored, how to delete or share them, or how to transfer them for future logins. These uncertainties **suggest that users may not have yet formed reliable mental models of passkey functionality**.

5.3. Synchronization of Passkeys

1,387 login attempts involved synchronization. Figure 5 shows frequencies and success rates by method and scope. The most prevalent synchronization method was via built-in cloud services, with 971 attempts (905 successful and 66 unsuccessful), resulting in a 93% success rate. Manual device-to-device transfers accounted for 285 attempts (132 succeeded and 153 failed), for a 46% success rate. PM-based synchronization was used 131 times (48 successful, 83 unsuccessful) for a 36% success rate. The results **indicate that cloud-based synchronization is reliable and widely adopted in practice, while manual transfers and PM-based methods pose substantial difficulties for users**.

When grouped by scope, platform-specific synchronizations comprised 1,017 attempts (924 successful, 93 unsuccessful), resulting in a 91% success rate. In contrast, cross-platform synchronizations succeeded in only 161 out of 370 attempts (44% success), **suggesting that platform-specific passkey synchronization is robust in practice, whereas cross-platform synchronization remains problematic**.

We examine the particular challenges as follows.

5.3.1. Built-in Cloud Services. Some participants noted that they first had to enable synchronization via the built-in cloud service. Many were unaware of this step and struggled to find the corresponding option. One participant described:

> *"Took me ages to realize I needed to enable synchronization first."* (P10, Group K)

Moreover, even when synchronization was enabled and participants were signed in to the same account on both devices, the service occasionally failed to sync. Although most attempts succeeded, these results **suggest that the primary barrier to using built-in cloud services is the initial activation of synchronization**.

5.3.2. Manual Device-to-Device Transfer. There are two manual transfer options. The first involved scanning a QR code with the device currently holding the passkey, typically a mobile device. Some participants reported believing they did not have a QR code scanner installed, despite most camera apps offering built-in scanning. One participant noted:

> *"I can't scan this [QR] code[.] I don't have a scanner installed."* (P13, Group K)

A few participants scanned the QR code but noted that nothing happened, preventing synchronization.

The second option used Bluetooth. Multiple users reported that transfers failed despite Bluetooth being enabled.

These findings **indicate that manual passkey transfer is perceived as overly complex and error-prone**.

5.3.3. Third-Party Password Managers. Participants face several challenges when leveraging PMs for passkey synchronization. Android 15, the latest release, currently lacks support for creating or inserting passkeys in browsers [41], which prevented participants from saving or auto-filling their credentials. Further, after installing a PM on their device, participants had to manually enable its passkey functionality in the system settings on mobile devices and install browser

extensions for desktop devices, a step many overlooked. Most OSs also lack the option to designate a PM as the default storage location for passkeys. Even when enabled, inserting passkeys from PMs sometimes failed, forcing users to resort to manual transfer or recovery:

> *"I have the passkey in Dashlane, it's on my phone, but I can't insert it [...]"* (P9, Group K)

Participants also had to install the PM's browser extension on desktop devices to use passkeys in a web browser.

In summary, these insights **indicate that synchronizing passkeys via a PM imposes technical constraints and involves overly complex configuration steps**.

5.4. Account Recovery

This section presents the account recovery results, including success rates, durations, and qualitative feedback.

5.4.1. Success Rates. In Group K, participants experienced 510 unsuccessful login sessions and initiated account recovery in 416 cases (82%), of which 377 recoveries succeeded (91%). In Group W, there were 1,121 failed attempts and 908 recovery initiations (81%), yielding 836 successful recoveries (92%). The results **suggest that success rates are similar for passkey and password recovery**.

5.4.2. Duration. The median durations of account recovery were 62.5 s for Group K and 72.0 s for Group W, **indicating that passkey recovery is faster than recovery with passwords and 2FA**.

5.4.3. Reasons for Unsuccessful Recoveries. In Group K, 39 account-recovery attempts failed, and 30 participants completed the follow-up survey. Of those, 29 (97%) reported SMS-OTP issues, failing to receive or locate the message, entering an incorrect code, or being unsure how to proceed, while one response was ambiguous. In Group W, 72 recovery attempts were unsuccessful, with 52 survey completions: 49 (94%) cited SMS-OTP problems and three timed out.

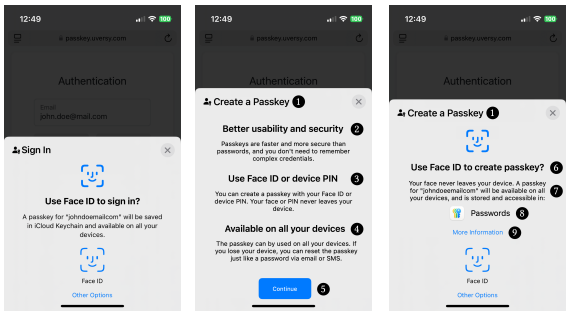
6. Discussion

We discuss the implications of our results and, alongside each topic, outline recommendations for future work.

6.1. Strategies to Accelerating Passkey Adoption

Our results show that passkeys deliver higher usability and faster authentication than passwords with 2FA, contrary to prior findings [65], [70]. We observe higher acceptance yet substantially lower adoption. Together, these findings suggest that passkeys can enhance UX while also revealing critical adoption barriers. We outline strategies to support users' choice of passkeys and overcome adoption hurdles.

Passkey Choice. We confirm prior findings [85], showing that users value the security and simplicity of passwordless authentication and the lack of memorization, yet



(a) Original UI (b) Step for No Exp. (c) Updated UI

Figure 6: Comparing the exemplary original iOS UI (a) with proposed enhancements: A informational overlay for inexperienced users (b) and an updated adoption UI (c).

they hesitate to choose passkeys because of concerns about cross-device use, technical failures, and recovery. Our study contributes novel insights by identifying concerns that appear more decisive for adoption, including entrenched password habits, limited passkey experience, and low perceived benefit. We also found that participants with prior passkey experience adopted passkeys far more often than novices.

We propose two recommendations. First, we advocate the use of digital nudges, which are interventions that preserve users' choices without materially altering incentives [73], [81]. Nudges have been shown to promote cybersecurity behavior change [6], [71], [72]. Beyond the information-salience nudges [80] already emphasized in current UX guidelines [28], we suggest:

- Offer passkeys as the default authentication method for users with passkey experience, while retaining a clear password fallback. Experience can be inferred locally, via an OS-level flag set after the user's first adoption on the device, or by the vendor, via prior passkey registrations tied to the user's account. Consider applying this nudge to sensitive accounts (e.g., online banking).
- Provide social proof by showing numerous users chose passkeys, encouraging them to follow the crowd [80].
- Increase the effort required to select passwords by adding a confirmation step, e.g., "Are you sure you want to use a password?" [11].

Second, we suggest emphasizing passkeys' benefits. Unlike prior work [65], our data show that passkeys are adopted much faster than passwords, yet few inexperienced users were aware of this. We propose augmenting the information text in the UX guidelines [28], such as: "Passkeys are faster and more secure than passwords, and you don't need to remember complex credentials." Future work should test the impact of the nudges and messages on passkey adoption.

Passkey Adoption. Passkey adoption faces usability challenges, leading to lower success rates than passwords with 2FA. We confirm biometric misconceptions from prior work [53] and uncovered novel ones: Many users interpreted the required passcode entry (PIN, pattern, or password)

as a security vulnerability, frequently resulting in adoption cancellations, particularly among first-time passkey users.

To address these issues, we propose revising the passkey adoption UI, as exemplified by the iOS UI in Figure 6. Most of the reported problems persist across OSs, so our recommendations generalize broadly. Since users without prior passkey experience had substantially lower success rates, we recommend adding an informational overlay on the first attempt (Figure 6b), also educating users when the service itself provides no passkey guidance. The OS can detect whether a user has previously created a passkey and display this screen accordingly. To tackle misconceptions, the overlay explicitly informs users that they are creating a passkey ❶, succinctly highlights its benefits ❷, and reassures them that their biometrics [53] and passcode never leave their device ❸. Concerns regarding multi-client use and account recovery are addressed ❹ before the user can proceed with the passkey adoption process ❺. We also propose updating the default passkey adoption interface (Figure 6c), which could appear initially in subsequent authentications. In this revised UI, users are informed that they are creating a passkey via Face ID ❻ and reminded that their biometrics and passcode never leave their device ❼. As most users were unaware of where passkeys are stored, and some feared less control, we explicitly state the storage location and how users can access their passkeys ❽. An option to reopen the informational overlay at any time ❾ ensures that users can revisit the guidance as needed. Consistent with prior work [53], [64], we urge OS vendors to adopt a standardized authentication UI with uniform terminology.

Beyond the UI, we newly identified that participants experienced friction when system settings had to be modified during passkey adoption. On iOS and macOS, users must enable iCloud Keychain, and Windows requires activation of Windows Hello. To use passkeys with a PM, mobile OSs require manual activation, and desktop OSs demand browser-extension installation. Thereby, users are seldom made aware of these prerequisites. To streamline adoption, we recommend either automatically enabling all necessary passkey-related settings or prompting users with a one-click option upon OS update or PM installation (or update). By preempting the required settings changes in advance, effort and confusion during the adoption process could be reduced. We further encourage Google to offer an API for PM support within its Chrome browser on Android [41].

Our results confirm that mobile devices and biometric second factors are associated with higher adoption rates [63], [65]. To extend these benefits to desktops, OS vendors should continue expanding biometric capabilities through hardware (e.g., Touch ID on macOS) and software (e.g., facial recognition in Windows Hello) and offer biometrics as the default second factor. Future work should empirically test our recommendations' impact on passkey adoption.

6.2. Addressing Challenges of Passkey Usage

Our longitudinal analysis found that passkey success rates and usability increased over time while authentication times decreased, aligning with prior research [65]. Further, we newly show that passkeys achieved markedly higher success rates after first usage than passwords, suggesting users adapt quickly to them. Still, we identified novel challenges, particularly involving passkey sharing and synchronization.

Dedicated Passkey Management App. We uncovered that passkeys are primarily stored in built-in cloud services, but users can't easily locate or manage them, leading to a loss of control. Since passkey management is often buried deep within settings, making it difficult to discover, we propose OSs to offer a standalone management app. While iOS and macOS include a "Passwords" app, its name conceals passkey functionality, and it lacks essential features. The app should streamline sharing by including a "Share" button for each passkey and support storage migration, enabling moving passkeys from cloud storage to a PM. Users should be introduced to this app during passkey adoption (Figure 6c).

Passkey Synchronization. We gained novel insights into the usability of passkey synchronization, identifying it as the primary cause of failed logins:

Built-in Cloud Services: Some OSs require users to enable passkey synchronization manually. We recommend enabling synchronization by default and, for users who haven't activated it, prompting after the first passkey creation with a one-click activation option. Because most users rely on built-in cloud services tied to a single ecosystem, vendor lock-in [24] is exacerbated, and platform switching is impeded. Future work could explore cross-cloud synchronization (e.g., adding a Windows Hello account to iCloud Keychain), and the FIDO Alliance should standardize such a system.

Manual Device-to-Device Transfer: Primarily used for cross-platform sync, it proved too complex and error-prone for most users. We recommend adding interactive guidance (e.g., a short animation or video) in the passkey login UI.

Third-Party Password Managers: PM challenges from adoption also persisted in use. Further, OSs should prompt users, during PM installation or update, to choose a default passkey storage, a feature currently offered only on iOS. Furthermore, PM vendors should validate that their implementations correctly insert passkeys during login.

Account Recovery. Unlike security keys, which lack scalable recovery and can lock users out if the sole key is lost [55], passkeys can be backed up via device synchronization [30]. Yet, our results uncover that synchronization, especially cross-platform, does not always succeed. While registering multiple passkeys on different devices would be ideal for security, it imposes major usability burdens [51]. Thus, prior work advocated exploring an OTP-based recovery option to enable users to register a new passkey [65], [85], which we implemented via SMS. Compared to password recovery, this approach achieves similar success rates with faster recovery times, suggesting a reasonable balance between security and usability for most services.

6.3. Limitations

Recruitment. Recruitment was not fully random, as participants needed to use our industry partner's platform, but demographics approximated the general population. Since all users were European, results may not generalize beyond this region; future work could replicate the study in other regions. **Field Study.** We traded experimental control for authentic behavior and real-world challenges. Data sensitivity of the healthcare context may have affected authentication choices. Attrition was similar, 31.8% in Group K and 29.5% in Group W, matching typical longitudinal research [65]. **Group Assignment.** Allowing users to self-select their authentication method reflects real choices but may introduce bias. The brief informational text, based on FIDO UX guidelines [28] and Lassak et al. [53], and the limitation on switching authentication methods may have introduced bias, but both mirror industry practice [34], [42], [44], [47]. **Self Reporting.** Our survey relies on self-reports, which may be imprecise, so we asked for immediate feedback after each authentication. **Design of Control Group.** The control group used passwords with at least eight characters from two classes (Section 3.1) and 2FA, which may have affected comparisons but reflects common practice [39], [56], [67]. **Retention.** The initially selected authentication method was retained during the study, which does not represent real-world conditions. Future work should permit method switching. **Autofill.** Password autofill was allowed but not tracked, which could impact authentication durations of Group W. We suggest future work to document password autofill use.

7. Conclusion

This paper presents a large-scale field study on the adoption and usage of passkeys. Although initial passkey adoption had lower success rates than passwords with 2FA, we showed that passkeys offer superior usability and acceptance. With repeated logins, they outperformed passwords with 2FA in success rates while usability and acceptance continued to grow. We found new adoption barriers, such as novel misconceptions and manual passkey activation, as well as key usage challenges, including cross-platform synchronization, passkey sharing, and interactions with password managers. Accordingly, we offer actionable recommendations to streamline passkey adoption and usability.

Availability

To facilitate future research, we made our study's implementation open-source[3], enabling researchers to replicate our study and capture key metrics. Although we are unable to share raw data due to a data protection agreement between the platform vendor and its users, all statistical analyses performed with SPSS and the codebook have been published.

3. Open-source code: https://github.com/PasskeyStudy/Availability

Declaration of Generative AI Technologies in the Writing Process

During the preparation of this work, the authors used DeepL, Grammarly, and ChatGPT (Version 4o) in order to improve the language and readability. After using the tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.[4]

Acknowledgments

We thank Magdalena Glas, Thomas Baumer, the reviewers, and our shepherd for their constructive feedback.

References

[1] 1Password. What are passkeys?, 2024. Accessed: 02/11/25. URL: https://1password.com/product/passkeys.

[2] Adobe. Login and security, 2025. Accessed: 02/11/25. URL: https://account.adobe.com/security.

[3] Elham Al Qahtani, Lipsarani Sahoo, Yousra Javed, and Mohamed Shehab. "why would someone hack me out of thousands of students": Video presenter's impact on motivating users to adopt 2fa. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, pages 139–150, 2022.

[4] Apple, Inc. About the security of passkeys, 2022. Accessed: 02/11/25. URL: https://support.apple.com/en-us/102195.

[5] Apple, Inc. Share passwords or passkeys with people you trust on iphone, 2025. Accessed: 02/11/25. URL: https://support.apple.com/en-gb/guide/iphone/iphe6b2b7043/ios.

[6] Thomas Baumer, Tobias Reittinger, Sascha Kern, and Günther Pernul. Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 239–258, Philadelphia, PA, August 2024. USENIX Association. URL: https://www.usenix.org/conference/soups2024/presentation/baumer.

[7] Arnar Birgisson. Security of passkeys in the google password manager, 2022. Accessed: 02/11/25. URL: https://security.googleblog.com/2022/10/SecurityofPasskeysintheGooglePasswordManager.html.

[8] Bitwarden. Innovating in passwordless, 2024. Accessed: 02/11/25. URL: https://bitwarden.com/passwordless-passkeys/.

[9] John Brooke et al. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[10] Andre Büttner and Nils Gruschka. Device-bound vs. synced credentials: A comparative evaluation of passkey authentication. In *Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 2: ICISSP*, pages 651–659. INSTICC, SciTePress, 2025. doi:10.5220/0013380600003899.

[11] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–15, 2019.

[12] Dhiman Chakraborty and Sven Bugiel. simfido: Fido2 user authentication with simtpm. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 2569–2571, New York, NY, USA, 2019. Association for Computing Machinery.

4. For transparency, we publish AI Usage Cards documenting our use of generative AI [83]: https://ai.uversy.com/passkeys

[13] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. Of two minds about Two-Factor: Understanding everyday FIDO U2F usability through device comparison and experience sampling. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 339–356, Santa Clara, CA, August 2019. USENIX Association.

[14] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. routledge, 2013.

[15] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible" exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2018.

[16] Silvia Convento, Court Jacinic, and Becca Shareff. Making authentication faster than ever: passkeys vs. passwords, 2023. Accessed: 02/11/25. URL: https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html.

[17] Harald Cramér. *Mathematical Methods of Statistics*. Princeton University Press, 1946.

[18] Alaa Daffalla, Arkaprabha Bhattacharya, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. A framework for abusability analysis: The case of passkeys in interpersonal threat models. In *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[19] Sanchari Das, Andrew Dingman, and L Jean Camp. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22*, pages 160–179. Springer, 2018.

[20] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th workshop on socio-technical aspects in security and trust*, pages 28–39, 2017.

[21] Vincent Delitz. Windows 11's upcoming passkey (windows hello) features, 2024. Accessed: 02/11/25. URL: https://www.microsoft.com/en-us/security/blog/2024/05/02/microsoft-introduces-passkeys-for-consumer-accounts/.

[22] Nicole M Deterding and Mary C Waters. Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociological methods & research*, 50(2):708–739, 2021.

[23] Florian M Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "you still use the password after all"–exploring fido2 security keys in a small company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 19–35, 2020.

[24] Joseph Farrell and Paul Klemperer. Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization*, 3:1967–2072, 2007.

[25] FIDO Alliance. Apple, google and microsoft commit to expanded support for fido standard to accelerate availability of passwordless sign-ins, 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/.

[26] FIDO Alliance. Client to authenticator protocol (ctap), 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[27] FIDO Alliance. Sc magazine: Finding fido: What fast identity online is, and how it works, 2022. Accessed: 02/11/25. URL: https://fidoalliance.org/sc-magazine-finding-fido-what-fast-identity-online-is-and-how-it-works/.

[28] FIDO Alliance. Fido alliance ux guidelines for passkey creation and sign-ins, 2023. Accessed: 02/11/25. URL: https://fidoalliance.org/wp-content/uploads/2023/05/FIDO-Alliance-UX-Guidelines-for-Passkey-Creation-and-Sign-ins.pdf.

[29] FIDO Alliance. Fido authentication, 2023. Accessed: 02/11/25. URL: https://fidoalliance.org/fido2/.

[30] FIDO Alliance. Passkeys, 2024. Accessed: 02/11/25. URL: https://fidoalliance.org/passkeys/.

[31] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, page 657–666, New York, NY, USA, 2007. Association for Computing Machinery. doi:10.1145/1242572.1242661.

[32] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human–Computer Interaction*, 35(6):456–467, 2019.

[33] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. " what was that site doing with my facebook password?" designing password-reuse notifications. In *Proceedings of the 2018 acm sigsac conference on computer and communications security*, pages 1549–1566, 2018.

[34] Google. The easiest and most secure way to sign in to your google account, 2025. Accessed: 02/11/25. URL: https://www.google.com/account/about/passkeys/.

[35] Google. Save, manage & protect your passwords, 2025. Accessed: 02/11/25. URL: https://support.google.com/accounts/answer/6208650.

[36] Google Cloud. Cybersecurity forecast 2024, 2024. Accessed: 02/11/25. URL: https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf.

[37] Google LLC. Mercari's passkey authentication speeds up sign-in 3.9 times, 2023. Accessed: 02/11/25. URL: https://developers.google.com/identity/passkeys/case-studies/mercari.

[38] Google LLC. Password manager dashlane sees 70% increase in conversion rate for signing-in with passkeys compared to passwords, 2023. Accessed: 02/11/25. URL: https://developers.google.com/identity/passkeys/case-studies/dashlane.

[39] Paul Grassi, James Fenton, Elaine Newton, Ray Perlner, Andrew Regenscheid, William Burr, Justin Richer, Naomi Lefkovitz, Jamie Danker, Yee-Yin Choong, Kristen Greene, and Mary Theofanos. Digital identity guidelines: Authentication and lifecycle management. Special Publication 800-63B, National Institute of Standards and Technology, Gaithersburg, 2020. URL: https://doi.org/10.6028/NIST.SP.800-63b.

[40] Eric Grosse and Mayank Upadhyay. Authentication at scale. *IEEE Security & Privacy*, 11(1):15–22, 2013.

[41] Travis Hogan. Save and sign in to android apps with passkeys using 1password, 2024. Accessed: 02/11/25. URL: https://blog.1password.com/save-use-passkeys-android/.

[42] Amazon.com Inc. Passkey, 2025. Accessed: 02/11/25. URL: https://www.amazon.com/ax/claim/webauthn/enroll.

[43] Apple Inc. Sign in with apple account, 2025. Accessed: 02/11/25. URL: https://www.icloud.com/.

[44] Uber Technologies Inc. Passkeys, 2025. Accessed: 02/11/25. URL: https://account.uber.com/passkeys.

[45] Mazharul Islam, Sunpreet S. Arora, Rahul Chatterjee, and Ke Coby Wang. Detecting compromise of passkey storage on the cloud. In *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[46] Michael B. Jones, Akshay Kumar, and Emil Lundberg. Web authentication: An api for accessing public key credentials level 3, 2023. Accessed: 02/11/25. URL: https://www.w3.org/TR/webauthn-3/.

[47] KAYAK. Sign in or create an account, 2025. Accessed: 02/11/25. URL: https://www.kayak.com/login.

[48] Jan H. Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. "make them change it every week!": A qualitative exploration of online developer advice on usable and secure authentication. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 2740–2754, New York, NY, USA, 2023. Association for Computing Machinery.

[49] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the sigchi conference on human factors in computing systems*, pages 2595–2604, 2011.

[50] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. Evaluating the security posture of real-world fido2 deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 2381–2395, New York, NY, USA, 2023. Association for Computing Machinery.

[51] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. Evaluation of account recovery strategies with fido2-based passwordless authentication. *arXiv preprint arXiv:2105.12477*, 2021.

[52] Markus Langer, Cornelius J König, and Andromachi Fitili. Information as a double-edged sword: The role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, 81:19–30, 2018.

[53] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "it's stored, hopefully, on an encrypted server": Mitigating users' misconceptions about fido2 biometric webauthn. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 91–108, 2021.

[54] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why aren't we using passkeys? obstacles companies face deploying fido2 passwordless authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7231–7248, Philadelphia, PA, August 2024. USENIX Association. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/lassak.

[55] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is fido2 the kingslayer of user authentication? a comparative usability study of fido2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 268–285. IEEE, 2020.

[56] Siqi Ma, Runhan Feng, Juanru Li, Yang Liu, Surya Nepal, Diethelm, Elisa Bertino, Robert H Deng, Zhuo Ma, and Sanjay Jha. An empirical study of sms one-time password authentication in android apps. In *Proceedings of the 35th annual computer security applications conference*, pages 339–354, 2019.

[57] Henry B Mann and Donald R Whitney. On a test of whether one of two random variables is stochastically larger than the other. *The annals of mathematical statistics*, pages 50–60, 1947.

[58] mdn web docs. Web authentication api, 2024. Accessed: 02/11/25. URL: https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API#browser_compatibility.

[59] Microsoft. Microsoft digital defense report 2023, 2023. Accessed: 02/11/25. URL: https://www.microsoft.com/de-de/security/security-insider/microsoft-digital-defense-report-2023.

[60] Microsoft. Microsoft digital defense report 2024, 2024. Accessed: 02/11/25. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

[61] Milica Mihajlija and Yumeji Hattori. How yahoo! japan increased passkeys adoption to 11% and reduced sms otp costs, 2023. Accessed: 02/11/25. URL: https://web.dev/case-studies/yahoo-japan-passkeys?hl=en.

[62] Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert. Sms-based one-time passwords: Attacks and defense: (short paper). In *Detection of Intrusions and Malware, and Vulnerability Assessment: 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings 10*, pages 150–159. Springer, 2013.

[63] Florian Nawrath. Quantitative analysis of fido2 client support. *Proc. WAY*, 2021.

[64] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. Observation study on usability challenges for fingerprint authentication using webauthn-enabled android smartphones. *Age*, 20:29, 2020.

[65] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. User perceptions of the usability and security of smartphones as {FIDO2} roaming authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 57–76, 2021.

[66] passkeys.dev. Device support, 2024. Accessed: 02/11/25. URL: https://passkeys.dev/device-support/.

[67] PayPal. Password security, 2025. Accessed: 01/29/25. URL: https://www.paypal.com/bb/webapps/mpp/security/secure-passwords.

[68] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[69] Karl Pearson. X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 50(302):157–175, 1900.

[70] Sangeeta Ranjit and Scott Bingham. Convincing a billion users to love passkeys: Ux design insights from microsoft to boost adoption and security, 2024. Accessed: 08/14/25. URL: https://www.microsoft.com/en-us/security/blog/2024/12/12/convincing-a-billion-users-to-love-passkeys-ux-design-insights-from-microsoft-to-boost-adoption-and-security/.

[71] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Employee motivation in organizational cybersecurity: Matching theory and reality. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 3–16. Springer, 2024.

[72] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. Motivational factors in cybersecurity: linking theory to organizational practice. *Information & Computer Security*, 2025.

[73] Tobias Reittinger and Günther Pernul. A taxonomy of positive incentives to motivate cybersecurity behaviors. In *Proceedings of the 58th HI International Conference on System Sciences (HICSS-58)*, 2025.

[74] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A tale of two studies: The best and worst of yubikey usability. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 872–888. IEEE, 2018.

[75] Ryan Schin. Despite increasing cybersecurity attacks, people still believe antiquated username and passwords are strong enough. Accessed: 02/11/25. URL: https://www.yubico.com/press-releases/despite-increasing-cybersecurity-attacks-people-still-believe-antiquated-username-and-passwords-are-strong-enough/.

[76] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. Feido: Recoverable fido2 tokens using electronic ids. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 2581–2594, New York, NY, USA, 2022. Association for Computing Machinery.

[77] Kateryna Semenova. How kayak reduced sign in time by 50% and improved security with passkeys, 2023. Accessed: 02/11/25. URL: https://developers.googleblog.com/2023/10/how-kayak-reduced-sign-in-time-and-improved-security-with-passkeys.html.

[78] Samuel Sanford Shapiro and Martin B Wilk. An analysis of variance test for normality (complete samples). *Biometrika*, 52(3-4):591–611, 1965.

[79] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4):1–34, 2016.

[80] Cass R Sunstein. The council of psychological advisers. *Annual Review of Psychology*, 67(1):713–737, 2016.

[81] Cass R Sunstein. Misconceptions about nudges. *Available at SSRN 3033101*, 2017.

[82] Jinke D Van Der Laan, Adriaan Heino, and Dick De Waard. A simple procedure for the assessment of acceptance of advanced transport telematics. *Transportation Research Part C: Emerging Technologies*, 5(1):1–10, 1997.

[83] Jan Philip Wahle, Terry Ruas, Saif M Mohammad, Norman Meuschke, and Bela Gipp. Ai usage cards: Responsibly reporting ai-generated content. In *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, pages 282–284. IEEE, 2023.

[84] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, 2016.

[85] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. Fido2 the rescue? platform vs. roaming authentication on smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023.

Appendix A. Survey Questionnaires

We present the survey questionnaires of both phases. Following [85], we displayed non-descriptive section names to participants (e.g., "Category A").

A.1. Phase 1

Motivating Factors. *Participants who chose passkeys (Group K) were asked the following questions.* (1) You selected a passkey as your authentication method. Did you choose this option intentionally? [*Yes / No*] (2) Why did you choose a passkey? [*Free text answer*] (3) Did you encounter any difficulties during the setup of the passkey? [*Free text answer*]

Barriers. *Participants who chose passkeys (Group K) and canceled the adoption were asked the following question.* (1) Why did you cancel the passkey setup process? [*Free text answer*]

Concerns. *Participants who chose passwords (Group W) were asked the following questions.* (1) You selected a password as your authentication method. Did you choose this option intentionally? [*Yes / No*] (2) Why did you not choose a passkey? [*Free text answer*] (3) Did you encounter any difficulties during the setup process? [*Free text answer*]

Computer Science Background and Prior Experience. (1) Do you have a background in computer science? [*Yes / No*] (2) How often have you used passwords before this study? [*0 times / 1-3 times / ≥3 times*] (3) Passkeys are a new authentication method. How often have you used passkeys before this study? [*0 times / 1-3 times / ≥3 times*] (4) SMS OTPs are one-time passwords (often six-digit codes) sent via text message to verify your identity. How often have you used an SMS OTP before this study? [*0 times / 1-3 times / ≥3 times*]

Affinity for Technology Interaction (ATI). In the following, we will ask you about your interaction with technical systems. The term "technical systems" refers to apps and other software applications, as well as entire digital devices (e.g., mobile phone, computer, TV, car navigation). Please indicate the degree to which you agree/disagree with the following statements.

[*Six options from "Completly disagree" to "Completly agree"*] (1) I like to occupy myself in greater detail with technical systems. (2) I like testing the functions of new technical systems. (3) I predominantly deal with technical systems because I have to. (4) When I have a new technical system in front of me, I try it out intensively. (5) I enjoy spending time becoming acquainted with a new technical system. (6) It is enough for me that a technical system works; I don't care how or why. (7) I try to understand how a technical system exactly works. (8) It is enough for me to know the basic functions of a technical system. (9) I try to make full use of the capabilities of a technical system.

Privacy Concerns. How much do you agree or disagree with the following statements? [*Seven options from "Strongly disagree" to "Strongly agree"*] (1) I am concerned that companies are collecting too much personal information about me. (2) I am concerned about my privacy. (3) To me, it is important to keep my privacy intact. (4) Novel technologies are threatening privacy increasingly.

Demographics. (1) What is your gender? [*Female / Male / Other / No answer*] (2) How old are you? [*18-19 / 20-29 / 30-39 / 40-49 / 50-59 / 60-69 / 70-79 / ≥80*] (3) What is your highest education? [*Still in school / Middle school / High school / Bachelor / Master / Doctorate / Other*]

A.2. Phase 2

Problems. (1) Did you encounter any problems with the [respective authentication method] during the login? [*No problems / Few problems / Some problems / Many problems*] (2) Please describe the problems you encountered with the [respective authentication method] during the login briefly. [*Free text answer*] (3) Your login attempt with the passkey was unsuccessful. What was the reason for that? [*Free text answer*]

Passkey Authentication Details. (1) Where did you store the passkey? [*Built-in Cloud service (e.g., iCloud Keychain, Google Password Manager, Windows Hello) / Third-Party Password Manager (e.g., 1Password, Bitwarden, Dashlane) / Another device / I don't know*] (2) Which second factor did you use for the passkey authentication? [*Fingerprint / Facial*

Recognition / PIN (e.g., six digits) / Pattern (gesture-based) / Password (e.g., letters, numbers, symbols)] (3) Did you experience any issues with your second factor authentication? If so, please briefly describe them. [*Free text answer*] (4) Have you synchronized your passkey or attempted to do so? If yes, please indicate whether the process was successful. [*Not synchronized / Built-in Cloud Service (e.g., iCloud Keychain, Google Password Manager, Windows Hello) / Manual Device-to-Device Transfer via QR code / Manual Device-to-Device Transfer via Bluetooth / Third-Party Password Manager (e.g., 1Password, Bitwarden)*] [*Successful / Unsuccessful*] (5) Did you experience any issues with the passkey synchronization? If so, please briefly describe them. [*Free text answer*]

Appendix B. Participants' variables

We list the variables of Phase 1 participants in Table 9.
System Usability Scale (SUS). The word "system" refers to [respective authentication method] you just used to log in. How much do you agree or disagree with the following statements? [*Five options from "Strongly disagree" to "Strongly agree"*] (1) I think that I would like to use this system frequently. (2) I found the system unnecessarily complex. (3) I thought the system was easy to use. (4) I think that I would need the support of a technical person to be able to use this system. (5) I found the various functions in this system were well integrated. (6) I thought there was too much inconsistency in this system. (7) I would imagine that most people would learn to use this system very quickly. (8) I found the system very awkward to use. (9) I felt very confident using the system. (10) I needed to learn a lot of things before I could get going with this system.
Acceptance Scale. Please evaluate [respective authentication method] by selecting the one option that best represents your assessment for each row of adjectives. [*Five options between these pairs: Useless vs. Useful; Unpleasant vs. Pleasant; Bad vs. Good; Annoying vs. Nice; Superfluous vs. Effective; Irritating vs. Likeable; Worthless vs. Assisting; Undesirable vs. Desirable; Sleep-inducing vs. Raising alertness*]
Account Recovery. (1) Did you encounter any problems during account recovery? [*No problems / Few problems / Some problems / Many problems*] (2) Please describe the problems you encountered during account recovery briefly. [*Free text answer*] (3) Your account recovery was unsuccessful. What was the reason for that? [*Free text answer*]

Appendix C. Survey Codebook

The codebook of the open-ended survey questions is available in the GitHub repository[3] We considered codes from previous studies on platform authentication with FIDO2 [53], [54], [55], [64], [85].

TABLE 8: Survey participants' characteristics.

Phase 1				Phase 2			
ID	**Group**	**Gender**	**Age**	**ID**	**Group**	**Gender**	**Age**
P1	Group W	M	45	P13	Group K	F	69
P2	Group K	M	41	P14	Group K	F	32
P3	Group W	F	44	P15	Group W	M	27
P4	Group K	M	34	P16	Group K	F	32
P5	Group W	F	36				
P6	Group K	M	32				
P7	Group K	F	37				
P8	Group K	F	55				
P9	Group K	M	54				
P10	Group K	M	34				
P11	Group K	M	54				
P12	Group W	M	59				

Note. For anonymity reasons and better readability, we reset ID numbers to consecutively start at one.

Appendix D. Quoted Survey Participants' Characteristics

We characterize participants with quotes in Table 8.

TABLE 9: Variables of participants in Phase 1, and their associations with passkey choice and adoption.

		Passkey Choice				Passkey Adoption Outcome (Group K)			
Category	**Variable**	**Group K** $n = 2,950$	**Group W** $n = 2,107$	**Statistic**	**ES**	**Successful** $n = 1,664$	**Unsuccessful** $n = 1,286$	**Statistic**	**ES**
Gender	Female	1493 (50.6%)	1057 (50.2%)	$\chi^2(2) = 0.57$ $p = .753$	.01	826 (49.6%)	667 (51.9%)	$\chi^2(2) = 5.48$ $p = .064$	.04
	Male	1454 (49.3%)	1049 (49.8%)			838 (50.4%)	616 (47.9%)		
	Other	3 (0.1%)	1 (0%)			0 (0%)	3 (0.2%)		
	No answer	0 (0%)	0 (0%)			0 (0%)	0 (0%)		
Age	18-19	59 (2.0%)	50 (2.4%)	$\chi^2(7) = 3.60$ $p = .825$	.03	34 (2.0%)	25 (1.9%)	$\chi^2(7) = 4.82$ $p = .682$	.04
	20-29	467 (15.8%)	329 (15.6%)			268 (16.1%)	199 (15.5%)		
	30-39	637 (21.6%)	464 (22.0%)			352 (21.2%)	285 (22.2%)		
	40-49	621 (21.1%)	429 (20.4%)			352 (21.2%)	269 (20.9%)		
	50-59	562 (19.1%)	385 (18.3%)			301 (18.1%)	261 (20.3%)		
	60-69	424 (14.4%)	330 (15.7%)			254 (15.3%)	170 (13.2%)		
	70-79	154 (5.2%)	100 (4.7%)			87 (5.2%)	67 (5.2%)		
	80+	26 (0.9%)	20 (0.9%)			16 (1.0%)	10 (0.8%)		
Education	Still in school	72 (2.4%)	39 (1.9%)	$\chi^2(6) = 3.64$ $p = .725$	.03	42 (2.5%)	30 (2.3%)	$\chi^2(6) = 12.27$ $p = .056$	.06
	Middle school	1203 (40.8%)	863 (41.0%)			657 (39.5%)	546 (42.5%)		
	High school	934 (31.7%)	646 (30.7%)			522 (31.4%)	412 (32.0%)		
	Bachelor	242 (8.2%)	183 (8.7%)			148 (8.9%)	94 (7.3%)		
	Master	127 (4.3%)	101 (4.8%)			70 (4.2%)	57 (4.4%)		
	Doctorate	59 (2.0%)	41 (1.9%)			44 (2.6%)	15 (1.2%)		
	Other	313 (10.6%)	234 (11.1%)			181 (10.9%)	132 (10.3%)		
ATI		3.78	3.78	$U = 2,992,336.5$ $p = .024$	.03	3.78	3.89	$U = 1,048,786.0$ $p = .356$	.02
PC		5.50	5.00	$U = 2,567,618.0$ $\mathbf{p < .001}$	.15	5.50	5.25	$U = 1,050,959.5$ $p = .405$	.02
CS bkgd.	Yes	279 (9.5%)	181 (8.6%)	$\chi^2(1) = 1.12$ $p = .290$	.01	177 (10.6%)	102 (7.9%)	$\chi^2(1) = 6.20$ $p = .013$	.05
	No	2671 (90.5%)	1926 (91.4%)			1487 (89.4%)	1184 (92.1%)		
Prior exp.	Yes	1721 (58.3%)	675 (32.0%)	$\chi^2(1) = 341.08$ $\mathbf{p < .001}$	.26	1235 (74.2%)	486 (37.8%)	$\chi^2(1) = 396.04$ $\mathbf{p < .001}$	.37
	No	1229 (41.7%)	1432 (68.0%)			429 (25.8%)	800 (62.2%)		
OS	Android	1554 (52.7%)	1124 (53.3%)	$\chi^2(3) = 7.46$ $p = .059$	.04	896 (53.8%)	658 (51.2%)	$\chi^2(3) = 70.39$ $\mathbf{p < .001}$	.15
	iOS	844 (28.6%)	541 (25.7%)			539 (32.4%)	305 (23.7%)		
	macOS	191 (6.5%)	160 (7.6%)			76 (4.6%)	115 (8.9%)		
	Windows	361 (12.2%)	282 (13.4%)			153 (9.2%)	208 (16.2%)		
Storage	Build-in Cloud	-	-			933 (56.1%)	695 (54.0%)	$\chi^2(3) = 21.05$ $\mathbf{p < .001}$	.08
	PM	-	-			104 (6.3%)	140 (10.9%)		
	Another device	-	-			21 (1.3%)	18 (1.4%)		
	I don't know	-	-			606 (36.4%)	433 (33.7%)		
2FA	Fingerprint	-	-			457 (27.5%)	308 (24.0%)	$\chi^2(4) = 68.71$ $\mathbf{p < .001}$	.15
	Facial Recog.	-	-			780 (46.9%)	476 (37.0%)		
	PIN	-	-			295 (17.7%)	361 (28.1%)		
	Pattern	-	-			63 (3.8%)	46 (3.6%)		
	Password	-	-			69 (4.1%)	95 (7.4%)		
SUS		75.0	67.5	$U = 2,640,040.5$ $\mathbf{p < .001}$	.13	82.5	55.0	$U = 255,974.5$ $\mathbf{p < .001}$	.66
Acceptance		1.11	0.67	$U = 2,508,831.0$ $\mathbf{p < .001}$	.17	1.56	0.56	$U = 461,774.0$ $\mathbf{p < .001}$	.49

Note. Depending on the variable, we display **frequencies (with in-group percentages) or the median** (to minimize outlier effects). n = Number of participants; ES = Effect Size; ATI = Affinity for Technology Interaction; PC = Privacy Concerns; CS bkgd. = Computer science background; Prior exp. = Prior passkey experience; OS = Operating system; PM = Third-party password manager; 2FA = Passkey second factor; Facial Recog. = Facial Recognition; SUS = System Usability Scale. - = not applicable; The statistic is either Pearson's chi-square test [69] or the Wilcoxon-Mann-Whitney test [57], and the effect size (ES) is either Cramér's V [17] for the chi-square test [69] or the rank-biserial correlation coefficient r for the Wilcoxon-Mann-Whitney test [57]. **Significance level of $\mathbf{p < 0.001}$**, highlighted in bold font.

E. Meta-Review

The following meta-review was prepared by the program committee for the 2026 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

E.1. Summary

The paper presents a large-scale field study of passkey adoption by partnering with a European healthcare service. Participants were users of this platform and, after agreeing to join the study, had the option to secure their account with 1) a passkey or 2) a password with 2FA (SMS 2FA). The study had two phases: first, a large-scale survey (n=5,057) about why participants chose a particular option, followed by six months of monitoring of authentication behavior (n=2,716) with in-situ surveys. The authors identified several reasons for adoption or refusal of passkeys, as well as barriers during usage (e.g., synchronization between devices). The authors concluded with recommendations on how to improve the passkey ecosystem.

E.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Provides a Valuable Step Forward in an Established Field

E.3. Reasons for Acceptance

1) The paper provides independent confirmation of important results with limited prior research. The results of this large-scale field study add to the field by confirming issues and benefits of passkeys ”in the wild.”
2) The paper provides a valuable step forward in an established field. It contributes new insights into the passkey ecosystem involving several stakeholders (e.g., synchronization across platforms or within a platform), adding to the growing literature on passkeys/FIDO2.

P3 Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption.

Current status:	Accepted for publication
Conference:	ACM CHI Conference on Human Factors in Computing Systems (CHI 2026)
Ranking:	A* ICORE 2026, 25% Acceptance Rate
Date of acceptance:	January 15, 2026
Date of publication:	To be determined.
Full citation:	Reittinger, T., Glas, M., & Pernul, G. (2026). Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. (accepted for publication).

Authors' contributions:		
	Tobias Reittinger	70%
	Magdalena Glas	20%
	Günther Pernul	10%

Conference description: The *ACM CHI Conference on Human Factors in Computing Systems* (peer-reviewed) is one of the most prestigious conferences and a leading cross-disciplinary showcase of research in human–computer interaction. It spans interaction design, systems, and human factors, bringing together cutting-edge findings, novel interaction techniques, and thoughtful critiques of technology in use. The 2026 edition will be hosted in Barcelona on April 13–17, 2026.

Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption

Tobias Reittinger
University of Regensburg
Regensburg, Germany

Magdalena Glas
University of Regensburg
Regensburg, Germany

Günther Pernul
University of Regensburg
Regensburg, Germany

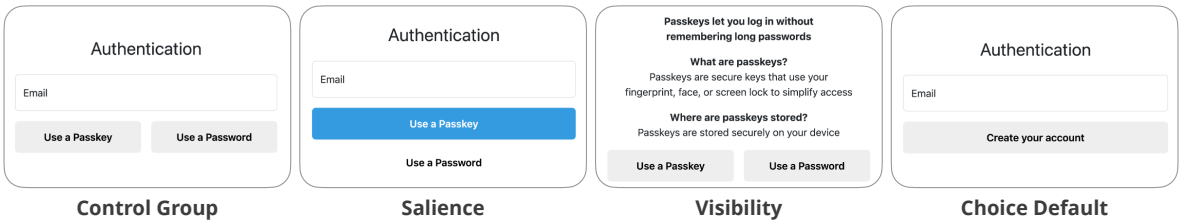


Figure 1: Digital nudges to increase passkey adoption at user registration.

ABSTRACT

Passwords suffer from major usability hurdles that foster insecure practices and undermine cybersecurity. Passkeys were introduced to address these issues, however, adoption remains low. Digital nudges offer a promising way to accelerate passkey adoption, yet research lacks empirical insight about when to nudge and which nudge types and designs are most effective. We therefore employed a mixed-methods approach to examine the impact of nudges on passkey adoption across five touchpoints in the digital user journey: During registration, login, account recovery, while in the settings menu, and during user activity. First, we conducted 15 expert interviews to identify candidate nudges and their design principles. We evaluate these nudges in a randomized controlled trial (RCT) with 3,680 participants on a commercial healthcare platform. Our results indicate that digital nudges can significantly increase passkey adoption when applied at the right touchpoints, encouraging users to move beyond passwords.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Authentication, Passkey, Password, FIDO2, Security, User Study, Field Study, Accounts

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CHI '26, April 13–17, 2026, Barcelona, Spain
© 2026 Copyright held by the owner/author(s). Publication rights licensed to ACM.
https://doi.org/XXXXXXX.XXXXXXX

ACM Reference Format:
Tobias Reittinger, Magdalena Glas, and Günther Pernul. 2026. Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption. In *Proceedings of CHI '26*. ACM, New York, NY, USA, 17 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Passwords remain the most widely used authentication mechanism and provide strong cryptographic security [6, 49]. However, users are expected to create high-entropy passwords [50, 84], keep them unique [32, 68], and remember them across an ever-growing number of accounts [24, 96]. These usability burdens foster insecure practices, including short or easily guessed passwords [24], cross-site reuse [13], and recording passwords in notes [38], thereby undermining security. Further, contrary to NIST guidance [88], many organizations still mandate periodic password expiration, which induces minor, predictable changes [73, 74]. Two common mitigations are Password Managers (PMs), which generate unique, high-entropy passwords while requiring users to remember only a single master password [85], and Multi-Factor Authentication (MFA), which adds an additional factor, typically an one-time password (OTP) [72]. Yet both introduce their own usability burdens: PMs impose installation overhead, migration effort, and remediation of weak legacy credentials [44, 69], whereas MFA adds authentication friction and recovery hurdles yet may remain susceptible to phishing [72], contributing to low adoption [12, 69]. Consequently, password-centric authentication continues to present a major attack surface [60].

The Fast IDentity Online (FIDO) Alliance developed FIDO2, a passwordless authentication standard that replaces passwords by creating a unique pair of cryptographic keys for each site, one private key stored securely on the user's device and one public key stored by the service. This way, FIDO2 provides phishing-resistant credentials, mitigates the insecure behaviors passwords encourage by eliminating password creation and memorization, and offers built-in MFA via on-device biometrics or a device passcode [23].

Nevertheless, a key limitation is that FIDO2 credentials are device-bound, complicating portability and account recovery [57, 66]. Passkeys address this by extending FIDO2 with multi-device credentials that synchronize across a user's devices, delivering higher usability and security than passwords [100]. Still, password-based authentication remains dominant [81]. A crucial challenge, therefore, is motivating users to adopt passkeys in practice.

One way to guide user behavior is through digital nudges, interventions that preserve choice [90], which have shown promising results in other cybersecurity domains [4, 83, 101]. Although the FIDO Alliance and vendors have begun to incorporate nudges into passkey adoption, these efforts are largely unstructured and sparsely evaluated [22, 37, 46, 71]. We identified two main challenges that hinder passkey adoption: First, it has not yet been empirically evaluated through a large-scale study at which touchpoints in the digital user journey users are inclined to adopt passkeys. Second, as vendors apply different and non-uniform nudges, it is unknown which nudge types and designs can encourage passkey adoption. Thus, we pose the following research question:

RQ *How can digital nudges improve passkey adoption?*

To address this research question, we conducted a mixed-methods study structured around user touchpoints, defined as specific stages in the digital journey where passkey adoption can occur. We draw on four touchpoints from the FIDO Alliance: *Registration*, *login*, *recovery*, and *settings*. To also reach users who rarely re-authenticate, we add a fifth touchpoint, *activity*, which targets users during actions within an application. Together, these five touchpoints organize both our qualitative and quantitative exploration. First, we conducted 15 semi-structured expert interviews to identify candidate digital nudges and derive design principles for fostering passkey adoption across these touchpoints. Second, we evaluated the resulting nudges on a commercial healthcare platform through a randomized controlled trial (RCT) with 3,680 participants, spanning all five touchpoints, to estimate their effects on passkey adoption. In the RCT, we focus on three evaluation questions: **(EQ1)** which nudges are most effective at each touchpoint, **(EQ2)** which touchpoints offer the highest overall potential for adoption across nudges, and **(EQ3)** whether nudge effects vary by touchpoint. In sum, we offer the following contribution:

- We designed and evaluated practical nudges across five touchpoints, identifying that experts cautioned against negative password framing, which could undermine trust in authentication and perceived security.
- Nudges could significantly increase passkey adoption at all touchpoints except *activity*, with the largest effects for the two nudges *choice default* and *salience*.
- Users were most likely to switch from passwords to passkeys at *recovery* and *registration*, pinpointing these as high-leverage moments for intervention.
- Nudges increased overall adoption but did not significantly raise the *success rate*—the proportion adopting among those who interacted—suggesting that nudges capture attention while additional factors (e.g., usability) shape final adoption.

2 BACKGROUND AND RELATED WORK

In this section, we review the background on passkeys (Section 2.1) and digital nudges (Section 2.2), and discuss related work (Section 2.3).

2.1 Passkeys

Passkeys are a passwordless authentication method that replaces the shared secrets of passwords with origin-bound public–private key pairs [21, 42].

Passkeys build on the FIDO2 standard: Relying parties (e.g., the website the user registers on) store only a public key, while the private key remains on the authenticator [42]. Sign-in requires *user presence*, a deliberate physical gesture indicating user consent to complete the operation with the authenticator [42, 57]; the relying party can also require local *user verification* via biometric or PIN when supported [42, 48, 51, 57]. Authenticators are either *roaming* security keys that work across devices [14, 20, 77, 82] or *platform* authenticators built into phones and laptops [42]. FIDO2 platform credentials were device-bound, which required enrollment on each device and complicated portability and recovery [66, 100]. To improve portability, Apple, Google, and Microsoft introduced passkeys as multi-device (synchronized) FIDO2 credentials, allowing the same credential to be used across a user's devices and reducing repeated enrollments, while enlarging the security perimeter because device ecosystems and synchronization must be protected [19, 39, 52].

Compared to passwords, passkeys do not require password creation and memorization, eliminating insecure coping such as predictable creation, reuse, and unsafe storage, and mitigate shared-secret attacks including phishing and credential stuffing [8, 13, 16, 51]. Because the private key never leaves the authenticator and authentication is origin-bound, passkeys provide phishing-resistant authentication without relying on users to detect spoofed sites [42, 57]. Despite these advantages, usage remains limited and many users still rely on passwords [81]. Digital nudges offer a promising approach to encourage passkey adoption.

2.2 Digital Nudges

In cybersecurity, users often deviate from commonly recommended practices [1, 24, 35]. Some choices reflect boundedly rational cost-benefit trade-offs under constraints such as limited time and attention, adoption friction, and uncertainty about risks and payoffs [5, 25, 35]. Other choices are shaped by systematic cognitive biases and heuristics, such as loss aversion and framing effects, that can lead to departures from normative models or even from individuals' stated goals [3, 34, 45, 92, 93]. These explanations are not mutually exclusive and likely vary by context.

These insights raise the question of how decision environments might be structured to guide humans towards more security-aligned behavior. One approach is the use of *nudges*, interventions that steer behavior without restricting options or materially changing incentives [90]. Nudging builds on psychological theories of shaping decision environments to reduce avoidable friction and make relevant trade-offs more salient, thereby supporting choices that better align with users' own preferences and long-term objectives while preserving freedom of choice [89, 90]. When implemented

in digital environments, these interventions are referred to as *digital nudges* [97]. Following Baumer et al. [4], we list 13 digital nudges from the literature review and classification by Jesse and Jannach [40]. These serve as the foundation for our expert interviews on promising digital nudges to encourage passkey adoption.

Decision Information. This category adjusts information for decision-makers without altering their choices [62].

- *Translation* reduces ambiguity and simplifies complex information, making it easier for users to understand and act upon [86, 87].
- *Salience* draws attention to certain options by enhancing their visibility, while downplaying less desirable options [11, 41, 87].
- *Visibility* makes information accessible and readily visible, using mechanisms like disclosure [36, 87], explanations [41], feedback [11, 91], or warnings [36, 55].
- *Phrasing* influences decisions by contextualizing information, such as through anchoring [43, 87] or framing options [11, 80].

Decision Structure. This category focuses on reshaping the organization of choices to guide decision-makers [62].

- *Range or composition* adjusts scale [41], breaks decisions into stages [59], reorders options [87], or partitions categories to highlight specific attributes [62].
- *Choice default* sets automatic enrollments [11], prompts active choices [62], and preselects options [55, 86].
- *Option consequences* links choices to minor social or personal consequences [62], using small benefits [62] or micro-incentives [36].
- *Effort* adjusts the effort required for options, for example, by altering ease [86, 87] or adding subtle friction to influence user choices [11].

Decision Assistance. This category includes mechanisms that support decision-makers in achieving their goals [62].

- *Reminders* keep users focused by reinforcing their goals [9, 86, 87], social expectations [62], or situational relevance [9].
- *Commitment facilitation* promotes follow-through by automating tasks [9], prompting intentions [36], and encouraging public commitment [11].

Social Decision Appeal. This category addresses the social and emotional dimensions of decision-making [40].

- *Messenger reputation* leverages credibility by anticipating user errors [41, 97] and building on the positive impression associated with the messenger [80].
- *Social reference* encourages alignment with popular opinions [28], conformity to group norms [61, 87], or comparing actions to those of others [36].
- *Empathy instigation* reflects users' actions [11], invokes reciprocity [11], appeals to a sense of responsibility [87], and provides positive reinforcement [9].

2.3 Related Work

Prior work finds that FIDO2/passkeys can yield higher perceived usability, acceptance, and security than passwords [18, 57, 66]. These advantages are most pronounced on mobile and when using platform authenticators (i.e., on users' existing devices) rather than external security keys [63, 100]. Nonetheless, comparative evaluations of web authentication schemes emphasize that possession-based approaches also introduce inherent drawbacks and new failure modes (e.g., device availability and loss/theft, provisioning and recovery burdens, and challenges on shared devices), which can offset benefits in some settings [8]. Consistent with this, users remain concerned about account recovery [18, 57, 66] and multi-device access of FIDO2 [100]. Adoption is further hindered by misconceptions about how biometrics are stored and used [53, 65] as well as entrenched password habits [18]. In a large-scale field, Reittinger and Pernul show that while passkeys are rated more usable and acceptable than passwords with 2FA, adoption is hindered by password habits, inexperience, and misconceptions, and longer-term use exposes cross-platform sync and password-manager friction [75]. Overall, the literature suggests that passkeys offer compelling security and usability benefits in many common scenarios, but adoption and real-world suitability are context-dependent, shaped by ecosystem maturity, recovery and synchronization support, and users' mental models and constraints. Targeted and touchpoint-specific nudges that increase salience, correct misconceptions, and disrupt default password use may help users move beyond passwords.

Research on digital nudging in security contexts shows that timely, salient, and tailored nudges can shift behavior. For example, Sharma et al. [83] demonstrate measurable improvements in everyday security practices via priming, Baumer et al. [4] show that choice defaults can drive substantial behavior change during access reviews, and Ebert et al. [17] find that concise, prominent privacy notices raise user awareness. This effect extends to authentication, where nudges translate into adoption at scale: Golla et al. [31] report large gains from optimized defaults and reminders, Lyastani et al. [30] document that many top-ranked websites nudge users to set up recovery options, while Kennison [47] cautions that simple message nudges may be insufficient for more effortful tasks such as creating strong passwords. Within the FIDO2 ecosystem, Lassak et al. [53] show that targeted prompts can mitigate biometric misconceptions, whereas Amer et al. [2] find that technical video explanations alone do not increase adoption intention. For passkeys, the FIDO Alliance UX guidelines [22] recommend making passkey information salient and visible, and a Microsoft white paper by Ranjit and Bingham [71] advocates highlighting passkeys' security and speed benefits at key decision points. Overall, digital nudges can guide security behavior, but effectiveness depends on careful design and tailored fit. Relative to this literature, our work contributes a large-scale RCT that systematically designs and quantitatively evaluates multiple nudges (including novel ones) across five touchpoints, yielding actionable recommendations for increasing passkey adoption.

3 QUALITATIVE METHOD: EXPERT INTERVIEWS

To address our research question, we employed a mixed-methods approach. First, drawing on the FIDO Alliance guidelines [22], we identified five key touchpoints for passkey adoption (Section 3.1). We then conducted 15 expert interviews to identify potential digital

nudges for each touchpoint, evaluate their practical applicability, and understand how industry professionals would design them. We chose interviews over a survey because they allow for richer, more nuanced insights and follow-up questions when exploring complex design decisions. The methodological approach for conducting these interviews is outlined below (Section 3.2). Finally, we describe the ethical considerations (Section 3.3). Insights from these interviews informed the selection and design of the nudges at the five touchpoints, thereby forming the basis for the quantitative user study described in Sections 5 and 6.

3.1 Selection of Touchpoints for Passkey Adoption

The FIDO Alliance enumerates steps for potential passkey adoption [22], which we map to four touchpoints: *registration*, *login*, *recovery*, and *settings*. Because authentication sessions are often long-lived [29], users may seldom re-authenticate and may also rarely visit *settings*. We therefore introduce *activity* as a fifth touchpoint to surface adoption opportunities during actions within the application. These touchpoints guided our discussions on digital nudging in the expert interviews and were each examined separately in the user study. They cover both the initial *choice* of new users between passwords and passkeys, and the option for existing users to *switch* from passwords to passkeys (see Table 2). Adapted from the FIDO Alliance [22], the touchpoints are:

- *Registration:* During account registration, new users can choose between passwords and passkeys.
- *Login:* For users with passwords, the login process provides a touchpoint to switch to passkeys.
- *Recovery:* A password reset for account recovery provides another touchpoint to switch to passkeys.
- *Settings:* When navigating the settings menu of an application, users can opt to switch to passkeys.
- *Activity:* User activities within an application (e.g., shopping), offer a touchpoint for passkey adoption.

3.2 Interview Method

In the following, we will detail the methodology of the expert interviews. The interviews were conducted between July 2024 and January 2025 and lasted between 43 and 106 minutes, averaging 69 minutes with a median of 65 minutes.

Pilot Study. We conducted a pilot with three participants prior to the expert interviews to pretest the questionnaire. Their feedback prompted revisions to wording and sequence to improve clarity and flow. Because the instrument was refined after the pilot, those data were excluded from the analysis.

Procedure. The interviews were conducted virtually via Microsoft Teams or Zoom. With participants' consent (see Section 3.3), we recorded the audio of each session to ensure accurate transcription.

The interviews were organized into four parts and followed the cognitive interviewing methodology [99]. In the *first part*, we provided experts with an overview of passkeys and the five identified touchpoints, then discussed their organizational experiences with this authentication method. We explored current industry practices by asking how they would raise awareness of passkeys and encourage adoption at each touchpoint. These insights informed the design of the control group in the user study. By discussing existing practices before introducing digital nudges, we aimed to minimize potential bias in responses.

In the *second part*, we introduced the concept of digital nudges and gathered information on the experts' experience with UI/UX design, development, and nudging strategies. Following Baumer et al. [4], we iteratively presented each of the 13 digital nudges proposed by Jesse and Jannach [40] in detail. For each nudge, we discussed its anticipated impact on passkey adoption at each touchpoint and elicited perspectives on practical implementation and design considerations. Experts also rated the expected effect of each nudge for each touchpoint on a 5-point Likert scale. This phase was critical for selecting and designing the digital nudges used in the user study.

The *third part* gathered demographic information about the participants and their organizations.

In the *fourth part*, each participant could select a nonprofit organization (NPO) to which we would donate €20 on their behalf as an incentive. Additionally, we inquired if they could refer other potential participants for the study. The complete interview guidelines are provided in Appendix A.1.

Recruitment and Participants. To thoroughly assess digital nudges that can promote passkey adoption and be practicable for organizations, the target group included both developers, designers, and cybersecurity decision-makers. While prior experience with passkeys and digital nudges was preferred, it was not mandatory. Due to the limited availability and challenging access to this specialized group, we employed multiple recruitment strategies. These included leveraging professional networks, our institution's alumni network, industry contacts, and requesting referrals from interview participants. Each participant was screened to ensure they met the criteria of our target group. We successfully recruited 15 experts from a diverse array of sectors, positions, organizational sizes, and levels of experience. A detailed overview of participants' experience and organizational backgrounds is provided in Table 1.

Coding and Analysis. We transcribed the audio recordings of the interviews using Microsoft Word and stored the resulting transcripts locally. Coding was conducted using a flexible coding framework [15]. Any conflicts in interpretation were resolved collaboratively. To strengthen our analysis, we considered codes from previous studies on digital nudges and passkeys [4, 54, 57, 100]. We published the codebook as open-source (see Availability).

Selection and Design of Nudges. For each touchpoint, we selected three digital nudges (alongside a control group) based on experts' anticipated impact on passkey adoption, practicality, and prior literature on nudges [7, 36, 40]. Designs were based on the expert interviews. Consistent with Thaler and Sunstein's claim that there is no neutral design [90], the control groups are not a neutral baseline but reflect the *industry status quo* identified in those interviews. Nonetheless, we sought to minimize bias in the control groups.

3.3 Ethical Considerations

Ethical considerations are integral to our research. Before conducting the study, our research methodology was approved by the

Table 1: Summary of interview participants and their organizations. For anonymity reasons, we provide ranges.

	Experience			Participant		Organization		
ID	**UX**	**Nudges**	**Passkeys**	**Position**	**Exp.**	**Sector**	**Size**	**CC**
E1	○	●	○	CISO	1-5	Consulting	250-999	DE
E2	●	○	●	Developer	10-20	IT services	1-9	AT
E3	●	●	●	Developer	5-10	IT services	50-249	DE
E4	●	○	○	Consultant	5-10	IT services	1-9	DE
E5	○	○	●	CISO	10-20	Finance	250-999	DE
E6	●	●	○	Developer	5-10	IT services	50-249	DE
E7	●	●	○	Developer	5-10	IT services	1-9	DE
E8	●	○	○	Consultant	1-5	Consulting	1-9	DE
E9	●	●	○	UX Designer	+20	Consulting	10-49	DE
E10	○	○	●	Manager	1-5	Marketing	50-249	DE
E11	●	●	○	UX Designer	+20	Marketing	10-49	AT
E12	○	○	●	Manager	5-10	Government	+1,000	DE
E13	●	●	○	UX Designer	10-20	Marketing	10-49	DE
E14	●	○	○	UX Designer	1-5	Fashion	+1,000	DE
E15	●	○	●	Developer	10-20	Technology	50-249	DE

UX: User Experience. **Exp.:** Experience. **CISO:** Chief Information Security Officer. **CC:** Country code. **DE:** Germany. **AT:** Austria.

German Association for Experimental Economic Research e.V, and we obtained an Institutional Review Board (IRB) certificate[1]. We detail the ethical considerations for our studies, along with the compensation approach, in line with the recommendations of Pater et al. [67]. At the start of the interviews, participants were asked for their consent to data recording and processing and were informed about their right to withdraw consent at any time. To protect participants' privacy, we transcribed the interviews and then deleted the recordings. Furthermore, we removed any identifying details related to participants' identities or their affiliated organizations from the transcripts. Accordingly, demographic data is reported in ranges, as shown in Table 1. Given that most interview participants were high-earning experts, we chose not to offer direct compensation. Instead, we incentivized participation by donating €20 per participant to an NPO of their choice from a list of verified NPOs,[2] resulting in a total donation of €300. We also committed to sending participants the study's findings. Ethical considerations of the quantitative user study are detailed in Section 5.2

4 QUALITATIVE RESULTS: EXPERT INTERVIEWS

In this section, we first present the qualitative results from the expert interviews on digital nudges aimed at encouraging passkey adoption (Section 4.1). We then describe the selection (Section 4.2) and the design (Section 4.3) of the nudges and the control group for the user study.

4.1 Digital Nudges for Passkey Adoption

Following Jesse and Jannach [40] and Baumer et al. [4], we discuss which digital nudges the interviewees consider most promising for encouraging passkey adoption. For readability, we describe the median anticipated effect by the interviewees for each nudge and touchpoint and visualize the results in Table 2.

Translation: The interviewees emphasized that effective *translation* requires speaking the users' language. As E7 noted, *"People know 'password,' but 'passkey' is a new term; a simple explanation that lands the concept is crucial."* (E7) Accordingly, they suggested that briefly clarifying what "passkeys" are and what they are for could positively influence most touchpoints, except for *activity*. At this touchpoint, the interviewees argued that even a simplified passkey message is unlikely to capture attention or prompt users to interrupt their activity, and thus, no effect is expected.

Salience: Assuming many users are unfamiliar with passkeys, the interviewees expect highlighting explanations or benefits of passkeys as a promising approach. However, they consider emphasizing interactive options even more effective. This can be achieved by making buttons for setting up passkeys more prominent, or by reducing the salience of the option to continue using passwords. The interviewees anticipate that users will perceive the highlighted option as the more advantageous choice, while the less prominent option may seem less ideal. The use of *salience* is expected by the interviewees to have a strongly positive effect across all touchpoints.

Visibility: Since the interviewees assume that most users are unfamiliar with passkeys, they emphasize the importance of clearly communicating the benefits of passkeys and explaining how to use them to ensure user understanding. Although presenting the drawbacks of traditional passwords may also be beneficial, it is considered impractical (see Section 4.3). The interviewees consider

[1] IRB certificate: https://gfew.de/ethik/NAPzzShc
[2] Verified NPO list is available at: https://www.dzi.de/spendenberatung/spendenauskunfte-und-information/hilfsorganisation-finden/

Table 2: Median anticipated impact of digital nudges [40] on passkey adoption at each touchpoint, as rated by the interviewed experts, with higher values indicating a greater anticipated effect [4].

	Choice	Switch			
Nudges / Touchpoints	**Registration**	**Login**	**Recovery**	**Settings**	**Activity**
Translation	4	4	4	4	3
Salience	**5★**	**5★**	5	**5★**	**5★**
Visibility	**5★**	**5★**	**5★**	**5★**	**5★**
Phrasing	4	4	5	4	4
Range or composition	4	4	4	4	3
Choice default	**5★**	**5★**	**5★**	1	1
Option consequences	2	2	2	2	2
Effort	4	4	**5★**	4	3
Reminders	4	4	5	4	**5★**
Commitment facilitation	3	3	3	3	3
Messenger reputation	3	3	3	3	3
Social reference	5	5	5	**5★**	5
Empathy instigation	3	3	4	3	3

Note: ★ Nudge was selected for the corresponding touchpoint in the user study.
The 5-point Likert scale spanned from strongly negative 1 over neutral 3 to strongly positive 5.

the visibility of information unfamiliar to users as strongly positive across all touchpoints, as it effectively helps users grasp the advantages and functionality of passkeys.

Phrasing: The interviewees view framing effects as a practical approach to increasing passkey adoption, anticipating a positive effect across all touchpoints, with a particularly strong positive effect for the *recovery*. There, the interviewees believe that the negative experience of account recovery makes users more receptive to framing effects that emphasize how passkeys can prevent these issues.

Range or composition: The interviewees consider deliberate option sorting as a method to increase passkey adoption. For example, they expect users to click more frequently on the first option in a vertical arrangement and the option on the right in a horizontal arrangement. The interviewees anticipate positive order effects at all touchpoints except N5, where no effect is expected, as the order change is unlikely to be noticeable during active user engagement.

Choice default: The interviewees anticipate a strong effect from defaults, emphasizing that users rarely change standard security settings. As E6 put it, *"Default is the strongest nudge: If passkeys are the default, users must actively choose the password instead. The tricky part is avoiding surprise [...], if someone hits 'Cancel,' the interface should fall back to the neutral baseline."* (E6) While users can opt out, doing so requires effort, making *choice default* a promising nudge. However, the interviewees assess its effectiveness differently across touchpoints. When passkeys are offered as the default authentication method, most interviewees expect a strongly positive effect on adoption at *registration*, *login*, and *recovery*, because users already anticipate configuring or using authentication and are thus likely to follow the default. At the same time, they cautioned that unfamiliar users may cancel if the default feels unexpected. Therefore, they stressed transparent default disclosure and a low-friction fallback to password setup. For *settings* and *activity*, the interviewees predict a strongly negative effect, as defaults that imply changing authentication in contexts where users do not expect it may feel intrusive, leading users to abandon the process and potentially discouraging future adoption.

Option consequences: The interviewees were skeptical about the effectiveness of this nudge for increasing passkey adoption. As E2 noted, *"Threats or penalties, 'we'll lock you out in ten days', won't nudge toward passkeys; they mostly alienate users."* (E2) Accordingly, they anticipated a negative effect across all touchpoints. While micro-incentives might in principle encourage passkey use, they were viewed as impractical, and framing continued password use in terms of social consequences or penalties was expected to backfire by discouraging authentication altogether rather than shifting users to passkeys.

Effort: The interviewees anticipate a positive effect from increasing effort at *registration*, *login*, and *settings*. As E6 suggested, *"A small confirmation, such as 'Are you sure you want to use a password?' could just add enough effort to make [users] reconsider without being heavy-handed."* (E6) While they do not see a practical way to simplify passkey adoption without modifying the passkey protocol itself, they believe that adding minor friction to password use (e.g., a confirmation dialog) could prompt users to reconsider and choose passkeys instead. At *recovery*, where users have just experienced difficulties with passwords, the interviewees expect an even stronger positive effect. No effect is anticipated at *activity*, as the interviewees consider it infeasible to meaningfully increase the effort of password use in this context.

Reminders: The interviewees expect reminders to have a positive effect on passkey adoption across all touchpoints, with a strongly positive effect anticipated for *recovery* and *activity*. As E14 noted, *"For reminders, I'd use a pop-up [...]. They actually see it. Email also costs nothing, but it's often not read."* (E14) During account recovery, users who have just had a negative experience

with passwords may be especially receptive to a timely reminder that highlights the benefits of passkeys. During activity, the interviewees expect that a push notification or pop-up is more likely to be noticed than passive channels, increasing engagement with the passkey prompt.

Commitment facilitation: The interviewees believe that a pre-commitment, such as committing in advance to adopt passkeys, would have no effect on actual passkey adoption, as only participants already inclined to set up passkeys would engage in such a commitment. Additionally, implementing a public commitment to adopt passkeys is considered impractical.

Messenger reputation: The interviewees found it challenging to devise an appropriate scenario for this nudge. They noted that having a well-known personality endorse passkeys would not represent a true messenger effect but would instead align more closely with a *social reference*. The only feasible option they considered was using the company's name as a messenger; however, the interviewees believe this would have no measurable impact on passkey adoption for all touchpoints.

Social reference: The interviewees identified two scenarios for this nudge. First, a known person recommending passkeys, though this is challenging to implement practically, as the individual would need to be widely recognized by most users. Second, indicating the number of users who already use passkeys, thus presenting passkeys as a widely used authentication method. Since users tend to favor aligning with the majority, the interviewees expect a strong positive effect from the latter scenario across all touchpoints.

Empathy instigation: Unlike passwords, where emoji-based password meters using *empathy instigation* can indicate weak or strong passwords as users type [27], passkey adoption is considered a binary decision. The interviewees expect no effect from *empathy instigation* across all touchpoints except for *recovery*. At this touchpoint, the interviewees suggest that a message encouraging users not to repeat the usage of a password could have a positive impact.

Key Results: Digital Nudges for Passkey Adoption

(1) High-potential nudges: **Salience**, **visibility**, and **social reference** across touchpoints.
(2) Context sensitivity: **Choice defaults** and **effort** work best where users expect authentication.
(3) Low/negative impact: **Option conseq.** seen as counterproductive; **commitment** and **messenger** negligible.

4.2 Selection of Digital Nudges for the User Study

At each of five touchpoints, we investigated three nudges and a control group. Nudge selections were based on interview results and prior literature.

For the *registration* and *login*, we chose *salience*, *visibility*, and *choice default*. Both *visibility* and *choice default* are among the nudges with the highest average effect size [36]. Given that the interviewees indicated limited user knowledge about passkeys, we opted to highlight information on passkeys (*salience*) rather than displaying choices made by other users (*social reference*).

For the *recovery*, we examined *visibility*, *choice default*, and *effort*. Although the interviewees anticipated strong effects from several nudges, we prioritized these three due to their high reported effect sizes in the literature [36].

For the *settings*, we selected *salience*, *visibility*, and *social reference*, as these were the only nudges that the interviewees anticipated to have a strong positive impact on passkey adoption.

For the *activity*, we selected *salience*, *visibility*, and *reminders*. The interviewees anticipated similar effects for *reminders* and *social reference*, and the literature also reports comparable average effect sizes for both [36]. However, since *social reference* is similar in UX design to *salience* and *visibility*, we chose *reminders* as a distinct nudge mechanism that is likely more noticeable during user activity.

Key Results: Selection of Digital Nudges for User Study

(1) **Registration/Login**: Chose *salience*, *visibility*, *choice default*, as interview expectations match prior work.
(2) **Recovery/Settings**: *Recovery* adds *effort*; *settings* investigate *social reference*.
(3) **Activity**: Selected *reminders* to provide a distinct, noticeable mechanism during ongoing tasks.

4.3 Design of Control Groups and Selected Nudges

We discussed the design of all 13 digital nudges with the interviewees; however, due to length restrictions, we will report only on the discussion of the selected nudges. The brand color of the healthcare platform is a medium-light shade of blue, which we used as the primary highlight color in the designs. As a secondary color, we used a light gray. The design of the selected nudges is displayed in Figure 2.

General Insights: Across all nudges and touchpoints, the interviewees emphasized the importance of avoiding negative wording or framing related to passwords. As E7 cautioned, *"Keep the wording positive. 'Passwords are insecure' sounds negative and can undermine trust in the site."* (E7) They advised against statements that portray password-based authentication as insecure or vulnerable (e.g., to phishing attacks), because this could trigger broader doubts about the service's security, lead users to abandon the process, and ultimately harm user retention and the organization's reputation. At *settings*, the interviewees recommended displaying a primary-color dot on the settings button across the control group and all nudge conditions, following industry practices [98], to ensure users notice passkeys as a new feature. At *settings* and *activity*, they further suggested offering only the option to create a passkey and omitting the option to continue using a password, since users who are not interested can simply ignore the passkey option (except for *reminders*, where users receive an explicit prompt via pop-up).

Control Groups: For the control groups, we used results from the *first part* of the interviews, conducted before introducing digital nudges, to minimize bias. The interviewees recommended placing the passkey and password buttons side by side in the secondary color and randomizing their order. In *registration* and *recovery*, where users lack a (working) authentication method, both options should be presented without any explanatory text to avoid biasing

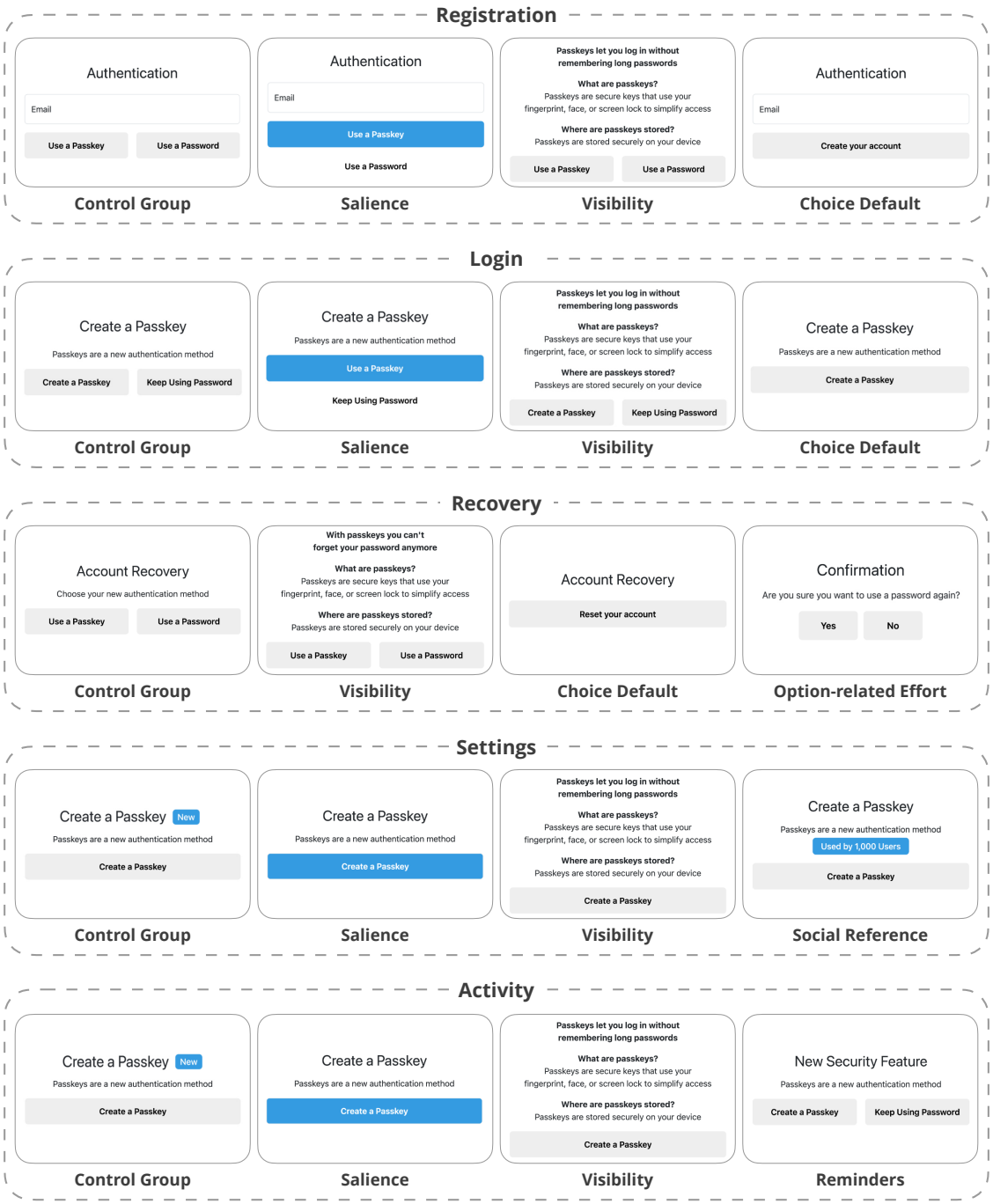


Figure 2: Design of selected nudges and control groups for all five touchpoints in the user study.

the choice. By contrast, in *login*, *settings*, and *activity*, where users already have established a password previously, the interface should include a brief note stating that passkeys are a new authentication method, without describing benefits or functionality. This minimal context helps users understand why the additional option is being shown while limiting potential bias in their decision. For *settings* and *activity*, the interviewees also recommended displaying a "New" badge to signal that the option has just become available; otherwise, users might overlook the feature.

Salience: The interviewees suggested highlighting the passkey button in the primary color at full width, with the password button placed below, without a background. This approach follows industry standards, as seen in the Uber app [94].

Visibility: They suggested extending the control group by adding informative details about passkeys, including the primary benefit (no need to remember passwords), a brief explanation of what passkeys are, and information on where they are stored.

Choice default: The interviewees recommended presenting a single secondary-colored button that, by default, prompts users to create a passkey. This was extensively debated, as this design inherently yields a 100% *interaction rate* for *choice default*. However, the interviewees noted no viable alternative to defaulting the decision to passkeys. If users cancel, the interface should revert to the control-group layout, offering options to create either a password or a passkey.

Effort: They advised extending the control group by adding a confirmation dialog after users clicked the password button, asking if they were sure they wanted to use a password. The "yes" and "no" options would appear in randomized order and increase the effort required to continue with a password slightly.

Reminders: The interviewees considered email or SMS reminders impractical, as users have ideally learned to treat such notifications as potential phishing attempts. Instead, they suggested a pop-up prompt informing users about passkeys as a new authentication method, with options to create a passkey or continue using passwords, displayed in randomized order, and both buttons in the secondary color.

Social reference: The interviewees recommended highlighting that a substantial number of users already use passkeys. After consulting the industry partner on the number of passkey users, we displayed the message, "Used by 1,000 Users", next to the option to adopt passkeys.

Key Results: Control Group Design and Selected Nudges

(1) **Neutral baselines**: Side-by-side, randomized options; minimal context to minimize bias.
(2) **Nudge implementations**: *Salient* button; *visible* information; *default* initiation; *effort* confirm dialog.
(3) **Tone and trust**: Avoid disparaging password language to maintain trust in the authentication process.

5 QUANTITATIVE METHOD: USER STUDY

Based on the results of our qualitative study, we examined the real-world effects of these nudges on passkey adoption in a user study on a commercial healthcare platform. We conducted five RCTs, one per touchpoint, involving 3,680 participants in total. Each touchpoint comprised four groups, three nudge groups, and one control, resulting in 20 groups. The methodology of the user study, which was conducted between February and July 2025, is described in the following (Section 5.1), including the ethical considerations specific to the user study (Section 5.2).

5.1 User Study Design and Procedure

Evaluation Questions. In order to evaluate the effectiveness of different nudging strategies in promoting passkey adoption, the study focused on three evaluation questions (EQs). These questions were designed to explore which nudges perform best in specific contexts, whether certain touchpoints in the authentication journey are more conducive to behavior change, and how the effectiveness of nudges may differ depending on when and where they are applied. First, we investigate the relative effectiveness of nudges within each individual touchpoint of the digital user journey:

EQ1. Which nudges are most effective at each individual touchpoint?

Second, we evaluate which touchpoints in the digital user journey are generally more receptive to nudging, regardless of the specific nudge used:

EQ2. Which touchpoints offer the highest overall potential for adoption?

Third, we assess whether the effectiveness of a given nudge depends on the stage of the process where it is implemented, indicating interaction effects between nudge type and touchpoint in the digital user journey:

EQ3. Do the effects of nudges vary depending on the touchpoint at which they are applied?

Together, these questions aim to provide an understanding of when and where nudges are most likely to drive users to adopt passkeys.

Recruitment and Sample Description. The first author is the owner and lead developer of a healthcare appointment booking service in Europe, available as a native iOS, Android, and web application. This **"platform"** was used to recruit participants and run the user study. The author implemented the selected digital nudges into the production system, building on an existing passkey functionality that uses platform authentication as the primary method (with roaming authentication disabled). The implementation is published as open source (see Availability).

Before the main study, we conducted a pilot with 14 participants to identify technical issues and ambiguities. Participants tested all nudges and control groups at the five touchpoints and completed the consent form in the overlay. Feedback led to minor adjustments, and pilot data were not included in the main study.

To incentivize participation, users could enter a raffle for a €50 gift card. They were informed through an overlay explaining the study's focus on authentication interactions (without explicitly mentioning passkeys to avoid bias) and outlining data collection.

An a priori power analysis indicated that 189 participants per condition were needed to detect a medium effect ($h = 0.3$) with 80% power at $\alpha = .001$. Since the smallest group (recovery) had 184 participants, all other groups were trimmed to match, yielding a

balanced sample of $N = 3680$ with only a marginal loss of power. Eligible users were over 18 and had not yet activated passkeys. New users were targeted at the *registration* touchpoint, while existing users were targeted at other touchpoints. No participants withdrew consent.

Data Collection Procedure. After recruitment, participants were randomly assigned to one of the nudge conditions at the respective touchpoint. Randomization was handled by the platform backend using uniform allocation. Each participant was eligible for exactly one assignment (one condition at one touchpoint), and the system prevented participation across multiple conditions or touchpoints. At *registration*, new users could choose between a password or a passkey. At the other four touchpoints, participants were offered the option to add a passkey, consistent with the FIDO Alliance's UX guidelines [22]. The design specifics for each group are detailed in Section 4.3. Participants were then asked to indicate prior passkey experience and level of education in a short survey. Active consent to data processing, including access to *age* and *gender* information from user profiles, was required. Only data from users who completed both consent and the survey were analyzed.

The survey was presented at different moments depending on the touchpoint: immediately after authentication or recovery for *registration*, *login*, and *recovery*; after exiting the settings tab for *settings*; and after interaction with the prompt or after 60 seconds for *activity*, assuming further engagement beyond this time was unlikely.

Measures. We analyze three binary outcomes in the passkey setup process: **Interaction rate**, the proportion who interacted with the passkey option (measured from click logs); **Adoption rate**, the proportion who completed adoption (measured via the success callback of the native passkey dialog); and **Success rate**, the proportion who adopted among those who interacted (*adoption rate* / *interaction rate*).

Touchpoint and nudge are the independent variables. *Touchpoint* indicates the stage of the digital journey (*registration*, *login*, *recovery*, *settings*, *activity*). *Nudge* represents the intervention type (*control*, *salience*, *visibility*, *choice default*, *effort*, *reminders*, *social reference*). For each touchpoint, three nudge conditions were selected based on a preceding interview study. An overview of all conditions is provided in Figure 2 in the Appendix.

Analyses. For EQ1, we conducted pairwise proportion tests to compare *interaction*, *adoption*, and *success rate* for nudges within the same touchpoint, applying Bonferroni correction to adjust for multiple comparisons. EQ2 compared the overall effectiveness of different touchpoints. Because not all nudges appeared at every touchpoint, we used binomial logistic regression with nudge, touchpoint, and their interaction as predictors, estimating the effect of each touchpoint independent of nudge distribution. The *activity* touchpoint was used as the reference category for touchpoints, because it represents the weakest-performing condition regarding interaction and adoption rates. Using this baseline allows all other coefficients to be interpreted as performance improvements relative to the least effective touchpoint. For EQ3, we tested whether specific nudges worked better at certain touchpoints by including interaction terms in the logistic regression models for all three outcomes.

To reduce the risk of Type I error from multiple comparisons, a conservative significance threshold of $\alpha = .001$ was used for all main analyses. All analyses were conducted in R (version 4.5.1) [70].

5.2 Ethical Considerations

Before starting the study, we displayed a GDPR-compliant privacy notice and obtained informed consent. To protect participants' privacy, we minimized the collection of personal data and collected only necessary information for analysis, such as authentication-related interactions/outcomes and demographics. At the start of the study, participants were informed about the study's topic (interactions with authentication on the platform), its approximate duration (~3 minutes), the categories of data being collected, and the incentive offered.

Participation was voluntary. Participants could withdraw at any time by revoking consent via a dedicated button in the platform's settings tab. In that case, any data collected for the study would be deleted and excluded from analysis. No participant revoked consent or withdrew from the study. Separately, participants could discontinue the passkey setup flow at any point and continue using the platform with passwords. Discontinuing passkey setup was treated as a valid behavioral outcome of the study, contributing to the interaction rate but not the adoption rate.

To reduce potential bias in this field setting, the initial description did not emphasize passkeys or the nudging interventions. After completing the study (or withdrawing), participants were debriefed with detailed information about the study's objectives and methodology.

Given the brief time commitment and the study's public-good focus on promoting safer authentication, we offered entry into a €50 gift-card raffle. Participants were assured that they would remain eligible for the raffle even if they withdrew or revoked consent. Participants' access to healthcare remained unaffected: the study could be skipped with a single click, and appointments could still be scheduled outside the platform via phone or email. Finally, we conducted extensive pre-deployment testing of the digital nudge implementation. No issues or bugs were reported by participants during the study.

6 QUANTITATIVE RESULTS: USER STUDY

In this section, we first describe the demographics of the user study (Section 6.1). We then report the nudge comparison within each touchpoint (EQ1; Section 6.2), compare touchpoints (EQ2; Section 6.3), and analyze interaction effects between nudges and touchpoints (EQ3; Section 6.4). Finally, we summarize the user study results (Section 6.5).

6.1 Description of Demographics

The demographics of the sample divided by each touchpoint are provided in Table 5 in the Appendix. To ensure that observed effects were not confounded by demographic imbalances, we tested for differences in demographic characteristics across touchpoints. Chi-square tests revealed no statistically significant differences for gender, $\chi^2(4) = 0.88$, $p = .928$, age group, $\chi^2(28) = 12.47$, $p = .995$,

education level, $\chi^2(16) = 8.05$, $p = .947$, or prior passkey experience, $\chi^2(4) = 2.32$, $p = .677$. To this end, background variables were not considered in the analyses.

6.2 Nudge Comparison per Touchpoint (EQ1)

We examined the relative performance of nudges within each touchpoint by comparing *interaction*, *adoption*, and *success rates*, conducting pairwise comparison tests with Bonferroni correction (see Section 5). The results are reported in Table 3. The *choice default* nudge was excluded from *interaction rate* comparisons, as it was designed to automatically prompt interaction in all cases.

Interaction rates varied significantly between groups at each touchpoint. At the *activity* touchpoint, the *reminder* nudge led to significantly more interactions than the control condition. At *login*, both the *salience* and *visibility* nudges performed better than the control condition. For the *recovery* touchpoint, *visibility* yielded the highest *interaction rate*, exceeding the control condition. At *registration*, the *salience* nudge achieved the highest *interaction rate*, outperforming the control condition. In the *settings* context, both *salience* and *social reference* triggered significantly more interactions than the control condition.

Adoption rates revealed significant differences across nudges as well. At every touchpoint except *activity*, at least one nudge condition significantly outperformed the control. The *choice default* nudge consistently produced the highest adoption rates, followed by *salience* and *visibility* nudges, depending on the context. At *registration* and *login*, the *salience* and *choice default* nudges significantly outperformed the respective control condition. At *recovery*, the *choice default* and *visibility* nudges yielded significantly higher adoption rates than the control condition. Lastly, at *settings*, only the *salience* nudge was significantly more effective than the control condition.

In terms of *success rates*, we observed only minor differences between nudges. No consistent pattern of significant superiority emerged, indicating that while nudges can increase interaction and overall adoption, they may not substantially improve the success rate once interaction has occurred.

Key Results: Nudge Comparison per Touchpoint (EQ1)

(1) Nudges increased **interaction** across touchpoints; the most effective nudge varied by stage.
(2) For **adoption**, *choice default* led overall, with *salience* or *visibility* next, depending on context.
(3) **Success** showed no consistent improvement, indicating effects concentrate on attention and uptake.

6.3 Comparison of Touchpoints (EQ2)

To evaluate which stages in the user journey offer the greatest opportunity for promoting passkey adoption, we compared *interaction, adoption* and *success rates* across touchpoints using binomial logistic regression, controlling for nudge differences, using the touchpoint *activity* as the reference category.

Interaction rates were significantly higher at the *recovery* ($OR = 4.33$,$B = 1.47$, $SE = 0.23$, $z = 6.28$, $p < .001$) and *registration* touchpoints ($OR = 3.19$,$B = 1.16$, $SE = 0.23$, $z = 4.98$, $p < .001$) compared to *activity*, indicating that users at these stages, regardless of the nudge employed, are particularly receptive to nudging. In detail, users were four times (*recovery*) and three times (*registration*) more likely to interact with the passkey prompt than those at the *activity* touchpoint. No significant difference was observed for *settings* or *login*.

For *adoption rate*, the model revealed a significant effect for the *recovery* touchpoint, $OR = 3.03$, $B = 1.11$, $SE = 0.32$, $z = 3.42$, $p < .001$, indicating that users at *recovery* were about three times more likely to adopt a passkey than users at the *activity* touchpoint. The other touchpoints showed no significant differences.

For *success rates*, the analysis did not reveal any statistically significant differences between touchpoints, suggesting that once users chose to engage with the passkey prompt, the likelihood of completing adoption was relatively stable across touchpoints.

Key Results: Comparison of Touchpoints (EQ2)

(1) **Recovery** and **registration** were the most receptive stages for **interaction**.
(2) Only **recovery** showed a clear edge for **adoption**; other stages showed no clear advantage.
(3) **Success** was broadly similar across touchpoints.

6.4 Interaction Effects of Nudges and Touchpoints (EQ3)

To determine whether certain nudges work better at specific stages of the digital user journey, we tested for statistical interaction effects between *nudge* and *touchpoint* across all three outcome measures. This was tested by including interaction terms (*nudge*touchpoint*) in the regression models.

For *interaction rate*, we found that *salience* showed a significantly stronger effect at the *registration* touchpoint ($OR = 5.54$,$B = 1.71$, $SE = 0.37$, $z = 4.58$, $p < .001$) meaning that *salience* increased the odds of interacting at *registration* by more than five times relative to *activity*. In addition, *visibility* had a significantly greater effect at the *recovery* touchpoint ($OR = 9.93$,$B = 2.30$, $SE = 0.43$, $z = 5.31$, $p < .001$), indicating that *visibility* increased the odds of interaction at *recovery* by almost ten times compared to *activity*.

For *adoption rate* and *success rate*, no significant interaction effects were observed between touchpoints and nudges. This suggests that while certain nudges gain particular strength at specific touchpoints for encouraging initial engagement, they do not differentially affect adoption or completion once interaction has taken place.

Key Results: Nudge–Touchpoint Interactions (EQ3)

(1) **Salience** was particularly effective for driving **interaction** at *registration*.
(2) **Visibility** was especially effective for **interaction** at *recovery*.
(3) No differential patterns emerged for **adoption** or **success**, indicating nudges mainly drive initial engagement.

Table 3: Pairwise proportion tests of *interaction*, *adoption*, and *success rates* by touchpoint and nudge

Touchpoint	Nudge	Interaction Rate	Adoption Rate	Success Rate
Registration	Control	0.462	0.185	0.400
	Salience	**0.902***	**0.462***	0.512
	Visibility	0.592	0.332	0.560
	Choice Default	-	**0.554***	0.554
Login	Control	0.348	0.141	0.406
	Salience	**0.734***	**0.391***	0.533
	Visibility	0.500	0.277	0.554
	Choice Default	-	**0.522***	0.522
Recovery	Control	0.538	0.212	0.394
	Visibility	**0.946***	**0.527***	0.557
	Choice Default	-	**0.543***	0.543
	Effort	0.717	0.266	0.371
Settings	Control	0.272	0.114	0.420
	Salience	**0.576***	**0.277***	0.481
	Visibility	0.380	0.217	0.571
	Social Reference	**0.511***	0.196	0.383
Activity	Control	0.212	0.082	0.385
	Salience	0.342	0.179	0.524
	Visibility	0.288	0.168	0.585
	Reminders	**0.402***	0.130	0.324

Note. * $p < .001$. The choice default nudge was not considered for interaction rates as it was 100% interaction rate by design.

6.5 Summary of Results

To summarize, our results show that the implemented nudges significantly increased both *interaction* and *adoption rates* compared to the control condition (**EQ1**). In contrast, no significant differences were observed for *success rates*. This indicates that higher *adoption rates* were primarily driven by increases in *interaction rates*. The key potential of nudges, therefore, lies in stimulating initial engagement, as adoption tends to follow once users interact. Looking more closely at interaction, the analyses of touchpoints in isolation (**EQ2**) revealed that *recovery* and *registration* were the most effective stages for engaging users with passkeys, suggesting that users are particularly receptive at these points. The interaction analyses (**EQ3**) further showed that, aside from *choice default* (which by design initiates user interaction), *registration* particularly benefited from the *salience* nudge, whereas *recovery* was especially responsive to the *visibility* nudge. Together, these findings indicate that *recovery* and *registration* are not only strong touchpoints for interaction overall but also especially responsive to targeted nudges, making them promising stages for interventions aimed at increasing adoption.

7 DISCUSSION

In this section, we discuss effective touchpoints for passkey adoption (Section 7.1) and recommend nudges to promote adoption (Section 7.2). We then address the ethical use of nudges in this context (Section 7.3) and outline the study's limitations (Section 7.4).

7.1 Effective Touchpoints for Passkey Adoption

The study results indicate that several touchpoints were suitable to nudge users toward passkey usage, consistent with prior work [22]. We further show that *registration*, *recovery*, and *login* demonstrated the highest *interaction* and *adoption rates*. This might be because these touchpoints are naturally suited for behavior change, as users are already engaged with authentication-related tasks. In particular, *recovery* appears to be a promising moment for promoting passkeys, as users are reminded of the drawbacks of passwords when facing a failed login, making them more receptive to alternative options. For these touchpoints, we could also observe the strongest effects of the different nudges compared to the control condition. In contrast, *interaction rates* at the *activity* touchpoint were relatively low across all nudges. This result is consistent with expectations and prior work [71], as the nudge disrupts the user's journey, e.g., when scheduling a doctor's appointment. Its effectiveness likely depends on the application context. In highly task-oriented use cases, such as in the present study, users focus on a specific outcome and may avoid deviations from their task. In contrast, applications with higher engagement or longer session duration, such as messaging or social media apps, may offer better conditions for introducing nudges during user activity.

While nudges consistently increased interaction, they did not significantly impact *success rate*. That is, users who engaged with the prompt were similarly likely to adopt a passkey regardless of the nudge condition. This indicates that nudges primarily influence attention and initial engagement, but not the final adoption. We

Table 4: Logistic regression results for interaction, adoption, and success rates including odds ratios (OR).

Predictor	Interaction Rate				Adoption Rate				Success Rate			
	B	SE	*z*	OR	B	SE	*z*	OR	B	SE	*z*	OR
(Intercept)	**-1.313***	0.180	-7.28	0.269	**-2.422***	0.269	-8.99	0.089	-0.470	0.329	-1.43	0.625
nudge												
choice_default	-	-	-	-	**1.703***	0.241	7.06	5.488	0.624	0.267	2.34	1.866
effort	**0.779***	0.221	3.53	2.179	0.300	0.246	1.22	1.349	-0.096	0.273	-0.35	0.908
reminders	**0.917***	0.235	3.90	2.501	0.525	0.347	1.51	1.690	-0.264	0.412	-0.64	0.768
salience	0.661	0.238	2.77	1.936	0.901	0.331	2.72	2.462	0.565	0.415	1.36	1.760
social_ref	**1.029***	0.222	4.64	2.799	0.635	0.297	2.14	1.888	-0.154	0.356	-0.43	0.857
visibility	0.408	0.243	1.68	1.504	0.825	0.334	2.47	2.283	0.813	0.431	1.89	2.255
touchpoint												
login	0.685	0.238	2.88	1.983	0.617	0.343	1.80	1.854	0.090	0.416	0.22	1.095
recovery	**1.466***	0.233	6.28	4.330	**1.109***	0.324	3.42	3.030	0.039	0.388	0.10	1.040
registration	**1.161***	0.233	4.98	3.192	0.938	0.330	2.84	2.554	0.065	0.397	0.16	1.067
settings	0.327	0.245	1.34	1.387	0.373	0.355	1.05	1.452	0.147	0.436	0.34	1.159
nudge:touchpoint												
choice_default:login	-	-	-	-	0.189	0.353	0.54	1.208	-0.157	0.397	-0.40	0.855
salience:login	0.982	0.329	2.98	2.669	0.462	0.421	1.10	1.587	-0.052	0.516	-0.10	0.949
visibility:login	0.220	0.324	0.68	1.247	0.021	0.428	0.05	1.021	-0.215	0.543	-0.40	0.806
choice_default:recovery	-	-	-	-	-0.215	0.335	-0.64	0.807	-0.019	0.368	-0.05	0.982
visibility:recovery	**2.296***	0.432	5.31	9.932	0.597	0.407	1.47	1.816	-0.151	0.502	-0.30	0.860
salience:registration	**1.714***	0.374	4.58	5.549	0.431	0.409	1.05	1.538	-0.112	0.495	-0.23	0.894
visibility:registration	0.118	0.322	0.37	1.125	-0.042	0.415	-0.10	0.958	-0.168	0.522	-0.32	0.846
salience:settings	0.632	0.326	1.94	1.881	0.190	0.436	0.43	1.209	-0.318	0.540	-0.59	0.728
visibility:settings	0.090	0.331	0.27	1.094	-0.057	0.444	-0.13	0.944	-0.202	0.571	-0.35	0.817

Note. * $p < .001$. Reference categories are *control* (nudge) and *activity* (touchpoint). The choice default nudge was not considered for interaction rates as it was 100% by design.

argue that for this step, other factors such as usability or perceived security likely play a role in actual adoption and may require additional strategies beyond nudging. We suggest that future work evaluate whether personalized assistance, potentially powered by large language models, delivered at the moment a user cancels enrollment can address situational concerns (e.g., recovery implications, cross-device use, or guidance through a failed step) and thereby convert engagement into adoption.

In the expert interviews, practitioners anticipated that *registration*, *login*, and especially *recovery* would be receptive moments, whereas *activity* would be challenging. The user study largely confirmed these expectations. One divergence concerned *settings*: Experts expected stronger receptivity there, but our data did not show a clear advantage over *activity*. Across touchpoints, both sources concur that the effectiveness of passkey nudges hinges on timing and context.

Recommendations for Touchpoints

(1) Use nudges to increase **users' initial interaction** with the option to set up a passkey.
(2) Prioritize **authentication-related touchpoints** (*registration, login, recovery*) when introducing nudges.

7.2 Selecting Nudges for Passkey Adoption

Nudges should preserve users' autonomy and support free choice in decision-making [90]. In the expert-proposed *choice default* design, passkey adoption is automatically initiated, and the option to cancel adoption and choose a password is not made explicit, which can limit perceived autonomy. Although *choice default* yielded the highest overall adoption, *salience* achieved comparable adoption rates at *registration* and *login*, and *visibility* did so at *recovery*, both preserving users' initial choice. This underscores a practical trade-off: Maximize adoption via *choice default* or prioritize perceived autonomy (and potentially user experience) via *salience* or *visibility*.

Given current passkey frictions (e.g., synchronization and shared-device use [54, 100]), we advise caution in deploying *choice default* universally. A risk-tiered approach appears suitable: Reserve *choice default* for high-risk contexts (e.g., email accounts, PMs, or tax accounts) where the consequences of authentication compromise are greatest, and the security benefits of passkeys are most critical. As these frictions diminish and user familiarity increases, *choice default* may become a suitable general nudge.

Although prominently displaying information can raise awareness [17] and is strongly recommended by the FIDO Alliance UX guidelines [22], the *visibility* nudge alone did not drive interaction as strongly as expected. In our data, the *interaction rate* of *visibility* was generally outperformed by *salience* and, depending on the touchpoint, also by *social reference* and *reminders*. Pairing *visibility* with one of these more attention-capturing nudges may therefore

amplify impact. However, organizations should avoid "nudge overload": Combining too many nudges can reduce perceived autonomy and dampen motivation [78]. Future work should examine which nudge combinations are most effective at specific touchpoints.

Interestingly, the quantitative results closely mirrored the experts' assessments: Most nudges produced significant increases in interaction, adoption, or both. Further, both sources converged on the view that tailoring nudges to the touchpoint yields better outcomes than one-size-fits-all deployments. We therefore recommend a staged approach in future work: Begin with formative interviews to surface practitioner knowledge and real-world constraints (e.g., avoiding negative password framing), use these insights to prioritize and refine nudge designs, and then proceed to quantitative evaluation.

Recommendations for Nudges

(1) Choose the ***salience* nudge** over the ***choice default* nudge** as it preserves user autonomy while providing similar adoption rates.
(2) Providing more information alone (***visibility* nudge**) is not successful, but might be used to **enhance the effect of other nudges**.

7.3 Ethical Application of Nudges for Passkey Adoption

As nudges steer behavior [36], they can also be misapplied to channel users toward outcomes they would not otherwise choose. Such misuse overlaps with *dark patterns*, interface designs that intentionally exploit cognitive biases to coerce, steer, or mislead users [33]. Common examples include highlighting add-ons, countdown timers that manufacture urgency, and default consent for data sharing [33, 58]. These practices can increase conversion while undermining user autonomy and welfare [56, 64].

The central ethical question is when the use of nudges is justified. We adopt the view that nudges are warranted when they are transparent, reversible, proportionate, and sensitive to user heterogeneity [76]. Applied to authentication, status-quo bias and ambiguity aversion may steer some users toward familiar passwords and away from passkeys [26, 66, 79], yet password use could also reflect considered preferences (e.g., due to shared-device workflows, or cross-ecosystem constraints) [35, 100]. Earlier comparative analyses, conducted before passkeys were available, further suggest that no single authentication scheme dominates across usability, deployability, and security dimensions [8]. Limitations remain for passkeys, including synchronization, shared-device use, and recovery [54, 100]. Nevertheless, passkeys provide meaningful gains relative to passwords in many contexts, such as memoryless sign-in and phishing-resistant credentials [57, 66, 100]. Thus, we advance the following position: Choice-preserving, preference-sensitive nudges toward passkey adoption are ethically defensible where welfare gains for the targeted user segment are reasonably anticipated. Concretely, platforms may present passkeys as the recommended option with a brief rationale, while also providing a password option or fallback and allowing users to opt out at any point. We further recommend monitoring outcomes (e.g., adoption, lockouts, and recovery failures) and adjusting nudges in response to observed adverse effects. In this form, nudging promotes user welfare while respecting autonomy.

7.4 Limitations

As with any research, the results of our study need to be seen in the light of certain limitations, which we address in the following.

7.4.1 Interviews. We conducted 15 interviews with industry experts spanning development, design, and cybersecurity decision-making. While modest, this sample size is typical for qualitative research with difficult-to-recruit expert populations, where depth of specific knowledge is the primary aim [10]. Recruitment was purposive rather than random, using professional networks and referrals, which may introduce selection bias. For our objectives, however, targeted sampling increased feasibility and ensured that participants had direct, practice-grounded experience with authentication and nudge design, enhancing the relevance of the insights that informed the subsequent user study.

7.4.2 User Study. We ran a field study on a European healthcare platform with active users. This setting increased ecological validity—participants made consequential, real-world authentication decisions—but reduced experimental control over external influences. Although a large sample cannot completely account for such confounds, it provides more precise effect estimates and supports nudge- and touchpoint-specific analyses. Eligibility required active platform use, which limits population-level randomness but enabled an in-depth assessment of this context. Finally, the healthcare and European setting may heighten security salience relative to other sectors or regions. We encourage replication in other contexts and publish our source code and R syntax to support future work.

8 CONCLUSION

In this paper, we investigated how digital nudges affect passkey adoption. We conducted expert interviews to identify candidate nudges and specify their designs, then evaluated the most promising ones in an RCT with 3,680 participants. Our results show that nudges, when delivered at the right touchpoints in the user journey, significantly increase passkey adoption. We conclude that well-designed digital nudges can help users move beyond passwords.

AVAILABILITY

We published the implementation of our study as open-source, supporting future work to replicate this study in other contexts and regions. While we cannot provide the raw data because of a data protection agreement between the platform vendor and its users, we published all R-based statistical analyses and the codebook.[3]

[3] Source code, analysis, and codebook: https://github.com/PasskeyNudges/Availability

DECLARATION OF GENERATIVE AI TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this work, the authors used DeepL, Grammarly, and ChatGPT (Version 5) in order to improve the language and readability.[4] After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[2] Youssef Amer, Ehsan Ul Haque, Zhelun Rong, and Mohammad Maifi Hasan Khan. 2025. Understandability of the Technology and Benefit May Not Be Enough to Nudge Users: An Exploratory Study in the Context of FIDO2 Adoption Behavior. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE Computer Society, Los Alamitos, CA, USA, 607–618. https://doi.org/10.1109/COMPSAC65507.2025.00083

[3] Amir Fard Bahreini, Ron Cenfetelli, and Hasan Cavusoglu. 2022. The Role of Heuristics in Information Security Decision Making. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS-55)*.

[4] Thomas Baumer, Tobias Reittinger, Sascha Kern, and Günther Pernul. 2024. Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 239–258.

[5] Adam Beautement, M Angela Sasse, and Mike Wonham. 2008. The Compliance Budget: Managing Security Behaviour in Organisations. In *Proceedings of the 2008 new security paradigms workshop*. 47–58.

[6] S.M. Bellovin and M. Merritt. 1992. Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. In *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*. 72–84. https://doi.org/10.1109/RISP.1992.213269

[7] Kristoffer Bergram, Marija Djokovic, Valéry Bezençon, and Adrian Holzer. 2022. The Digital Landscape of Nudging: A Systematic Literature Review of Empirical Research on Digital Nudges. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–16.

[8] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*. 553–567. https://doi.org/10.1109/SP.2012.44

[9] Chris Brown. 2019. Digital Nudges for Encouraging Developer Actions. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*. IEEE, 202–205.

[10] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 981–992.

[11] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 2019. 23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–15.

[12] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–11.

[13] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. In *NDSS*, Vol. 14. 23–26.

[14] Sanchari Das, Andrew Dingman, and L Jean Camp. 2018. Why Johnny Doesn't Use Two Factor a Two-Phase Usability Study of the Fido u2f Security Key. In *International Conference on Financial Cryptography and Data Security*. Springer, 160–179.

[15] Nicole M Deterding and Mary C Waters. 2021. Flexible Coding of In-Depth Interviews: A Twenty-First-Century Approach. *Sociological methods & research* 50, 2 (2021), 708–739.

[16] Rachna Dhamija, J. D. Tygar, and Marti A. Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 581–590. https://doi.org/10.1145/1124772.1124861

[17] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 67, 12 pages. https://doi.org/10.1145/3411764.3445516

[18] Florian M Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. "You still use the password after all"–Exploring FIDO2 Security Keys in a Small Company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 19–35.

[19] FIDO Alliance. 2022. Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins. https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/ Accessed: 08/14/25.

[20] FIDO Alliance. 2022. Client to Authenticator Protocol (CTAP). https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html Accessed: 08/14/25.

[21] FIDO Alliance. 2022. White Paper: Multi-Device FIDO Credentials. https://fidoalliance.org/white-paper-multi-device-fido-credentials/ Accessed: 12/01/25.

[22] FIDO Alliance. 2023. FIDO Alliance UX Guidelines for Passkey Creation and Sign-ins. https://fidoalliance.org/wp-content/uploads/2023/05/FIDO-Alliance-UX-Guidelines-for-Passkey-Creation-and-Sign-ins.pdf Accessed: 08/14/25.

[23] FIDO Alliance. 2023. FIDO Authentication. https://fidoalliance.org/fido2/ Accessed: 08/14/25.

[24] Dinei Florencio and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web* (Banff, Alberta, Canada) *(WWW '07)*. Association for Computing Machinery, New York, NY, USA, 657–666. https://doi.org/10.1145/1242572.1242661

[25] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. 2014. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *23rd USENIX Security Symposium (USENIX Security 14)*. 575–590.

[26] Craig R Fox and Amos Tversky. 1995. Ambiguity Aversion and Comparative Ignorance. *The quarterly journal of economics* 110, 3 (1995), 585–603.

[27] Steven Furnell and Rawan Esmael. 2017. Evaluating the Effect of Guidance and Feedback Upon Password Compliance. *Computer Fraud & Security* 2017, 1 (2017), 5–10.

[28] Cristina Gena, Pierluigi Grillo, Antonio Lieto, Claudio Mattutino, and Fabiana Vernero. 2019. When Personalization Is Not an Option: An In-The-Wild Study on Persuasive News Recommendation. *Information* 10, 10 (2019), 300.

[29] Mohammad Ghasemisharif, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, and Jason Polakis. 2018. O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web. In *27th USENIX security symposium (USENIX security 18)*. 1475–1492.

[30] Sanam Ghorbani Lyastani, Michael Backes, and Sven Bugiel. 2023. A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites. In *30th Annual Network & Distributed System Security Symposium (NDSS'23)*. The Internet Society.

[31] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M Redmiles. 2021. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *30th USENIX Security Symposium (USENIX Security 21)*. 109–126.

[32] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. 2018. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *Proceedings of the 2018 acm sigsac conference on computer and communications security*. 1549–1566.

[33] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–14.

[34] Valerică Greavu-Şerban, Floredana Constantin, and Sabina-Cristiana Necula. 2025. Exploring Heuristics and Biases in Cybersecurity: A Factor Analysis of Social Engineering Vulnerabilities. *Systems* 13, 4 (2025), 280.

[35] Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. 133–144.

[36] Dennis Hummel and Alexander Maedche. 2019. How Effective Is Nudging? A Quantitative Review on the Effect Sizes and Limits of Empirical Nudging Studies. *Journal of Behavioral and Experimental Economics* 80 (2019), 47–58.

[37] Amazon.com Inc. 2025. Passkey. https://www.amazon.com/ax/claim/webauthn/enroll Accessed: 08/14/25.

[38] Philip G. Inglesant and M. Angela Sasse. 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 383–392. https://doi.org/10.1145/1753326.1753384

[39] Mazharul Islam, Sunpreet S. Arora, Rahul Chatterjee, and Ke Coby Wang. 2025. Detecting Compromise of Passkey Storage on the Cloud. In *Proceedings of the 34th USENIX Security Symposium*. USENIX Association.

[40] Mathias Jesse and Dietmar Jannach. 2021. Digital Nudging With Recommender Systems: Survey and Future Directions. *Computers in Human Behavior Reports* 3 (2021), 100052.

[41] Eric J Johnson, Suzanne B Shu, Benedict GC Dellaert, Craig Fox, Daniel G Goldstein, Gerald Häubl, Richard P Larrick, John W Payne, Ellen Peters, David Schkade, et al. 2012. Beyond Nudges: Tools of a Choice Architecture. *Marketing*

[4] For full transparency, we report AI Usage Cards [95]: https://ai.uversy.com/passkey-nudges

letters 23 (2012), 487–504.

[42] Michael B. Jones, Akshay Kumar, and Emil Lundberg. 2023. Web Authentication: An API for accessing Public Key Credentials Level 3. https://www.w3.org/TR/webauthn-3/ Accessed: 08/14/25.

[43] Dominik Jung, E. Erdfelder, and Florian Glaser. 2018. Nudged to win - Designing robo-advisory to overcome decision inertia. In *Proceedings of the 26th European Conference on Information Systems (ECIS2018), Portsmouth, UK, June 23-28, 2018.*

[44] Emiram Kablo, Katharina Kader, and Patricia Arias-Cabarcos. 2024. "I'm actually going to go and change these passwords": Analyzing the Usability of Credential Audit Interfaces in Password Managers. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 2, 13 pages. https://doi.org/10.1145/3613905.3650889

[45] Daniel Kahneman and Amos Tversky. 1979. Prospect Theory: An Analysis of Decision Under Risk. *Econometrica* 47, 2 (1979), 363–391.

[46] KAYAK. 2025. Sign in or create an account. https://www.kayak.com/login Accessed: 08/14/25.

[47] Shelia M Kennison, Ian T Jones, Victoria H Spooner, and D Eric Chan-Tin. 2021. Who Creates Strong Passwords When Nudging Fails. *Computers in Human Behavior Reports* 4 (2021), 100132.

[48] Eiji Kitamura. 2024. userVerification deep dive. web.dev. https://web.dev/articles/webauthn-user-verification Accessed: 12/01/25.

[49] Jan H. Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2023. "Make Them Change it Every Week!": A Qualitative Exploration of Online Developer Advice on Usable and Secure Authentication. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (Copenhagen, Denmark) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 2740–2754.

[50] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of Passwords and People: Measuring the Effect of Password-Composition Policies. In *Proceedings of the sigchi conference on human factors in computing systems*. 2595–2604.

[51] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. 2023. Evaluating the Security Posture of Real-World FIDO2 Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (Copenhagen, Denmark) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 2381–2395.

[52] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. 2021. Evaluation of Account Recovery Strategies With FIDO2-Based Passwordless Authentication. *arXiv preprint arXiv:2105.12477* (2021).

[53] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *30th USENIX Security Symposium (USENIX Security 21)*. 91–108.

[54] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 7231–7248. https://www.usenix.org/conference/usenixsecurity24/presentation/lassak

[55] George Loewenstein and Nick Chater. 2017. Putting Nudges in Perspective. *Behavioural Public Policy* 1, 1 (2017), 26–53.

[56] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* 13, 1 (2021), 43–109.

[57] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 268–285.

[58] Arunesh Mathur, Gunes Acar, Michael J Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings From a Crawl of 11K Shopping Websites. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–32.

[59] Christian Meske and Tobias Potthoff. 2017. The DINU-Model – A Process Model for the Design of Nudges. In *Proceedings of the 25th European Conference on Information Systems (ECIS 2017) (Research-in-Progress Papers)*. Guimarães, Portugal, 2587–2597.

[60] Microsoft. 2024. Microsoft Digital Defense Report 2024. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 Accessed: 08/14/25.

[61] Tobias Mirsch, Christiane Lehrer, and Reinhard Jung. 2018. Making Digital Nudging Applicable: The Digital Nudge Design Method. In *Proceedings of the 39th International Conference on Information Systems (ICIS) (Proceedings of the International Conference on Information Systems)*. Association for Information Systems. AIS Electronic Library (AISeL).

[62] Robert Münscher, Max Vetter, and Thomas Scheuerle. 2016. A Review and Taxonomy of Choice Architecture Techniques. *Journal of Behavioral Decision Making* 29, 5 (2016), 511–524.

[63] Florian Nawrath. 2021. Quantitative Analysis of FIDO2 Client Support. *Proc. WAY* (2021).

[64] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems*. 1–13.

[65] Wataru Oogami, Hidehito Gomi, Shuji Yamaguchi, Shota Yamanaka, and Tatsuru Higurashi. 2020. Observation Study on Usability Challenges for Fingerprint Authentication Using Webauthn-Enabled Android Smartphones. *Age* 20 (2020), 29.

[66] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. 2021. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 57–76.

[67] Jessica Pater, Amanda Coupe, Rachel Pfafman, Chanda Phelan, Tammy Toscos, and Maia Jacobs. 2021. Standardizing Reporting of Participant Compensation in Hci: A Systematic Literature Review and Recommendations for the Field. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–16.

[68] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let's Go In for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 295–310.

[69] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why People (Don't) Use Password Managers Effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 319–338. https://www.usenix.org/conference/soups2019/presentation/pearman

[70] R Core Team. 2025. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

[71] Sangeeta Ranjit and Scott Bingham. 2024. Convincing a Billion Users to Love Passkeys: UX Design Insights From Microsoft to Boost Adoption and Security. https://www.microsoft.com/en-us/security/blog/2024/12/12/convincing-a-billion-users-to-love-passkeys-ux-design-insights-from-microsoft-to-boost-adoption-and-security/ Accessed: 08/14/25.

[72] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 357–370.

[73] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. 2024. Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality. In *International Symposium on Human Aspects of Information Security and Assurance*. Springer, 3–16.

[74] Tobias Reittinger, Magdalena Glas, Sarah Aminzada, and Günther Pernul. 2025. Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice. *Information & Computer Security* (2025).

[75] Tobias Reittinger and Günther Pernul. 2026. No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage. In *2026 IEEE Symposium on Security and Privacy (SP)*. IEEE. Accepted for publication.

[76] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35.

[77] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A Tale of Two Studies: The Best and Worst of Yubikey Usability. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 872–888.

[78] Richard M. Ryan and Edward L. Deci. 2017. *Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness* (hardcover ed.). The Guilford Press. 756 pages.

[79] William Samuelson and Richard Zeckhauser. 1988. Status Quo Bias in Decision Making. *Journal of risk and uncertainty* 1, 1 (1988), 7–59.

[80] Armando Schär and Katarina Stanoevska-Slabeva. 2019. Application of Digital Nudging in Customer Journeys – A Systematic Literature Review. In *Proceedings of the 25th Americas Conference on Information Systems (AMCIS 2019)*. Cancún, Mexico.

[81] Ryan Schin. 2024. Despite Increasing Cybersecurity Attacks, People Still Believe Antiquated Username and Passwords Are Strong Enough. https://www.yubico.com/press-releases/despite-increasing-cybersecurity-attacks-people-still-believe-antiquated-username-and-passwords-are-strong-enough/ Accessed: 08/14/25.

[82] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. 2022. FeIDo: Recoverable FIDO2 Tokens Using Electronic IDs. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2581–2594.

[83] Kavya Sharma, Xinhui Zhan, Fiona Fui-Hoon Nah, Keng Siau, and Maggie X Cheng. 2021. Impact of Digital Nudging on Information Security Behavior: An

Experimental Study on Framing and Priming in Cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People* 1, 1 (2021), 69–91.
[84] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security (TISSEC)* 18, 4 (2016), 1–34.
[85] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. 2021. Systematization of Password Manager Use Cases and Design Paradigms. In *Proceedings of the 37th Annual Computer Security Applications Conference*. 528–540.
[86] Cass R Sunstein. 2014. Nudging: A Very Short Guide. *Journal of Consumer Policy* 37 (2014), 583–588.
[87] Cass R Sunstein. 2016. The Council of Psychological Advisers. *Annual Review of Psychology* 67, 1 (2016), 713–737.
[88] David Temoshok, James L. Fenton, Yee-Yin Choong, Naomi Lefkovitz, Andrew Regenscheid, Ryan Galluzzo, and Justin P. Richer. 2025. *NIST SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.* NIST Special Publication (SP) NIST SP 800-63B-4. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-63B-4
[89] Richard H. Thaler and Cass R. Sunstein. 2003. Libertarian Paternalism. *American Economic Review* 93, 2 (May 2003), 175–179. https://doi.org/10.1257/000282803321947001
[90] Richard H Thaler and Cass R Sunstein. 2021. *Nudge: The Final Edition.* Yale University Press.
[91] Richard H Thaler, Cass R Sunstein, and John P Balz. 2014. Choice Architecture. *The behavioral foundations of public policy* (2014).
[92] Aggeliki Tsohou, Maria Karyda, and Spyros Kokolakis. 2015. Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs. *Computers & security* 52 (2015), 128–141.
[93] Amos Tversky and Daniel Kahneman. 1981. The Framing of Decisions and the Psychology of Choice. *science* 211, 4481 (1981), 453–458.
[94] Uber Technologies, Inc. 2024. *Uber - Request a ride.* https://apps.apple.com/app/uber/id368677368
[95] Jan Philip Wahle, Terry Ruas, Saif M Mohammad, Norman Meuschke, and Bela Gipp. 2023. AI Usage Cards: Responsibly Reporting Ai-Generated Content. In *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL).* IEEE, 282–284.
[96] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-Used Across Websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).* 175–188.
[97] Markus Weinmann, Christoph Schneider, and Jan vom Brocke. 2016. Digital Nudging. *Business & Information Systems Engineering* 58 (2016), 433–436.
[98] WhatsApp. 2024. How to view, like, and reply to status updates. https://faq.whatsapp.com/2544894022567526/ Accessed: 08/14/25.
[99] Gordon B Willis. 2004. *Cognitive Interviewing: A Tool for Improving Questionnaire Design.* Sage Publications.
[100] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems.*
[101] Verena Zimmermann and Karen Renaud. 2021. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 1 (2021), 1–45.

A APPENDIX

A.1 Guidelines of Expert Interviews

I. Passkeys

- *[Explaining passkeys and touchpoints to the experts]*
- Do you have experience using or deploying FIDO2 or passkeys in your organization?
- You have implemented passkeys as a new feature. For each touchpoint, how would you approach making both new and existing users aware of the passkey feature, and how would you encourage them to adopt passkeys?

II. Digital Nudges

- *[Explaining digital nudges in general to the experts]*
- Do you have experience designing or developing user interfaces (UI) or user experiences (UX)?
- Do you have experience with digital nudges in your organization?
- For each of the 13 digital nudges [40] and five touchpoints [22] (see Table 2):
  - *[Explaining the digital nudge to the experts]*
  - What impact do you expect the digital nudge to have on users for the touchpoint?
  - Would you consider using this nudge, and how would you approach designing it to encourage passkey adoption for the touchpoint?
  - Do you anticipate a strongly negative (1), negative (2), neutral (3), positive (4), strongly positive (5) effect of this digital nudge on passkey adoption for the touchpoint?

III. Information about Participants

- What is your job position?
- How many years of experience do you have?
- In which sector does your organization operate?
- How many employees does your organization have?
- What is the country code of the location of your organization where you are primarily employed?

VI. Incentive and Referral

- As a thank you for participating in the interview, we will donate €20 to an NPO of your choice. Which of these verified NPOs do you want to benefit from the donation?
- Do you know another person who would be suitable for such an interview?

A.2 User Study Demographics per Touchpoint

Table 5 describes the user demographics per touchpoint.

Table 5: Participant demographics by touchpoint.

	Reg.	Login	Recov.	Settings	Activity
Gender					
Female	381	380	375	379	365
Male	355	356	361	357	370
Other	-	-	-	-	1
Age					
18–19	17	14	14	14	17
20–29	110	117	119	123	113
30–39	159	167	164	153	146
40–49	161	153	144	166	165
50–59	153	138	145	137	156
60–69	101	106	105	109	106
70–79	34	39	44	33	33
80+	1	2	1	1	-
Education					
In school	15	15	13	10	15
Middle school	310	295	304	298	279
High school	214	230	234	236	256
Higher educ.	113	115	111	112	108
Other	84	81	74	80	78
Passkey exp.					
Yes	427	428	426	432	406
No	309	308	310	304	330

P4 Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations.

Current status:	Published
Conference:	Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)
Ranking:	A ICORE 2026, 21% Acceptance Rate
Date of acceptance:	May 14, 2024
Date of publication:	August 12, 2024
Full citation:	Baumer, T., Reittinger, T., Kern, S., & Pernul, G. (2024). Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, pp. 239–258.

Authors' contributions:		
	Thomas Baumer	40%
	Tobias Reittinger	25%
	Sascha Kern	25%
	Günther Pernul	10%

Conference description: The *USENIX Symposium on Usable Privacy and Security (SOUPS)* (peer-reviewed) is a premier, interdisciplinary forum for human-centered privacy and security research, uniting perspectives from HCI, security, and privacy to study how people understand, use, and are affected by protective technologies. The 2024 symposium, the twentieth in the series, was held in Philadelphia on August 11–13, 2024, co-located with the USENIX Security Symposium.



Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations

Thomas Baumer, *Nexis GmbH;* Tobias Reittinger, *Universität Regensburg;*
Sascha Kern, *Nexis GmbH;* Günther Pernul, *Universität Regensburg*

https://www.usenix.org/conference/soups2024/presentation/baumer

This paper is included in the Proceedings of the
Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7



Open access to the Proceedings
of the Twentieth Symposium
on Usable Privacy and Security
is sponsored by USENIX.

Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations

Thomas Baumer
Nexis GmbH

Tobias Reittinger
University of Regensburg

Sascha Kern
Nexis GmbH

Günther Pernul
University of Regensburg

Abstract

Organizations tend to over-authorize their members, ensuring smooth operations. However, these excessive authorizations offer a substantial attack surface and are the reason regulative authorities demand periodic checks of their authorizations. Thus, organizations conduct time-consuming and costly access reviews to verify these authorizations by human decision-makers. Still, these deciders only marginally revoke authorizations due to the poor usability of access reviews. In this work, we apply digital nudges to guide human deciders during access reviews to tackle this issue and improve security. In detail, we formalize the access review problem, interview experts ($n = 10$) to identify several nudges helpful for access reviews, and conduct a user study ($n = 102$) for the *Choice Defaults Nudge*. We show significant behavior changes in revoking authorizations. We also achieve time savings and less stress. However, we also found that improving the overall quality requires more advanced means. Finally, we discuss design implications for access reviews with digital nudges.

1 Introduction

The Open Web Application Security Project (OWASP) lists "broken access control" as the Top 1 vulnerability and discovers it in 94% of the tested web applications [36]. Excessive authorizations are one driver for this OWASP vulnerability, as these are granted without an actual need and thus open an unnecessary attack surface. More precisely and within this paper, we ask highly qualified Identity and Access Management (IAM) experts to estimate the ratio of excessive authorizations in mid- and large-sized organizations. Our experts expect about a fifth to a quarter of the authorizations to be excessive and vulnerable ($M = 22.8\%$, $SD = 6.4\%$, $n = 10$).

To mitigate this vulnerability, regulative authorities demand organizations to evaluate their authorizations with periodic access reviews. Well-known regulations include SOX [52], Basel III [6], MARisk [12], or HIPAA [51]. In large organizations, this involves hundreds of access review deciders for six figures of authorizations [18, 39]. These deciders (e.g., department heads) evaluate these authorizations within their responsibility. Although accountable, deciders face a time-consuming and frustrating task, as their expertise and objectives might not primarily match with security. Responsible deciders must also avoid mistakes: While revoked authorizations can interrupt their organization shortly, falsely confirmed excessive authorizations drive security risks [25]. Research [18] shows in a real-world case study that deciders only revoke 1.2% of the reviewed authorizations instead of the expected one-fifth excessive ones. Besides this clear need for improvement, only a few papers [18, 22, 26, 39] study access reviews.

As shown by Jaferian et al. [26], crucial issues for access reviews are rooted in poor usability. Using digital nudges to guide decisions [53] is thus a promising approach to improve access reviews. However, we identify several research gaps: First, current research does not formalize access reviews. Second, it is unknown how digital nudges address access review challenges. Third, it is unclear whether digital nudges actually improve access reviews. We investigate these research gaps with the following research questions:

- **Q1** *How to formalize the access review problem?*
- **Q2** *How do access review challenges map to digital nudges?*
- **Q3** *Does an applied digital nudge (the Choice Defaults Nudge) benefit the access review problem?*

This work follows a mixed methods approach in an exploratory sequential design. We use qualitative methods to define a formal and precise notation of the underlying problem (Q1) and to interview highly qualified experts ($n = 10$) about

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

applying digital nudges for access reviews (Q2). Moreover, our quantitative methods use insights of Q1 and Q2 to conduct a user study ($n = 102$) with an application of the *Choice Defaults Nudge* for access reviews (Q3). Consequently, our methods lead to the following contributions:

- We are first to formalize the access review problem.
- We map the expected effects of digital nudges to access review challenges based on 10 expert interviews. We find that access reviews benefit from digital nudges.
- We show behavior changes leading to quality improvements and more revoked authorizations by applying the *Choice Defaults Nudge* within a user study ($n = 102$). Moreover, we achieve time savings and lower frustration.

The remainder of this work is outlined as follows: Section 2 covers the background of this work, including relevant terminology, access review challenges, digital nudges, and related work. Section 3 provides details about our mixed method approach. Subsequently, we present the three-fold results of our paper. In Section 4, we first formalize the access review problem. Second, we map digital nudges with the access review challenges through the expert interviews in Section 5. Third, we conduct a user study on the *Choice Defaults Nudge* for access reviews in Section 6. Following the results, we discuss the general findings of this work in Section 7. Finally, Section 8 concludes and gives an overview for future work.

2 Background

2.1 Terminology

Identity and Access Management (IAM) is a cornerstone of modern cybersecurity, as it manages users and their access to sensitive data and services of organizations. Therefore, IAM provides tools to administer, authorize, and authenticate identities. Regulative authorities acknowledge the relevance of IAM and demand proper security controls. Besides state-of-the-art authentication, one crucial control is to demonstrate that the users still require granted access. Access reviews are a typical tool to prove the actuality of the granted access. These access reviews are the main focus of this work.

Access reviews are a periodic and compliance-driven process to verify users' authorizations. A team of domain experts, managers, application owners, and security admins typically reviews the granted authorizations with their knowledge of current processes, people, and resources. Especially in large organizations, access reviews are labor-intensive. Because of the recurring workload of access reviews, an organization might not finish an access review before the next one starts. The primary goal of access reviews is *revoking excessive authorizations*. Secondary goals are the determination of responsibilities for authorizations, requesting missing authorizations, or organization-specific data quality requirements. [18,22,26]

Nudges help humans make choices in analogous and digital systems. While these individuals must make their choices freely, *choice architects* design *choice architectures* to support their decisions by *nudging* towards a desired option. A nudge is thus a characteristic, influencing a decision in the interest of the decider. An example of a nudge in a supermarket is making healthy food easily accessible while making the unhealthy one harder to reach. From an ethical perspective, a nudge does not prevent a human from making a specific choice and only influences the decision in the best interest of the human. A *digital nudge* applies the idea of nudges to information systems. With features of user interfaces for guidance, users can make their choices freely and supported by the best advice of the choice architecture. [27,45,50]

2.2 Access Review Challenges

Based on expert interviews, Jaferian et al. [26] summarize access review challenges (C1-C5). We utilize these challenges throughout the paper, and thus detail them in this section.

C1: Scale outlines the number of involved IAM entities for the access review. The scale of the users, roles, permission, accounts, or assignments quickly grows into large numbers [18,26,39], making careful considerations for organizing the access review's workload necessary. Furthermore, the heterogeneity of these entities within real-world organizations intensify this challenge [30].

C2: Lack of Knowledge refers to the understandability of roles and permissions [26,30,31]. IAM entities might not have telling names, comprehensive descriptions, or concepts like roles or permissions might not have been fully understood. Experts thus might take uninformed or *best guess* decisions, leading to a bias for keeping unnecessary granted authorizations, violating the Principle of Least Privilege (PoLP) [18]. Additionally, for large organizations, the knowledge about these entities is distributed (or even missing completely), making the advice of responsible domain experts necessary [30].

C3: Frequency describes a dilemma for the managers: access reviews are not their *actual* responsibility, but they are frequently asked for it [26]. The experts might not feel a need to participate, leading to failing access reviews. Ultimately, this may cause even more access reviews, since successfully executed access reviews are part of compliance and audits. Thus, while access reviews usually are only required yearly, some organizations execute them quarterly, hoping not to fail access reviews due to lack of participation [26].

C4: Human Errors are common due to the scale and manual execution of access reviews by human deciders. These experts ultimately decide about required or excessive access by applying the best of their knowledge. This process is, therefore, inherently error-prone, as decisions to the best of the experts' knowledge might be incorrect or uninformed [18,26].

C5: Exceptional Cases occur due to the scale and complexity of access reviews. Context knowledge is sometimes

required for an informed authorization decision. For example, some members of organizations might replace others while on leave, trainings or tests might require temporary access, etc. might cause disturbances [26].

2.3 Digital Nudges

Based on a literature survey, Jesse and Jannach [27] propose a taxonomy for digital nudges. The authors distinguish four primary categories with further sub-categories of digital nudges (N01-N13): decision information (N01-N04), decision structure (N05-N08), decision assistance (N09-N10), and social decision appeal (N11-N13). We refer to these nudges throughout the paper, and thus explain them in this section.

Decision Information tries to present information helpful for the decision-maker without altering the available choices. This category comprises information translation (N01), salience (N02), visibility (N03), and phrasing (N04).

- *N01: Information Translation* targets reducing the cognitive effort for a decision by simplifying information or decreasing vagueness and ambiguity [48].
- *N02: Information Salience* aims to raise or decrease the prominence of information, by visualizations or making information harder or easier to notice [11, 48].
- *N03: Information Visibility* fosters decision information. This category includes mechanisms to disclose [24, 28, 48], compare [11, 48] or warn with [24, 33, 48] (tailored [28, 33] or external [35, 49]) information.
- *N04: Information Phrasing* puts presented information in context to intervene with the decisions to make. This category comprises the utilization of heuristics or biases like anchoring [33, 34, 48], availability [44, 50], the endowment effect [11, 44], framing [11, 33, 48], loss aversion [34, 44, 48], priming [11, 48, 50], etc.

Decision Structure alters the decision arrangement, comprising the decisions' range & composition (N05), defaults (N06), consequences (N07), and required effort (N08).

- *N05: Range & Composition* groups and categorizes choices. Therefore, choice architects or the decision-makers themselves break large decision structures into smaller category partitions [28, 48, 53], to present these one after another [28, 33] or to make them more comparable to each other [28, 35]. Choice architects can also utilize ordering effects for the presented options [11, 48].
- *N06: Choice Defaults* is one of the most effective and well-studied nudges [24]. The nudge preselects choices without hindering the decision maker from actively making another choice. On the one hand, a decision-maker is more invested in an actively made decision [35, 48]. On the other hand, decision-makers rather accept the preselected status quo than actively decide against it [11, 24, 35, 48].
- *N07: Option Consequences* add further yet rational insignificant effects to the choice without changing the overall economic incentives. These consequences include social outcomes or minor benefits & costs [24, 35].
- *N08: Option-related Effort* modifies the effort or ease to make decisions. This nudge includes capping [11, 48] or raising financial & physical effort [24, 35] of decision-makers choices to mitigate mindless actions. Furthermore, eased and more convenient choices speed up decisions, e.g., making desired choices more accessible [48].

Decision Assistance aids decision-makers to realize their intentions. This category includes the usage of reminders (N09) and commitment facilitation (N10).

- *N09: Reminders* actively put already available information into or out of the attention focus of the decision-makers. This nudge includes reminding of underlying goals, deadlines, and their relevance [11, 24, 33, 35, 48, 49] or stating social expectations for decisions [35].
- *N10: Commitment Facilitation* helps decision-makers to (timely) finish their asked for decisions. This nudge includes precommitment strategies (e.g., user-defined sub-goals) [24, 33, 35, 48] or public commitment (e.g., pressure by publicly communicating own goals) [11, 35].

Social Decision Appeal category focuses on the social implications of nudges, including the Messenger Reputation (N11), Social Reference Point (N12), and Empathy Instigation (N13).

- *N11: Messenger Reputation* considers the reputation of the messenger delivering the information for the nudge. On the one hand, the messenger effect nudges a decision-maker since the messenger provides a certain and influencing impression about itself. For example, an actually well-designed and important choice architecture might dilute its seriousness if it contains many spelling mistakes [44]. On the other hand, the reputation of a system can be improved when choice architects expect and forgive the errors of their decision-makers [28, 53].
- *N12: Social Reference Point* nudges a decision based on social opinions. E.g., the opinion of a majority (Argentum-Ad Populum), group (Group-Ad Populum) [16], or an opinion leader [35] can influence decision-makers. Additionally, deciders tend to follow a herd [34, 44, 48] and might desire a comparison with their peers influencing their own decisions [24, 33, 35].
- *N13: Empathy Instigation* uses feelings to influence deciders. For example, an avatar might smile or cry upon the choices of a decision-maker (moral suasion) [11, 48], or a choice architect can trigger reciprocity by doing something good for the decision-makers to nudge them into returning the favor with good choices [11].

2.4 Related Work

Access control ensures users can only act within their intended authorizations and is characterized by its necessary yet cumbersome maintenance. Related research on maintenance covers more efficient access control models, optimization, and general maintenance processes like access reviews. By evolving from access control matrices [41], the most dominant access control models are Role-Based Access Control (RBAC) [15, 37, 43] and Attribute-Based Access Control (ABAC) [23, 46] as these reduce maintenance costs. Modeling access control policies considers bottom-up, top-down, or hybrid approaches [14] but often overlook their actual optimization without recalculating them [31, 38]. Therefore, access control maintenance targets up-keeping authorizations in changing needs and environments based on IAM goals [25, 30]. This includes periodically reviewing and revoking excessive access [18, 22, 26], granting missing access [47, 54], and timely propagation [7] to maintain secure authorizations. This paper especially relates to work on maintenance by access reviews: Jaferian et al. [26] study its challenges and usability. Puchta et al. [39] show positive effects on using external data for access reviews. Groll et al. [18] assess decision quality. Hill [22] conducts a case study for HIPAA [51] compliant access reviews.

Digital nudges are a popular research topic, as shown by various surveys: While Bergram et al. [9] conduct a general literature review, Schaer and Stanoevska-Slabeva [44] analyze digital nudges in customer-journeys and Jesse and Jannach [27] in recommender systems. Additionally, a survey of Caraban et al. [11] covers a practical and ethical application. As an established means to shape human behavior, applications of (digital) nudges exist for many domains. Examples include e-commerce [2, 13], sustainable smart home [8], contract tracing [17], or cybersecurity. In detail, cybersecurity examples include digital nudges to prevent phishing [55] or increase password quality [29, 56, 57]. An application of digital nudges for access reviews remains open so far.

3 Methods

This research uses mixed methods in an exploratory sequential design. First, we use qualitative methods to formalize the Access Review Problem (ARP) (Q1) and relate access review challenges to digital nudges (Q2). Second, we use these qualitative insights in quantitative methods to study the effect of the *N06: Choice Defaults* for access reviews (Q3). Third, a discussion wraps up the findings. Figure 1 depicts our mixed methods. In the following, we detail each part.

3.1 Formalizing the Access Review Problem

While the access review challenges comprise a global view, we formalize the actual Access Review Problem (ARP) in Section 4. Its goal is to understand the underlying problem better. This formalization targets a quantifiable and comparable foundation for the solution of the ARP. Thus, we argue access review as a transition between two authorization states, depicted as confusion matrices. This precise formalization of the ARP is the basis for the hypotheses of the user study.

3.2 Relation of Access Review Challenges to Beneficial Digital Nudges

Complementary challenges to the ARP are discussed in the literature, including scale, lack of knowledge, frequency, human errors, and exceptional cases [26]. Digital nudges are a promising approach to address the ARP and its challenges. But it is unknown, whether digital nudges can help and which effects can be expected from their application (Q2).

To better understand this relationship between access review challenges and digital nudges, we investigate and map access review challenges from Jaferian et al. [26] with the digital nudge taxonomy of Jesse and Jannach [27] by conducting semi-structured expert interviews based on the guidelines of Adams [1]. The interviewed industry experts provide practical experience in access control and reviews. Therefore, we target highly qualified professionals with at least five years of experience working with large IAM systems, periodical executed access reviews, and managing thousands of identities or consultants with practical experience for many enterprises. Of course, these highly qualified experts are not readily available, but we managed to acquire 10 of these experts through personal and professional contacts. The experts are located in Germany. We use their expertise for a well-grounded argumentation for the relationship between access review challenges and digital nudges. Section 5.1 details further on the method for the expert interviews.

3.3 User Study for the Choice Defaults Nudge

After laying out theoretical foundations for digital nudges and access reviews in Sections 4 and 5, we study the application of a selected digital nudge in-depth. The expert mapping of digital nudges and access review challenges suggests several digital nudges. To sharpen the scope of the use study, we select *N06: Choice Defaults* based on the following reasons:

- Literature considers *N06: Choice Defaults* among the most effective digital nudges [24].
- The expert interviews had strong positive and negative expectations, inviting a more detailed examination.
- We felt confident to apply the *N06: Choice Defaults* to an access review and study its effects precisely.

We design an access review, simulating a real case: experts often describe access reviews as repetitive, time-consuming, and tedious tasks, requiring a strenuous thought process to

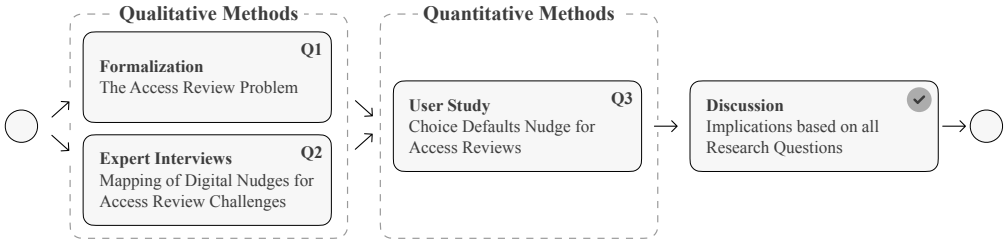


Figure 1: Mixed methods approach for this study.

determine correct authorizations. We thus hand out each participant a one-pager about the case. Participants manage a fictitious marketing department containing three teams within the case: graphic design, social media, and event management. The instruction describes the functions and tasks of each team and explains the unwanted implications of excessive or missing authorizations. While it is theoretically possible to review each decision using the document correctly, it takes some thought to make a correct decision.

To study the *N06: Choice Defaults* in-depth, we use three distinct configurations for access reviews with the same data basis: default accept, default reject, and a neutral default. This directly compares the default accept and reject configuration with a neutral state. The default accept configuration preselects every decision with an accept, the default reject vice versa, and the neutral default does not preselect.

We acquire 102 participants from a university context in Germany and randomly assign them to one of the three *N06: Choice Defaults* configurations. We select our sample size based on similar papers (c.f. Caine [10], also for the expert interviews). The (under-)graduate students have mostly a background in business informatics and IT security, indicating that they know essential IT security concepts and enterprise information systems. Furthermore, the participants are unaware of the research objective on digital nudges. We raffle a €100 gift card to one lucky participant to motivate participation. The participants must log in with authenticated accounts to avoid repeated participation and enable remote participation. We pilot the study with fellow researchers. Section 6.1 provides further details for the method.

3.4 Ethical considerations

Our experts were informed and consented to an anonymous publication of parts of their interviews. We will not share the recordings and delete the data one year after the publication.

The Institutional Review Board (IRB) *German Association for Experimental Economic Research e.V* approved the user study to comply with ethical requirements for working with humans. The certificate is available online.[1]

[1] https://gfew.de/en-ethik/HQwmKGTZ

4 Q1: The Access Review Problem

To better understand access review and benchmark our user study design, we introduce a representation of granted authorizations and security policies within a confusion matrix depicting User Permission Assignments (UPAs). Figure 2 maps the actually granted authorizations with security policies. We assess authorizations as effective access grants (which may contain errors), while security policies define the conceptual access users should have (ground truth). We construct a classical confusion matrix by mapping these authorizations and security policies with a binary distinction. Thus, the effectively granted UPAs are Predicted Positive (PP) as $PP = TP + FP$, while $P = TP + FN$ should be granted. PN and N are vice versa not-granted UPAs. Therefore, the True Positives (TPs) describe UPAs, granted in reality and conceptually. The sensitivity $SEN = \frac{TP}{P}$ represents the rate of correctly granted UPAs. Vice versa, True Negatives (TNs) describe UPAs, not granted in reality and in concept. The specificity $SPC = \frac{TN}{N}$ represents the rate of correctly not-granted UPAs. Together, sensitivity and specificity express the balanced accuracy $BA = \frac{SEN+SPC}{2}$, equaling 100% in a perfect world without errors.

		Authorization	
		Positive PP	Negative PN
Security Policy	Positive P	TP	FN
	Negative N	FP	TN

Figure 2: Confusion matrix for UPAs.

However, type I (False Positives (FPs)) and type II (False Negatives (FNs)) errors are present in reality. On the one hand, FPs are granted authorizations not considered by security policies (excessive UPAs). These excessive authorizations drive security risks, as over-privileged users are a target for threat actors. The primary goal for access reviews is lowering FP, which is highlighted in Figure 2. On the other hand, FNs are mistakenly not granted authorizations (missing UPAs). An example of their impact is when users cannot do their legitimate tasks because they do not have access to the required systems. This causes dissatisfaction for the users and slows down processes. In a relative notation, the False Discovery Rate (FDR) describes the percentage of excessive UPAs FP

based on PP as $FDR = \frac{FP}{PP}$. Vice versa, the False Omission Rate (FOR) describes missing UPAs as $FOR = \frac{FN}{PN}$.

Thus, an access review can be understood as transitioning from one UPA set depicted as confusion matrix C^1 to another C^2. The primary goal is to reduce the FDR while retaining or improving BA. We introduce definitions for Access Reviews (ARs) and the Access Review Problem (ARP) as:

Definition 4.1 (Access Review (AR))**.** Given a confusion matrix C^1 describing an UPA^1 set, an access review AR revokes a subset of the effectively granted authorizations $R \subset PP^1$. When executing AR a confusion matrix C^2 describes the resulting set as $UPA^2 = UPA^1 \setminus R$.

Definition 4.2 (Access Review Problem (ARP))**.** Design AR in such a way that a (human) deciders can review and revoke UPAs $R \subset PP^1$ according to their knowledge about security policies P^1, that the FDR is reduced ($FDR^1 > FDR^2$), without lowering BA ($BA^1 \leq BA^2$). The ARP is solved on a $FDR^2 = 0\%$ without decreasing BA: $BA^1 \leq BA^2$.

The following hypotheses hence allow testing whether an access review design improves the ARP:

H_0 An access review design does not improve the ARP as the FDR remains or rises $FDR^1 \leq FDR^2$ or BA remains or decreases $BA^1 \geq BA^2$.

H_1 An access review design improves the ARP as the FDR decreases $FDR^1 > FDR^2$ and the BA raises $BA^1 < BA^2$.

5 Q2: IAM Experts on Digital Nudges

5.1 Method Details

The interviews comprise three phases: an interviewee introduction, an explanation of access review challenges and digital nudges, and a workshop to generate the mapping of access review challenges and digital nudges. (i) The interviewee's introduction collects data about their access review experience, their perspective on its challenges, and their estimation of excessive authorizations (FP). (ii) The explanation phase ensures essential knowledge about digital nudges, reminds the interviewee of access review challenges, and ensures a common vocabulary. We use the interviewees' perspectives on access review challenges to explain to them the access review challenges of Jaferian et al. [26]. (iii) The procedure for querying the mapping for each considered digital nudge [27] follows this scheme: First, we explain the digital nudge in general and provide a suitable example for the interviewee. Afterward, we let the expert freely reflect on the effect of this digital nudge and its benefit to all access review challenges. Finally, we ask the expert to rate each access review challenge on a five-level Likert scale from very positive (+2) to very negative (-2). This rating scheme helps the expert to express their arguments more comparable to each other. The complete interview script is available in Appendix A.1.

We interviewed 10 highly qualified experts with experience in conducting several Access Reviews (ARs) specialized for IAM by implementing IAM tools (engineers), responsible for managing thousands of users in IAM systems (inhouse), or advising clients (consultants). Table 1 protects their identities but depicts their high expertise for ARs. The interviews took an average of 60 minutes and were recorded, transcribed, coded, and evaluated. We translated relevant parts of the interviews into English during the coding process.

Table 1: Participants for expert interviews.

Interview	Experience				Sector
	Years	Clients	Users	ARs	
E01: IAM consultant	8	40		20	Multiple
E02: IAM consultant	5	15		10	Multiple
E03: IAM engineer	12	40		15	Multiple
E04: IAM inhouse	8	15	1k	40	Insurance
E05: IAM consultant	19	25		10	Multiple
E06: IAM consultant	13	40		25	Multiple
E07: IAM consultant	6	15		50	Multiple
E08: IAM inhouse	15	2	19k	4	Biotech
E09: IAM consultant	11	4		10	Banking
E10: IAM inhouse	7	1	13k	120	Insurance

We recorded the interviews with Microsoft Teams, transcribed them with Word, and summarized and coded them with Excel. For the coding, we use both deductive and inductive coding [3]. Since we already know the access review challenges [26], we first applied deductive coding based on these challenges for each digital nudge. This deductive coding already sorts large parts of the interviews in proven codes. However, we noticed that several augmentations exist within these codes. Thus, we also developed inductive codes for each nudge and challenge combination to capture the interviews comprehensively. For the rating of each nudge and challenge pair, we initially used the mean expert ratings. After coding and comparing the interviews, we slightly adapted the ratings, to balance well-reasoned arguments across the experts. The resulting codebook is available in Appendix A.2.

5.2 Results

This section presents the experts' mapping. We build on the presented background of the access review challenges (C1-C5) in Section 2.2 and digital nudges (N01-N13) in Section 2.3. The resulting mapping is depicted in Table 2, whereas the challenges serve as columns and the digital nudges as rows. The cells summarized a rating for each challenge and nudge. In the following, we detail each digital nudge.

N01: The experts stress the benefits of comprehensible data. While C1 and C3 do not decrease, comprehensible data indirectly increases its learnability and comfort for the deciders, easing management eventually. For C2 and C4, the

Table 2: Nudges [27] and access review challenges [26].

Nudges	C1	C2	C3	C4	C5
N01: Information Translation	1	2	1	2	0
N02: Information Salience	1	0	1	1	2
N03: Information Visibility	1	2	0	1	2
N04: Information Phrasing	0	-1	0	1	0
N05: Range & Composition	2	1	1	2	2
N06: Choice Defaults	2	-2	2	-2	0
N07: Option Consequences	0	-1	1	-1	-1
N08: Option-related Effort ↗	-1	1	-1	1	1
N08: Option-related Effort ↘	1	-1	1	-1	-1
N09: Reminders	0	1	2	-1	0
N10: Commitment Facilitation	1	0	1	1	0
N11: Messenger Reputation	1	2	1	2	2
N12: Social Reference Point	0	2	0	1	2
N13: Empathy Instigation	1	1	1	1	0

Note: Option-related effort is ↗ = increased, ↘ = decreased. The Likert scale spans from very positive +2 to very negative -2.

experts anticipate a strong positive effect, as comprehension is essential for C2: *"If data is displayed more comprehensibly, it's helpful for users with little knowledge [C2] about the decision." (E06)*. Being comfortable with the data is relevant for C4: *"If the user is comfortable with the displayed data, you can expect fewer human errors [C4]." (E07)*

N02: The experts emphasize the focus: *"In my opinion is the highlighting of C5 the only option to manage large data sets." (E05)* However, *"it depends on the quality of the highlighting" (E03)*, since excessive or missing highlighting might draw away attention from relevant decisions. But upon sufficient and reliable quality, decision-makers can efficiently focus on the highlighted decisions or attributes and decide the remainder quicker (benefit for C1 and C3). Decision-makers *"actually want to decide diligently but are hindered by its scale. These decision-makers could diligently and mindfully decide just the highlighted decisions in an efficiency tradeoff." (E09)*

N03: Showing additional data is crucial for C2 and C5 to make informed decisions while streamlining the focus to relevant attributes (C4). By only offering limited attributes for each decision in default, the management of C1 is eased. However, the user might not know the relevancy of specific hidden attributes as these move out of focus (C4).

N04: Our interview partners express reservations as decisions might not be based on rational knowledge but on biased phrasing (C2). However, for a well-executed implementation, its utilization can raise the access review acceptance (C4) as its relevancy could be communicated more effectively.

N05: The setup of meaningful partitions and sorting imposes overhead compared to just showing all decisions in one turn, thus worsening C1 and C3. However, the experts anticipate quite positive effects on all challenges. Similar sorted or clustered partitions leverage efficiencies as decisions transfer to whole partitions. These efficiencies ease the management for C1 and C3 since the workload decreases, while more consistent and mindful decisions mitigate C2 and C4. Furthermore, clustering and appropriate communication of exceptional cases (C5) can positively influence.

N06: The experts discuss the strong effects of *N06: Choice Defaults*. Due to the reduced workload by the preselection, the experts rate a positive effect on C1 and C3. However, the experts worry that deciders adopt a preselected default without further thought, leading to uninformed (C2) and mindless (C4 and C5) decisions. While a mindful default prevents errors on uncertainty (like for C5) or on evident cases, just adopting the recommended default can become a fallacy, assuming the recommendation algorithm's imperfections. This is especially an issue if the decision-makers trust the preselection so that they mindlessly adopt the default instead of a mindful decision. A falsely set default would then lead to a systematic bias, endangering the next audit relevant to compliance. In sum, the experts anticipate the potential of *N06: Choice Defaults*, but advise careful application.

N07: *"In practice, negative consequences dominate. For example, we will tell your boss if you don't finish your access review tasks within 14 days." (E01)* The experts acknowledge that creative and positive consequences could be feasible and reasonable, making frequent access reviews more comfortable (C3). However, they doubt there would be a game-changer in the long term because the effects would wear down over time (C3), and the decisions might be based on avoiding pressure or pursuing benefits (C4) instead of reason (C2 and C5). In this context, it is also worth noting that *"disadvantaged individuals need special consideration" (E09)* because finishing an access review in time might not be fair for these (C5).

N08: This nudge's influence on the access review challenges is ambivalent, as it depends on whether the option-related effort is increased (↗) or decreased (↘). If the effort *increases* (vice versa for decrease), the users take more time to decide. For C1 and C3, this worsens the situation as the workload rises with its time consumption. Taking more time for a decision (e.g., requiring a reason for confirming a high-risk authorization) also benefits C2, C4, and C5, as the decider would need to consider a reason or reconsider the decision. But the experts also stressed the efficiency and acceptance of the access review, as some users easily become annoyed by increased effort: E.g., *"We once required the users to set a note for the reviewed authorizations, but one user just put question marks for every note to bypass the input check." (E04)*

N09: *"By a simple reminder [email], we observe more participation." (E10)* While reminders are especially relevant for C3 to communicate open tasks or instructions and goals for access reviews (C2), they can also pressure decision-makers to decide quickly but uninformed (C4). The audience and channel of reminders are also essential for C4. E.g., an inexperienced decider might require instructions or training. The experts also noted that reminders via an email channel

dominate in practice but are quickly perceived as spam. *"Everybody wants something from all colleagues. Ironically, some colleagues even configure automated email filters which they won't check afterward." (E09)* In this sense, a personal or multichannel address is most effective, but it is a considerable effort for the IAM team conducting the access review.

N10: The experts appreciate the autonomic commitment in combination with semantic partitioning (N05) of the decisions. An autonomic configuration of sub-goals and sub-deadlines suitable for the deciders benefits C1 and C3 as the deciders *"perceive control over scale and frequency" (E06)*. This leads to more comfort, as sub-goals and sub-deadlines become meaningful for the deciders, mitigating C4.

N11: The experts stress the importance of this nudge: *"Most important point; If the IAM team is not accepted, it is going be tough." (E04)* Furthermore, they note its failure in practice: *"Access reviews are usually perceived negatively." (E10)* With a suitable messenger reputation, users will trust and endure the tedious tasks of the access reviews more, which is beneficial for C1 and C3. The experts also anticipate strong benefits for C2, C4, and C5 as the decision-makers will dare to ask or tell an approachable IAM team their relevant questions or mistakes: *"If the IAM team is approachable, users communicate errors more eagerly or at all." (E07)*

N12: Similar to N11, if the social reference point sympathizes with the access review, decision-makers are likely to endure the tedious workload (C1 and C3). However, on low sympathy, the opposite effect might apply. The experts anticipate positive effects for C2, C4, and C5 because deciders discuss the access review: *"For example, we introduced access review chat groups for business units. Decision-makers can talk about access reviews, like showing their own or seeing others' progress, asking questions, etc." (E07)* In this sense, exceptional cases (C5) might become evident after a discussion and sharing knowledge about similar cases (C2), while noticing the colleagues' progress might remind stragglers or expose them to peer pressure (C4).

N13: *"On large scale [C1] and high frequency [C3], the decision-makers want to work with a pleasant tool." (E06)* Moral suasion and empathetic feedback (C2) can inform and convince the decision-maker about odd user behavior (e.g., mindlessly accepting all authorizations) without losing their motivation (C4). Reciprocity also fosters mitigation of C4 by *"always addressing the positive side: the access review is meant to help you, the decision-maker, to compliantly and securely maintain your authorizations." (E08)*

Furthermore, the experts estimate a mean on excessive authorizations (FP) at 22.8% ($SD = 6.4\%$). Since we also asked our experts about common AR challenges, we confirm the AR challenges first published by Jaferian et al. [26].

In summary, our experts conclude positive and negative effects when using digital nudges. Table 2 summarizes these key takeaways. We hope to motivate future work with it as most digital nudges invite dedicated research on access reviews.

6 Q3: Choice Defaults in Access Reviews

6.1 Method Details

In the data set of the user study (Appendix B.1), we let participants review (accept or remove) granted UPAs $PP = TP + FP$ (legit TP or excessive FP), leading to UPA revoke operations only. Not granted UPAs $PN = FN + TN$ (missing FN or legit TN) are not considered. After piloting, we determined 160 UPAs serving as decisions to align an estimated study duration of 20-30 minutes and not to deter participation. Therefore, the crafted data set comprises 160 UPAs (PP) split into 80 legitimate ones (TP) and 80 excessive ones (FP), clearly distinguished by a case study document (see Appendix B.2). Figure 3 summarizes the initial UPAs as a confusion matrix.

		Authorization	
		$PP = 160$	$PN = 232$
Security Policy	$P = 80$	$TP = 80$	$FN = 0$
	$N = 312$	$FP = 80$	$TN = 232$

Figure 3: Confusion matrix for the case of the user study.

We configure and execute the access reviews with the commercial tool NEXIS4[2]. The tool can import our data set, configure *N06: Choice Defaults*, execute large-scale access reviews, and collect relevant data points. Figure 4 displays a simplified screenshot of the review process. Further screenshots for all groups are available in Appendix B.3. For data collection, we make three observations for each access review participant: their decisions for the 160 UPAs, their time consumption, and their self-assessment for the NASA Task Load Index (TLX) [20]. (i) The tool stores each binary decision out-of-the-box, leading to a total of 16,320 manual decisions for 102 participants and 160 UPAs. (ii) We measure the time consumption for each participant by comparing the events for starting the access review and confirming the final completion prompt. (iii) After completion, we ask the participants to fill out a questionnaire for the NASA TLX [20] to capture their perceived workload. These questions are based on a Likert scale (-3 to +3) and include:[3]

- Mental Demand: How mentally demanding was the task?
- Temporal Demand: How hurried or rushed was the pace of the task?
- Performance: How successful were you in accomplishing what you were asked to do?
- Frustration Level: How insecure, discouraged, irritated, stressed, or annoyed were you?

[2] https://nexis-secure.com/en/

[3] We omitted the questions for physical demand and effort, as these are not applicable or relevant for our study.

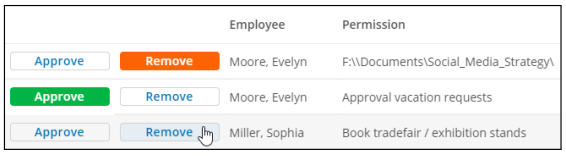


Figure 4: Simplified screenshot of the access review.

During the post-processing of the study, we used Microsoft Excel and R[4] for data cleansing or data analysis. Data cleansing primarily comprises capping the time consumption for the AR to 60 minutes, as some participants took a break. We calculate the means, standard deviations, and non-parametric ANOVA of the AR confusion matrix, time-consumption, and NASA TLX indices. For our exploratory analysis of correlations (Spearman) and local regressions, we utilize a pair plot generated in R (see Appendix Figure 9). Supporting the open data idea, we publish all data to replicate our results on GitHub: https://github.com/AccessReview/Availability.

6.2 Results

This Section summarizes our observations of the user study (see Table 3). A post-hoc power analysis based on ANOVA for our three groups ($n = 34$) and an $\alpha = .05$ results in effect powers of .13 for a small effect ($f = .1$), .6 for a medium effect ($f = .25$), and .95 for a large effect ($f = .4$).

For all 102 participants, the mean review time t for the 160 decisions is $t = 22$ minutes with $SD = 13$ minutes. Deciders of all groups used to over-accept authorizations, amounting to a total accept rate of $1 - \frac{R}{PP} = 56.1\%$ (rather than a $SEN = 50\%$). H_0 is rejected for 99 of 102 reviews. The remaining 3 participants failed to achieve an ARP improvement. All participants' mean BA increased from 87.2% to 91.2% (SD = 7.9%). The false discovery rate FDR, which represents the amount of excessive authorizations, was reduced from 50.0% to 21.6% (SD = 14.7%). This improvement came at the cost of some erroneous revokes, leading to a mean FOR of 2.9% (SD = 3.5%). In sum, most participants improved the ARP. The result data shows that two deciders behaved as "spammers" by either blindly accepting all authorizations (one decider in the accept group) or blindly rejecting them all (one decider in the reject group). These participants are among the three who failed to improve the ARP. While the data set is too small to make this finding statistically significant, it seems evident that the spammers just adopted the default.

The neutral configuration group is a control group for the default accept and reject nudge. Users from this group took a mean time of t = 26 minutes (SD = 15) and accepted 57.8% of the authorizations. The neutral group estimated the temporal demand as slightly low, with a mean score of -.8. On average, neutral users stated the mental demand to be slightly high (.9) and their frustration to be neutral to slightly high (.5). They estimated their performance to be slightly above average (.9). The achieved BA is 91.9% (SD = 5.8%), with the error rates FDR of 21.0% (SD = 10.7%) and FOR of 2.6% (SD = 2.5%).

The accept group only took t = 19 minutes (SD=10). With a time save of 24.3% to the neutral group. While the perceived TD was unchanged at -.8, both FL and MD were reduced by almost one point to a score of -.2 (Δ = -.7) and .2 (Δ = -.7). The accept rate was slightly higher than in the neutral group with 58.7% (+.9%). The default accept group achieved a BA of 92.3% (SD = 5.3%), scoring .4% higher than the neutral one. The error rates were also marginally better than in the neutral group with FDR = 20.8% (Δ = -.2%, SD = 9.3%) and FOR = 2.2% (Δ = -.4%, SD = 2.6%).

Like the accept group, deciders of the reject group finished quicker than the neutral group with t = 21 minutes (Δ = -16%, SD = 13). Again, the estimated TD of -.4 did not reflect this (Δ = +.4), but the stated FL and MD were reduced to -.6 (Δ = -1.1) and -.2 (Δ = -1.1). Unlike the accept group, however, the reject group showed a considerably reduced accept rate of 51.8% (-6.0%), which is very close to the initial $SEN = 50\%$. Unfortunately, the increased willingness to revoke did not improve the results: The deciders revoked fewer excessive authorizations than the neutral group (FDR = 22.9%, Δ = +1.9%, SD = 21.4%) and more correct ones (FOR = 3.9%, Δ = +1.3%, SD = 4.7%). With BA = 89.4% (SD = 11.2%), BA was still improved regarding the initial state (Δ = +2.2%), but worse than the neutral configuration (Δ = -2.5%).

We ran a non-parametric Kruskal-Wallis test ($\alpha = .05$) to check for the significance of our observations between the three groups. We detect differences for the number of revokes R ($p = 0.039$), indicating that *N06: Choice Defaults* did affect users' willingness to accept or reject authorizations. We also confirm differences for MD ($p = .049$) and FL ($p = .038$), indicating that lower stress perceptions result from the applied *N06: Choice Defaults*. We used Dunn's test for pairwise comparisons, showing that the neutral and reject groups differ for MD ($p.adj = .045$) and FL ($p.adj = .038$). However, the quality metrics BA, FDR, and FOR did not differ significantly between the study groups, which is unsurprising since the data set balances TP and FP at 80.

A test for Spearman correlation showed no significant correlation between review duration t and any of the quality metrics (BA, FDR, FOR), indicating that quality did not depend on the time spent. The data shows a significant positive correlation between the deciders' frustration level FL and t for the total population (.286) and the neutral group (.403), as well as between the stated mental demand MD and t (total: .237, neutral: .423). FL and MD are strongly correlated for all groups (total: .646, neutral: .589, accept: .672, reject: .664). We follow that deciders did not strictly distinguish between MD and FL and that longer reviews are perceived as more frustrating and/or mentally demanding. Interestingly, the per-

[4] https://www.r-project.org/

Table 3: General summary of the user study, including arithmetic means and standard deviations.

Group	*n*	Fails	*t*		*R*		*BA*		*FDR*		*FOR*		*MD*		*TD*		*PF*		*FL*	
			M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD	M	SD
Initial	-	-	-	-	-	-	.872	-	.500	-	.000	-	-	-	-	-	-	-	-	-
Total	102	3	22	13	70.3	19.2	.912	.079	.216	.147	.029	.035	.3	1.6	-.6	1.5	1.1	1.6	-.1	1.7
Neutral	34	0	26	15	67.5	12.4	.919	.058	.210	.107	.026	.025	.9	1.4	-.8	1.5	.9	1.5	.5	1.7
Accept	34	1	19	10	66.1	19.5	.923	.053	.208	.093	.022	.026	.2	1.5	-.8	1.5	1.2	1.6	-.2	1.8
Reject	34	2	21	13	77.2	22.8	.894	.112	.229	.214	.039	.047	-.2	1.8	-.4	1.6	1.1	1.7	-.6	1.6

Note: M for arithmetic mean and *SD* for standard deviation. *n* for the participant count and *Fails* for executions in rejecting $\mathbf{H_0}$. *BA*, *FDR* and *FOR* for measuring the Access Review Problem (ARP). *t* for the time-consumption of the AR and *R* for the amount of rejected UPAs. *MD* (Mental Demand), *TD* (Temporal Demand), *PF* (Performance) and *FL* (Frustration Level) for the NASA TLX.

ceived temporal demand TD did not correlate with t, possibly due to a missing baseline of a "normal" review duration. The result data showed a strong positive correlation between the perceived performance PF and actual performance BA (total: .607, neutral: .635, accept: .605, reject: .639), and a negative one between PF and the error rates FDR (total: -.336, neutral: -.516, reject: -.422; accept: not significant) and FOR (total: -.541, neutral: -.568, accept: -.480, reject: -.603). Therefore, the deciders had a realistic estimation of their performance. The result data also showed significant negative correlations between FL / MD and BA as well as positive ones between FL / MD and the error rates FDR / FOR, each for some groups. However, the causality remains unclear if deciders who find the task more difficult experience more stress, more stressed deciders deliver poor results, or both. Figure 9 (Appendix) shows the Spearman correlation and the local regressions.

➤ **Key takeaways of our user study:** (i) Almost all deciders improved the ARP. (ii) The required time differed substantially but was unrelated to quality (BA). (iii) *N06: Choice Defaults* led to reduced time effort and stress perception. (iv) A default reject led to more rejects. (v) A simple *N06: Choice Defaults* did not affect quality (BA) significantly but influenced the number of rejects. In detail, however, some increase in false rejects is tolerable as false accepts legitimate excessive authorizations leading to a false sense of security. (vi) Deciders' self-assessed performance correlates significantly with BA, indicating the deciders' realistic self-assessment.

7 Discussion

7.1 Acceptance Bias

Participants of the user study tend to accept existing authorizations. Existing research already documents and analyzes over-granting in real-world scenarios [18, 47, 54]. However, such scenarios involve strongly imbalanced data (see expert interviews: $1 - 22.8\% = 77.2\%$ of authorizations are estimated to be correct), social implications (a revoke acts against the interests of a real person), and unequal visibility of the two error types. Erroneous revokes are detected quickly, and the decider alone is responsible, while erroneous accepts are not immediately visible and all previous approvers share the responsibility for also not resolving the error. With an initial SEN of 50% and no personal repercussions, the study had none of these biases and made no implication that acceptance is favorable to revocation. Still, deciders accept authorizations too often, with an average accept rate of 57.8% in the neutral group (see Section 6.1). While the study data does not explain this behavior, a possible explanation might be that the status-quo bias discourages deciders from revoking [42]: Following a real-world scenario, the study description states that participants need to review *existing* authorizations, which would be revoked upon rejection. The existence of a general status quo bias could also explain the relatively weak effect of the default accept bias on the accept rate: Study participants with default accept or reject nudge configuration needed to change an existing preselection to make an active decision and are thus also confronted with a status quo bias. If a status quo bias is already the reason for over-accepting in the neutral group, the effect of the default accept nudge would only repeat an already present bias. In contrast, the default reject nudge creates a new status quo that nudges the deciders in the opposite direction. The explanation seems plausible based on the study results, as the accept rate of the default accept group is closer to the neutral group (58.7%), and the accept rate of the default reject group is closer to the actual 50% (51.8%).

7.2 Implications for Access Review Challenges

➤ **Decider motivation affects quality (C4):** As described in Section 6.2, the user study participants had a reasonable estimation of their own performance. The user study design is fair, with a planned execution time of 20-30 minutes and no hurdles for *N01: Information Translation* or *N03: Information Visibility*. Still, some deciders submitted results with relatively low quality. The correlations between perceived stress (FL, MD) and quality (BA, FDR, FOR) may also indicate that decider motivation was an important factor. It must be assumed that poor decider motivation contributes stronger in real-world scenarios with larger scale and poorer information basis, indicating that nudges targeting decider motivation (*N09-N13*) may be a valuable contribution to AR quality.

➤ **Longer reviews are more demanding (C1, C4):** The user study results showed significant correlations between the review duration t and the perceived stress (FL, MD), underlining the importance of a reasonable scale. While the user study already confirms that *N06: Choice Defaults* considerably reduces review time, *N05: Range & Composition* also seems promising. Choice architects should take care not to overwhelm deciders with too many decisions. Distributing review responsibilities to many instead of a few decision-makers might be helpful. Considering *N10: Commitment Facilitation* or splitting reviews into multiple suitable sub-reviews carried out at different times or limiting them to unreviewed or changed authorizations could also improve quality.

➤ **N06: Choice Defaults effectivity does not seem to depend on decision difficulty (C2, C4, C5):** We tried to assess whether the impact of *N06: Choice Defaults* depends on the difficulty of a decision. For this purpose, we grouped the user study decisions by the 160 UPAs and their respective study group (neutral, default accept, default reject), resulting in $3 * 160$ groups of 34 review decisions. We then calculated the error rate and standard deviation for the decisions in the neutral group as indicators of the decision difficulty or uncertainty of UPA. To measure the effect of the default accept nudge for any UPA, we subtract the number of accepts in the neutral group from the amount of accepts in the default accept group. The resulting difference is the amount of *additional* accepts achieved by the nudge. The default reject effectivity was calculated as equivalent to the difference of rejects in the neutral and default reject groups. A Spearman correlation test with a $\alpha = .05$ significance level showed no significant correlation between the indicators for a decision's difficulty and the amount of additional accepts or rejects. The lack of correlation indicates that the effectivity of *N06: Choice Defaults* does not directly depend on the difficulty of a decision.

➤ **Spammers are an error source (C4):** Unlike the user study but in reality, a ground truth of detecting low-quality AR results is not available. Hence, it is helpful to identify "spammers" (deciders actually not trying to achieve an ARP improvement). The user study results suggest two possible ways to determine low-quality AR results: (i) While the review duration t did not correlate significantly with the quality metrics, we found that for the $n = 6$ deciders only taking $t = 6$ minutes or less, the mean BA ($M = 77.1\%$, $SD = 22.1\%$) drops a considerably $\Delta = -14.1\%$ comparing to BA of all participants ($M = 91.2\%$, $SD = 7.9\%$). (ii) Two spammers acted obviously ignorant by blindly accepting or rejecting all authorizations. In real-world scenarios, it might be helpful to use thresholds that, when undercut, classify the review as spam. We do not propose to dismiss such results categorically: it could be correct to accept all authorizations, or a decider could be quick. However, such deciders could be explicitly addressed to improve their result quality, e.g., by applying a custom nudge (like *N13: Empathy Instigation*) or requesting another person to check their decisions.

Table 4: Virtual best and worst advice.

Group	*n*	*R*	*BA*	*FDR*	*FOR*
Initial	-	-	.872	.500	.000
Total	102	70.3	.912	.216	.029
Virtual Best Advice	34	71.2	.931	.178	.023
Virtual Worst Advice	34	72.1	.885	.238	.043

Note: n for the participant count and *R* for the mean of rejected UPAs. *BA*, *FDR* and *FOR* are means for measuring the Access Review Problem (ARP).

➤ **Deciders have the last say (C4):** We re-grouped the user study decisions to simulate reviews with only correct and only incorrect *N06: Choice Defaults* (compare smart defaults [4, 5]). In reality, every decider had to make 160 decisions, of which 80 were TP (should be accepted) and 80 were FP (should be removed). This means that the default accept group had a correct preselection for exactly 80 authorizations, whereas the default reject group had a correct preselection for the other 80 ones. By virtually re-grouping these decisions, we create two sets of $34 * 160$ decisions each, for which one contains only correct default preselections and the other contains only incorrect ones. We then calculated the quality metrics BA, FDR, and FOR for both groups. Unsurprisingly, the virtual best advice group scored a higher overall quality than each of the three real study groups with $BA = 93.1\%$, and the lowest error rates with $FDR = 17.8\%$ and $FOR = 2.3\%$. The virtual worst advice group scored worse than all real groups with $BA = 88.5\%$, $FDR = 23.8\%$, and $FOR = 4.3\%$. However, the virtual best advice group's results are closer to those of all real groups than a perfect result, for which BA would be 100% and both error rates would be 0%. Similarly, the virtual worst advice group did not perform terribly but, in fact, still achieved a mean improvement in the ARP. Results for both groups show that users are affected by the *N06: Choice Defaults* and that the quality of the applied nudge affects the quality of the AR result. However, deciders have the last say and may choose not to follow a default, attenuating the worst assumptions of some interviewed experts. Table 4 summarizes the figures for both virtual groups.

7.3 Two Undesired Responsibility Shifts

Real-world access reviews (without nudge support) assume reflective decision-makers in transparent environments, leading to two assumptions: reflection and transparency [11]. However, the expert interviews and the user study discard both assumptions. For the reflection assumption, experts report several instances of human errors (C4), and the user study shows that deciders are affected by *N06: Choice Defaults*. Additionally, the deciders make errors despite having all the necessary data (even for the best advice in Table 4). For the transparency assumption, experts report the troublesome endeavor to present the information needed (*N01-N03, N09*) as too many or too few details lead to an unclear big picture.

Hansen and Jespersen [19] evaluate ethical considerations for nudge applications by the nudge's transparency and the decider's reflective or automatic mode of thinking. As mentioned earlier, access reviews should strive for transparency and reflective decisions. Access reviews in the real world and those with nudges can fail one of these: the real-world access reviews can lack transparency, and the nudged ones can lack reflective choices. On the one hand, real-world access reviews force reflective decisions as overwhelmed deciders actively need to choose, leading to a lack of transparency and constructing an unpleasant ethical situation. While reflective choices make the deciders fully responsible for their actions, the sheer scale (C1) and frequency (C3) put so many decisions on the table that the actual big picture for the access review becomes non-transparent. Therefore, the deciders have to bear the responsibility for a volume of decisions above their capabilities as human decision-makers, raising ethical concerns. On the other hand, the access reviews with the *N06: Choice Defaults* stay more transparent but allow for less reflective decisions, leading to a responsibility split. As soon as scale (C1) and frequency (C3) make the deciders give up on reflective choices, the choice architect shares responsibility for the decision-makers adopting its defaults.

In summary, neither burdening the deciders with the responsibility of choices they do not comprehend nor splitting the responsibility between the choice architect and the deciders are desired responsibility shifts for access reviews.

7.4 Design Implications for Usability

Following Hansen and Jespersen [19], design implications for future access reviews (with digital nudges) involve facilitating meaningful decisions based on transparency and reflective choices. When applied properly, digital nudges empower deciders to make confident and meaningful decisions with transparent and honest guidance [19]. Most importantly, this implies perceiving access review deciders and their decisions not as hyper-rational but as human, including their strengths and flaws [21, 40]. In the following, we derive three implications for usability based on our results.

➤ **Partition meaningfully:** Several experts find *N05: Range & Composition* relevant as it allows for meaningful partitions of access review decisions. Partitions effectively mitigate the deciders' scale perception and give a context for grouped decisions. Additionally, this allows abstract decisions for the whole partition. For example, deciding to revoke all authorizations of a person can be one meaningful decision instead of rejecting each of its authorizations one by one. Our experts name meaningful ways to partition decisions within access reviews, e.g., people leaving an organization, specific applications, critical authorizations, known past changes, organization-specific attributes, or processes. Ways to determine these partitions can range from choice architects' or deciders' experience to AI-based clustering.

➤ **Apply partition-specific digital nudges:** Digital nudges can be applied individually and combined for each partition. Based on the expert interviews, various digital nudges are suitable. For example, *N06: Choice Defaults* can preselect accepting security-uncritical authorizations (e.g., utility software) or rejecting security-critical ones (e.g., server access). Additionally, security-critical authorizations can be highlighted with a warning by *N02: Information Salience*. Thus, digital nudges can improve each partition's usability to guide access review deciders, also considering individual organizational contexts.

➤ **Query performance perception:** In the user study results, we find a strong correlation in all groups for the objective quality metric *BA* and the deciders' performance self-assessment *PF*. It shows that our user study participants had a reasonable perception of their performance. In contrast, a real-world access review cannot determine *BA* easily, as the underlying ground truth is unknown. This implies querying the deciders' performance self-assessment (*PF*) can be a valid and easy-to-implement estimator for the access review's quality (*BA*).

In summary, transparent digital nudges can guide human decision-makers to make meaningful, confident, and reflective choices. While the positive and negative effects of nudging require careful consideration, their anticipated effects are useful and promising tools for access review designs.

8 Conclusion

In this paper, we investigated digital nudges for access reviews. We formalized the access review problem. Subsequently, we interviewed highly qualified IAM experts to map the expected effects of digital nudges on access review challenges. Furthermore, we conducted a user study with *N06: Choice Defaults*. We found its influence on deciders' behavior in revoking authorizations. Additionally, we achieve time savings (up to 24.3%) and lower frustration. A simple *N06: Choice Defaults* did not significantly influence the overall quality, but it can shift the decisions to more revokes. While these revokes cause some false rejects, false accepts would be worse as they create a false sense of security by legitimating excessive authorizations. For future work, we invite researchers to study the ARP, to investigate other digital nudges of Table 2 or their combinations, or to replicate this study with a larger sample size or smart defaults [4, 5]. In sum, digital nudges are a promising tool to improve access reviews but need careful application.

Availability

For transparency and future research, we make the case study, all collected data, and the analysis of the user study open-source (https://github.com/AccessReview/Availability). In detail, we publish the instructions and data set of the case study, participants' results ($n = 102$), their choices ($n = 16,320$), and the *R* code to replicate our statistical evaluations.

Acknowledgments

The German Federal Ministry of Education and Research supported the research leading to these results as part of the DEVISE project (https://devise.ur.de).

This work would not have been possible without the help of our 10 interviewed experts and 102 user study participants. The experts invested a total of 10 hours and the participants a total of 42 hours to support our endeavor. Thank you!

References

[1] William C. Adams. *Conducting Semi-Structured Interviews*, chapter 19, pages 492–505. John Wiley & Sons, Ltd, 2015.

[2] Marvin Auf der Landwehr, Maik Trott, and Christoph von Viebahn. Consumers choice? fostering sustainability in grocery deliveries through digital nudging. In *Twenty-Ninth European Conference on Information Systems (ECIS 2021)*, ECIS 2021, page 1–16. Association for Information Systems, 2021.

[3] Theophilus Azungah. Qualitative research: deductive and inductive approaches to data analysis. *Qualitative Research Journal*, 18(4):383–400, Jan 2018.

[4] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. A data-driven approach to developing iot privacy-setting interfaces. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces*, IUI '18, page 165–176, New York, NY, USA, 2018. Association for Computing Machinery.

[5] Paritosh Bahirat, Martijn Willemsen, Yangyang He, Qizhang Sun, and Bart Knijnenburg. Overlooking context: How do defaults and framing reduce deliberation in smart home privacy decision-making? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[6] Basel Committee on Banking Supervision. Basel III: A global regulatory framework for more resilient banks and banking systems, June 2011.

[7] Thomas Baumer, Mathis Müller, and Günther Pernul. System for cross-domain identity management (scim): Survey and enhancement with rbac. *IEEE Access*, 11:86872–86894, 2023.

[8] Michelle Berger, Elias Greinacher, and Linda Wolf. Digital nudging to promote energy conservation behavior - framing and default rule in a smart home app. In *Thirtieth European Conference on Information Systems (ECIS 2022)*, ECIS 2022, page 1–16. Association for Information Systems, 2022.

[9] Kristoffer Bergram, Marija Djokovic, Valéry Bezençon, and Adrian Holzer. The digital landscape of nudging: A systematic literature review of empirical research on digital nudges. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[10] Kelly Caine. Local standards for sample size at chi. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 981–992, New York, NY, USA, 2016. Association for Computing Machinery.

[11] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–15, New York, NY, USA, 2019. Association for Computing Machinery.

[12] Federal Financial Supervisory Authority (BaFin). Rundschreiben 05/2023 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk, June 2023.

[13] Sandro Franzoi and Jan vom Brocke. Sustainability by default? nudging carbon offsetting behavior in e-commerce. In *Thirtieth European Conference on Information Systems (ECIS 2022)*, ECIS 2022, page 1–15. Association for Information Systems, 2022.

[14] Ludwig Fuchs and Günther Pernul. HyDRo – hybrid development of roles. In *Information Systems Security*, pages 287–302. Springer Berlin Heidelberg, 2008.

[15] Ludwig Fuchs, Günther Pernul, and Ravi Sandhu. Roles in information security – a survey and classification of the research area. *Computers & Security*, 30(8):748–769, 2011.

[16] Cristina Gena, Pierluigi Grillo, Antonio Lieto, Claudio Mattutino, and Fabiana Vernero. When personalization is not an option: An in-the-wild study on persuasive news recommendation. *Information*, 10(10), 2019.

[17] Abdul Muqeet Ghaffar and Thomas Widjaja. Framing as an app-design measure to nudge users toward infection disclosure in contact-tracing applications. In *Thirty-first European Conference on Information Systems (ECIS 2023)*, ECIS 2023, page 1–16. Association for Information Systems, 2023.

[18] Sebastian Groll, Sascha Kern, Ludwig Fuchs, and Günther Pernul. Monitoring access reviews by crowd labelling. In Simone Fischer-Hübner, Costas Lambrinoudakis, Gabriele Kotsis, A. Min Tjoa, and Ismail

Khalil, editors, *Trust, Privacy and Security in Digital Business*, pages 3–17, Cham, 2021. Springer International Publishing.

[19] Pelle Guldborg Hansen and Andreas Maaløe Jespersen. Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation*, 4(1):3–28, 2013.

[20] Sandra G. Hart. Nasa-task load index (nasa-tlx); 20 years later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 50(9):904–908, 2006.

[21] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees who Don't accept the time security takes are not aware Enough": The CISO view of Human-Centred security. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 2311–2328, Anaheim, CA, August 2023. USENIX Association.

[22] Linda Hill. How automated access verification can help organizations demonstrate HIPAA compliance: A case study. *J Healthc Inf Manag*, 20(2):116–122, 2006.

[23] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Arthur R. Friedman, Alan J. Lang, Margaret M. Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone, et al. Guide to attribute based access control (abac) definition and considerations (draft). Technical report, National Institute of Standards and Technology, 2014.

[24] Dennis Hummel and Alexander Maedche. How effective is nudging? a quantitative review on the effect sizes and limits of empirical nudging studies. *Journal of Behavioral and Experimental Economics*, 80:47–58, 2019.

[25] Matthias Hummer, Sebastian Groll, Michael Kunz, Ludwig Fuchs, and Günther Pernul. Measuring identity and access management performance - an expert survey on possible performance indicators. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pages 233–240. SCITEPRESS - Science and Technology Publications, 2018.

[26] Pooya Jaferian, Hootan Rashtian, and Konstantin Beznosov. To authorize or not authorize: Helping users review access policies in organizations. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 301–320, USA, 2014. USENIX Association.

[27] Mathias Jesse and Dietmar Jannach. Digital nudging with recommender systems: Survey and future directions. *Computers in Human Behavior Reports*, 3:100052, 2021.

[28] Eric J. Johnson, Suzanne B. Shu, Benedict G. C. Dellaert, Craig Fox, Daniel G. Goldstein, Gerald Häubl, Richard P. Larrick, John W. Payne, Ellen Peters, David Schkade, Brian Wansink, and Elke U. Weber. Beyond nudges: Tools of a choice architecture. *Marketing Letters*, 23(2):487–504, Jun 2012.

[29] Shelia M. Kennison, Ian T. Jones, Victoria H. Spooner, and D. Eric Chan-Tin. Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, 4:100132, 2021.

[30] Sascha Kern, Thomas Baumer, Ludwig Fuchs, and Günther Pernul. Maintain high-quality access control policies: An academic and practice-driven approach. In Vijayalakshmi Atluri and Anna Lisa Ferrara, editors, *Data and Applications Security and Privacy XXXVII*, pages 223–242, Cham, 2023. Springer Nature Switzerland.

[31] Sascha Kern, Thomas Baumer, Sebastian Groll, Ludwig Fuchs, and Günther Pernul. Optimization of access control policies. *Journal of Information Security and Applications*, 70:103301, 2022.

[32] Stefan Meier, Ludwig Fuchs, and Günther Pernul. Managing the access grid - a process view to minimize insider misuse risks. In *11th International Conference on Wirtschaftsinformatik (WI2013)*, pages 1051–1065, 2013.

[33] Christian Meske and Tobias Potthoff. The dinu-model - a process model for the design of nudges. In *European Conference on Information Systems*, pages 2587–2597, 06 2017.

[34] Tobias Mirsch, Christiane Lehrer, and Reinhard Jung. Making digital nudging applicable: The digital nudge design method. In *International Conference on Information Systems*. AIS, 2018.

[35] Robert Münscher, Max Vetter, and Thomas Scheuerle. A review and taxonomy of choice architecture techniques. *Journal of Behavioral Decision Making*, 29(5):511–524, August 2015.

[36] OWASP Top 10 team. Owasp top10, 2021. Accessed: 11/15/23.

[37] Simon Parkinson and Saad Khan. A survey on empirical security analysis of access-control systems: A real-world perspective. *ACM Comput. Surv.*, 55(6), dec 2022.

[38] Alexander Puchta, Fabian Böhm, and Günther Pernul. Contributing to current challenges in identity and access management with visual analytics. In Simon N. Foley, editor, *Data and Applications Security and Privacy*

XXXIII, pages 221–239, Cham, 2019. Springer International Publishing.

[39] Alexander Puchta, Sebastian Groll, and Günther Pernul. Leveraging dynamic information for identity and access management: An extension of current enterprise iam architecture. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP*, pages 611–618, Online Streaming, 2021. INSTICC, SciTePress.

[40] Ita Ryan, Utz Roedig, and Klaas-Jan Stol. Unhelpful assumptions in software security research. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, page 3460–3474, New York, NY, USA, 2023. Association for Computing Machinery.

[41] Pierangela Samarati and Sabrina Capitani de Vimercati. Access control: Policies, models, and mechanisms. In Riccardo Focardi and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design*, pages 137–196, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[42] William Samuelson and Richard Zeckhauser. Status quo bias in decision making. *Journal of risk and uncertainty*, 1:7–59, 1988.

[43] Ravi S. Sandhu. Role-based access control. portions of this chapter have been published earlier in sandhu et al. (1996), sandhu (1996), sandhu and bhamidipati (1997), sandhu et al. (1997) and sandhu and feinstein (1994). In Marvin V. Zelkowitz, editor, *Advances in Computers*, volume 46 of *Advances in Computers*, pages 237–286. Elsevier, online, 1998.

[44] Armando Schär and Katarina Stanoevska-Slabeva. Application of digital nudging in customer journeys - A systematic literature review. In *25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019*. Association for Information Systems, 2019.

[45] Christoph Schneider, Markus Weinmann, and Jan vom Brocke. Digital nudging: Guiding online user choices through interface design. *Commun. ACM*, 61(7):67–73, jun 2018.

[46] Daniel Servos and Sylvia L. Osborn. Current research and open problems in attribute-based access control. *ACM Comput. Surv.*, 49(4), jan 2017.

[47] Bingyu Shen, Tianyi Shan, and Yuanyuan Zhou. Improving logging to reduce permission Over-Granting mistakes. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 409–426, Anaheim, CA, August 2023. USENIX Association.

[48] Cass R. Sunstein. The council of psychological advisers. *Annual Review of Psychology*, 67(1):713–737, 2016. PMID: 26393867.

[49] Barnabas Szaszi, Anna Palinkas, Bence Palfi, Aba Szollosi, and Balazs Aczel. A systematic scoping review of the choice architecture movement: Toward understanding when and why nudges work. *Journal of Behavioral Decision Making*, 31(3):355–366, 2018.

[50] Richard H. Thaler and Cass R. Sunstein. *Nudge: Improving decisions about health, wealth, and happiness.* Nudge: Improving decisions about health, wealth, and happiness. Yale University Press, New Haven, CT, US, 2008.

[51] United States Congress. Health Insurance Portability and Accountability Act of 1996, 1996.

[52] United States Congress. Sarbanes-Oxley Act of 2002. Corporate responsibility, 2002.

[53] Markus Weinmann, Christoph Schneider, and Jan vom Brocke. Digital nudging. *Business & Information Systems Engineering*, 58(6):433–436, Dec 2016.

[54] Tianyin Xu, Han Min Naing, Le Lu, and Yuanyuan Zhou. How do system administrators resolve access-denied issues in the real world? In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 348–361, 2017.

[55] Sarah Y. Zheng and Ingolf Becker. Checking, nudging or scoring? evaluating e-mail user security tools. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 57–76, Anaheim, CA, August 2023. USENIX Association.

[56] Samira Zibaei, Dinah Rinoa Malapaya, Benjamin Mercier, Amirali Salehi-Abari, and Julie Thorpe. Do password managers nudge secure (random) passwords? In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 581–597, Boston, MA, August 2022. USENIX Association.

[57] Samira Zibaei, Amirali Salehi-Abari, and Julie Thorpe. Dissecting nudges in password managers: Simple defaults are powerful. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 211–225, Anaheim, CA, August 2023. USENIX Association.

Appendix

A Expert Interviews

A.1 Interview Script

I. Intro Section

Interview partner

- *What is your job position at organization XY?*
- *What is your IAM experience (years, clients, access review projects, managed identities, etc.)?*

Access review and its problems

- *Estimate the ratio of excessive granted access.*
- *Name 2-3 major challenges for access reviews.*

II. Explanation Section

- *Explain to the participant the access review challenges of Jaferian et al. [26]. Connect them to the major challenges of access review the participant named before.*
- *Explain to the participant digital nudges in general.*

III. Workshop Section
Mapping digital nudges and access review challenges
For each nudge in Table 5

1. *Explain the nudge and give an example fitting for the interview participant's environment.*
2. *The participant then freely reflects on the digital nudge and their relationship on access review challenges.*
3. *Finally, the participant rates each access review challenge, anticipating a very positive (+2), positive (+1), neutral (0), negative (-1), or very negative (-2) effect.*

Table 5: Digital Nudges [27] presented to the experts for mapping them to access review challenges [26].

Nudges	***C1***	***C2***	***C3***	***C4***	***C5***
Decision Information					
N01: Information Translation					
N02: Information Salience					
N03: Information Visibility					
N04: Information Phrasing					
Decision Structure					
N05: Range & Composition					
N06: Choice Defaults					
N07: Option Consequences					
N08: Option-related Effort					
Decision Assistance					
N09: Reminders					
N10: Commitment Facilitation					
Social Decision Appeal					
N11: Messenger Reputation					
N12: Social Reference Point					
N13: Empathy Instigation					

Wrap-up

- *Name your TOP 3 digital nudges benefiting access review challenges.*

A.2 Codebook

We apply deductive and inductive coding to the expert interviews. The feasibility of digital nudges (based on the collection of Jesse and Jannach [27]) for access reviews suffice as interview questions. The access review challenges of Jaferian et al. [26] suffice as deductive codes, which we applied a priori to the interviews. Therefore, we trained and asked the interview partners about these challenges and asked for a Likert scale-based rating (2 (best), 1, 0, -1, -2 (worst)). The experts answered with different arguments, for which we extracted inductive codes. The rating for digital nudge, challenge and the inductive codes are detailed in the codebook (Table 6).

B User Study

B.1 Data Set

For the user study, we used a crafted data set (160 UPAs). We can pinpoint which UPAs are correctly (TP) and incorrectly (FP) assigned. Figure 5 (using a grid representation based on [32]) depict the data set. A processable format is available at GitHub.

B.2 Ground Truth Document

Access Review Case Study
You work as a busy head of the marketing department in a large industry company with many concurrent projects to maximize the income for your company. Your time is limited, and you have marketing goals to fulfill.
The security teams reminded you via email that your company is legally required (compliance) to review the permission assignments for the employees in your department. You must follow the **principle of least privilege**: Employees must have permissions required for their job, but not more. If you decide to revoke an excessive permission for one of your employees, the employee will no longer be able to access the associated resources by tomorrow.
While the security team points out that any excessive permission poses a security threat, you are aware that missing ones might prevent your employees from working until they re-obtain it via a time-consuming help-desk or self-service request.
The marketing department consists of three teams:

I. Graphic design team

- Create and edit images for the company's media and advertisement presence. This includes banners, logos, websites, or campaign designs that are used in advertisements or social media posts.
- Require a Photoshop license to work.

II. Social media team

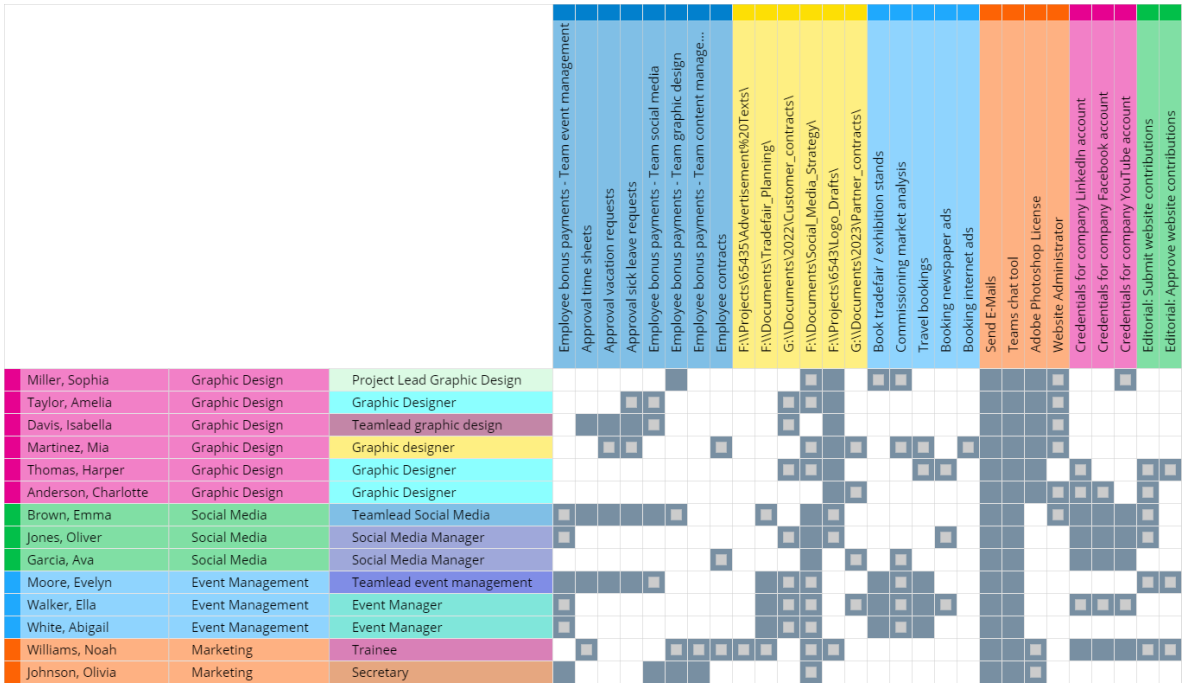


Figure 5: Grid visualization [32] of the user study data set. Blue cells resemble TP, gray ones FP, white ones TN, and FN were not present in the data set.

- Manage the company's social media accounts.
- Need to communicate with potential customers, candidates for recruiting, and partners online.

III. Event management team

- Organize trade fairs and partner events across West and Central Europe.
- Book trade fair stands.
- High self-organization; often need to attend remote events without long preparation.

IV. Department hierarchies

- Every team is led by a team lead who overlooks the employee's attendance and work results.
- Team leads have an annual budget for bonus payments, which they can distribute among their team members based on last year's performance. The secretary reads the specified bonus payments defined by the team leads from the HR system and arranges for the salary to be posted.
- The department's trainee used to intern in the graphic design team. Now, he is working in the social media team.

V. Misc

- Everybody communicates with MS Teams and Outlook.
- You can sort the columns.

B.3 Screenshots Access Review

We used three configurations of the access reviews with the same data basis. Figure 6, the neutral default, has two white buttons without a preselection. Figure 7 displays the default accept with a preselected *Approve*. Figure 8 shows the default reject with a preselected *Remove*.

B.4 Statistical Analysis

Figure 9 depicts a pair plot for each metric separated for their group. Green shows the default accept group, red the default reject, and blue the neutral one. The upper right part depicts Spearman correlations. The stars indicate the significance levels as "***": $p < .001$; "**": $p < .01$; "*": $p < .05$, and "." $p < .1$. The lower left depicts local regressions. Finally, the diagonal, the first row and column show metric distributions.

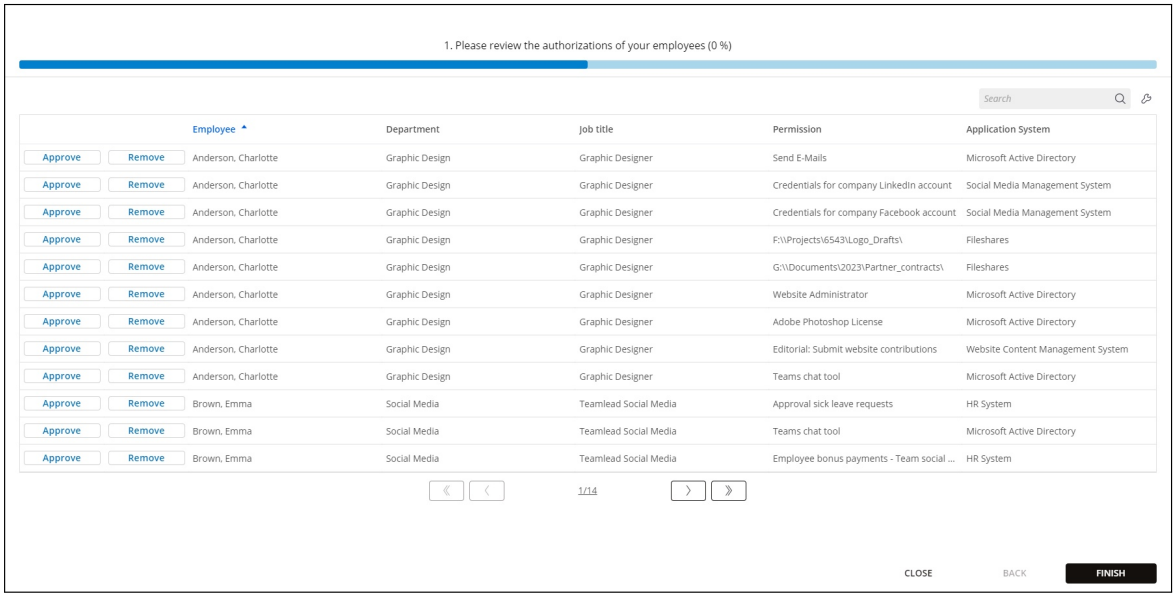


Figure 6: Screenshot of the neutral group for the user study.

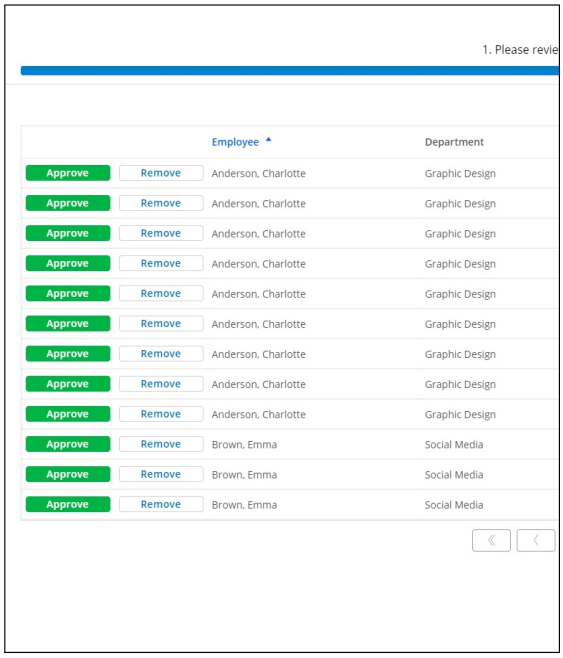


Figure 7: Screenshot for the accept group.

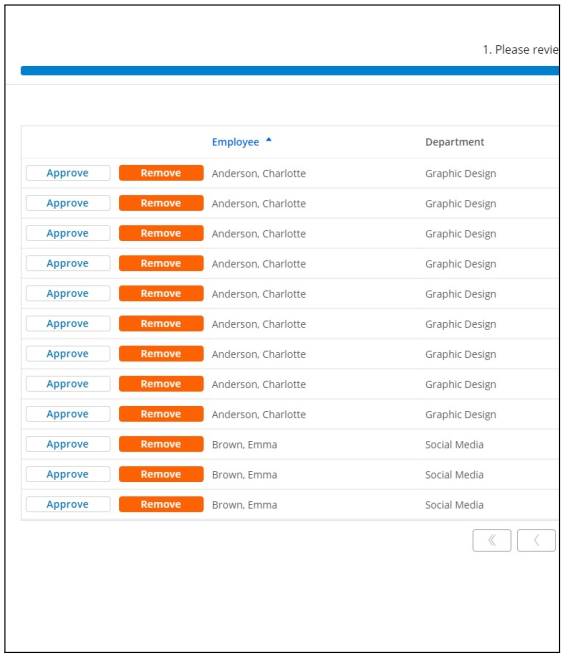


Figure 8: Screenshot for the reject group.

Table 6: Codebook for expert interviews.

N	C	Likert	Inductive Codes
N01	C1	1	Understandability (E02, E03, E04, E09); No effect (E03, E06, E08, E10); Feel-Good (E02, E03); Uniqueness (E04, E09); Structure (E09)
N01	C2	2	Understandability (E02, E05, E06, E07, E08, E09, E10); Mental Load (E03, E05, E07, E09); Acceptance (E05, E07, E10); Wording (E05, E06, E07)
N01	C3	1	Recognition (E01, E04, E05, E06, E09); Learning (E04, E05, E09); Feel-Good (E05, E06)
N01	C4	2	Understandability (E02, E05, E07, E08, E09, E10)
N01	C5	0	Understandability (E05, E06); Recognition (E04)
N02	C1	1	Focus (E01, E02, E04, E05, E09); No effect (E06, E08, E10)
N02	C2	0	Focus (E06, E09, E10); No effect (E03, E07, E09)
N02	C3	1	Economic Efficiency (E01, E02, E04, E07, E09); Focus (E01, E02); Acceptance (E09)
N02	C4	1	Focus (E03, E05, E06, E07, E08, E09, E10); Algorithm-Quality (E03, E06, E09); Backlash (E03, E06, E09)
N02	C5	2	Focus (E03, E04, E05, E07, E10); Algorithm-Quality (E09)
N03	C1	1	More relevancy (E03, E04, E05, E07, E09); Less confusion (E03, E04, E05, E09); No reduction of decisions (E06, E08)
N03	C2	2	Showing more data (E01, E05, E08, E09, E10); Relevancy (E03, E04, E06)
N03	C3	0	Run-time (E05); Recognition (E07)
N03	C4	1	Mistake mitigation (E05, E07, E09, E10); Focus (E06, E07)
N03	C5	2	Showing more data (E01, E07, E09, E10); Need to know (E07, E10)
N04	C1	0	Insecurities of decision-maker (E09); Sense of responsibility (E07)
N04	C2	-1	Context-Awareness (E05, E07, E08, E09, E10); Bias (E04, E05, E09), Base direction (E05, E09)
N04	C3	0	Acceptance (E07)
N04	C4	1	Acceptance (E06; E08; E09; E10); Focus (E06, E09, E10); Pressure (E02)
N04	C5	0	Focus (E06, E07, E10)
N05	C1	2	Similarities (E01, E03, E04, E05, E07, E08, E09); Overhead (E08, E10)
N05	C2	1	Focus (E04, E08, E09, E10); Audience (E08, E09)
N05	C3	1	Economic Efficiency (E03, E05, E06); More Tasks (E09, E10)
N05	C4	2	Focus (E01, E03, E05, E06, E07, E09, E10); Similarities (E01, E05, E06, E07); Smaller Batches (E09, E10)
N05	C5	2	Exceptional Case Detection and View (E02, E03, E04, E07, E09)
N06	C1	2	Less work (E01, E02, E04, E05, E06, E09); No reduction of decisions (E07, E10)
N06	C2	-2	Recommendation Fallacy (E02, E04, E05, E06, E07, E09, E10); Recommendation Support (E06, E09)
N06	C3	2	Less work (E01, E02, E04, E05, E06, E08, E09)
N06	C4	-2	Less diligence/Focus (E01, E02, E04, E05, E06, E07, E09, E10); Recommendation Fallacy (E02, E04, E05, E06, E07, E09, E10)
N06	C5	0	Not in Focus (E05, E07, E10); Default handling (E06, E09); Special treatment (E04)
N06	Misc		Not Compliant (E01, E03, E07, E09); Needs good recommendation (E01, E03, E08, E09); Is it really a decision? (E03, E07, E09)
N07	C1	0	Speed (E01, E09)
N07	C2	-1	Recommendation Fallacy (E09)
N07	C3	1	Speed (E01, E04, E09); Gamification (E04, E05, E09); Feel-Good (E04, E07); Acclimatation (E09)
N07	C4	-1	Pressure (E01, E03, E07, E09, E10); Recommendation Fallacy (E06, E07, E09, E10); Less diligence (E01, E03, E07)
N07	C5	-1	Recommendation Fallacy (E07, E09); Fairness for disadvantaged individuals (E09)
N08	C1	-1 / 1	Ambivalence (E01, E03, E05, E06, E07, E08, E09, E10); Economic Efficiency (E02, E03, E05, E07, E08); Acceptance (E04, E07, E09, E10)
N08	C2	1 / -1	Ambivalence (E01, E03, E05, E06, E07, E08, E09, E10)
N08	C3	-1 / 1	Ambivalence (E01, E03, E05, E06, E07, E08, E09, E10); Economic Efficiency (E02, E03, E05, E07, E08); Acceptance (E04, E07, E09, E10)
N08	C4	1 / -1	Ambivalence (E01, E03, E05, E06, E07, E08, E09, E10); Economic Efficiency (E02, E03, E05, E07, E08); Acceptance (E04, E07, E09, E10)
N08	C5	1 / -1	Ambivalence (E01, E03, E05, E06, E07, E08, E09, E10)
N09	C1	0	No effect (E03, E07); More participation (E04, E10);
N09	C2	1	Instructions and Goals (E02, E03, E04, E05, E07, E08, E09, E10); Spam (E01, E02, E03, E07, E09, E10);
N09	C3	2	Spam (E01, E02, E03, E07, E09, E10); Attention (E04, E06, E07, E09, E10)
N09	C4	-1	Revisit (E03, E07, E08); Pressure (E05); Multi-Channel (E07, E09, E10); Audience (E03, E09)
N09	C5	0	Open Task (E01); No effect (E07)
N10	C1	1	Combination with N05 - Commitment for partitions (E02, E04, E06, E07, E08, E09, E10)
N10	C2	0	Autonomic planning and understanding (E04, E05, E08, E09)
N10	C3	1	Combination with N05 - Sub-Deadlines for partitions (E05, E07, E08, E09, E10); Comfort (E02, E06, E07, E08, E09, E10)
N10	C4	1	Focus (E04, E06, E07, P8, E10); Comfort (E02, E06, E07, E08, E09, E10)
N10	C5	0	Focus (E07, E10)
N11	C1	1	Endurance (E01, E02, E03, E04, E05, E07, E09, E10); Trust (E02, E03, E07, E08, E09)
N11	C2	2	Approachable IAM team (E01, E02, E03, E04, E05, E07, E08, E09, E10)
N11	C3	1	Endurance (E01, E02, E03, E04, E05, E07, E09, E10); Trust (E02, E03, E07, E08, E09)
N11	C4	2	Approachable IAM team (E01, E02, E03, E04, E05, E07, E08, E09, E10); Acceptance (E01, E02, E03, E04, E08, E10)
N11	C5	2	Approachable IAM team (E01, E02, E03, E04, E05, E07, E08, E09, E10)
N12	C1	0	Endurance (E02, E03, E06, E09); Backlash (E09)
N12	C2	2	Approachable Peer-Group (E02, E03, E04, E07, E08, E09, E10)
N12	C3	0	Endurance (E02, E03, E06, E09); Backlash (E09)
N12	C4	1	Acceptance (E02, E03, E06, E07, E09, E10); Peer-Pressure (E03, E10)
N12	C5	2	Approachable Peer-Group (E02, E03, E04, E07, E08, E09, E10)
N12	Misc		Similarity to N11 messenger reputation (E01, E05)
N13	C1	1	Feel-Good (E02, E04, E06, E07, E09)
N13	C2	1	Feedback on odd behavior (E02, E03, E04, E07, E09)
N13	C3	1	Feel-Good (E02, E04, E06, E07, E09)
N13	C4	1	Feel-Good (E02, E05, E07, E08); Focus (E02, E04, E07, E09)
N13	C5	0	Feel-Good (E05)

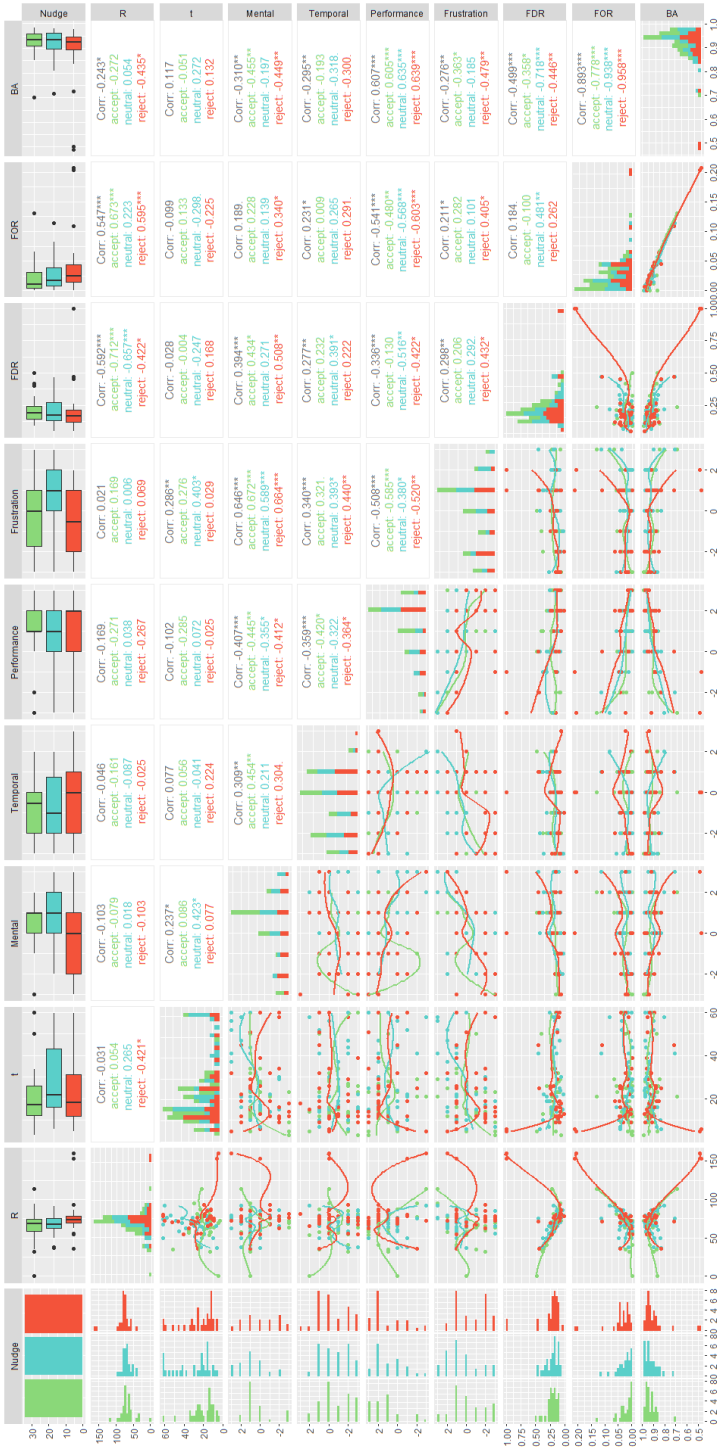


Figure 9: Pair plot of correlations (Spearman) and local regressions for the user study.

P5 Share and Benefit: Incentives for Cyber Threat Intelligence Sharing

Current status:	Published
Journal:	International Journal of Information Security
Ranking:	3.1 Impact Factor
Date of acceptance:	November 17, 2025
Date of publication:	January 22, 2026
Full citation:	Reittinger, T., Grill, J., & Pernul, G. (2026). Share and Benefit: Incentives for Cyber Threat Intelligence Sharing. *International Journal of Information Security*, *25*, Article 37.

Authors' contributions:	Tobias Reittinger	45%
	Johannes Grill	45%
	Günther Pernul	10%

Journal description: The *International Journal of Information Security (IJIS)* (peer-reviewed) is a Springer Nature journal publishing timely technical advances in information security, spanning theory, practical applications, and implementations. It covers areas such as system and network security, content protection, privacy, access control, authentication, applied cryptography, and formal methods.

International Journal of Information Security (2026) 25:37
https://doi.org/10.1007/s10207-025-01165-2

REGULAR CONTRIBUTION



Share and benefit: incentives for cyber threat intelligence sharing

Tobias Reittinger[1] · Johannes Grill[1] · Günther Pernul[1]

Received: 30 July 2025 / Accepted: 17 November 2025
© The Author(s) 2025

Abstract

Cyber threat intelligence (CTI) provides actionable insights into the threat landscape, helping organizations strengthen their defenses. Because commercial CTI is costly, inter-organizational sharing can reduce expenses, yet adoption remains limited. Still, the design of effective incentives for CTI sharing and their embedding in a sharing platform remains underexplored. We conducted 15 semi-structured interviews with security professionals to elicit incentive requirements and design options. We find that organizations prefer to share CTI with known recipients to build trust and support GDPR compliance. They also value mechanisms that lower coordination costs, such as a reputation system and price guidance to help prioritize scarce analyst time. Further, a major barrier is skepticism about the net benefits of sharing. To address this, we propose financial compensation for contributed CTI and a marketing label that signals proactive cybersecurity to partners and customers. We implemented these incentives in a platform prototype and assessed their effects in 14 hands-on sessions with security experts. Participants reported increased willingness to share, suggesting that well-designed incentives can catalyze CTI-sharing ecosystems. Put simply, organizations can share and benefit.

1 Introduction

As cyberattacks continue to increase [1], most organizations have encountered a cyber incident or breach [2]. However, the consequences of a cyberattack can be severe. In 2025, cyberattacks are expected to cause over 10 trillion US dollars in damage worldwide [3]. Beyond direct financial losses, these incidents undermine customer trust, disrupt critical operations, and often lead to declines in share price [2].

However, organizations can prevent cyberattacks by joining forces with other organizations [4]. The transition from individual to collaborative teamwork can occur through collaborative cybersecurity. A promising approach to joint cybersecurity is the sharing of cyber threat intelligence (CTI). In short, CTI are attack information that can be used to prevent, detect, and recover from cyberattacks in a timely manner [5]. CTI can be classified into three types:

- **Technical CTI**: Mainly indicators of compromise (IoCs) such as IP addresses or file hashes [6] that are used to sharpen security instruments and eliminate attack vectors.
- **Tactical CTI**: In-depth analyses of adversaries' tactics, techniques, and procedures (TTPs), enabling analysts to detect and defend against specific attack patterns [5].
- **Strategical CTI**: High-level information about attack trends and tailored for managerial decision-makers [6].

Organizations acquire CTI through both internal and external channels. Internally, they can analyze security logs and investigate incidents as they occur [6]. However, this reactive approach provides only a narrow, organization-specific perspective [7]. Externally, they can leverage open-source feeds, though these typically supply only IoCs [8, 9], or subscribe to commercial vendors, whose comprehensive intelligence often comes at a prohibitive cost [7]. Alternatively, by participating in CTI-sharing communities, organizations, especially small and medium-sized enterprises, gain affordable access to diverse CTI via platforms that integrate directly with their existing security infrastructures.

Despite its benefits, CTI sharing remains underutilized in practice due to several obstacles [5, 10]. First, the processing of internal security incidents requires effort and know-how. Second, organizations must trust recipients to handle shared intelligence confidentially and responsibly. Although early proposals have explored sharing communities [11] and technical implementations for CTI sharing [12], critical questions

Tobias Reittinger
tobias.reittinger@ur.de

[1] University of Regensburg, Universitätsstr. 31, Regensburg, Germany

Published online: 22 January 2026

persist: It is unclear how to design incentives to effectively increase the motivation of organizations for CTI sharing [10]. Further, prior research lacks insights into how to integrate incentives into a CTI sharing platform. We address these gaps by answering the following research questions:

RQ1 *How to design incentives for CTI sharing?*
RQ2 *How can incentives be integrated into a CTI sharing platform?*

Our study comprised three phases: Phase 1 involved 15 semi-structured expert interviews to identify CTI-sharing incentives (RQ1). Phase 2 saw the design and implementation of a prototype platform embedding these motivators (RQ2). Phase 3 evaluated its impact via 14 hands-on interviews. We provide the following contributions:

- We identified three incentivizing features to increase the acceptance of the CTI sharing platform. First, we enable sharing CTI with known recipients to foster trust. Second, a reputation system designed for CTI sharing improves on traditional approaches. Third, a novel price suggestion mechanism offers valuable guidance on CTI pricing.
- We identified two incentive mechanisms that address increasing platform usage. First, financial payments integrate recurring deposits that simplify CTI sharing by preventing a lack of funds to purchase CTI records. Second, we highlight the participation in proactive cybersecurity to partners and customers with a novel marketing label.
- We implemented the incentives into an open-source CTI sharing platform,[1] exemplarily built atop a private permissioned blockchain.
- We evaluated the incentives with the industry professionals in hands-on interviews. We conclude that the identified incentives encourage an active sharing dynamic.

The paper is organized as follows. Section 2 reviews relevant background. Section 3 details our research method. Section 4 presents the incentives identified from the interviews. Section 5 integrates these incentives into a prototype CTI-sharing platform. Section 6 evaluates their impact, and Section 7 includes the discussion. We contrast our work with existing studies in Section 8, then conclude in Section 9.

2 Background

This section provides basic theoretical concepts. We present motivation and incentives, CTI sharing, and blockchain.

2.1 Motivation and incentives

We draw on three complementary behavioral theories to explain CTI sharing incentives: **Self-Determination Theory (SDT)** distinguishes intrinsic motivation, based on interest and sustained by autonomy, competence, and relatedness, from extrinsic motivation, driven by external rewards (financial or social) that trigger immediate but often short-lived action. Combining both can yield prompt behavior change with lasting engagement [13]. We operationalize intrinsic motivation by supporting *autonomy* through contributor control over what to share and with which community; enhancing *competence* via reputation insights, feedback, and automatic price suggestions that help allocate analyst time; and fostering *relatedness* through exchange within a trusted community. We leverage extrinsic motivation with financial payments to offset analyst effort and a marketing label that signals proactive cybersecurity to external stakeholders.

Institutional Theory (IT) suggests that organizations conform to coercive, normative, and mimetic pressures to gain legitimacy [14, 15]. We reflect these through sharing within a community and a marketing label that recognizes proactive cybersecurity behavior, including visible contribution metrics that enable benchmarking of CTI sharing.

Resource Dependence Theory (RDT) argues that firms exchange resources to reduce uncertainty and reliance on external actors [16, 17]. Price suggestions, financial payouts, and reputation-based indicators create a market that broadens access to high-quality CTI and lowers search/transaction costs, reducing dependence on commercial providers.

In summary, we apply SDT to explain *why* our identified incentives enhance individual and collective CTI-sharing motivation, IT to explain *how* normative pressures entrench these incentives within organizational fields, and RDT to demonstrate *how* they minimize reliance on outside providers.

We incorporate insights on cybersecurity incentives. Reittinger and Pernul [18] propose a taxonomy of positive incentives and catalogue diverse motivators for cybersecurity. Moreover, Reittinger et al. [19, 20] find that incentives are a viable means of shaping cybersecurity behavior. We also draw on incentive research from non-security domains. Kamenica [21] investigates incentives' economics and psychology, identifying that incentives are powerful but should be achievable, as too steep incentives diminish motivation. Bryson et al. [22] examine the effect of financial incentives on performance and discover that increased payment results in enhanced productivity and effort. Furthermore, Malaga [23] and Tadelis [24] conclude that reputation systems minimize fraudulent activity and suggest rewarding users who rate others. Jahn et al. [25] conclude that marketing labels can signal reputation. We transfer these insights to CTI sharing.

[1] Open-source code: https://github.com/techplus2024/Platform
Prototype instance to interact with: https://platform.uversy.com/

2.2 CTI sharing

To exchange CTI effectively between different organizations, several data formats have emerged [26]. A well-known and widely used open-source standard is Structured Threat Information Expression (STIX), which relies on semi-structured information in JavaScript Object Notation (JSON) [27]. A STIX document is a CTI record that contains STIX Domain Objects (SDOs). There are various SDOs, such as an attack pattern, which can document attacker behavior (TTPs). STIX Relationship Objects (SROs) can link different SDOs and show relationships between them. STIX enables a flexible representation of CTI, such as a threat report.

Furthermore, MITRE ATT&CK is well-known for describing attack patterns [28]. The framework categorizes attack techniques into individual phases of a cyberattack. 14 cyberattack phases describe a cyberattack's life cycle, such as initial access and impact. In this paper, we utilize STIX to exchange CTI on the platform and use MITRE ATT&CK to implement one of our interview findings.

2.3 Distributed ledger and blockchain

Distributed Ledger Technology (DLT) is a decentralized and replicated database with multiple nodes in which various participants can agree on the database state with consensus mechanisms [29]. DLT is best suited when participants do not fully trust each other or a centralized third party with their data and processing. The technology enables transparency by executing *Smart Contracts*, a program logic decentralized on all nodes, and the result is determined by a majority vote [30]. Thus, data integrity is ensured. The blockchain is the best-known DLT implementation.

In a blockchain, data is stored in a growing chain of coherent blocks, where a block contains several transactions. Each participant has a cryptographic key pair, representing the pseudonymous blockchain identity, to sign and verify transactions, thus ensuring data authenticity [30]. Blockchain can be distinguished into different types [31]. On *public permissionless* blockchains, anyone can create an identity, participate, and read all transactions. In contrast, on *private permissioned* blockchains, only selected participants can create an identity, conduct transactions, and read transactions. We use a private permissioned blockchain as an example architecture for implementing our CTI sharing platform, as it inherently supports some of the incentives we have identified.

3 Methodology

The study was conducted between October 2023 and May 2025 and comprised three sequential phases to uncover how to motivate professionals to share CTI, visualized in Figure 1. Our aim was to qualitatively explore effective incentives for CTI sharing, based on specific sharing impediments. In **Phase 1**, we identified sharing impediments and key incentives by interviewing industry experts. In **Phase 2**, we incorporated these incentives into a prototype CTI-sharing platform. Finally, in **Phase 3**, we evaluated the impact of the embedded incentives by conducting hands-on interviews. Participants represented unique organizations, except for P4 and P8, who were from the same organization.

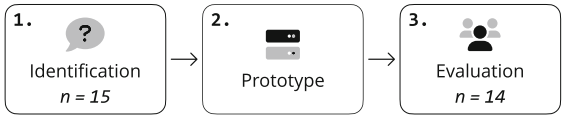


Fig. 1 Research method encompassing three phases

3.1 Identification (Phase 1)

We sought both strategic and operational insights by interviewing two stakeholder groups: business executives, who oversee CTI-sharing decisions, and cybersecurity practitioners, who execute and manage them. To uncover a full spectrum of barriers and motivations, we recruited participants from organizations that both do and do not currently share CTI, as well as from smaller security service providers that manage CTI exchange on behalf of larger clients. Leveraging professional networks (e.g., LinkedIn), industry contacts, and our institution's alumni network, we ultimately enlisted 15 participants during Phase 1. Despite time constraints and the sensitive nature of the topic, our sample spans multiple sectors, regions, regulatory regimes, roles, and organization sizes (see Table 1). Several participants from smaller organizations (e.g., P1, P6, P7, P9, P18) worked at security service providers responsible for cybersecurity across numerous client organizations, providing extensive cross-organizational insight.

To develop the questionnaire, we followed the established methodology of cognitive interviewing [32]. Before interviewing the participants, we conducted a pretest with two fellow researchers to improve the clarity and structure. The interview questionnaire was structured into four parts. *(1) Demographic Questions* characterize the background and experience of the participants. Subsequently, we explore the participants' current *(2) CTI Sharing*. Based on these insights, we ask about *(3) Incentives for CTI Sharing (Open Questions)*. Our open questions encourage participants to suggest unbiased ideas for incentives and their design. Finally, we ask about *(4) Incentives for CTI Sharing (Specific Questions)* that participants did not previously address. We added the interview structure in the Appendix A.

All interviews were conducted in German and English, using Zoom and Microsoft Teams. First, we informed participants that we would record the audio to transcribe quotes and use them anonymously in this paper. After the participants had consented, we began recording and asked them to repeat their consent to document it. We then started with demographic questions, ensuring all participants matched the target population. Subsequently, the remaining three parts of the interview guide were asked. As new ideas for incentives and their design were suggested by participants throughout the interviews, not all incentives were discussed with every participant in the interview because these suggestions were not yet available at the time of their interview. We contacted these participants by email and asked them about the incentives that had not yet been discussed. All participants responded to our message, thus ensuring that each participant addressed every question. The duration of the interviews ranged from one hour to two hours.

We transcribed the audio recordings using Microsoft Word after the interviews. Following the flexible coding approach [33], two authors of this paper independently performed the coding process and then jointly merged the individual codings into the final coding scheme. This final coding scheme was then jointly applied to assign the coding to the corresponding themes of the interview structure using thematic analysis [34].

3.2 Prototype development (Phase 2)

Based on our interviews, we identified the key incentives for organizational CTI sharing. To test feasibility, we built a prototype CTI-sharing platform that embeds these incentives. Leveraging insights from the interviews, we first designed the system architecture and selected appropriate technologies. Next, we implemented each incentive mechanism within the prototype. Finally, we published the source code as an open-source artifact and deployed the platform. Thus, our prototype can be fully interacted with as a website in the browser without coding experience or hardware requirements.

3.3 Hands-on evaluation (Phase 3)

To evaluate how the implemented incentives shaped sharing dynamics, we deployed the prototype platform. Our initial plan was to monitor a community's sharing activity over several months, yet this proved infeasible due to privacy constraints (see Section 4.2.1). Instead, we conducted hands-on interviews in which participants explored the live prototype and experienced its incentive mechanisms firsthand. Mirroring our Phase 1 approach, we enlisted fourteen participants in total: three new experts and eleven individuals who had taken part in Phase 1. The questionnaire of the evaluation is listed in Appendix A.

3.4 Ethics

Ethical considerations are a crucial part of our research. Thus, before conducting our study, we received approval for our research approach from the German Association for Experimental Economic Research e.V. [2] and obtained an Institutional Review Board certificate. The certificate has the number "1gpKGsYr" and can be viewed online. Our study design minimizes the collection of personal information, which is used only to characterize the participants' demographics. Furthermore, we obtained informed consent for the participation and audio recording at the beginning of the interview, and participants could withdraw their consent at any time during and after the interview. After the transcription and coding, the audio recordings were deleted to safeguard the participants' privacy. Additionally, we removed any characteristics that identified the participants or their affiliations from the collected transcripts. Thus, quotes are anonymized, and the number of employees is given as a range in the demographics summary (Table 1). To mitigate inaccuracies, we gave participants the opportunity to review and correct the citations they used.

3.5 Limitations

Our results should be interpreted in light of the following limitations. First, the data are self-reported and thus subject to recall inaccuracies. Second, recruitment was nonrandom and likely overrepresents European organizations. Regional and cultural differences, such as GDPR-driven privacy guidelines, regulatory breach-disclosure requirements, or social norms around reciprocity, may impact generalizability and shape which incentives resonate across regions. The sample may also overrepresent organizations that already share CTI, which helped us learn from their experiences but may bias the results. Third, many participants took part in both the identification and evaluation phases, introducing possible commitment bias, though this enabled a deeper assessment of the prototype. Nevertheless, as Table 1 shows, our sample spans diverse regulations, organizations, and backgrounds. We conducted 15 interviews in Phase 1 and 14 hands-on interviews in Phase 3, numbers comparable to similar qualitative studies [35]. Finally, because a long-term community deployment was infeasible, we approximated real-world impact through hands-on, task-based interviews, which may not capture longitudinal dynamics.

[2] Link: https://gfew.de/ethik/1gpKGsYr

Table 1 Summary of interview participants' characteristics.

ID	Phase 1	Phase 3	Job title	Sector	Employees	Gen.	Exp.	Org. Location	Sharing CTI
P1	✓		IT Security Consultant	Penetration testing	1-9	M	4	EU	
P2	✓	✓	Security Analyst	Software development	10-99	F	20	EU	
P3	✓	✓	IT Security Consultant	Consulting	100-999	M	12	EU	✓
P4	✓	✓	CISO	Software development	1,000-9,999	M	8	EU, NA, SA, AS	✓
P5	✓	✓	Security Architect	Automotive	+10,000	M	11	EU, NA, SA, AS	
P6	✓	✓	CEO	IT service provider	1-9	M	14	EU	✓
P7		✓	IT Security Consultant	Penetration testing	1-9	F	7	EU	✓
P8	✓	✓	ISO	Software development	1,000-9,999	M	3	EU, NA, SA, AS	✓
P9	✓	✓	Director of Cybersecurity	IT service provider	10-99	M	25	EU	
P10	✓		CEO	Automotive	10-99	F	15	EU	
P11		✓	Cybersecurity Engineer	Penetration testing	100-999	M	7	EU, NA, AS	✓
P12	✓		ISO	Consulting	10-99	M	10	EU	
P13		✓	Senior Incident Handler	Security services	100-999	M	24	EU	✓
P14	✓	✓	Cybersecurity Engineer	Manufacturing	1,000-9,999	M	4	EU	
P15	✓	✓	Security Manager	Pharmaceuticals	1,000-9,999	M	11	EU, NA, SA	
P16	✓		CISO	Manufacturing services	+10,000	M	9	EU	
P17	✓	✓	CEO	Retail	10-99	M	35	EU	✓
P18	✓	✓	CEO	Penetration testing	1-9	M	23	EU	

CISO: Chief Information Security Officer. ISO: Information Security Officer. CEO: Chief Executive Officer. Gen.: Gender. Exp.: Experience. Org: Organization. EU: Europe. NA: North America. SA: South America. AS: Asia

Table 2 Summary of interview findings with identified problems and solutions of CTI sharing

Identified Problems		Identified Solutions	
Occurrence	Impediments (4.1)	Incentives (4.2, 4.3)	Platform Architecture (4.4)
14 / 15	Distrusting recipients	Community Sharing, Reputation System	Decentralized Platform, Pseudonymous Payments
13 / 15	Doubtful benefit	Reputation System, Price Suggestion, Financial Payments, Marketing Label	Decentralized Platform, Pseudonymous Payments
4 / 15	Time constraints	Reputation System, Price Suggestion	
2 / 15	GDPR	Community Sharing	

4 Incentives identification

In this section, we outline the interview results, summarized in Table 2. First, we describe participants' prior *Sharing Experiences and Impediments* to CTI sharing. Next, we cover *Incentivizing Features* to increase the platform's acceptance and *Incentive Mechanisms* to address enhancing the platform's usage. Finally, *Platform Architecture* outlines the foundational architecture of the platform. "Members" refer to general participants within a CTI sharing community, and "participants" refer to our 18 interview participants.

4.1 Sharing experience and impediments

Eight participants have prior sharing experience, which we outline as follows. Participants primarily share IoCs, in particular IP addresses, and brief threat reports, such as exploitable vulnerabilities. IoCs are typically put on block lists, and the system administrators read threat reports. Most participants from small organizations can often only capture "*high-level insights in 90% of incidents*" ($P12$) due to fewer security systems in place. In contrast, participants from larger organizations with their own cybersecurity departments can create sophisticated threat reports: "*We document root cause, mitigation measures, and preventive measures as part of our incident response processes*" ($P4$) . Yet, these participants only rarely do so. Participants P4, P7, and P8 share self-collected CTI data within closed groups. This exchange primarily occurs via email, Slack, or Telegram, and in one case through a CTI sharing platform. However, they emphasize that the lack of anonymity options and the limited amount of data received in return often slow down the exchange. Consequently, they refrain from sharing more sensitive information. Participants P6, P13, and P17 are either security service providers themselves or use such services. These providers analyze their clients' threat IoCs, store them in proprietary databases, and distribute them across the security systems of their own client base. As a result, information sharing is limited to the provider's customer network, with no exchange taking place between different service providers. In contrast, participants P3 and P11 engage in informal exchanges about current threat developments through personal workshops or regular discussion groups. Overall, our participants offer insights into diverse sharing experiences.

Furthermore, we identified impediments to CTI sharing, displayed in Table 2 with the number of interview occurrences. The most important obstacle to CTI sharing is distrusting recipients (14 / 15 participants). Most participants refrain from sharing CTI records, which are sensitive data for them, with unknown or untrustworthy recipients. They fear an incident could be made public, resulting in a loss of reputation. One participant describes this impediment "*is mainly due to human concerns and less to organizational obstacles*" ($P3$)3. In addition, many participants see only doubtful benefits in CTI sharing (13 / 15), as "*there is no incentive to take on the work*" ($P5$) or they "*cannot assess the impact for their own organization*" ($P18$). In contrast, time constraints are a minor impediment for participants (4 / 15). The processing and sharing of CTI records require efforts that, combined with a doubtful benefit, are perceived as not beneficial by some participants. Finally, the General Data Protection Regulation (GDPR) is the least important impediment to CTI sharing (2 / 15). Here, the participants' organizations lack legal expertise and are concerned about "*which data in CTI records are personal data that fall under regulation*" ($P1$). Nevertheless, GDPR allows the processing and sharing of CTI as a legitimate interest while minimizing personal data [36].

In the following, we discuss each identified incentive and indicate which participant-reported impediment it helps to mitigate (see Table 2 for an overview).

4.2 Incentivizing features

We identified three incentivizing features. While a CTI sharing platform requires a basic set of functionalities, such as an engaging user interface, the incentivizing features are requirements that go beyond and increase the motivation to

share CTI. We present *Community Sharing*, *Reputation System*, and *Price Suggestion*.

4.2.1 Community sharing

Participant P2 explains the reasoning for community sharing: "*We do not want our own CTI records to end up on servers of unknown third parties. We only want to share CTI with a known group.*" (*P*2) A community can be grouped by sector, location, or interest. In Germany, every company is required by law to join one of 79 Chambers of Industry and Commerce [37]. These chambers are local groupings and offer free workshops on cyberattacks. Thus, "*every organization is already in a community suitable for CTI sharing.*" (*P*17) In addition, most participants are in one or more additional communities. Thus, organizations can conveniently participate in the CTI sharing community. The member-restricted communities mitigate the impediments of *trusting unknown parties* and *GDPR*, as this regulation requires measures to minimize the data protection incident risk, according to Article 32 of GDPR [38]. Following SDT, this feature increases relatedness to the community and facilitates intrinsic motivation; it also supports *autonomy* by letting contributors choose the audience and scope of disclosure. From an IT perspective, it taps into *normative* and *coercive* pressures of established communities to legitimize CTI exchange, and adds a *mimetic* channel as organizations emulate respected peers' sharing practices. In line with RDT, this feature reduces uncertainty and dependence on external actors by pooling critical intelligence, lowering search/transaction costs, and increasing collective resilience and bargaining power.

Design. It is crucial to organizations that they "*know it is a well-known or trusted community. [They] don't need to know all members personally [...]. Still, the restriction to a closed community is crucial.*" (*P*10) Within a community, organizations "*do not want to know who is explicitly providing and receiving CTI because when it is possible to pinpoint a CTI record to a specific organization, [they] are concerned about a loss of reputation.*" (*P*5) Organizations only "*want to know that [they] delegate CTI to and from a trusted community, but not who exactly is providing or receiving it.*" (*P*17) Thus, organizations require pseudonymity within a community. Such a closed and trusted community also ensures that attackers cannot access the shared CTI data. In contrast, an open-access platform could allow attackers to realize that their IoCs are being tracked and their attack patterns detected, enabling them to adapt their approaches accordingly.

As our interview participants come from different sectors and company sizes, their communities differ regarding the number of community members, the average number of employees, and activity. To address the different needs of the communities, we introduce community properties. These properties, described in Section 5.4, allow communities to set individual parameters that precisely align with the features and incentives.

Threat Modeling. However, merging into a community has potential drawbacks for pseudonymity. Outliers, e.g., organizations smaller or larger than average, could be identified based on their distinctive activity. Thus, a community must maintain a certain member size and homogeneity. This ensures that an individual organization cannot be identified by combining the community's external context with a limited member size and available metadata. Nevertheless, community sharing suits all organization sizes, combining large organizations' offerings and purchasing capabilities alongside small organizations' domain insights.

4.2.2 Reputation system

When utilizing CTI, organizations want to ensure that it "*provides value and strengthens cybersecurity*" (*P*18). To evaluate the quality of a CTI before obtaining it, participants want a "*reputation system that rates individual CTI records*" (*P*2). Thus, organizations have a higher level of trust in the platform and are more willing to use CTI from the platform. The reputation system thus mitigates the impediments *doubtful benefit*, *time constraint*, and *distrusting unknown participants*. Following SDT, reputation systems build *competence* via feedback and transparent impact and foster *relatedness* through peer recognition. From an IT view, reputation sets *normative* quality expectations, enables *mimetic* benchmarking, and meets *coercive* pressures from standards and regulators. In RDT terms, community-vetted scores reduce uncertainty and information asymmetry and lower search and transaction costs.

Design. There are three approaches to determining CTI quality. First, external experts evaluate each record before publication, but participants "*don't want to pay experts to evaluate [their] CTI*" (*P*1) and "*want to keep [their] CTI inside the community*" (*P*10). Second, expert members within the community assess records proactively, though security analysts "*would prefer not to spend time proactively assessing masses of CTI records that might not even be purchased.*" (*P*2) Third, members rate CTI after receiving it. While "*members must actually rate CTI records for the reputation system to work*" (*P*8), most organizations (13/15) "*are willing to adopt a mandatory rating system because [they] recognize that this helps everyone*" (*P*8).

A reputation system based on individual ratings is thus introduced. Communities can adjust two properties: the time horizon for submitting ratings and the rating percentage, i.e., the minimum share of received CTI that must be evaluated. Before these "*requirements are met, members should not be able to further participate in the platform.*" (*P*4) Ratings can be updated if a CTI record improves. For new, unrated records, "*the average rating of all CTI records of a member*

should be displayed as a substitute" (*P*2), which "*motivates [organizations] to be well rated and to offer CTI in the long term.*" (*P*17)
Threat Modeling. The reputation system could be exploited if two organizations collaborate and give each other positive ratings, creating a zero-sum incentive. Monitoring can help detect such behavior, for example, by flagging above-average frequencies of mutual ratings, allowing the community to investigate and potentially exclude bad actors. However, collaborating to exploit the system has significant downsides: organizations lose pseudonymity with their collaborators, and past or future CTI sales could be exposed, damaging their reputation. Therefore, legitimate users are unlikely to engage in such collusion.

4.2.3 Price suggestion

As organizations lack CTI sharing experience, participants noted that they "*don't know what a reasonable price per CTI record is*" (*P*2). Because external experts are not supposed to assess quality, they cannot determine the value of a CTI record. Thus, organizations must set the price of CTI themselves. However, the value of CTI varies greatly, as an IoC provides a value different from that of a threat report. Thus, organizations "*want a recommendation on how to price individual CTI records.*" (*P*17) Additionally, analysts who share CTI "*don't want to spend [their] time considering a price, as time is short*" (*P*2). There is no concrete approach to pricing CTI, so we introduce price suggestions to automate this process. P17 highlights the advantages of the price suggestion: "*It allows us to upload CTI faster and requires less prior knowledge. It can also increase sales as prices are set realistically.*" (*P*17) In sum, price suggestion lowers the entry barrier of CTI sharing and supports the platform economy. Hence, it addresses the impediment of *time constraints* and *doubtful benefits*, as it finds suitable prices and maximizes sales and revenue. Following SDT, price suggestions bolster *competence* through clear guidance and feedback on market fit while preserving *autonomy* by allowing contributors to accept or adjust suggested prices. According to IT, it codifies community-wide pricing norms that legitimize the CTI exchange. In RDT terms, they reduce uncertainty and transaction costs, lessen dependence on external pricing advisors or dominant vendors.
Design. To enable realistic suggestions, we define a minimum number of purchases as a community property to determine which existing CTI records are included in the calculation. This ensures that only reasonably priced records are considered, taking into account any price changes. Organizations want the price suggestion implemented in two parts: a quick summary of the average price and an in-depth comparison of previous sales. We identify three factors for comparing a new CTI record with similar records on the platform:

- **Size:** "*How many elements are in it*" (*P*4), for example the number of IoC and attack patterns
- **Content:** "*What elements are included*" (*P*2), for example an IoC or attack pattern
- **Attack Phases:** "*What phases of the attack lifecycle the CTI record covers*" (*P*3), e.g., initial access or execution

Participants find it "*challenging to determine how the factors should be specifically designed and weighted.*" (*P*17) Thus, the price suggestion offers guidance rather than a perfect solution. At the platform's launch, the feature may suffer from a cold start, providing limited value to sellers due to a small database. Novel CTI records may yield inaccurate suggestions, which can be flagged to indicate a small sample size and potential bias. Over time, as the database grows, the suggestions become more accurate, supporting the platform's longevity and benefits for all members. This initial design "*helps especially small and medium-sized organizations, as [they] have little experience in CTI pricing.*" (*P*17)
Threat Modeling. If multiple members collude to trade CTI at unrealistically high or low prices, this could bias the price suggestion. The impact is limited by using numerous purchases in the calculation and applying monitoring from Section 4.2.2. Indicators such as mutually excessive purchases can flag potential collusion. Additionally, collaborators would lose pseudonymity.

4.3 Incentive mechanisms

In addition to incentivizing features, we identified two incentive mechanisms. They encompass rewards for active participation in CTI sharing. We introduce *Financial Payments* and *Marketing Label*.

4.3.1 Financial payments

Financial payments are "*compensation for the time spent providing CTI [...] and for potential damages caused by the security incident.*" (*P*5) Additionally, "*the revenue from the sales can be used to increase the security department by covering the salaries.*" (*P*5) Organizations would prefer not to give away their CTI for free, thereby not allowing free riding and addressing the impediment *doubtful benefit*. Following SDT, financial payments increase extrinsic motivation, and the design of this incentive enhances autonomy, thus maintaining intrinsic motivation. From an IT perspective, payments formalize fair-reward norms, satisfy coercive accounting expectations, and create mimetic pressure as peers adopt compensated sharing. According to RDT, they reduce uncertainty and dependence on external funding by creating self-sustaining, internal revenue streams.
Design. Organizations must first deposit capital on the platform to purchase CTI, and participants prefer a pay-per-use

subscription. As P4 explains, "*It is easier to pay in periodic amounts automatically [...] as the funds are on the platform when you need them.*" (*P*4) This enables rapid CTI purchases in response to threats, and participants note they are "*clearly more willing to buy CTI because there is always a balance available.*" (*P*8) Periodic subscriptions should be tailored to each organization, with unused balances "*accumulating over several periods.*" (*P*4) Each CTI record should have an individual price and be purchasable directly from the balance. Manual deposits must be possible once the periodic funds are exhausted. Although participants consider "*a subscription with unlimited CTI access is convenient, the platform economy is likely not sustainable.*" (*P*5) Finally, deposits and sales revenues "*should be possible to be withdrawn at any time.*" (*P*17)

Threat Modeling. One disadvantage of financial payments is that the buyer must make the payment first and only knows whether the CTI record provides value afterward. We counteract this issue with the reputation system to give a strong indicator of the expected quality and value. Even if a CTI record has not yet been rated, a seller's average rating of all CTI records is displayed.

4.3.2 Marketing label

The marketing label is an "*excellent way to show customers and business partners that [an organization is] proactively increasing cybersecurity*" (*P*3), thus mitigating the impediment *doubtful benefit*. Additionally, the marketing label enhances the activity within the platform because, as we explain in the following, organizations have to fulfill requirements to obtain the label, which results in more purchases and sales. Furthermore, the marketing presentation increases awareness within the community and on the platform. Beyond serving as a social reward that increases extrinsic motivation, this mechanism strengthens relatedness due to peer recognition and, thus, intrinsic motivation, according to SDT. From an IT standpoint, marketing labels leverage normative and mimetic pressures to legitimize and normalize CTI sharing. In accordance with RDT, they also reduce reliance on external trust signals by creating a community-endorsed marker of quality and reliability.

Design. The marketing label is issued per community, allowing organizations to hold multiple labels from different communities. Each label displays the community name for distinction. For the label, it is "*accepted that people outside the community get limited insight to verify the label.*" (*P*9) To ensure its value, the "*issuance should be linked to requirements, specifically a minimum number of sales, purchases, or membership duration.*" (*P*1) As "*the marketing label would be worthless if the requirements are too low,*" (*P*6) each community must define appropriate thresholds that are challenging yet attainable for active members. This, in turn, increases supply, demand, and overall engagement on the platform. As a result, "*the popularity and reputation of the marketing label and the community will also increase.*" (*P*10)

To maintain long-term value, "*the requirements must be verified periodically. Thus, the marketing label is only valid for a limited period.*" (*P*17) After each validity phase, it should be renewed or withdrawn. A "*verified since*" field further incentivizes members to remain active across periods.

Organizations are "*reluctant to publish the specific sales thresholds required to earn the marketing label, since doing so could indirectly reveal that a security incident has occurred.*" (*P*2) However, they agree that sharing aggregated metrics–such as total purchases or average rating scores–can enhance transparency. To foster trust, each label receives a unique identifier and can be publicly verified through an external service.

Threat Modeling. Organizations joining forces could attempt to exploit the marketing label through coordinated trading to fulfill the requirements or transfer it to members who have not met the requirements. Such behavior can be detected using the monitoring described in Section 4.2.2, for example, by identifying mutually above-average purchase patterns. Yet, exploiting the system would require collaborators to give up pseudonymity between each other. As participant P4 concludes: "*[The proposed design] is the best you can do, most members will be honest and have a major incentive to sell and buy more CTI.*" (*P*4)

4.4 Platform architecture

In addition to incentivizing features and incentive mechanisms, we identified two requirements for the platform's design, which are crucial for the willingness to engage in CTI sharing. They determine the underlying architecture of the platform for the subsequent implementation of incentivizing features and incentive mechanisms. We present *Decentralized Platform* and *Pseudonymous Payment System*.

4.4.1 Decentralized platform

We described in Section 4.1 that for participants, the most significant impediment to organizational CTI sharing is trusting recipients (14/15 participants). Thus, they not only want to restrict the number of platform members (addressed by community sharing) but also distrust centralized platform providers holding their data: "*We don't want to hand over our sensitive data to a platform provider, only to buyers*" (*P*4). Participants are concerned about a single entity controlling the CTI platform and misusing their data: "*Centralized providers might analyze or use my CTI data for their own purposes, which is what large platform providers usually do*" (*P*12). These concerns reflect challenges already observed in

the field of cloud computing, particularly regarding security, as well as the limited transparency and control over stored sensitive data [39, 40].

Also, the participants consider centralized data storage and processing to be unnecessary, as the acquired CTI must be directly integrated into their own security systems. "*We integrate malicious indicators into local systems such as firewalls, and use threat reports to enrich our own threat knowledge bases*" ($P8$). This leads to the conclusion that a peer-to-peer exchange model is more efficient: "*A direct transfer of CTI data between participants makes sense, as it eliminates the unnecessary middleman*" ($P8$).

Furthermore, the sharing community wants to "*define [its] properties and approve members collectively*" ($P2$), rather than entrusting a single entity with administrative control. This approach prevents the risk of unauthorized participants being registered by a sole administrator without notice.

As a result, we consider a decentralized architecture for the platform, as it enables organizations to administer the platform themselves and to store their CTI records physically on their own infrastructure within their security domain. Thus, they do not have to transfer their CTI records to a central instance to offer them on the platform. Organizations only have to give buyers access to their purchased CTI records.

4.4.2 Pseudonymous payment system

The identified incentives have shown that the network must be limited to selected participants and that these can operate pseudonymously within the network (Section 4.2.1). In addition, monetary rewards increase the motivation to share one's own CTI data records (Section 4.3.1). To enable this process, it must also be possible to carry out such transactions pseudonymously between the participants. A crucial aspect is that there "*must be no invoice documents that reveal the names of the buyer and seller organizations*" ($P5$). At the same time, it is essential for the long-term participation of the organizations in the platform that this "*pseudonymous payment system is both trustworthy and compliant with regulations*" ($P16$). Traditional payment service providers for online marketplaces, such as PayPal, therefore cannot be integrated into the platform architecture.

5 Prototype

We integrate the findings in Section 4 into a newly developed prototype. First, we describe the implementation of the *Platform Architecture*, then we present the *Incentivizing Features* and *Incentive Mechanisms* building on it.

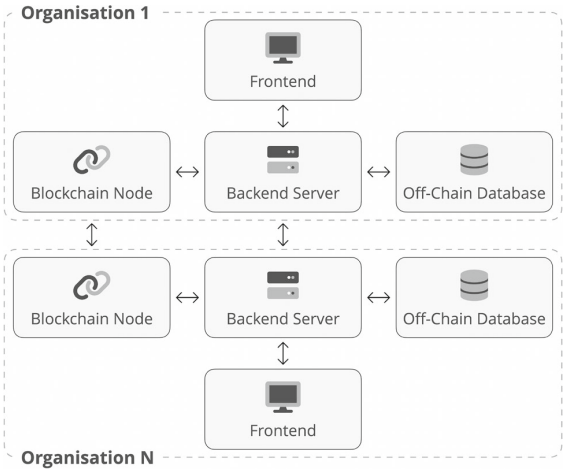


Fig. 2 Overview of the architectural components

5.1 Implementation of platform architecture

In order to implement *Decentralized Platform* and *Pseudonymous Payment System*, the architecture of the prototype is based on the four components *Blockchain*, *Off-Chain Database*, *Backend Server*, and *Frontend*. Figure 2 visualizes the components and their data flow between multiple organizations. Every organization hosts all components. We selected open-source technologies based on their maintenance activities, as well as their suitability for our requirements.

5.1.1 Blockchain

To implement the envisioned decentralized sharing platform, we adopted a blockchain-based approach. The primary motivation is that blockchain technology inherently provides a mature framework for implementing a pseudonymous payment system (as identified in Section 4.4.2), which is essential to enable monetary incentives for the exchange of CTI data within the platform. However, a public permissionless blockchain is not suitable for this purpose. Such networks do not restrict participation, and our CTI marketplace and all its transactions would be publicly visible worldwide, compromising the confidentiality required for CTI sharing. Furthermore, public blockchains fail to meet the expectations of our participants regarding a stable and trustworthy payment environment, as they are subject to significant volatility in token value and transaction fees, have experienced cases of fraud, and remain affected by regulatory uncertainty [41].

Instead, we selected Hyperledger Besu [42] as the underlying blockchain framework. It enables the creation of a private permissioned blockchain network with selected members, supports pseudonymity, and, being self-hosted, can be flexibly adapted to comply with local regulatory require-

ments. In addition, it offers scalability for high-volume data exchange and enables the creation and transfer of monetary tokens without transaction fees. This design allows us to support pseudonymous payments while maintaining control over membership and data access in a trusted community environment.

We save CTI record's metadata on the blockchain, such as the ratings. Thus, the necessary information is transparent for all members to buy a CTI record, but the record itself remains at the organization until it is purchased.

5.1.2 Off-Chain database

CTI records are stored in an off-chain database to allow each member control over their data. The records are stored in STIX format, a JSON document, enabling a standardized CTI exchange on the platform. Thus, we leverage the document-oriented NoSQL database Couchbase [43].

5.1.3 Backend server and frontend

The backend server hosts the frontend for an organization to interact with the sharing platform. Additionally, the server listens to the activity on the blockchain node, delegating purchased and sold CTI records to and from the off-chain database. For the backend server, we select Node.js [44] to interact with the blockchain node and PHP Laravel [45] to process the communication with the HTML frontend and the off-chain database.

5.1.4 Platform registration and token deposit

To enable initial onboarding and the issuance of pseudonymously usable tokens on the platform (see Figure 6 in Appendix E), we use a payment trustee that can be chosen by the platform members – e.g., a locally regulated provider operating within the same legal framework as the members. The underlying private permissioned blockchain (Hyperledger Besu) supports private transactions, allowing certain data and transactions to be accessible only to authorized members. Although the trustee is part of the platform, their access is technically limited to specific smart contracts for member registration and token deposit/withdrawal. The trustee has no visibility into the actual CTI sharing marketplace. As a result, they cannot infer the transaction behavior of participating organizations – in particular, their purchases or sales of CTI data.

An organization seeking to join the CTI sharing community must first apply for membership. Existing members review whether the applicant meets the criteria defined by the community, for example, being a registered entity from an approved country or operating in a specific industry sector. Once a consensus on the organization's admission is recorded on the blockchain, the new member generates a cryptographic key pair and submits the public key to the payment trustee. The trustee then verifies the organization's identity and confirms the recorded admission decision on the blockchain. Upon successful verification, the trustee registers the public key via the member registration smart contract. The organization can then deposit fiat currency with the trustee, who issues an equivalent amount of pseudonymous tokens using the token deposit smart contract and assigns them to the submitted public key. At this point, the new member is authorized to pseudonymously purchase or offer CTI data on the marketplace via the marketplace smart contract.

This design ensures that the platform is compliant with the regulation for identity verification of all members [46], before issuing pseudonymous tokens. The system maintains pseudonymity while disallowing anonymity (in line with the prohibition of anonymous crypto-asset accounts [46]). Authorized regulatory authorities may request access to both blockchain transaction records and token deposit/withdrawal data from the trustee in the context of a fraud investigation.

5.2 Implementation of incentivizing features

We outline the implementation of *Community Sharing*, *Reputation System*, and *Price Suggestion* as follows.

5.2.1 Community sharing

Initially, organizations have to form a closed CTI sharing community of trustworthy participants. Subsequently, they can deploy the sharing platform and generate their cryptographic key pairs. The platform stores each member's backend server's IP address and port. As the members communicate directly with each other in this decentralized system, they must take additional measures to maintain their pseudonymity. A member should not use an IP address that can be used to identify their organization. IP anonymization services, such as a VPN, can be utilized for this purpose.

5.2.2 Reputation system

o ensure the quality of CTI on the platform, members can rate a CTI record they purchased from one to five stars. Optionally, buyers can add a text-based comment to their review. We store the rating tamper-proof and transparently on the blockchain as part of the metadata of CTI records. For new and unrated CTI records, we display the average rating of a seller based on all their prior CTI records in such cases. This approach helps reduce the subjectivity of individual CTI ratings. To further minimize subjective bias, we complement member ratings with objective CTI quality metrics [47]. For instance, the *Relevancy* metric utilizes contextual information to enable potential consumers to assess

the usefulness of CTI for their specific environment. It compares characteristics such as the industry sector (e.g., finance or retail) and technologies in use (e.g., specific Linux distributions) between the publishing and consuming members. These attributes can be voluntarily provided by each member without compromising their pseudonymity within the platform.

Furthermore, to increase the number of ratings, organizations are willing to be compelled to rate purchased CTI records. If members fall below the required rating percentage or exceed the mandatory rating period, the smart contract disables further uploads or purchases of CTI records until the requirements are met. After each login, we highlight pending ratings and inform members early that they must provide additional ratings for a seamless experience without disruptions.

5.2.3 Price suggestion

As outlined in Section 4.2.3, we identified three factors in the interviews that should be integrated into the price suggestion: *Size*, *Content*, and *Attack Phases*. As the prototype utilizes CTI records in STIX format, we use the STIX elements to calculate the factors. To suggest a price for a new CTI record, we identify the similarity to prior CTI purchases based on these factors and outline their purchase prices. Thus, members get an overview of the prices of similar CTI. We describe each factor as follows.

First, *Size* counts the number of elements in a CTI record, indicating the amount of threat intelligence information stored within it. The elements are either an SDO, representing the actual content in a CTI record, or an SRO, describing the relationships between the SDOs. In addition, SDO elements such as attack patterns can define which attack phase (e.g., initial access) they are used for and which specific technique (e.g., phishing) is applied. As MITRE ATT&CK defines 14 attack phases, the number of occurring phases in a CTI record can be counted and compared to the number of phases in the new CTI record.

Second, *Content* describes the elements of a CTI record. As a record can represent IoCs or threat reports, many potential SDO elements enable a flexible composition. Thus, we can differentiate the content of CTI records based on three components: SDO, SRO, and attack phases. If SDOs of CTI records match, they offer similar content. SROs provide an additional content-related context. Two CTI records with identical SDOs can still have different SRO relationships, resulting in different content. CTI records can address the same attack phases, thus representing similar content.

Third, the factor *Attack Phases* is incorporated into *Size* as the count of attack phases and included in *Content* by addressing the attack phases of CTI records.

Using these factors, we compute a total difference delta between the new CTI record and each previously purchased record. We present the most similar CTI records and their prices, along with the average price across them. We formally define the calculation of the price suggestion in Appenidx C and demonstrate it with a specific example.

5.3 Implementation of incentive mechanisms

In the following, we describe the implementation of the *Financial Payments* and the *Marketing Label*.

5.3.1 Financial payments

We create two processes to implement Financial Payments into a CTI sharing platform, allowing an organization to sell its CTI to other interested organizations on the platform. The first process enables offering a CTI record on the platform, displayed in Figure 7 in the Appendix E. The seller (S) creates a STIX-compliant CTI record and can further specify metadata like description or type (IoC or threat report) in the frontend. The backend server performs the price suggestion by retrieving the metadata of all other CTI records from the blockchain and calculating the similarity to the new CTI record. The seller selects the final price, and the CTI record is stored locally in the seller's off-chain database. In addition, the backend signs the CTI offer, which includes the metadata of the CTI record, with the seller's private key $PrivKey_{ShareS}$. This signed offer is then published on the blockchain so all other members can view it.

The second process facilitates the purchase of a CTI record for the required amount of tokens. This process is shown in Figure 8 in the Appendix E. Based on metadata such as the rating, the buyer (B) can initiate an informed purchase. The buyer's backend then utilizes the private key $PrivKey_{ShareB}$ to create and sign the purchase transaction. The backend sends the signed transaction to the blockchain, validating and storing the transaction. This means that all members agree that the buyer's pseudonym $PubKey_{ShareB}$ has transferred the tokens required by the purchase price to the pseudonym $PubKey_{ShareS}$ of the seller and has therefore made a valid purchase. The seller's backend listens for events from the blockchain and is notified of the purchase. The seller's backend initiates an encrypted communication with the buyer's backend and sends the purchased CTI record to the buyer. The buyer's backend validates the integrity of the CTI record by comparing its hash with the one stored on the blockchain. The backend saves the CTI record in the off-chain database, and the buyer is now authorized to submit a rating using the reputation system.

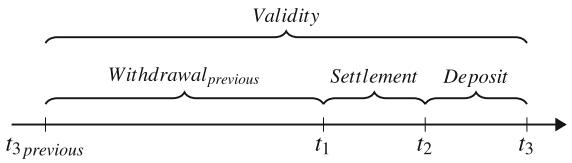


Fig. 3 Timeline of Quality Label Issuance

5.3.2 Marketing label

The **Marketing Label (ML)** is issued for a pre-defined validity period for each community member who fulfills the defined requirements. The validity period and the requirements for issuance can be specified in the community properties. The process of the marketing label issuance is displayed in Figure 9 in Appendix E and consists of multiple phases. We visualize the phases in Figure 3 and describe them as follows.

Settlement. The community defines a recurring issuance date for the ML in its properties. When this date t_1 is reached, the smart contract iterates through all the trading wallets ($PubKey_{,Share}$) and verifies whether each member meets the ML requirements. For eligible wallets, the contract issues and transfers a new ML token. In addition to the trading token representing monetary value, the ML token serves solely to prove the validity of the marketing label for the defined period.

Deposit. As the trading wallet represents only a pseudonymous identity, the marketing label cannot be directly linked to an identifiable organization. To associate it, the member transfers the marketing label token from the trading wallet to their marketing label wallet that stores the member's name. To preserve pseudonymity, this transfer is conducted through a mixer smart contract that uses Zero-Knowledge Proofs (ZKPs). Each member deposits a hashed secret together with the token into the mixer, and later proves ownership of one of the deposits without revealing which one [48, 49].

Withdrawal. During the subsequent withdrawal phase, members can reclaim an ML token to their registered marketing label wallet. To do so, they generate a Zero-Knowledge Proof demonstrating that they previously deposited a valid token without revealing which specific deposit was theirs. The mixer smart contract verifies this proof and, if valid, issues a new ML token to the member's ML wallet. This process ensures that no link between the trading and marketing label wallets can be established while maintaining continuous token validity across periods.

Validity. After withdrawal, members can display the marketing label on their website. We outline the validation of the ML in Figure 10 in Appendix E. External partners or customers can verify its authenticity through a backend verification service, which queries the associated ML wallet and retrieves the stored tokens from the blockchain. Based on the number of valid tokens, the service confirms the member's current and past validity periods. To ensure trust in the decentralized community, verification can also be performed across multiple backend servers. An example of the marketing label is shown in Figure 5 in Appendix D.

5.4 Community properties

As CTI sharing communities differ, we implement community properties to individually adjust each community's configuration of the incentivizing features and incentive mechanisms. Community properties are global variables that each community can set and modify as needs change over time. Each member can propose a new set of community properties, and other members can approve or reject the proposal. If a proposal receives a majority of approval on the blockchain, the new community properties are put in place. We describe all community properties in Appendix B.

5.5 Open-source artifact and live prototype

We publish our prototype as an open-source artifact on GitHub.[3] Thus, the community can adopt and extend our prototype with additional functionality. We deployed a running instance as a live prototype that everyone in the browser can use.[4] Thereby, the incentives and CTI sharing platform can be fully interacted with.

6 Evaluation

Below, we summarize key findings from blockchain network performance and hands-on interviews evaluating the embedded incentive mechanisms. Overall, managers prioritized incentives that increase the net benefits of CTI sharing, whereas security practitioners emphasized features that alleviate required time, effort, and coordination costs.

6.1 Performance and latency

In contrast to public blockchains such as Bitcoin or Ethereum, the private blockchain Besu employs proof-of-authority consensus mechanisms like QBFT or IBFT [42]. These protocols enable significantly higher transaction throughput and lower latency within private networks. A comprehensive performance analysis demonstrated that Besu, under high load, achieves an average transaction throughput of approximately 400 transactions per second with an average transaction latency of 1–2 seconds [50].

[3] Open-source code: https://github.com/techplus2024/Platform

[4] Prototype instance to interact with: https://platform.uversy.com/

In our platform, the actual data exchange occurs off-chain, meaning that on-chain transactions primarily consist of metadata and purchase records. Moreover, members do not trade individual IoCs, which are typically high-volume CTI data. Instead, a single transaction usually represents the purchase of a large bundle or a continuous stream of IoCs. Given that the platform is also restricted to approved members, feedback from our interview participants confirmed that their expected transaction volume would remain well below this threshold, indicating that the platform can readily sustain an active and scalable sharing community.

6.2 Community sharing

Participants emphasized that community-based sharing is essential for platform adoption: "*It builds trust and fosters sharing motivation*" ($P2$). They also predicted greater engagement if the platform served as a "*[...] one-stop store [...]*" ($P11$) for all their cybersecurity needs.

6.3 Reputation system

The feedback about the reputation system was positive. Participants find the rating with giving stars and a brief comment justifiable in terms of the time required, "*more complex rating systems with additional entries would be pointless as people would not do this*" ($P2$).

Participants expected the description for threat reports to be more extensive and frequent than for IoCs due to the scope and complexity, as "*there are more opportunities for feedback*" ($P5$). They also agreed that a minimum of 50-70% of purchased datasets should be rated, which is recognized as a "*balanced threshold between time and value*" ($P9$). Participants noted that only 2-3 ratings per dataset could be sufficient to obtain a first quality indicator, and a description would be particularly insightful. "*There are thousands of reviews on Amazon, but with such a complex topic, just a few reviews are enough*" ($P11$) because "*quality is more important than quantity*" ($P3$).

The method of soliciting feedback also gained insights. Pop-up notifications on the platform would interrupt users at inopportune moments. In contrast, email notifications were considered the most effective reminder mechanism for evaluations, catching users at more convenient times. It was recommended that "*emails should be sent within two weeks after purchase to prompt timely reviews*" ($P6$).

Furthermore, the feedback in the evaluation indicated that "*mandatory descriptions are more beneficial, even if it resulted in slightly more effort*" ($P18$). Additionally, integrating marketing labels into the review overlay was suggested to "*highlight the competence of the reviewers*" ($P11$). Finally, the average rating of sellers would help assess new datasets that had not yet accumulated ratings, and could "*provide an initial quality indicator*" ($P9$).

6.4 Price suggestion

In the hands-on interviews, participants noted that they "*have no idea what price to set*" ($P14$) for a CTI record. Thus, the price suggestion was perceived as "*beneficial and helpful*" ($P4$). While participants argued that the price suggestions could have a limited initial impact due to the few reference records available (cold start problem), they expect the suggestions to improve with usage.

We discovered that not all CTI records should be included in calculating the price suggestion, as outdated CTI records with lower values could bias the results. Participants recommended applying type-specific time windows for including them in the calculation of the price suggestion: IoCs are usually relevant for "*90 days because they can change quickly*" ($P11$), and threat reports have a "*lifespan of about 6 to 12 months*" ($P18$) according to the participants. Thus, we suggest minimizing the weighting of the current value of older CTI records that no longer reflect a comparable value in the calculation. The three used factors (size, content, and attack phases) were emphasized as "*optimal for distinguishing one record from another*" ($P3$).

6.5 Financial payments

Participants explained that "*financial payments are a major driver for activity*" ($P17$). One participant elaborated that this incentive does add enormously to the perceived value of CTI sharing: "*Financial payments demonstrate sharing's worth to management, and I could participate actively.*" ($P2$) The pay-per-use subscription model received positive feedback, allowing organizations to pre-plan their budgets for accessing the platform. Participants expected the prices of threat reports to top those of IoCs, due to the expected complexity and depth of the reports. As one participant observed, "*a more sophisticated report justifies a higher price to compensate for the effort involved*" ($P11$). Our evaluation also uncovered strong demand for a subscription model, enabling organizations to subscribe to a CTI provider and automatically purchase and receive all new data records via an API.

6.6 Marketing label

Participants acknowledged that the "*marketing label is a bigger incentive than you [initially] think*" ($P8$). They "*feel confirmed in their intention, the achievement is there*" ($P11$). To ensure the marketing label remains meaningful and achievable, we identified reasonable thresholds for achieving it. Participants agreed that the validity of the marketing label should last one year, analog "*as an ISO 27001*

doesn't last forever either" (*P*6). According to the participants, further requirements regarding purchase and sale volumes should be determined individually per community. We suggest keeping the sales requirement low to ensure organizations can acquire the label, as they have limited control over their sales volume. Additionally, participants suggested incorporating the rating of CTI records into the requirements, further incentivizing active participation and engagement within the CTI sharing community. Participants find 10 ratings as a practicable threshold.

7 Discussion

In this section, we discuss our findings and future work.

7.1 Community sharing

In a CTI sharing community, large and small organizations are complementary. Large organizations contribute curated datasets and mature analytics backed by sophisticated tooling and greater budgets, while small organizations add niche, regional, and early-warning signals that broaden coverage. In turn, large organizations gain richer telemetry and real-world validation, which reduces blind spots and false positives, while small organizations gain affordable access to high-quality CTI that they couldn't produce alone. The proposed incentives help balance contribution asymmetries and distribute curation costs through financial compensation, raising the security baseline for all.

Community sharing currently requires multiple participants to register simultaneously to preserve pseudonymity. To enable independent onboarding, we propose the use of a Self-Sovereign Identity (SSI) [51]: a trusted authority (e.g., a public institution or EU body) issues a verifiable credential with basic attributes (legal name, sector, location). Applicants then selectively disclose only eligibility attributes (e.g., finance sector, Germany) for peer validation, thereby cryptographically proving eligibility while maintaining pseudonymity; an external payment trustee still performs full identity verification. This approach allows organizations to join at any time without compromising pseudonymity.

Currently, a payment trustee, also referred to as a broker in public blockchain systems, remains a crucial component of all blockchain-based payment mechanisms, as it verifies identities and manages fiat funds, thereby bridging decentralized ledgers and the banking system. As regulations evolve, verification could be distributed across multiple independent entities that must agree on the outcome, thereby reducing reliance on a single intermediary.

7.2 Reputation system

The incentive model helps mitigate analysts' time constraints, for example, through automatic price suggestions and periodic payouts. Still, some components, notably the reputation system, introduce overhead. Future work should streamline these mechanisms, for instance, by developing an automated reputation system that leverages large language models to infer CTI quality dimensions [47] from contributed records.

7.3 Price suggestion

We identified three criteria for the price suggestion in the interviews. As our concept is a first approach, we demonstrated the demand for a price suggestion. Future work could expand this feature by researching possible additional criteria. For example, the size or sector of the organization could be considered to refine the price suggestion. Additionally, the cold start problem could be tackled by developing general guidelines or pricing standards for CTI. Therefore, the price difference between CTI types can be investigated to enhance the price suggestion. Furthermore, sellers would benefit from continued price suggestions for already offered CTI, as the value can change over time. Moreover, future work could explore digital nudges to encourage adoption of the price suggestion, given prior findings that nudges influence behavior in other cybersecurity contexts [57]. Thus, the CTI prices could be improved, increasing sharing activity.

7.4 Financial payments

We suggest initially filling the platform with some CTI records and making them available to participants free of charge. This addition would initiate the sharing dynamic, allowing participants to try out CTI records without risk. Thus, participants could be more willing to make financial payments and participate actively. A future analysis could investigate this effect.

7.5 Marketing label

It is essential that the requirements for obtaining a marketing label are achievable for the average member. Otherwise, the effect of the incentives could be diminished, and pseudonymity could be compromised as an outlier would be identifiable within a limited number of marketing labels. Hence, the requirements for the marketing label should be selected carefully and adjusted as the community evolves.

Table 3 Comparison of our findings to related platform proposals

	[52]	Blocis [53]	[54]	Trident [55]	Dealer [12]	MISP [56]	This Paper
Community Sharing	○	○	●	○	○	◑	●
Reputation System	◑	◑	◑	●	◑	◑	●
Price Suggestion	○	○	○	○	○	○	●
Financial Payments	●	●	◑	●	●	○	●
Marketing Label	○	○	○	○	○	○	●
Open-Source Code	○	○	○	○	●	●	●

Our findings are ● fully addressed, ◑ insufficiently addressed, ○ not addressed

7.6 Platform governance

The platform has been released as open source, enabling the community to extend and further develop its functionality in the future. The architecture components, backend services, off-chain databases, and the blockchain are operated by the participants themselves. The blockchain does not have to be maintained by all participants, but can also be managed by a subgroup of them. If desired, certain organizations, such as chambers of commerce or security service providers, can take over hosting of the entire infrastructure on behalf of their members or customers. In such a setup, a security service provider could assist a client in analyzing and mitigating an incident, and subsequently publish the related CTI information for sale on the platform. For the affected organization, it is acceptable that CTI data are processed within the backend and off-chain database of its trusted security provider, as long as the provider ensures responsible handling of the data and preserves the pseudonymity of the organization towards other platform participants. This approach reduces the infrastructure requirements for individual participants, who in turn may provide financial compensation to the entities operating the components.

8 Related work

We compare related approaches, including incentivized blockchain-based CTI sharing solutions and MISP [56], one of the most widely used threat intelligence sharing platforms [58], as summarized in Table 3.

Riesco et al. [52] use Ethereum to trade CTI records. They introduce a platform-specific CTI token and an additional member role, the investors, using the marketplace as an investment opportunity. The more trading takes place on the platform, the higher the price of the CTI token. The data producers are additionally incentivized to share data by being able to purchase CTI tokens at a reduced price, thus receiving a second income stream. A seller can be rated, although this is not explicitly addressed in the paper. Furthermore, individual CTI records cannot be evaluated based on quality.

Gong and Lee [53] leverage Ethereum for the CTI sharing Platform "Blocis". Consumers can store their evaluation function for data quality in a smart contract. The evaluation is automatically executed when a data producer uploads new CTI records to the blockchain. The feed pays the data producer with Ether tokens if the quality evaluation is positive. Although data quality is addressed in Blocis, there are no details of how this automated evaluation can be conducted, meaning that the reputation system remains abstract.

Nguyen et al. [54] propose a member-restricted community sharing architecture based on the Hyperledger Fabric permissioned blockchain for industrial control systems. A member must pay a periodic subscription fee to gain unlimited access to all data on the platform. However, according to our interview findings, consumers' unlimited access limits the monetary incentive for data producers. In addition, internal community verifiers have to check the quality of the data before it is uploaded to the platform. However, we find that members only want to evaluate CTI records that they have purchased and consider relevant for themselves.

Alexopoulos et al. [55] use the public blockchain Ethereum for the CTI marketplace "Trident", where subscribed IoC streams can be purchased and rated. A buyer must deposit tokens in the smart contract, which they can only receive again after submitting their rating. Thus, members are compelled to use the reputation system.

Menges et al. [12] propose the platform "Dealer" based on the public blockchain EOS, where members can sell their CTI pseudonymously and report a cyberattack to legal authorities based on reporting obligations. Random verifiers rate a CTI record independently before uploading. Despite this, these verifiers are unknown and require a fee to rate the CTI records. This contradicts our findings of the reputation system. Dealer offers the software code as open source.

While MISP [56, 59] is not based on blockchain technology, it still functions as a decentralized system. Participants can host their own MISP instances, which synchronize with each other through push and pull mechanisms. Threat data can be shared either with selected organizations within a sharing community or, for broader dissemination, with additional MISP instances. However, participating organizations

are registered in the system with their real names and are clearly identifiable. To avoid being directly associated with an incident, an organization can delegate its threat data to another organization, which then distributes the data on the platform. Nevertheless, the delegated organization still becomes aware of the security incident, meaning that true pseudonymity is not ensured within the platform. MISP also includes a sighting system that allows participants to provide feedback on shared CTI, particularly IoCs. They can confirm having observed the data or mark it as a false positive or expired. However, textual comments or ratings cannot be added, which is a limitation, especially for threat reports.

In summary, related publications primarily use public blockchain systems, thus not meeting organizations' requirements of a known and limited group of recipients. While related work implements a reputation system and financial payments, most papers insufficiently address organizations' needs. Furthermore, no work introduces a price suggestion or marketing label; only one publication presents a prototype as open-source. MISP offers only limited community sharing and reputation mechanisms and does not address the remainder of our incentives. Its primary focus is on sharing IoCs rather than the often more sensitive threat reports. Thus, our paper offers profound insights into incentives designed to encourage the sharing of all types of CTI.

9 Conclusion

In this paper, we investigated incentives for CTI sharing. Based on interviews with professionals, we identify that the acceptance of a CTI sharing platform can be enhanced by sharing with a known group of recipients and by obtaining crucial information about CTI records through a reputation system and a price suggestion. Furthermore, organizations' platform activity can be increased by financial payments for their CTI records and a marketing label to outline their proactive cybersecurity efforts to partners and customers. We implemented the identified incentives into an open-source prototype and evaluated their impact with hands-on interviews, indicating that they promote the sharing dynamic. Simply put, organizations can share and benefit.

Appendix A Interview questions

In the following, the questions from the semi-structured interviews are listed.

I. Demographic Questions

- What is your job title?
- In which sector is your organization?
- How many employees does your organization have?
- What is your gender?
- How many years of experience do you have in your field?

II. CTI Sharing

- Is your organization actively sharing CTI?
- In how many communities is your organization a member that are suitable for CTI sharing?

III. Incentives for CTI Sharing (Open Questions)

- Why does your organization share / not share CTI?
- What impediments did you encounter when sharing / trying to share CTI?
- What incentives increase your organization's motivation to start or increase CTI sharing?
- How should incentives be designed to motivate your organization to share CTI?
- How should the platform architecture for CTI sharing incentives be chosen?

IV. Incentives for CTI Sharing (Specific Questions)
The following questions were asked if they had not already been answered in the previous group of questions to ensure each participant addressed every question.

- How do financial payments influence your organization's motivation for CTI sharing?
- How does a marketing label influence your organization's motivation for CTI sharing?
- How does community sharing influence your organization's motivation for CTI sharing?
- How do anonymity and pseudonymity inside the community influence your organization's motivation for CTI sharing?
- How does a reputation system influence your organization's motivation for CTI sharing?
- How does a price suggestion for CTI records influence your organization's motivation for CTI sharing?
- How does a centralized or distributed platform influence your organization's motivation for CTI sharing?
- How does a transaction fee influence your organization's motivation for CTI sharing?
- How do a fee and external validators for the quality validation of offered CTI influence your organization's motivation for CTI sharing?

V. Evaluation
Following an introduction to the prototype, participants were given the opportunity for hands-on interaction. Subsequently, they were asked the following questions.

- What are your thoughts on the practicality of the community sharing, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed reputation system, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed price suggestion, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed financial incentives, and what modifications would you recommend?
- What are your thoughts on the practicality of the proposed marketing label, and what modifications would you recommend?
- What are your expectations or concerns regarding the platform's ability to handle the expected transaction volumes?
- Are there any additional features, incentives, or process changes you would suggest to further encourage active CTI sharing?

Appendix B Community properties

All community properties are listed as follows.

I. Reputation System

- **Evaluation quantity:** What percentage of purchases must be evaluated.
- **Evaluation period:** How much time a member has for the pending evaluations.

II. Price Suggestion

- **CTI Record Selection:** How many times the CTI record must be purchased before it is included in the price suggestion. This ensures that unsuitable records are filtered out and do not bias the price suggestion.

III. Marketing Label

- **Community Name:** Name of the community that will be displayed on the marketing label.
- **Requirements:** Which conditions must be met for issuing the marketing label.
- **Validity Period:** Validity period of an issued marketing label.
- **Deposit Period:** Period during which a newly issued marketing label token can be deposited in the mixer smart contract.
- **Mixer Size:** Minimum number of marketing label tokens stored in the mixer smart contract before withdrawal is permitted. A sufficiently large number of deposited tokens is necessary to ensure pseudonymity.

Appendix C Formal definition of price suggestion

The following explains how the price suggestion is calculated based on the identified criteria and uses an example to illustrate this. The size criterion for a CTI record is calculated from the sum of the number of STIX domain objects $\#SDO$, the number of STIX relationship objects $\#SRO$, and the number of represented attack phases $\#AP$. It should be noted that elements of the same type are also taken into account multiple times; for example, two or more SDO attack patterns in one record would be included in the calculation according to their quantity.

$$Size = \#SDO + \#SRO + \#AP \tag{1}$$

To examine two different CTI records A and B for the difference in the amount of information they contain, the delta $Size_\Delta$ is formed by the difference in the size of $Size_A$ and $Size_B$.

$$Size_\Delta = |Size_A - Size_B| \tag{2}$$

SDOs, SROs, and attack phases are considered to calculate the difference in content. For the content difference $C_\Delta SDO$ between A and B, the number of SDO matches found $\#Match_{AB}SDO$ between the two CTI records is subtracted from the total number of SDO elements. It is important to note that the total number of SDOs from the record with the smaller quantity of SDOs is used in the calculation. If the larger record were used, the difference in size would also be considered and thus evaluated twice, as this was already considered in the previous step.

$$C_\Delta SDO = min(\#SDO_A, \#SDO_B) - \#Match_{AB}SDO \tag{3}$$

$$C_\Delta SRO = min(\#SRO_A, \#SRO_B) - \#Match_{AB}SRO \tag{4}$$

$$C_\Delta AP = min(\#AP_A, \#AP_B) - \#Match_{AB}AP \tag{5}$$

Figure 4 shows an example to illustrate the content comparison. CTI record A has four SDOs, whereas record B only has three, which results in a difference in $Size_\Delta = 1$. However, both have one attack pattern and one course of action, which means there are two content matches. Subtracting the two matches from the smaller record B results in a difference

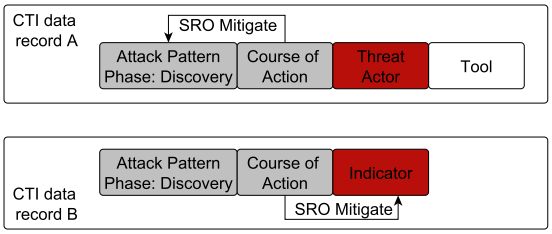


Fig. 4 Example of calculating the similarity of two CTI records A and B for the price suggestion

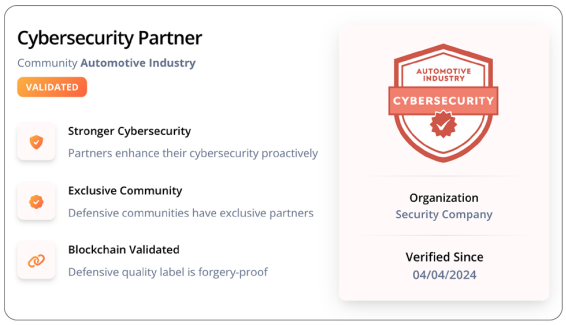


Fig. 5 Validation page of the marketing label

in the content of the SDO elements of $C_{\Delta}SDO = 3-2 = 1$ according to formula (3).

The content difference of the SROs $C_{\Delta}SRO$ and the attack phases $C_{\Delta}AP$ are calculated according to the formulas (4) and (5). In the example in Figure 4, CTI records A and B both have a SRO "mitigate" but with different content, as different SDO elements are involved with Attack Pattern and Indicator. This results in no match and a deviation of $C_{\Delta}SRO = 1 - 0 = 1$. Both records also have an attack phase "Discovery" assigned to the attack pattern, which means that both CTI records describe the same phase of an attack, resulting in $C_{\Delta}AP = 1 - 1 = 0$.

After the deviations $C_{\Delta}SDO$ and $C_{\Delta}SRO$ have been calculated, they can be added to a CTI record structure deviation $C_{\Delta}Struct$.

$$C_{\Delta}Struct = C_{\Delta}SDO + C_{\Delta}SRO \tag{6}$$

Following the example results in $C_{\Delta}Struct = 1+1 = 2$. In contrast, the attack phases do not define a structure but are a special case of the content analysis of a CTI record. As requested by the interview participants, the difference between the provided attack phases is therefore included as a third factor in the final calculation of the total deviation $Total_{\Delta}$ in addition to the size and the content structure. All three factors have a weighting factor w in order to make their influence on the calculation of the total deviation adjustable. Nevertheless, whether certain factors are more important than others, and if so, which ones, has not yet been investigated, which is why each weighting factor has a default value of $w = 1$.

$$Total_{\Delta} = w_s * Size_{\Delta} + w_{st} * C_{\Delta}Struct + w_{ap} * C_{\Delta}AP \tag{7}$$

The final total deviation for the example is:
$Total_{\Delta} = 1 * 1 + 1 * 2 + 1 * 0 = 3$

Appendix D Validation of the marketing label

We outline an exemplary validation page of the marketing label.

Appendix E Prototype process diagrams

We describe the process of member registration and token deposit in Figure 6. We outline the process of uploading a new CTI record in Figure 7 and the purchase of a CTI record in Figure 8. Additionally, we display the process of the marketing label issuance in Figure 9 and the marketing label verification in Figure 10.

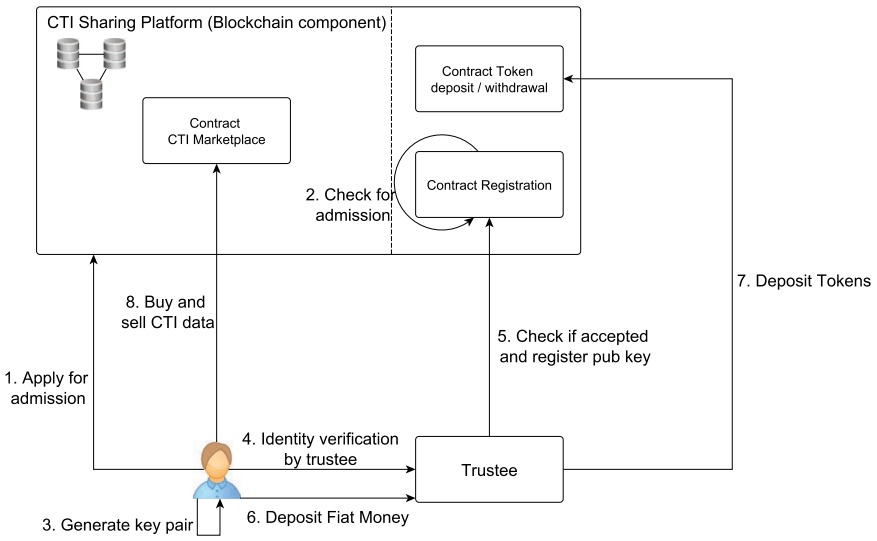


Fig. 6 Existing member registration and deposit of tokens on the sharing platform. The Trustee is only able to access and interact with the token deposit/withdrawal and registration contracts. The Trustee does not have access to the CTI Marketplace contract and therefore has no insight into member sharing behavior

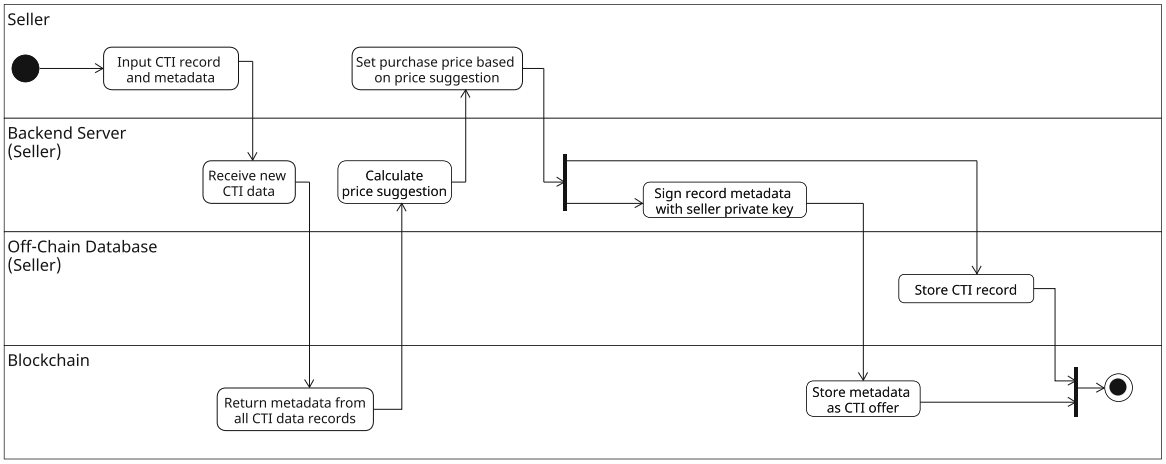


Fig. 7 Upload of a new CTI record for sale in the sharing platform

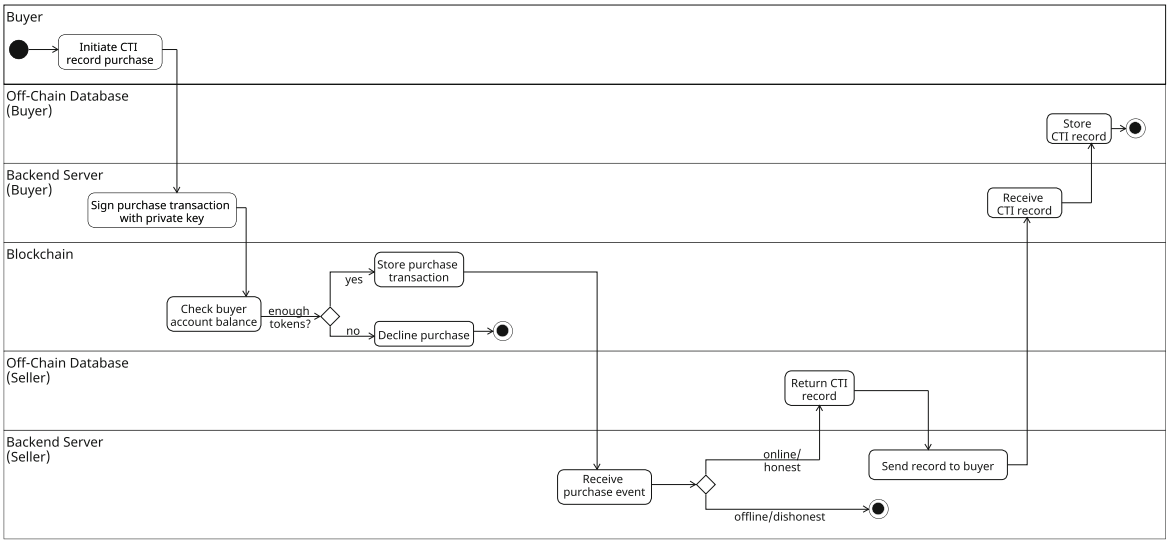


Fig. 8 Purchase of a CTI record in the sharing platform

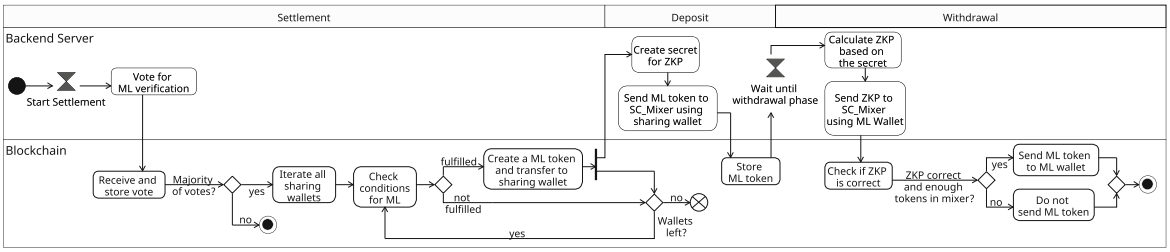


Fig. 9 Issuance of the marketing label (ML) for a new validity period

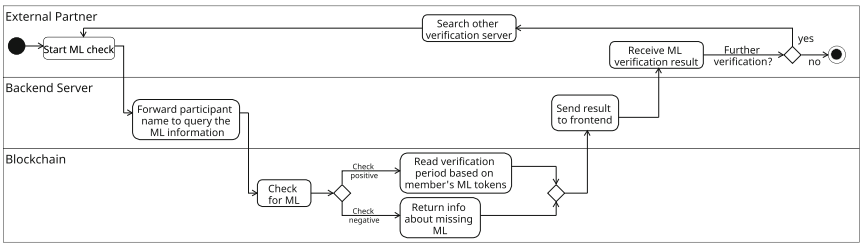


Fig. 10 Verification of the marketing label by an external partner

Author Contributions All authors contributed to the study conception and design. Material preparation, data collection, analysis, and first draft were performed by T.R. and J.G.. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL. This research is part of the DEFENSIVE project, funded by the German Federal Ministry of Research, Technology, and Space (16KIS1568K).

Data Availability The full source code of the developed CTI-sharing platform with incentives is published on GitHub: https://github.com/techplus2024/Platform

Declarations

Conflicts of Interest The authors declare no competing interests.

AI Acknowledgement During the preparation of this work, the authors used DeepL, Grammarly, and ChatGPT (Version 4o) in order to improve readability and language. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Competing interests One of the authors, Günther Pernul, is a member of the editorial board.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Microsoft Corporation. Microsoft digital defense report 2024: The foundations and new frontiers of cybersecurity (2024). https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024. Accessed: 07/06/25
2. Deloitte Global. The promise of cyber: Global future of cyber survey (4th edition) (2024). https://www.deloitte.com/global/en/services/consulting-risk/research/global-future-of-cyber.html. Accessed: 07/06/25
3. Statista. Estimated cost of cybercrime worldwide 2018-2029 (2025). https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Accessed: 11/14/25
4. Hausken, K.: Security investment, hacking, and information sharing between firms and between hackers. Games **8**(2), 23 (2017)
5. Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E.: Cyber threat intelligence sharing: Survey and research directions. Computers & Security **87**, 101589 (2019)
6. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security **72**, 212 (2018)
7. Bouwman, X., Griffioen, H., Egbers, J., Doerr, C., Klievink, B., Van Eeten, M.: A different cup of ti the added value of commercial threat intelligence, In: 29th USENIX security symposium (USENIX security 20), pp. 433–450 (2020)
8. Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., Beyah, R.: Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence, In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp. 755–766 (2016)
9. Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., Kim, H.: Sharing cyber threat intelligence: Does it really help?, In: 31st Annual Network and Distributed System Security Symposium, NDSS 2024, San Diego, California, USA, February 26 - March 1, 2024 The Internet Society, (2024)
10. Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., Foo, E.: Current approaches and future directions for cyber threat intelligence sharing: A survey. Journal of Information Security and Applications **83**, 103786 (2024)
11. Geras, T., Schreck, T.: Sharing communities: The good, the bad, and the ugly, In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, pp. 2755–2769 (2023)
12. Menges, F., Putz, B., Pernul, G.: Dealer: decentralized incentives for threat intelligence reporting and exchange. Int. J. Inf. Secur. **20**(5), 741 (2021)
13. Deci, E.L., Ryan, R.M.: Intrinsic motivation and self-determination in human behavior. Springer Science & Business Media, Berlin (2013)
14. DiMaggio, P.J., Powell, W.W., et al.: The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. **48**(2), 147 (1983)
15. PAMELA, S.T.: The institutionalization of institutional theory, Studying organization: Theory and method p. 169 (1999)
16. Hillman, A.J., Withers, M.C., Collins, B.J.: Resource dependence theory: A review. J. Manag. **35**(6), 1404 (2009)
17. Pfeffer, J., Salancik, G.: In: Organizational behavior 2 Routledge, pp. 355–370, (2015)
18. Reittinger, T., Pernul, G.: A taxonomy of positive incentives to motivate cybersecurity behaviors, In: Proceedings of the 58th HI International Conference on System Sciences (HICSS-58) (2025)
19. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Employee motivation in organizational cybersecurity: Matching theory and reality, In: International Symposium on Human Aspects of Information Security and Assurance, Springer, pp. 3–16 (2024)
20. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Motivational factors in cybersecurity: linking theory to organizational practice, Information & Computer Security (2025)
21. Kamenica, E.: Behavioral economics and psychology of incentives. Annu. Rev. Econ. **4**(1), 427 (2012)
22. Bryson, A., Freeman, R., Lucifora, C., Pellizzari, M., Perotin, V., et al.: Paying for performance: incentive pay schemes and employees' financial participation. CEP discussion paper **1112**, 52–75 (2012)
23. Malaga, R.A.: Web-based reputation management systems: Problems and suggested solutions. Electron. Commer. Res. **1**, 403 (2001)
24. Tadelis, S.: Reputation and feedback systems in online platform markets. Annual Review of Economics **8**, 321 (2016)
25. Jahn, G., Schramm, M., Spiller, A.: The reliability of certification: Quality labels as a consumer policy tool. J. Consum. Policy **28**, 53 (2005)
26. de Melo e Silva, A., Costa Gondim, J.J., de Oliveira Albuquerque, R., García Villalba, L.J.: A methodology to evaluate standards and

platforms within cyber threat intelligence. Future Internet **12**(6), 108 (2020). https://doi.org/10.3390/fi12060108
27. OASIS. Oasis stix documentation (2024). https://oasis-open.github.io/cti-documentation/stix/intro. Accessed: 07/06/25
28. Corporation, M.: Mitre ATT&CK website (2025). https://attack.mitre.org/. Accessed: 07/06/25
29. Sunyaev, A.: In: Internet Computing, vol. 2, ed. by A. Sunyaev Springer International Publishing, Cham, (2020), pp. 265–29. https://doi.org/10.1007/978-3-030-34957-8_9
30. El Ioini, N., Pahl, C.: A review of distributed ledger technologies, In: On the Move to Meaningful Internet Systems. OTM 2018 Conferences, ed. by H. Panetto, C. Debruyne, H.A. Proper, C.A. Ardagna, D. Roman, R. Meersman Springer International Publishing, Cham, pp. 277–288 (2018)
31. De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F., Sassone, V.: Blockchain and cybersecurity: a taxonomic approach, In: Workshop. EU Blockchain Observatory (2019)
32. Willis, G.B.: Cognitive interviewing: A tool for improving questionnaire design, sage publications, (2004)
33. Deterding, N.M., Waters, M.C.: Flexible coding of in-depth interviews: A twenty-first-century approach. Sociological methods & research **50**(2), 708 (2021)
34. G.R. Gibbs, Thematic coding and categorizing, Analyzing qualitative data **703**(38-56) (2007)
35. Caine, K.: Local standards for sample size at chi, In: Proceedings of the 2016 CHI conference on human factors in computing systems (2016), pp. 981–992
36. Nweke, L.O., Wolthusen, S.: Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection, In: 2020 12th International Conference on Cyber Conflict (CyCon), vol. 1300 (IEEE, 2020), vol. 1300, pp. 63–78
37. DIHK. Industrie- und handelskammern (german trade associations). https://www.dihk.de/de/ueber-uns/die-ihk-organisation/industrie-und-handelskammern. Accessed: 07/06/25
38. European Union. General data protection regulation (gdpr) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Accessed: 07/06/25
39. Netwrix. Netwrix cloud data security report (2019). https://www.netwrix.com/2019cloudsecurityreport.html. Accessed: 07/06/25
40. Capgemini. Capgemini cloud sovereignty: The road ahead (2022). https://www.capgemini.com/insights/research-library/cloud-sovereignty/. Accessed: 07/06/25
41. Federal Bureau of Investigation. 2023 cryptocurrency fraud report released (2024). https://www.fbi.gov/news/stories/2023-cryptocurrency-fraud-report-released. Accessed: 07/06/25
42. The Linux Foundation. Hyperledger besu (2025). https://github.com/hyperledger/besu. Accessed: 07/06/25
43. Couchbase, Inc. Couchbase (2025). https://github.com/couchbase. Accessed: 07/06/25
44. OpenJS Foundation. Node.js (2025). https://github.com/nodejs. Accessed: 07/06/25
45. Laravel Holdings Inc. Laravel (2025). https://github.com/laravel/framework. Accessed: 07/06/25
46. European Union. Regulation (eu) 2024/1624 of the european parliament and of the council of 31 may 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (2024). https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng. Accessed: 07/06/25
47. Schlette, D., Böhm, F., Caselli, M., Pernul, G.: Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Secur. **20**, 21 (2021)
48. Rinberg, R., Agarwal, N.: Privacy when everyone is watching: An sok on anonymity on the blockchain, Cryptology ePrint Archive (2022)
49. Petkus, M.: Why and how zk-snark works, arXiv preprint arXiv:1906.07221 (2019)
50. C. Fan, C. Lin, H. Khazaei, P. Musilek, Performance analysis of hyperledger besu in private blockchain, In: 2022 IEEE international conference on decentralized applications and infrastructures (DAPPS) (IEEE, 2022), pp. 64–73
51. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Computer Science Review **30**, 80 (2018)
52. Riesco, R., Larriva-Novo, X., Villagrá, V.A.: Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and smart contracts to foster the cyber threat and risk intelligence exchange of information. Telecommun. Syst. **73**(2), 259 (2020)
53. Gong, S., Lee, C.: Blocis: blockchain-based cyber threat intelligence sharing framework for sybil-resistance. Electronics **9**(3), 521 (2020)
54. K. Nguyen, S. Pal, Z. Jadidi, A. Dorri, R. Jurdak, A blockchain-enabled incentivised framework for cyber threat intelligence sharing in ics, In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) (IEEE, 2022), pp. 261–266
55. Alexopoulos, N., Vasilomanolakis, E., Roux, S.L., Rowe, S., Mühlhäuser, M.: Trident: towards a decentralized threat indicator marketplace, In: Proceedings of the 35th Annual ACM Symposium on Applied Computing (2020), pp. 332–341
56. Wagner, C., Dulaunoy, A., Wagener, G., Iklody, A.: MISP: the design and implementation of a collaborative threat intelligence sharing platform, In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS 2016, Vienna, Austria, October 24 - 28, 2016 (ACM, 2016), pp. 49–56
57. Baumer, T., Reittinger, T., Kern, S., Pernul, G.: Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations, In: Twentieth Symposium on Usable Privacy and Security (SOUPS 2024) (2024), pp. 239–258
58. Fischer, D., Sauerwein, C., Werchan, M., Stelzer, D.: An exploratory study on the use of threat intelligence sharing platforms in germany, austria and switzerland, In: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES 2023, Benevento, Italy, 29 August 2023- 1 September 2023 (ACM, 2023), pp. 30:1–30:7
59. CIRCL. MISP documentation (2024). https://www.circl.lu/doc/misp/. Accessed: 07/06/25

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.