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

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

Magdalena Glas
University of Regensburg
Regensburg, Germany
magdalena.glas@ur.de

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

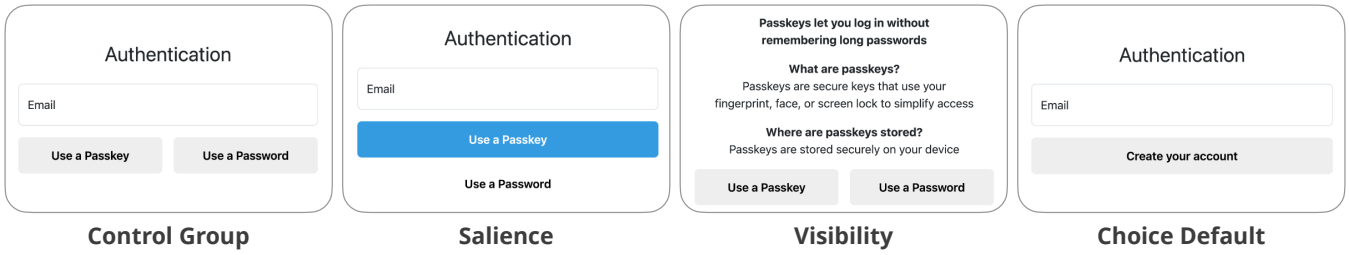

Figure 1: Digital nudges to increase passkey adoption at user registration.

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

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 the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3772318.3791425

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791425

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 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

[1]IRB certificate: https://gfew.de/ethik/NAPzzShc

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.

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 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.

[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.

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 precommitment, 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 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.

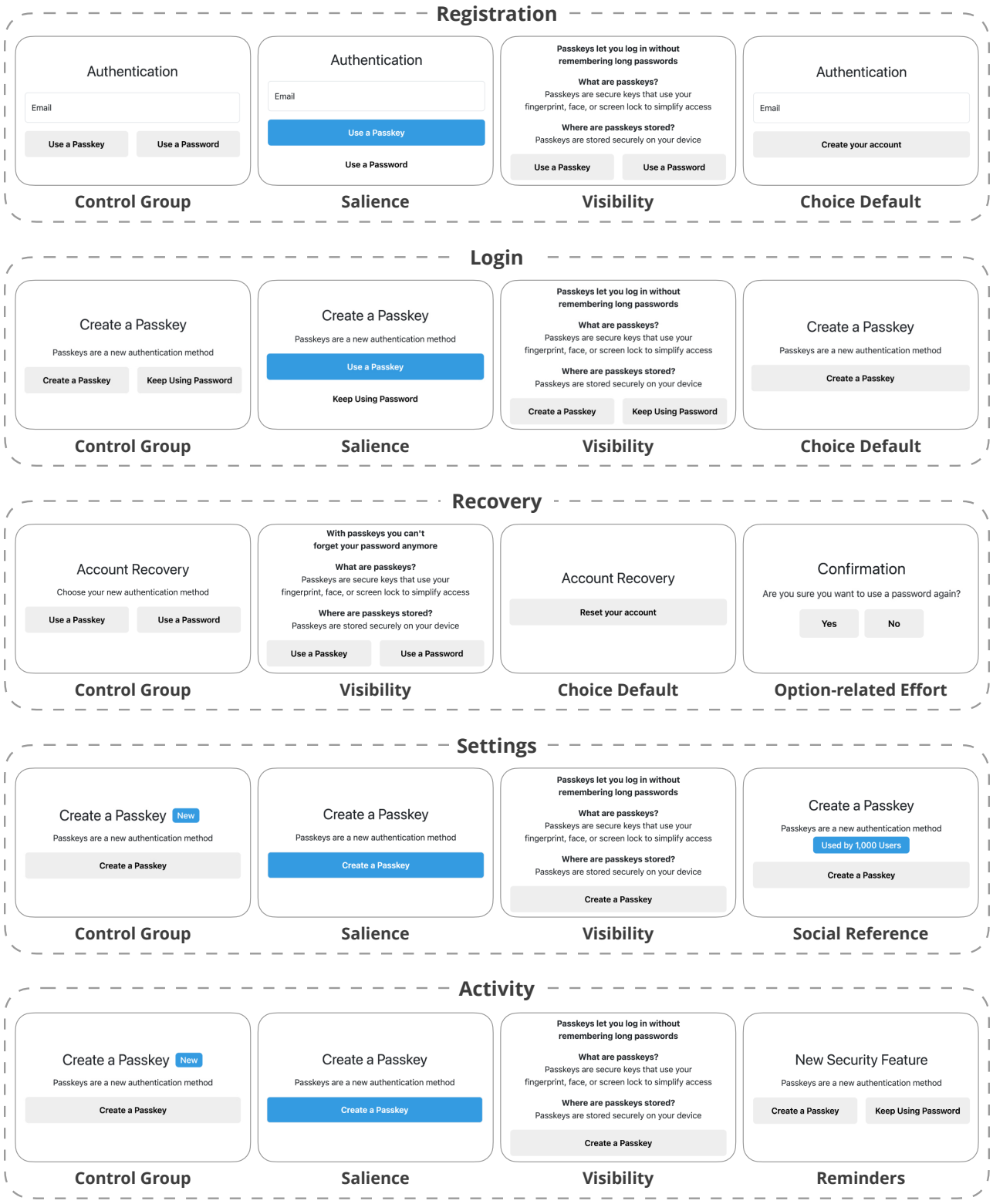

Figure 2: Design of selected nudges and control groups for all five touchpoints in the user study.

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.

6.5 Summary of Results

To summarize, our results show that the implemented nudges significantly increased both *interaction* and *adoption rates* compared

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.

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 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

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.

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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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. doi: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