PREPRINT

On the Influence of Passkey Enrollment Strategies

Florian Nawrath, Sven Bugiel, and Maximilian Golla

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
golla@cispa.de

Abstract. The transition from passwords to passwordless authentication offers the potential to improve online account security. Passkeys promise faster, more secure, and more user-friendly authentication. Yet, their adoption hinges not only on technical compatibility but also on user acceptance and the strategies employed to encourage their enrollment. In this work, we examine how three different enrollment strategies influence user perceptions and willingness to engage with passkeys. We conducted a mixed-methods study with 36 participants, combining a practical authentication task with follow-up semi-structured interviews. We observed differences in completion confidence, understanding, and adoption willingness, with the fastest enrollment flow also producing the greatest uncertainty about task completion. While our participants generally regarded passkeys as secure and convenient, we observed gaps in user understanding that could hinder adoption. We discuss the implications of these findings for service providers, offering guidance for designing effective enrollment experiences that support the broader transition to passwordless authentication.

Keywords: Adoption · Passkey · FIDO · Passwordless Authentication.

1 Introduction

The limitations of password-based authentication have become increasingly apparent, with well-documented issues, both when it comes to usability and security [64,51,52]. Although several password security reinforcements and management tools have been introduced, core issues remain, including password reuse, susceptibility to phishing attacks, memorability challenges, and weaknesses in account recovery [67,49,26,15]. As a result, there has been an increasing interest in developing solutions that offer enhanced security and usability [55,19,23,9]. Passkeys, a development based on the *Fast Identity Online 2 (FIDO2)* [12] standard, offer a promising and increasingly practical way to reduce our overreliance on passwords on the web. By relying on phishing-resistant cryptographic credentials, they eliminate the need for memorization and can support faster and more successful sign-ins [55]. Companies such as Apple, Google, and Microsoft strongly support the transition toward this passwordless ecosystem [19], contributing to the growing availability of passkeys across a wide range of web services [1,32].

Although the security of passkeys is well studied [44,32], the adoption of FIDO2 technologies is not purely a function of technical superiority but also of user experience. The FIDO Alliance calls first-time passkey creation one of the biggest hurdles in passkey adoption [24]. To achieve widespread adoption, it is essential that users

PREPRINT

understand and trust the technology. This introduces the challenge for web services of designing effective enrollment strategies that encourage adoption without sacrificing autonomy or comprehension. A Microsoft Security Blog post [55] examined nudging and prioritization in shaping user interactions with passkeys. Subsequent field studies have examined adoption and continued use [58] and demonstrated the effectiveness of enrollment nudges [3,37,57], motivating closer examination of how users interpret these enrollment experiences.

To fill this gap, we examine three enrollment strategies used by major web services: a **forced** approach (KAYAK), where passkeys replace passwords without any explanation; a **nudging** approach (eBay), where passkeys are suggested at opportune moments; and a **passive** approach (SONY), where passkeys are supported but hidden in the account settings. In this work, we investigate the impact of these three strategies on adoption willingness, user acceptance, understanding, and perceptions of passkeys. In a controlled mixed-method study, participants were assigned to one of the strategies and interacted with a real-world website to complete a passkey registration task. Their experiences were evaluated through semi-structured interviews and quantitative performance metrics. Accordingly, we address the following research question:

> **Research Question**
>
> *How do passkey enrollment strategies shape users' acceptance, understanding, and trust?*

Web services, or relying parties, enroll users in passkeys through different strategies. Recent work has shown that nudges can increase passkey adoption at scale, but less is known about how concrete strategies affect users' perceptions and comprehension during enrollment. This matters because users may approach passkeys with different technical questions, misconceptions, and expectations about security, recovery, and device dependence. We therefore examine how different enrollment strategies influence perceived security, transparency, autonomy, and willingness to adopt passkeys.

Our findings reveal that while passkeys are generally regarded as secure and convenient, user understanding of their mechanisms remains limited. Participants in the *nudging* condition generally described passkeys as easy to use and expressed willingness to continue using them. The *forced* strategy, although highly efficient for passkey enrollment, often led to confusion and lower willingness to adopt. Participants in the *passive* condition expressed the highest willingness to adopt and showed comparatively clear understanding, although their enrollment tasks required more time and interaction. Outside an instructed laboratory task, however, users may not discover a passkey option offered only in account settings. Proactive prompts can increase its visibility and uptake [55,57]. Based on these findings, we provide actionable insights into designing enrollment experiences that support the adoption and acceptance of passwordless authentication.

PREPRINT

2 Background and Related Work

In this section, we briefly introduce passkeys, relevant UX guidelines related to passkeys, and the closest related work.

2.1 FIDO and Passkeys

The FIDO ("Fast IDentity Online") Alliance [18] specifies standards for passwordless authentication using public-key cryptography. Passkeys are FIDO credentials that support passwordless authentication and may be either synced across devices or bound to a single authenticator [20]. Synced passkeys can be made available across a user's devices through platform providers [19] or third-party password managers [31,53], reducing the need for separate enrollment and facilitating recovery after device loss.

Authentication is based on a challenge–response protocol: the client device signs a server challenge with the private key, which can only be accessed after the user locally verifies with a biometric, PIN, pattern, or device password. Passkeys are resistant to phishing [15,4,36], circumvent weak or reused credentials [28,49], and do not require server-side storage of secrets, mitigating the impact of data breaches [33,46]. Industry case studies demonstrate that passkeys can reduce online authentication times by 50% compared to passwords [21].

2.2 Passkey UX Guidelines

Google, Microsoft, and other FIDO Alliance members provide UX guidelines for passkey registration and sign-in flows, recommending clear visual indicators, the usage of canonical icons, and the confirmations of important actions [23,22,29,5]. They commonly recommend prompting passkey creation alongside account-related tasks, such as creating a new account, logging in, updating security settings, or account recovery. The FIDO Alliance also describes Conditional Create, which enables automatic passkey creation after an eligible password-based sign-in without an additional user confirmation step [24]. This adoption challenge has led platform providers to revise enrollment strategies and awareness campaigns. For example, Microsoft [55] found that passive enrollment accounted for less than 1% of total enrollments, while well-timed prompts during sign-up, after sign-in, or during password resets achieved engagement five times higher than its pre-launch expectations. Messages emphasizing security and speed were more effective than convenience. Ramat et al. [54] systematically compared passkey user journeys across 111 websites and found that core passkey support is converging, while supporting features remain inconsistently implemented. Jannett et al. [32] further found substantial variation in passkey management flows and security across websites.

Our study complements these analyses by examining users' experiences with *forced, nudged, and passive* enrollment on three prominent web services. We compare understanding, completion confidence, and initial adoption willingness across these implementations, providing user-level evidence relevant to passkey enrollment design.

PREPRINT

2.3 Related Work

Prior research highlights the benefits and challenges of FIDO adoption. For example, Lyastani et al. [41] conducted a lab study comparing passwords with FIDO2 hardware security keys used without PIN entry. Participants valued the keys' convenience and perceived security, but some were reluctant to adopt them because they feared losing access to their accounts if a key was lost. The study used a single enrollment flow in which participants registered their keys directly on the mock websites' registration pages. It therefore left open how the choice of enrollment strategy affects users' experience. More recently, Kupris and Schreck [35] compared passkeys, security keys, and one–time passwords in a university setting, finding favorable usability and acceptance for passkeys alongside contextual barriers and recovery concerns.

At the organizational level, prior work identified account recovery and fallback authentication [43,38], technical constraints, regulatory requirements, legacy-system integration, and user resistance as challenges relevant to deploying passkeys at scale [39]. Lassak et al. [37] showed that misunderstandings of biometric local verification in WebAuthn can reduce trust. Together with Farke et al.'s [17] findings on biometric privacy concerns, this highlights the need for enrollment strategies that address misconceptions while fostering confidence. To avoid such concerns, our study uses a PIN instead of biometrics for local verification while explaining its purpose to participants. Furthermore, Lassak et al. [37] suggested evaluating "opinionated nudging" as a UI design to encourage adoption. Golla et al. [27] explored messaging and UX patterns to increase 2FA adoption. They found that tailored messages, such as interstitial prompts and opinionated reminders, addressing user motivations and mental models, together with established UX principles, can encourage users to enable 2FA.

Matzen et al. [44] reviewed passkey research and identified key obstacles to user acceptance. Although passkeys improve security and usability, adoption is hindered by low user awareness and persistent misconceptions, particularly around security, functionality, and account recovery. Concerns about device failure and limited credential access further reduce confidence. Their review emphasizes the need for better user education and clearer communication to build trust and adoption, while highlighting a gap in user-centered research on perception and usability concerns. Beyond adoption, recent work has also examined later stages of the passkey lifecycle. Giacomello et al. [25] studied users' views on revocation and found that current per-service removal is perceived as cumbersome, particularly after device loss or compromise. Daffalla et al. [14] further found that users struggled to identify and remove adversarial passkeys, including uncertainty about whether account remediation was complete. These findings motivate examining whether enrollment interfaces help users understand that a credential has been created and how it relates to their account.

Building on this, related work has questioned whether education alone is sufficient to drive adoption, examining whether clearer explanations of FIDO2's mechanics or benefits change user behavior. Amer et al. [3] showed that neither technical explanations nor highlighting security advantages meaningfully affect willingness to adopt. Instead, adoption is shaped by perceived risk, self-efficacy, and response costs, suggesting that enrollment strategies must not only inform users but also reduce perceived effort and foster confidence. Reittinger and Pernul [58] examined passkey adoption and subsequent use in

PREPRINT

a six-month field study, identifying initial setup difficulties alongside improvements with repeated use. Reittinger et al. [57] combined expert interviews with a large-scale randomized controlled trial to evaluate enrollment nudges across several touchpoints. Their findings demonstrate increased adoption and highlight tradeoffs between default enrollment and user autonomy. Our study complements this evidence through interviews and task observations that examine how users interpret three deployed enrollment strategies, recognize task completion, and express willingness to continue using passkeys.

3 Method

As our work examines how the enrollment process shapes perception and adoption willingness, we analyze how online services implement their passkey onboarding process.



(a) Force Strategy (b) Nudge Strategy (c) Passive Strategy

Fig. 1. Evaluated Enrollment Strategies: The *forced* approach, where passkeys replace passwords without any explanation; a *nudging* approach, where passkeys are suggested at opportune moments; and a *passive* approach, where passkeys are hidden in the account settings.

3.1 Enrollment Strategies

We identified three distinct enrollment strategies by analyzing stakeholder recommendations [23,30,55] and testing various passkey-enabled websites [1]. We call these three enrollment strategies *forced*, *nudged*, and *passive*. A visual representation of the strategies can be found in Figure 1. We selected prominent, consistent, and guideline-adherent services to represent the two recommended strategies. Additionally, at the time of the study design, KAYAK employed a mandatory passkey enrollment approach [60], without a preceding website-level explanation of passkeys.

The three strategies work as follows:

– **Force (KAYAK):** When creating a new account, users are required to register a passkey, with no option to use a password. Users are not informed about passkeys in advance, similar to how many websites request a password without providing any explanation about what a password is or how to choose a secure one.

PREPRINT

– **Nudge (eBay):** Users are prompted to create a passkey when they interact with their existing credentials, for example, when changing or resetting their password, or logging in. In this approach, users are gently encouraged to try out passkeys, rather than being forced to adopt them. Google and Microsoft [23,55,30] recommend this strategy in their guidelines to foster adoption.
– **Passive (SONY):** This strategy neither enforces nor actively promotes passkeys. Instead, passkeys are buried within the account settings and typically discovered only by users who are specifically interested in strengthening their account security or by those with prior experience.

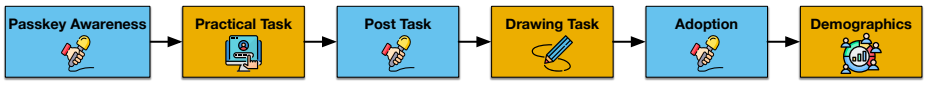


Fig. 2. Study Protocol: Our study includes a practical task with one of the three websites, a drawing task, and a demographics questionnaire. In between, we interview participants about their passkey awareness, impressions from the practical task, and their willingness to adopt passkeys.

3.2 Study Protocol and Design

We designed a study, consisting of an interview and accompanying practical tasks, to investigate participants' awareness and perception and their willingness to adopt passkeys. Figure 2 summarizes the study protocol. The full interview guide can be found in Appendix A. The flow of the practical task is outlined in Appendix C. Our study was structured as follows:

1. ***Introduction.*** We welcomed participants, explained the study purpose and procedure, and briefly introduced passkeys and local verification using a PIN or biometrics, following the script in Appendix A. We emphasized that we were interested in their perspectives with no right or wrong answers. Moreover, we also offered a selection of snacks and water to comfort participants.
2. ***Informed Consent.*** Each participant signed a consent form at the beginning of the interview. The form outlined the study goals, participants' rights, and the methods for data collection and processing. All information regarding the purpose and processing of the study contained on the consent sheet was explained beforehand. Before starting with the first questions, we once more requested oral consent to record the interview.
3. ***Passkey Awareness Questions.*** To ease participants into the interview and build rapport, we began with simple questions about their device usage and unlocking habits. We then asked whether these unlock methods were used beyond unlocking their device. Finally, we asked about any direct contact with FIDO-based passwordless authentication or passkeys to establish their familiarity.
4. ***Practical Task.*** Participants were randomly assigned to one of the three strategies and received instructions for their group-specific website, which asked them to

PREPRINT

register a passkey. The credentials, including the Windows Hello PIN to unlock the device and register a passkey, were provided. During the task, we collected data via observation and screen recording on the lab device provided for the task.

5. ***Post-Task Questions.*** Following the practical part, we interviewed the participants about their experience, focusing on their perceptions. We mainly investigated perceived pros and cons, as well as their understanding of how passkeys work.
6. ***Drawing Task.*** Participants then completed a drawing task to capture their mental models of passkeys and encourage deeper reflection on the experience [34].
7. ***Concluding Questions.*** Finally, building on new insights by the participant, we concluded the interview by asking adoption questions. These included their willingness to adopt, if passkey availability is desired, and what they see as the biggest obstacle to passkey adoption.
8. ***Demographics.*** We collected demographics in line with best practices [56,62], including age, gender, IT background, and their current level of education.
9. ***Compensation.*** Finally, participants received 15€ for the study, which took 35 minutes on average. Although all participants completed the study, compensation was guaranteed after signing the consent sheet, regardless of how far the interviews proceeded.

3.3 Recruitment and Demographics

The entire study took place in December 2024. Participants were recruited through multiple channels. We primarily targeted the authors' social environment and the members of our university. There were no selection prerequisites. We recruited 37 participants in total. However, one participant was excluded from our analysis due to technical reasons, as the nudge failed to appear during their practical task. The remaining 36 participants were randomly assigned by the researcher and evenly distributed into the three groups, with 12 participants each: $Group_f$ (Forced), $Group_n$ (Nudged), and $Group_p$ (Passive).

3.4 Data Collection

To evaluate the different strategies, a mix of qualitative and quantitative data was collected through three methods: an interview, a practical task, and a drawing task.

- ***Interviews.*** All interviews were recorded and pre-processed using a local transcription software [11].
- ***Practical Task.*** Participants were instructed to visit one of the three websites with different enrollment strategies and register a passkey. We provided a laptop with Windows 11, Google Chrome, and the Windows Hello PIN required to locally verify and interact with a passkey. We ensured all participants were familiar with the OS and browser. All required usernames, passwords, and access to a study email account were provided to the participants. The idea behind this task was to simulate first-time passkey registration on the given websites. During the task, we recorded the screen for easier analysis. The data collected during the task included the time taken to register a passkey, the total time spent on the task, the number of clicks, the amount of help needed, and the confidence in successful task completion. In

PREPRINT

case the participant was assigned to the nudging condition, the success rate of the nudge was measured (i.e., whether the participant engaged and used the nudge, or just skipped it).
– ***Drawing Task.*** After the practical task and the corresponding follow-up questions, participants were provided a pen and paper and asked to create a simple drawing that illustrates the passkey registration process from their point of view. This activity helped to assess participants' mental models and conceptual understanding of how they believed passkeys work [34].

3.5 Data Analysis

Next, we explain how we analyzed the interviews, practical tasks, mental models, and screen recordings. As this work is exploratory in nature, with a small sample size of only 12 participants per enrollment strategy, we refrain from conducting statistical tests and instead focus on qualitative observations and descriptive comparisons.

Qualitative Analysis. We analyzed the interview data applying a thematic analysis approach as outlined in Braun and Clarke [10]. For this, we developed our codebook iteratively. First, two members of the research team independently coded 25% of the interview transcripts. This step ensured that initial codes captured a wide range of participant perspectives and provided a basis for refining the qualitative coding. The coders then compared their code sets, discussed discrepancies, and consolidated overlapping codes into a shared codebook, adding definitions to each code for consistency. Using this revised codebook, both coders independently recoded the nine interviews. Before resolving disagreements from this round, we calculated Cohen's kappa separately for each interview, comparing the presence or absence of each code in the revised codebook. The mean Cohen's kappa across these interviews was 0.84, indicating almost perfect agreement. Finally, the codebook was applied to the full dataset by a single coder. During this process, codes were organized into broader conceptual groups (e.g., *Adoption*, *Acceptance*, *Passkey Perception*), which served as the foundation for identifying and refining higher-level themes. The complete codebook, including the applied codes, their definitions, and broader conceptual groups, is provided in Appendix B. We gained additional insights from the participants' drawings. Using the collected data, we explored how each enrollment strategy influenced participant perceptions, looking at whether strategies such as forced or nudged enrollment led to a clearer understanding or confusion. In addition, participant statements were used to assess whether they capture or summarize important themes.

Quantitative Analysis. We analyzed the following data:

– ***Time to Register a Passkey & Time to Task Completion.*** The time required to register the passkey and the time until the participant stated or asked whether they were finished, or the interviewer confirmed completion.
– ***Adoption Willingness.*** The self-reported willingness to continue using passkeys.
– ***Clicks.*** The number of mouse clicks required to register the passkey and the total clicks to complete the task.

PREPRINT

- ***Completion Confidence.*** Whether participants confidently stated that they had finished, were unsure, or did not realize that the task was complete.
- ***Help Intensity (Requests and Interventions).*** The number of questions asked by the participant and interventions required from the interviewer.
- ***Nudge Success Rate.*** (Only applicable in $Group_n$) The success rate of the nudge (i.e., the number of times the prompt was not skipped).

3.6 Ethics Statement

This study was reviewed and approved by the ethical review board (ERB) of the Department of Computer Science at Saarland University. In designing the research protocol, we adhered to the principles of the Menlo Report [66], namely, "respect for persons," "beneficence," and "justice."

Participants received detailed information about the study's purpose, procedures, potential risks, and their rights, including the voluntary nature of their participation and the option to withdraw at any time without consequence. Written and oral informed consent was obtained prior to each interview. Names and email addresses were collected to document consent and enable participants to withdraw and request deletion of their study data. However, these identifiers were deleted after the study was completed. Participants were never required to disclose personal data to the evaluated websites, and all accounts created by the researchers for the study were deleted afterwards. To protect participant privacy, especially regarding authentication practices and personal perceptions, audio recordings were transcribed locally and immediately anonymized to minimize the retention of potentially identifiable data. Transcripts were stored under pseudonyms to mitigate risks of inadvertent disclosure. All data handling and storage complied with the GDPR.

4 Results

Next, we present our results comparing the three strategies. We begin with demographics and primary themes, followed by participants' mental models and quantitative findings.

4.1 Demographics

Table 1 summarizes the demographics of our participants. Most participants (31 out of 36; 86.1%) were aged 25–34, with similar numbers in each study group. Gender distribution was balanced: 18 men (50.0%), 17 women (47.2%), and one non-binary participant (2.8%). Regarding education, the majority of participants (30; 83.3%) had a higher education degree, which is not uncommon for studies in a university setting. Here, "Higher" denotes higher education qualifications (e.g., bachelor's or master's degrees, university diplomas, state examination qualifications, or doctorates), "Intermediate" denotes secondary school-leaving qualifications, and "Trade/Technical" denotes vocational or technical training. Four of the five participants with intermediate education were in the passive group. In terms of computer science background, we have an almost balanced sample (55.6% versus 41.7%). However, participants with CS background were mainly in $Group_f$ and $Group_n$.

PREPRINT

Table 1. Overview of Demographics.

Category	$Group_f$ (n = 12)	$Group_n$ (n = 12)	$Group_p$ (n = 12)	**Total** (n = 36)
Age Groups				
18–24	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (8.3%)
25–34	10 (83.3%)	10 (83.3%)	11 (91.7%)	31 (86.1%)
45–54	1 (8.3%)	0 (0.0%)	0 (0.0%)	1 (2.8%)
55–64	0 (0.0%)	1 (8.3%)	0 (0.0%)	1 (2.8%)
Gender				
Man	5 (41.7%)	7 (58.3%)	6 (50.0%)	18 (50.0%)
Woman	7 (58.3%)	5 (41.7%)	5 (41.7%)	17 (47.2%)
Non-Binary	0 (0.0%)	0 (0.0%)	1 (8.3%)	1 (2.8%)
Education				
Higher	11 (91.7%)	12 (100.0%)	7 (58.3%)	30 (83.3%)
Intermediate	1 (8.3%)	0 (0.0%)	4 (33.3%)	5 (13.9%)
Trade/Technical	0 (0.0%)	0 (0.0%)	1 (8.3%)	1 (2.8%)
Computer Science Background				
Yes	8 (66.7%)	9 (75.0%)	3 (25.0%)	20 (55.6%)
No	4 (33.3%)	3 (25.0%)	8 (66.7%)	15 (41.7%)
N/A	0 (0.0%)	0 (0.0%)	1 (8.3%)	1 (2.8%)

4.2 Qualitative Analysis

For the qualitative analysis, we sorted the codes for each group by frequency and identified unique or interesting codes. We first present three primary themes across all groups, followed by the findings for $Group_f$, $Group_n$, and $Group_p$.

All Groups. We discuss three overarching findings.

- ***Security.*** Security was the most prevalent theme, with 28 of 36 participants viewing passkeys as secure. For example, *P6* (Nudge) mentioned *"I can't think of anything that might be even more secure."* Additionally, a total of 32 stated that passkeys are stored on the device.
- ***Usability.*** Participants found passkeys highly usable, mentioning memorability, ease of use, and speed. Of all participants, 21 participants noted memorability issues with passwords or that passkeys do not require memorization. As an example, *P36* (Force) said *"What I like is that you don't have to remember lots of passwords, but just one."* And 28 participants felt that passkeys are easy to use, either by stating the speed of the system, the convenience, or how easy it felt. *P9* (Force) summarized this feeling: *"That was very quick and easy."* This is supported by 22 participants who stated a preference for passkeys, compared to other authentication methods.
- ***Mistrust and Lack of Transparency.*** The third widespread theme we observed was mistrust: *"Well, and everything is only secure until the first person comes along who has hacked it."* by *P14* (Force). This mistrust appears to stem primarily from a lack of transparency in communicating how passkeys work. *P28* (Nudge) phrased

PREPRINT

this representatively; *"If you don't understand how it works, it's difficult to trust it."* A total of 25 participants expressed concerns related to the insufficient information provided by the websites. Specifically, 17 participants voiced their mistrust in case they would need to use passkeys with biometrics, 10 were concerned about the storage of passkeys, and two questioned the general simplicity of the system (i.e., a system that is this simple to use cannot be trusted). An additional 7 participants expressed general concerns about the simplicity, though without explicitly labeling it as mistrust. Generally, 18 participants were uncertain about the functionality, further increasing mistrust.

Forced Strategy. Participants in $Group_f$ registered a passkey as part of creating a new KAYAK account, whereas those in $Group_n$ and $Group_p$ registered passkeys for existing accounts. After entering an email address provided for the study, participants selected "Create your account" and completed the Windows Hello prompt. KAYAK provided no website-level explanation before passkey creation or confirmation afterward, despite UX recommendations for informative prompts [29]. This limited feedback may help explain why participants were unsure whether enrollment had succeeded, even though the process was quick. The interviews highlighted three themes.

- ***Lack of Information.*** This group has the highest number of participants who requested more information (10 out of 12), since the website's registration process provides little explanation. For example, *P16* suggested *"An additional view to say: Hey, it worked. That would help."* This also resulted in the greatest concern about user education in the registration process, although the number here is rather low, with three participants. With the same number of mentions, participants in this group felt that missing information hinders the adoption of passkeys. As *P9* said: *"I feel like I'd need to inform myself a bit more about it."*
- ***Security Concerns.*** Eight of twelve participants perceived passkeys as insecure. One potential explanation is that half of the participants in this group perceived the simplicity of the strategy as insecurity and some even expressed mistrust into passkeys as a result. *P29* noted that *"When it's so very straightforward and quick, then it feels more insecure"* and *P34* said that it is *"somehow a bit weird, because I wasn't sure whether something else was coming, whether I still had to confirm something or anything like that."* The participants' understanding of passkeys left them feeling insecure, as a system this simple cannot be safe. Adding to this, some believed that passkeys are only as secure as their device's unlocking mechanism.
- ***Multiple Devices.*** Seven participants in our study, six of which are in this $Group_f$, were concerned about passkey synchronization between devices, either when configuring a new device or in the event of device loss. For example, *P9* asked *"Is it a big problem if I have a new device and want to log in?"* and *P10* noted *"If you change devices, for example, I can imagine that's a bit of a bummer, because then you lose the passkeys and then I wouldn't know how to log in again."* The concerns of *P34* were even rooted in a misunderstanding: *"In the end, I still have to remember three or four different passkeys for four different devices."* These concerns also included that configuring a new device is easier with a password.

PREPRINT

Nudging Strategy. After signing in to an existing eBay account, participants in $Group_n$ saw a prompt titled "Simplify your sign-in." The timing of the prompt followed recommendations to offer passkey enrollment after login [23,55,30]. Selecting "Continue" opened the Windows Hello prompt to create a passkey. Participants who selected "Skip for now" could still register a passkey later through the account's security settings.

- ***Passkeys are Secure.*** Almost all participants in this group (11 out of 12) perceived passkeys as secure, and all believed that the passkey was stored on the device. For instance, *P17* said *"It has to be some kind of secure method, but I don't know how it works."* Furthermore, half of the participants mentioned that passkeys are somehow related to two-factor authentication, as exemplified by *P15*: *"So it is a kind of two-factor authentication."*
- ***Passkeys are Easy to Use.*** All participants in this group described passkeys as easy to use, with most (9 out of 12) stating that passkeys are preferred over other authentication mechanisms. Furthermore, seven participants expressed the desire for broader passkey support on other websites.
- ***Security Concerns and Mistrust.*** Although 11 of 12 participants described passkeys as secure, security-related concerns were also common in this group, occurring in nine interviews. *P27* stated: "*I'm actually not sure how secure the whole thing is. I suppose it's safer than putting my data in there in public.*" This group also showed notable mistrust in biometrics (seven participants).

Passive Strategy. After signing in to Sony, participants in $Group_p$ had to locate "Log in with Passkey" in their account's security settings. Selecting "Edit" opened a dialog explaining passkeys and offering a "Create Passkey" button. This guidance and the confirmation after setup were consistent with UX recommendations [55,30,40]. Across the interviews, we recorded fewer occurrences of qualitative codes in $Group_p$ than in either $Group_f$ or $Group_n$.

- ***Sufficient Information.*** Only 6 out of 12 participants asked for more information about passkeys, which we suspect is due to the nature of the website, as it provides the most information before registering a passkey. However, this group did not mention concerns about user education or the impact of missing information on acceptance. Sony tells users to *"Use a passkey to quickly and securely sign into your account using your fingerprint, face, or other security method."* and provides a "Further Information" link [61] explaining passkeys with the help of videos [3].
- ***Passkeys Feel Secure.*** Participants of this group expressed the strongest sense of perceived security. *P7* stated *"That's a threshold where I feel safe."* In contrast, concerns about passkeys being device-bound or difficult to synchronize were minimal. Seven participants in this group described biometrics as secure.
- ***User Verification.*** Participants in this group demonstrated the clearest understanding of the user verification underlying passkeys. *P19* explained that the PIN is used locally and that *"the website simply asks the PC whether the correct sequence of numbers was entered, without the website itself knowing what the sequence is or which one was entered."* Similarly, *P24* remarked that *"the passkey is, in the end, a confirmation that I'm sitting at the PC."*

PREPRINT

Additional Findings. Next, we highlight further insights.

- ***Passkeys are like Password Managers.*** Almost half the participants compared passkeys to traditional password managers. Their interpretations encompassed several overlapping notions, including the use of device-level authentication (such as unlocking a phone) to authorize access, a perceived local mapping between the passkey, the website, and the associated email account, as well as the idea of a unified credential in the sense of "one passkey to rule them all." *P5* (Force) explained passkeys as *"a password that gives my computer access to multiple passwords."* *P11* (Passive) perceived the task as *"similar to saving passwords in the browser"* and *P26* (Force) saw a similarity *"with my password manager, it works the same way."* *P22* (Passive) explained *"this passkey basically generates—or I think it basically generates—a unique password for the website, which I actually can't even see."* From a user perspective, the functional similarities between password managers and passkeys help to make passkeys familiar and trustworthy [22], especially for those who already perceive password managers as secure and convenient [52,45,50]. However, this analogy highlights a limited understanding of passkeys' unique properties. These keys are inherently passwordless and mitigate issues such as password reuse, database leaks, and weak credentials. Using familiar mental models like password managers may effectively introduce passkeys, helping users understand the system while providing a foundation to clarify the technical differences, particularly regarding the visibility and tangibility of passkeys.
- ***Device Sharing.*** Six participants highlighted a potential limitation of passkeys: they rely on the device's unlock method. This creates a vulnerability in the threat model of these participants because anyone with access to the device, whether by knowing the PIN or obtaining it through shoulder surfing [7,16,8], can authenticate. *P10* (Force) explained, "*it may feel a little more insecure. Especially because you have some kind of device password [...] or Touch ID for several people.*" *P6* (Nudge) added, "*It does not even have to be stolen. It could be your boyfriend, your mother or your father. And then he has access to everything.*" *P24* (Passive) explained that *"even if the PIN were 00000, it would only matter if someone had my device, and then I'd have a problem anyway"* and *"if passkeys really only work by being stored on the device, then they would only be insecure if someone had access to my device."* Device sharing is common in multi-person households around the world [59,2]. While sharing usually involves trusted individuals, it remains a factor to consider, especially given evidence that intimate partner abuse can increase access-related risks [42,13]. With passkeys depending on device unlock methods, anyone with physical access to the device could gain entry to apps and sensitive accounts.
- ***Visibility of Secrets.*** Six participants talked about the visibility of secrets or the lack thereof, which relates to the perceived simplicity of passkeys. Four of these participants complained that not seeing the secret pasted, e.g., a password autofilled by a password manager, feels insecure. In contrast, two participants noted that not seeing the secret increased their sense of security. *P23* (Nudge) replied to "*Is there anything you don't feel so secure with?*" with "*You just can't see a password from A to B in that sense.*" *P12* (Force) stated "*when I see that I had a password before, which is then only released by my passkey, which then allows me to log in, that actually*

PREPRINT

felt secure so far, even safer." This implied that seeing an obscured secret, such as a password obscured with asterisks (∗ ∗ ∗ ∗ ∗), increases security perception, at least for some users [6]. This raises the question of whether awareness and perception can be influenced by *reducing* the perceived simplicity of the system.

– ***Adoption Problems.*** A total of 15 participants mentioned potential adoption hurdles. Nine participants suspect that the authentication habits on the web may hinder adoption. This mainly focuses on the use of known authentication systems, with passwords being the predominant one. Six participants described the effort of learning a new authentication method or switching existing accounts as a barrier to adoption. They mainly spoke about their reluctance to inform themselves about a new system or their unwillingness to switch their many online accounts to it.

Qualitative Analysis Summary

Three main themes shaped users' perceptions of passkeys: security, usability, and mistrust. Participants generally saw passkeys as secure and convenient, but their perceptions differed across the three tested implementations. Participants in the *forced* condition frequently expressed uncertainty alongside concerns about limited explanation and control. *Nudging* made passkeys visible while preserving choice, balancing security perceptions with remaining concerns. Participants in the *passive* condition expressed comparatively clear understanding and trust, although the option may be difficult to discover outside an instructed task.

Mental Models. Each participant was asked to sketch the passkey registration process as they perceived it. We asked them to focus on the interaction between the user and the website. Figure 3 provides an illustrative example of a password-manager analogy observed during the interviews; it is not intended to represent the drawings as a whole. Due to the substantial variation in the level of detail and overall quality of drawings, we refrained from a more systematic categorization.

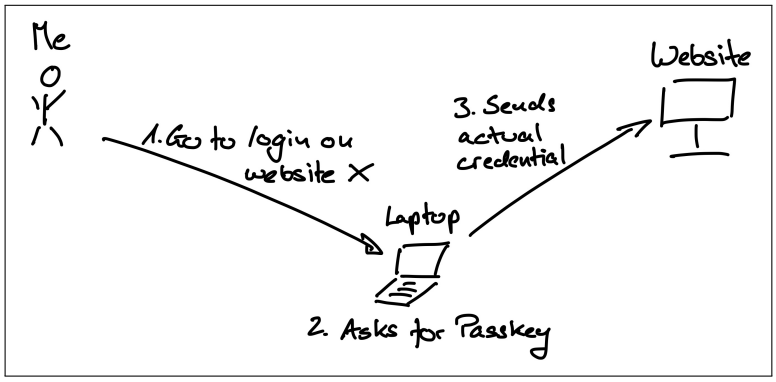


Fig. 3. Drawing of P31 (Nudge): A 3-step login process between user, device, and website is shown. The process resembles using a password manager. (Digitalized)

PREPRINT

The sketch of P31 reflects a relatively linear understanding of the login process. The drawing is organized as a sequence of three steps from the user to the website, passing through their device. The participant sketches the perceived flow: first accessing the login page, followed by a prompt to use the passkey. A key misconception emerges in the third step, where the participant annotates that the computer sends the "actual credentials" to the website. The participant stated in the follow-up questions that the website still uses some kind of password. This implies that the password is transmitted directly to the website as the "actual credential." The drawing nicely captures the participant's awareness of multiple stages of the login process. Their focus on visible interaction steps and the phrasing "actual credentials" suggest a mental model closer to a password-based login with a password manager.

Table 2. Overview of the Quantitative Results.

Data	$Group_f$	$Group_n$	$Group_p$	Overall
Time to Register a Passkey (Seconds)				
Q1 (25%)	58	71.5	171.5	69.3
Q2 (50%; Median)	66.5	105.5	224.0	105.5
Q3 (75%)	76.0	135.75	263.5	199.5
Time to Completion (Seconds)				
Q1 (25%)	90.5	102.8	249.8	107.0
Q2 (50%; Median)	108.5	154.5	286.0	184.0
Q3 (75%)	186.5	184.0	319.0	268.5
Additional Clicks* to Register a Passkey				
Q1 (25%)	0.0	0.8	2.0	0.0
Q2 (50%; Median)	0.0	2.5	4.0	2.0
Q3 (75%)	2.0	6.3	7.8	4.0
Additional Clicks* to Completion				
Q1 (25%)	1.8	1.8	2.0	2.0
Q2 (50%; Median)	3.0	3.5	4.0	4.0
Q3 (75%)	12.0	6.3	7.8	7.5
Help Intensity (Requests and Interventions)				
Q1 (25%)	0.0	0.0	0.0	0.0
Q2 (50%; Median)	0.5	1.0	1.0	1.0
Q3 (75%)	1.0	2.3	1.0	1.0
Completion Confidence (Count)				
Not Realized	3	0	0	3
Uncertain	4	4	1	9
Confident	5	8	11	24
Adoption Willingness (Count)				
No	1	3	1	5
Maybe	6	1	2	9
Yes	5	8	9	22

*Minimum clicks per group: $Group_f$ = 8, $Group_n$ = 10, $Group_p$ = 19.

PREPRINT

4.3 Quantitative Analysis

Next, we present the results of our quantitative analysis. This mainly includes metrics from the tasks, such as time on task and clicks, as well as scaled answers to questions such as the adoption willingness and completion confidence. We report the 25th, 50th (median), and 75th percentiles for numerical data, such as time in seconds, number of clicks, and number of support tasks. For ordinal and categorical data, including completion confidence and adoption willingness, we report frequencies. Table 2 provides an overview of the quantitative data presented in the following. We provide additional plots of the quantitative data in Appendix D.

Time to Register a Passkey. The time to register a passkey was measured from the participant's first click or keyboard input until the Windows Hello confirmation prompt appeared. Table 2 shows that participants in $Group_f$ were faster than the other two groups. However, this does not come as a surprise considering their user journey (see Appendix C) where the very first thing they need to do during account registration is to create a passkey. In contrast, participants of $Group_n$ and $Group_p$ need to first log in and react to the nudge or find the corresponding account settings, respectively.

Time to Completion. The task was considered complete when a participant stated it was complete, asked whether it was complete, or the interviewer told the participant that it was complete. After the passkey was enrolled, the participant was not necessarily aware of completion. Instead, some participants searched for the passkey in the settings or experimented with it, which is reflected in a higher time to completion and additional clicks, as explained below. Moreover, participants in $Group_f$ were unaware of their task completion and tried to enroll another passkey. This is reflected in the comparatively high time to completion relative to their time to passkey registration and is particularly evident in their completion confidence reported in Table 2. This variance for $Group_f$ is also apparent in the frequency distributions in Figure 10 and the KDE and CDF plots in Figure 11 in Appendix D.

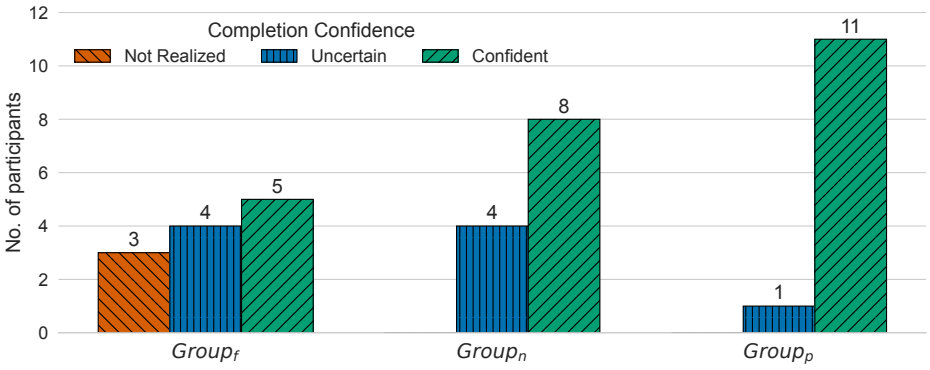


Fig. 4. Completion Confidence: Number of participants in each enrollment group who were confident they had completed the task, were unsure, or did not realize they had completed it.

PREPRINT

Completion Confidence. Figure 4 shows that $Group_p$ had the most confident participants, with 11 of 12 believing they completed the task. Only one participant was uncertain about the completion. In $Group_n$, eight participants were confident, and the remaining four were uncertain. $Group_f$ was the only group in which participants did not realize they had completed the task and insisted on continuing. This was the case for three participants. Four more participants were unsure about task completion, and only five others were confident about it.

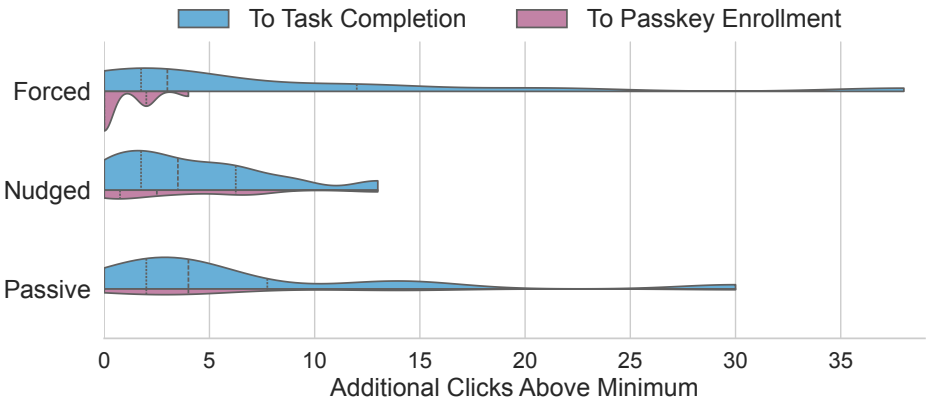


Fig. 5. Additional Clicks: Distribution of clicks beyond the minimum required to register a passkey in each group, measured at registration and again at task completion.

Additional Clicks. Generally, the three chosen websites follow different user journeys and thus require different numbers of interactions (see Appendix C). To account for this, we derived the minimum number of clicks required to register a passkey from the different user journeys. For $Group_f$ the minimum was 8, for $Group_n$ it was 10 and for $Group_p$ it was 19. We subtract this number from the observed number of clicks to compute the "superfluous" clicks by participants. Figure 5 shows the distribution of user interface interactions (measured as clicks) per group to register a passkey and until task completion. The data aligns with the observed time to *passkey registration* and *task completion*, where most participants in $Group_f$ only needed a minimum number of clicks to register their passkey but spent additional time interacting with the website. For participants in $Group_n$ and $Group_p$, the additional clicks for passkey registration and completion align closely, indicating that participants generally did not interact much more with the website after registration.

Help Intensity. To assess the intensity of help, we measured how often participants asked questions on how to proceed with the practical task or how often the interviewer had to intervene. Although the help intensity between groups was relatively close, participants in $Group_n$ required slightly more help interventions, suggesting either greater difficulty in completing the task or a higher tendency to seek guidance.

PREPRINT

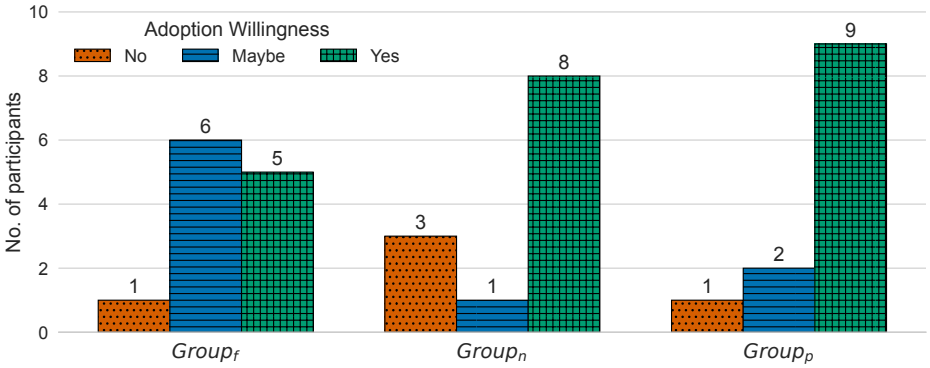


Fig. 6. Adoption Willingness: Responses to the question "Are you interested in continuing to use passkeys?" by enrollment strategy. Responses were classified as yes, maybe, or no.

Adoption Willingness. Figure 6 illustrates participants' self-reported willingness to adopt passkeys across the three strategies (see also Table 2). We categorized the data into three responses based on the interviewer's perception: **Yes**, **Maybe**, and **No**. $Group_f$ had the highest number of uncertain participants and the lowest overall willingness to adopt. In contrast, $Group_p$ demonstrated the strongest adoption tendency, with nine participants expressing willingness to adopt, two remaining uncertain, and one unwilling to adopt. In $Group_n$, eight participants were willing to adopt passkeys, one was uncertain, and three were unwilling.

Nudging Success Rate. For $Group_n$, we additionally measured the success rate of the nudging prompt (not reported in Table 2). The prompt was considered successful if participants selected *Continue* when encountering the prompt after logging in. 10 of 12 participants chose to do so, yielding an observed prompt success rate of 83.3%.

> **Quantitative Analysis Summary**
>
> Forced enrollment was associated with the fastest passkey registrations, but also the greatest confusion, the lowest completion confidence, and the weakest adoption willingness. Nudging and passive enrollment required more time and interaction, yet participants in both conditions expressed greater willingness to adopt passkeys. Passive enrollment yielded the highest completion confidence and perceived clarity, while nudging provided a stronger balance between visibility, usability, and user autonomy.

5 Discussion

Next, we discuss what our results suggest about how enrollment strategies shape users' understanding and acceptance of passkeys. We then interpret participants' views, consider implications for automatic passkey upgrades, and outline the study's limitations.

PREPRINT

5.1 Research Question

Passive Enrollment: Confidence and Effort. Participants in $Group_p$ showed relatively high confidence in task completion and a higher degree of understanding of passkeys. Similarly, these participants expressed the highest willingness to continue using passkeys. However, the variability in task completion times and higher click counts indicate greater interaction effort in this condition.

Nudged Enrollment: Visibility and Choice. Self-reported adoption willingness among $Group_n$ participants was high, at 67%. As explained in Section 4.2, participants' sense of security and perception of the system's usability contributed to increased confidence, which likely fostered acceptance of the system. The success of the nudging prompt (83%) further supports the idea that lightweight guidance can effectively encourage them to engage with passkeys without overwhelming them. This group seemed to trust passkeys, though their lack of understanding still caused some concerns about security. We suspect this stems from the relatively low level of information combined with the guided enrollment process, which fosters trust but requires little independent exploration of settings and thus limits deeper engagement. This aligns with Reittinger et al. [57], who show that nudges are effective for increasing passkey adoption. Our findings add that the design of such nudges also matters for users' interpretation of passkeys. In particular, nudges should not only make passkeys visible, but also preserve users' sense of choice and provide enough context to support trust and understanding. This positions nudging as a promising middle ground between passive availability, which may not scale, and forced enrollment, which may reduce perceived autonomy.

Forced Enrollment: Speed and Uncertainty. $Group_f$ showed the lowest willingness to adopt with 42%. Despite having the shortest time to completion, this group also showed the highest confusion with the widest spread in click variance, in particular after passkey registration, and the highest uncertainty about task completion. Participants in this condition also expressed lower initial willingness to adopt passkeys than those in the other two conditions. Our data does not indicate whether the lack of control or the lack of information causes this effect, but we suspect both. In 2023, Kayak reported that their integration of passkeys cut the average account registration and login time in half [60]. But it has to be kept in mind that users generally respond badly to being forced onto a new technology [65] and that previous work has shown that passwordless technology is more approachable for mobile users [48]. This raises the question of how many of these users retain passkeys in the mid-term.

Takeaway. Our data suggests that autonomy and control may contribute to acceptance. While a fully passive, unguided approach may promote understanding and trust through active engagement, strategic nudging appears to be a more scalable and user-friendly tradeoff. This is especially true *in the wild*, where most users will not adopt passkeys unless made aware of their existence. In contrast, forcing the enrollment process may reduce user effort but also hinder perceived transparency, autonomy, and trust. Our participants indicated that this led to a lower willingness to adopt. Unfortunately, we lack the data to comment on the mid-term passkey retention among these users. Taken together, our findings support nudging as a practical strategy that combines visibility, ease of use, and user choice.

PREPRINT

5.2 Participant Perceptions

Lack of Information. Participants often felt inadequately informed about passkeys, which is understandable given that 2 out of 3 websites offered little explanation beyond the use of biometrics. This lack of information can create mistrust or limit understanding, reducing acceptance [68,52,37]. Another factor is their perceived simplicity. Without deeper knowledge, some viewed the system as *too easy to be secure* [6]. Although only a quarter of our participants explicitly mentioned this, it may be reasonable to assume that the problem affected other participants who expressed mistrust. We recommend providing additional information about passkeys without overwhelming users and, at least during the current rollout of this new technology, contributing to educating users to foster self-driven adoption. Nudging users to passkeys might only be effective in its simplicity, as the chosen text for a nudging prompt should conform to current UX recommendations [37,55] by keeping it short. Thus, nudging can only be the entry point to education.

Secondary Task. This raises the broader question of how to effectively nudge users. Users generally prefer authentication to be fast and unobtrusive, enabling them to achieve their desired outcome quickly [55]. This creates a challenge, as not all users appreciate being forced or nudged to use a specific method [65], particularly immediately after the login. Alternative nudging opportunities exist, such as sending emails about the availability of passkeys and their benefits, suggesting them during account creation instead of a password, or prompting the user while they are modifying their account authentication settings [30]. Careful nudging can balance visibility and user autonomy [55,57], addressing the discovery barrier described by *P18* (Passive): "*I would probably wait until someone offers it to me. Simply because I don't really feel like searching for it.*"

5.3 Upgrades via Conditional Create

Where supported by the browser and credential provider, WebAuthn's Conditional Create [24] enables automatic passkey upgrades for existing accounts, reducing enrollment friction. Our findings distinguish successful passkey creation from awareness of completion. Although we did not evaluate Conditional Create, this distinction raises questions about whether users notice and understand automatic enrollment. Brief feedback could explain that a passkey was created, how to use it, and where to manage it. Future work should assess whether such feedback supports understanding without disrupting users' primary tasks, and examine its effects on perceived control and continued passkey use.

5.4 Limitations

Validity. The laboratory setting provided a consistent device and study procedure across conditions, reducing variation attributable to the testing environment. *Ecological validity*, however, was limited: participants used an unfamiliar device in a supervised environment, removing factors such as trust in hardware or real-world login habits. Moreover, the study is biased toward young, educated individuals, with most participants aged 25-34

PREPRINT

and highly educated. With 36 participants and 12 per condition, our exploratory findings do not establish population-level differences. Imbalances in educational and computer science backgrounds may also have influenced the results. The introductory explanation and awareness of the study's focus may have influenced participants' understanding and responses.

Websites. Using real-world websites introduced some bias. Two websites, *sony.com* and *ebay.com*, are well known, providing a sense of familiarity. When asked, none of the participants voiced any dislikes for the websites or companies providing them. In contrast, *kayak.com* was less known to the participants. We selected it because, at the time of study design, its account-creation flow provided an example of mandatory passkey enrollment. Additionally, only the forced group was required to create a new account. Thus, unlike the other two groups, we did not provide participants with a password. Each strategy was represented by a different website, with differences in explanations, feedback, and task requirements. We therefore cannot isolate the effects of enrollment strategy from these implementation differences, particularly mandatory enrollment from the amount of information provided. Our findings describe the flows encountered in December 2024 and may not reflect subsequent implementations.

Device and Operating System. The scope of this study was limited to a laptop running Windows 11, with a PIN for Windows Hello instead of biometric verification. This choice was made because Windows represents the most widely deployed desktop OS [63], and PIN-based local authentication constitutes the default non-biometric credential in Windows Hello [47]. We intentionally avoided biometrics due to well-documented concerns regarding their sensor reliability and privacy concerns as noted in prior research [68]. Different devices and configurations may yield different results, with mobile platforms in particular demonstrating greater acceptance of passwordless authentication [48].

6 Conclusion

Our work explores how forced, nudging, and passive enrollment affect users' understanding, perceptions, and initial willingness to adopt passkeys. To this end, we conducted a mixed-method study with 36 participants. Our findings show that users generally perceived passkeys as secure and convenient, and expressed a willingness to adopt. However, the differences among the three enrollment strategies were noticeable, and service providers need to make an informed choice about how they roll out passkeys. Our analysis underscores the importance of aligning enrollment flows with user autonomy and system transparency. Autonomy emerged as a possible factor influencing trust and initial acceptance. Users responded more positively when they retained the freedom to choose whether and how to engage with passkeys. Alongside autonomy, structured, well-timed guidance, such as nudging, may support comprehension and foster trust. This strategy also aligns with best practices recommended by industry [55].

Our findings also underline the need for clear and accessible explanations. Participants frequently noted a lack of information, particularly about security. These gaps not only led to misunderstandings but also hindered trust. Passkey implementations should integrate brief, well-placed explanations or visual cues, avoiding overwhelming users

PREPRINT

while providing enough clarity and confidence to support informed decision-making. Extending our exploratory results presents challenges that warrant further investigation. We consider it valuable to study different strategies for nudging users towards passkeys and their effects on acceptance and adoption, as well as different ways to educate users along their journey to reduce misconceptions and increase trust. Future studies should compare adoption across operating systems (e.g., Windows, macOS, Android, iOS), as platform-specific designs, such as biometric prompts, credential storage, and UI flows, may influence usability, trust, and ultimately adoption willingness. Recent field studies have examined passkey adoption and continued use [57,58]. Building on this evidence, future work should investigate how different enrollment experiences relate to subsequent understanding, retention, and account recovery on users' own devices. Future research should also refine user interface and user experience design, building on existing recommendations for nudging and on prior lessons from 2FA adoption. Subtle design interventions, such as visual confirmations or brief notifications that make otherwise "invisible" processes visible, could strengthen mental models, enhance perceptions of security, and address discomfort due to the lack of visible secrets.

Acknowledgments. This work is based on the first author's master's thesis at Saarland University. We thank Paul Frerichs for his contribution to our data analysis, Divyanshu Bhardwaj for his feedback and proofreading, and the participants for sharing their thoughts and experiences.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

PREPRINT

A Interview Guide

Table 3. Interview guideline for the semi-structured interview (Part 1).

Part	Section	Questions and Explanation
1	**Introduction and Agenda**	This study is about passkeys, a passwordless alternative for logging into user accounts, whether in applications or on websites. With a passkey, instead of using a password, you log in using a PIN or a simple method like fingerprint or facial recognition. This login method is only used on your own device, such as a laptop, tablet, or smartphone, which then logs you in automatically. The web service therefore no longer needs your password to log in and no longer saves it. This study aims to explore the adoption and acceptance of passkeys. Hence, there are no wrong answers, we are merely interested in your experiences and opinions and want to see how it functions with the help of a short practical section. In the practical part, you'll activate passwordless login for the provided study account. Afterwards, I will ask a few questions about your experience, and we will ask you to sketch the process of the practical task to get an idea of your technical understanding. Again, there are no right or wrong answers, our goal is simply to understand how the system is perceived. An audio recording of the interview will be made to help us better analyze the responses. During the practical part, your screen will be recorded to identify any potential issues. All other personal data, such as your name and email address, will only be stored to facilitate participation and to document your consent. This data will be deleted after the study has concluded. The transcribed interview, screen recording, and sketch may be stored in anonymized form for up to 10 years. Do you consent to recording this interview?
2	**Informed Consent**	*Written and orally.*
3	**Passkey Awareness Questions**	1. How do you unlock your phone? Follow-up: Do you use this unlocking method for apps or accounts on your device as well? 2. How do you unlock your computer? Follow-up: Do you use this unlocking method for apps or accounts on your device as well? 3. Is there an application or website where you log in using a password alternative? Follow-up: Why/Why not? 4. How often do you use this login? Follow-up: How does it feel in daily use? 5. Have you heard of FIDO2 or passkeys? Follow-up:Where or from whom? *Help ease participants into the interview with some simple questions.*
4	**Practical Part**	Now let's start the practical part of this interview. Your task will be to register/login to a website using a study email account provided by me and set up a passkey. I have already prepared an email address for you, so that you don't have to share any of your personal data with us. Please imagine that you are logging into this website with your own account. To enable the creation of the passkey you will need to enter the PIN specified on the handout. We are only using a PIN in the study to avoid your biometric data being stored on this study computer. You can do the same on your own device using biometrics instead of a PIN. Please proceed to the following website and follow the instructions as described. If you encounter any issues or get stuck, I will be happy to answer your questions.
5	**Post-Task Questions**	1. Have you ever had a similar experience with passwordless login? 2. Did you have any problems with the website we used? 3. What did you like or dislike about passkeys? Follow-up: What did you especially like? Follow-up: What did you especially dislike? 4. In your own words, what exactly do you think a passkey is?
...	...	...

PREPRINT

Table 4. Interview guideline for the semi-structured interview (Part 2).

Part	Section	Questions and Explanation
6	**Mental Model**	Next, I would ask you to make a sketch. Your task is to sketch what happens when you register a passkey, just as you did just now. Nothing you sketch can be wrong; we just want to understand how the system is perceived. Please focus on what happened between you and the website. Paper and pens are provided. You may start to sketch as soon as you are ready. Mental Model Follow-up Questions: 1. Where do you think the passkey is stored? 2. What is stored on your device? 3. Which of your data are stored on the website? 4. Do you feel secure with this login method?
7	**Concluding Questions**	We are almost finished; just a few final questions regarding your opinion. Are you interested in continuing to use passkeys? Follow-up: Why? Would you like to see more passkeys available on other websites? Follow-up: Why? In your opinion, what will be the biggest problem for passkeys in the future? Follow-up: Why? Do you have any final questions?
8	**Demographic Questionnaire**	Age Gender Education Technical Experience
9	**Compensation**	*The participant was compensated for their time.*

PREPRINT

B Codebook

Table 5: Codebook

Code	Description	Force	Nudge	Passive	Total
Acceptance Problems					
more_info_needed	The user stated the need for more information or complained about lack of information.	10	9	6	25
insecurity	The user is insecure about some passkey functionality.	4	9	5	18
mistrust_biometrics	The user stated mistrust in biometrics.	5	7	5	17
mistrust	The user stated general mistrust.	5	5	6	16
concern_simplicity	The user stated concern that the simplicity of the system was perceived insecure.	6	0	1	7
mistrust_device_unlock	The user stated mistrust regarding the usage of the device unlock method for user verification.	3	2	1	6
concern_user_education	The user stated concerns about the missing user education, when using passkeys.	3	1	0	4
missing_info_hinders_ acceptance	The user stated that the lack of information hinders the acceptance of passkeys.	3	1	0	4
Adoption					
memorability	The user positively mentions that no memorability is needed or negatively mentions the memorability of passwords.	6	7	8	21
more_passkeys	The user stated a desire for passkey availability on websites.	5	7	4	16
no_visibility_bad	The user stated that not seeing the secret entered (e.g., pasting the password via the password manager) feels insecure.	3	1	0	4
no_visibility_good	The user stated that not seeing the secret entered (e.g., pasting the password via the password manager) feels secure.	0	1	1	2
Adoption Problems					
habit_hinders_adoption	The user stated that users' authentication habits hinder the adoption of passkeys.	5	3	1	9

Continued on next page

PREPRINT

Code	Description	Force	Nudge	Passive	Total
concern_multiple_devices	The user stated concern about passkey usage on multiple devices (e.g., synchronization, multiple registrations or passkey reuse).	6	1	0	7
missing_info_hinders_adoption	The user stated that the lack of information hinders the adoption of passkeys.	3	1	3	7
mistrust_os	The user stated mistrust regarding the operating system (Windows, Apple, Android).	3	0	3	6
laziness_hinders_adoption	The user stated that laziness hinders the adoption of passkeys (e.g., configuration of a new authentication method).	2	2	2	6
mistrust_websites	The user stated mistrust of the websites or third-party providers (e.g., data collection).	3	0	2	5
mult_auth_system_hinder_ adoption	The user stated that the usage of multiple authentication systems (e.g., passkeys, passwords, etc.) hinders adoption.	3	1	0	4
concern_device_loss	The user stated concerns about the recoverability in case of device loss.	2	0	2	4
concern_company	The user stated concerns about the adoption of passkeys in companies (e.g., implementation, availability, remote access to servers).	2	1	1	4
mistrust_simplicity	The user stated mistrust and the feeling of insecurity regarding the perceived simplicity of passkeys.	2	0	0	2
Passkey Comparison					
passkey_equal_pwmanager	The user compared passkeys to password managers.	6	6	5	17
passkey_equal_2FA	The user compared passkeys to second factor authentication.	1	6	3	10
passkey_equal_device_unlock	The user compared passkeys to device unlock methods.	3	0	0	3
passkey_equal_user_verification	The user compared passkeys to user verification.	0	0	3	3
passkey_preferred	The user stated a preference for passkeys (e.g. “passkeys are better than passwords”).	6	9	7	22

Continued on next page

PREPRINT

Code	Description	Force	Nudge	Passive	Total
Passkey Perception					
passkey_stored_on_device	The user perceived that passkeys are stored on the device.	11	12	9	32
passkey_ease_of_use	The user perceived passkeys as easy to use.	9	12	7	28
user_verification	The user perceived user verification.	5	4	8	17
passkey_good	The user perceived passkeys as positive (e.g., convenient, interesting, necessary).	4	3	8	15
passkey_fast	The user perceived passkeys as fast.	4	4	3	11
passkey_device_bound	The user perceived the passkey as device bound.	3	1	2	6
Security Perception					
passkey_secure	The user perceived passkeys as secure.	9	11	8	28
concern_security	The user stated concern about the perceived security of passkeys.	5	9	5	19
biometrics_secure	The user perceives biometrics as secure.	3	5	7	15
passkey_insecure	The user perceived the passkeys as insecure.	8	4	1	13
challenge_response	The user suspected or knew about the underlying challenge response concept.	4	4	2	10
concern_storage	The user stated concern about the storage of “passkey components” (e.g. keys, biometrics, passwords).	3	4	3	10

PREPRINT

C Task Flows

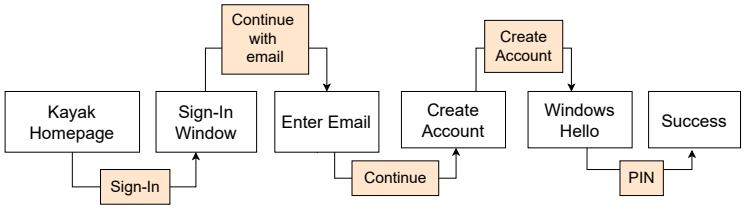


Fig. 7. Passkey registration flow for the *Force* group ($Group_f$) on kayak.com. Orange boxes on the arrows mark the main steps.

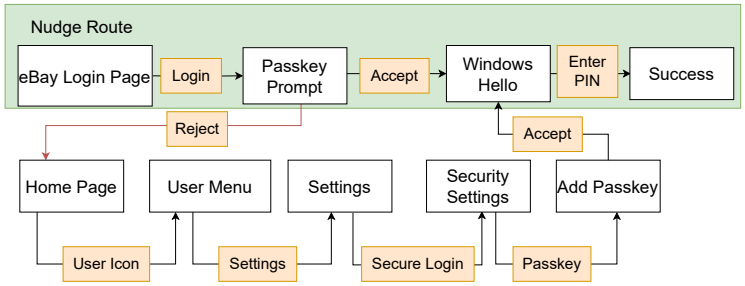


Fig. 8. Passkey registration flow for the *Nudge* group ($Group_n$) on ebay.com. Orange boxes on the arrows mark the main steps. The green long box at the top highlights the path for participants who accept the prompt, and *reject* marks the alternative.

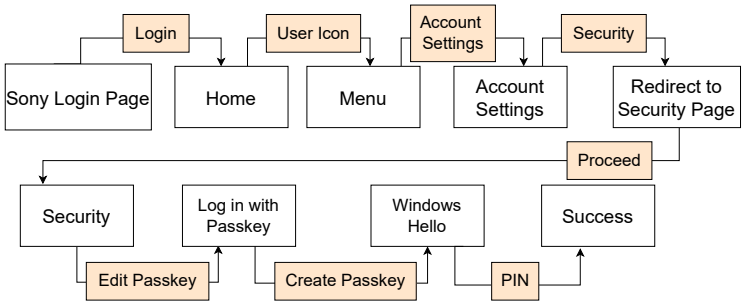


Fig. 9. Passkey registration flow for the *Passive* group ($Group_p$) on sony.com. Orange boxes on the arrows mark the main steps.

PREPRINT

D Quantitative Data

Figures 10 and 11 offer further depictions of the times to register a passkey and to complete the task as presented in Table 2. Foremost, the data indicate that while $Group_f$ very quickly finishes the passkey registration, the overall time on the task does not differ much from the time of $Group_n$, indicating that participants in this group spent additional time on the task after passkey registration. $Group_p$ required the most time for task completion and passkey registration; however, both times are close to each other, indicating that the participants considered the task completed when the passkey was registered. The same observation holds for $Group_n$; however, the participants were faster than $Group_p$ for passkey registration and task completion.



Fig. 10. Distribution of the times to complete the task and to register the passkey by group.

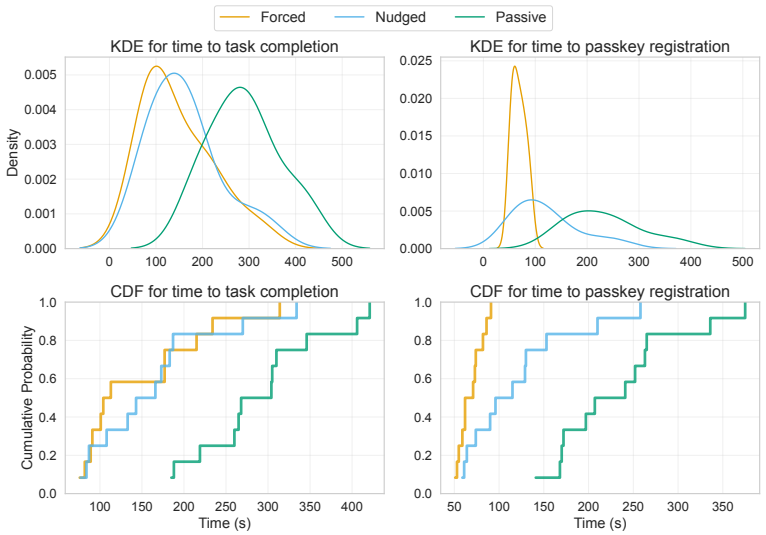


Fig. 11. The Kernel Density Estimation (KDE) and empirical Cumulative Distribution Function (CDF) of the times to task completion and to register a passkey by group.

PREPRINT

References

1. AgileBits, Inc.: Passkeys.Directory: A Community-Driven Index of Passkey-Enabled Websites (Nov 2022), https://passkeys.directory, as of November 19, 2026
2. Alam, A., Stobert, E., Biddle, R.: "This Is Different from the Western World": Understanding Password Sharing Among Young Bangladeshis. In: Workshop on Usable Security and Privacy. USEC '23, ISOC, San Diego, California, USA (Feb 2023). https://doi.org/10.14722/usec.2023.237848
3. Amer, Y., Haque, E.U., Rong, Z., Hasan Khan, M.M.: Understandability of the Technology and Benefit May Not Be Enough to Nudge Users: An Exploratory Study in the Context of FIDO2 Adoption Behavior. In: IEEE Annual Computers, Software, and Applications Conference. pp. 607–618. COMPSAC '25, IEEE, Toronto, Ontario, Canada (Jul 2025). https://doi.org/10.1109/compsac65507.2025.00083
4. Aonzo, S., Merlo, A., Tavella, G., Fratantonio, Y.: Phishing Attacks on Modern Android. In: ACM Conference on Computer and Communications Security. pp. 1788–1801. CCS '18, ACM, Toronto, Ontario, Canada (Oct 2018). https://doi.org/10.1145/3243734.3243778
5. Arora, N., Athwani, V.: Android Developer Blog: Best Practices for Migrating Users to Passkeys with Credential Manager (Sep 2025), https://android-developers.googleblog.com/2025/09/best-practices-migrating-users-passkeys-credential-manager.html, as of November 19, 2026
6. Atwater, E., Bocovich, C., Hengartner, U., Lank, E., Goldberg, I.: Leading Johnny to Water: Designing for Usability and Trust. In: Symposium on Usable Privacy and Security. pp. 69–88. SOUPS '15, USENIX, Ottawa, Canada (Jul 2015)
7. Aviv, A.J., Davin, J.T., Wolf, F., Kuber, R.: Towards Baselines for Shoulder Surfing on Mobile Authentication. In: Annual Conference on Computer Security Applications. pp. 486–498. ACSAC '17, ACM, Orlando, Florida, USA (Dec 2017). https://doi.org/10.1145/3134600.3134609
8. Bhardwaj, D., Hashmi, S.I., Krombholz, K., Golla, M.: Understanding How Users Prepare for and React to Smartphone Theft. In: USENIX Security Symposium. pp. 5987–6005. SSYM '25, USENIX, Seattle, Washington, USA (Aug 2025)
9. Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: IEEE Symposium on Security and Privacy. pp. 553–567. SP '12, IEEE, San Jose, California, USA (May 2012). https://doi.org/10.1109/SP.2012.44
10. Braun, V., Clarke, V.: Thematic Analysis: A Practical Guide. SAGE Publications, Los Angeles, California, USA, 1 edn. (2021)
11. Bruin, J.: MacWhisper: Whisper (Large v3) (Jan 2023), https://goodsnooze.gumroad.com/l/macwhisper, as of November 19, 2026
12. Cappalli, T., Kumar, A., Lundberg, E., Miller, M., Pascoe, Satragno, N.: Web Authentication: An API for Accessing Public Key Credentials – Level 3 (Aug 2026), https://www.w3.org/TR/2026/REC-webauthn-3-20260825/, as of November 19, 2026
13. Daffalla, A., Bhattacharya, A., Wilder, J., Chatterjee, R., Dell, N., Bellini, R., Ristenpart, T.: A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models. In: USENIX Security Symposium. pp. 7819–7838. SSYM '25, USENIX, Seattle, Washington, USA (Aug 2025)
14. Daffalla, A., Myers, G., Bellini, R., Ristenpart, T., Dell, N.: "Maybe there's only one passkey?": Challenges Investigating and Remediating Adversarial Passkeys. In: USENIX Security Symposium. pp. 5413–5432. SSYM '26, USENIX, Baltimore, Maryland, USA (Aug 2026)

PREPRINT

15. Dhamija, R., Tygar, J.D., Hearst, M.: Why Phishing Works. In: ACM Conference on Human Factors in Computing Systems. pp. 581–590. CHI '06, ACM, Montreal, Quebec, Canada (Apr 2006). https://doi.org/10.1145/1124772.1124861
16. Eiband, M., Khamis, M., von Zezschwitz, E., Hussmann, H., Alt, F.: Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In: ACM Conference on Human Factors in Computing Systems. pp. 4254–4265. CHI '17, ACM, Denver, Colorado, USA (May 2017). https://doi.org/10.1145/3025453.3025636
17. Farke, F.M., Lassak, L., Pinter, J., Dürmuth, M.: Exploring User Authentication with Windows Hello in a Small Business Environment. In: Symposium on Usable Privacy and Security. pp. 523–540. SOUPS '22, USENIX, Boston, Massachusetts, USA (Aug 2022)
18. FIDO Alliance: FIDO Alliance: The FIDO Story (Dec 2020), https://fidoalliance.org/fido-alliance-the-fido-story/, as of November 19, 2026
19. FIDO Alliance: Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins (May 2022), https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/, as of November 19, 2026
20. FIDO Alliance: FIDO Alliance: Passkeys (Nov 2024), https://fidoalliance.org/passkeys/, as of November 19, 2026
21. FIDO Alliance: FIDO Alliance: Case Studies (Jul 2026), https://fidoalliance.org/content/case-study/, as of November 19, 2026
22. FIDO Alliance: Passkey Central: Design User Journeys (Jul 2026), https://www.passkeycentral.org/design-user-journeys, as of November 19, 2026
23. FIDO Alliance: Passkey Central: Passkey Roll-Out Guides (Jul 2026), https://www.passkeycentral.org/plan-your-rollout, as of November 19, 2026
24. FIDO Alliance: The Frictionless Upgrade: Conditional Create (Jan 2026), https://www.passkeycentral.org/news-and-events/passkey-upgrades-and-improvements, as of November 19, 2026
25. Giacomello, A., Lassak, L., Hielscher, J., Golla, M.: Exploring the Complexities of Passkey Revocation. In: ACM Conference on Computer and Communications Security. pp. 5016–5030. CCS '26, ACM, The Hague, Netherlands (Nov 2026). https://doi.org/10.1145/3830454.3846647
26. Golla, M., Dürmuth, M.: Analyzing 4 Million Real-World Personal Knowledge Questions (Short Paper). In: International Conference on Passwords. pp. 39–44. PASSWORDS '15, Springer, Cambridge, United Kingdom (Dec 2015). https://doi.org/10.1007/978-3-319-29938-9_3
27. Golla, M., Ho, G., Lohmus, M., Pulluri, M., Redmiles, E.M.: Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In: USENIX Security Symposium. pp. 109–126. SSYM '21, USENIX, Virtual Conference (Aug 2021)
28. Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E., Ur, B.: "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In: ACM Conference on Computer and Communications Security. pp. 1549–1566. CCS '18, ACM, Toronto, Ontario, Canada (Oct 2018). https://doi.org/10.1145/3243734.3243767
29. Google, Inc.: Google Developer Guidelines: Passkeys User Interface Design (Sep 2025), https://developers.google.com/identity/passkeys/ux/user-interface-design, as of November 19, 2026
30. Google, Inc.: Google Developer Guidelines: Passkeys User Journeys (Sep 2025), https://developers.google.com/identity/passkeys/ux/user-journeys, as of November 19, 2026
31. Hogan, T.: Save and Sign in with Passkeys Using 1Password in the Browser (Jun 2023), https://blog.1password.com/save-sign-in-passkeys-1password/, as of November 19, 2026

PREPRINT

32. Jannett, L., Mayer, A., Westers, M., Mladenov, V., Mainka, C., Schwenk, J.: The State of Passkeys: Studying the Adoption and Security of Passkeys on the Web. In: USENIX Security Symposium. pp. 5039–5058. SSYM '26, USENIX, Baltimore, Maryland, USA (Aug 2026)
33. Karunakaran, S., Thomas, K., Bursztein, E., Comanescu, O.: Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. In: Symposium on Usable Privacy and Security. pp. 217–234. SOUPS '18, USENIX, Baltimore, Maryland, USA (Aug 2018)
34. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., von Zezschwitz, E.: "If HTTPS Were Secure, I Wouldn't Need 2FA" – End User and Administrator Mental Models of HTTPS. In: IEEE Symposium on Security and Privacy. pp. 246–263. SP '19, IEEE, San Francisco, California, USA (May 2019). https://doi.org/10.1109/SP.2019.00060
35. Kupris, E., Schreck, T.: The Passkey Promise: A Comparative Usability Study of MFA Methods. In: IEEE Symposium on Security and Privacy. pp. 3647–3666. SP '26, IEEE, San Francisco, California, USA (May 2026). https://doi.org/10.1109/SP63933.2026.00055
36. Lain, D., Kostiainen, K., Capkun, S.: Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In: IEEE Symposium on Security and Privacy. pp. 842–859. SP '22, IEEE, San Francisco, California, USA (May 2022). https://doi.org/10.1109/SP46214.2022.9833766
37. Lassak, L., Hildebrandt, A., Golla, M., Ur, B.: "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In: USENIX Security Symposium. pp. 91–108. SSYM '21, USENIX, Virtual Conference (Aug 2021)
38. Lassak, L., Markert, P., Golla, M., Stobert, E., Dürmuth, M.: A Comparative Long-Term Study of Fallback Authentication Schemes. In: ACM Conference on Human Factors in Computing Systems. pp. 970:1–970:19. CHI '24, ACM, Maui, Hawaii, USA (May 2024). https://doi.org/10.1145/3613904.3642889
39. Lassak, L., Pan, E., Ur, B., Golla, M.: Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In: USENIX Security Symposium. pp. 7231–7248. SSYM '24, USENIX, Philadelphia, Pennsylvania, USA (Aug 2024)
40. Lyastani, S.G., Backes, M., Bugiel, S.: A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites. In: Symposium on Network and Distributed System Security. NDSS '23, ISOC, San Diego, California, USA (Feb 2023). https://doi.org/10.14722/ndss.2023.23362
41. Lyastani, S.G., Schilling, M., Neumayr, M., Backes, M., Bugiel, S.: Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In: IEEE Symposium on Security and Privacy. pp. 268–285. SP '20, IEEE, Virtual Conference (May 2020). https://doi.org/10.1109/SP40000.2020.00047
42. Maftei, A., Dănilă, O.: Give Me Your Password! What Are You Hiding? Associated Factors of Intimate Partner Violence Through Technological Abuse. Current Psychology **42**(2023), 8781–8797 (Aug 2021). https://doi.org/10.1007/s12144-021-02197-2
43. Markert, P., Golla, M., Stobert, E., Dürmuth, M.: A Comparative Long-Term Study of Fallback Authentication (Work in Progress). In: Workshop on Usable Security and Privacy. USEC '19, ISOC, San Diego, California, USA (Feb 2019). https://doi.org/10.14722/usec.2019.23030
44. Matzen, A., Rüffer, A., Byllemos, M., Heine, O., Papaioannou, M., Choudhary, G., Dragoni, N.: Challenges and Potential Improvements for Passkey Adoption – A Literature Review with a User-Centric Perspective. Applied Sciences **15**(8), 4414:1–4414:34 (Apr 2025). https://doi.org/10.3390/app15084414
45. Mayer, P., Munyendo, C.W., Mazurek, M.L., Aviv, A.J.: Why Users (Don't) Use Password Managers at a Large Educational Institution. In: USENIX Security Symposium. pp. 1849–1866. SSYM '22, USENIX, Boston, Massachusetts, USA (Aug 2022)

PREPRINT

46. Mayer, P., Zou, Y., Schaub, F., Aviv, A.J.: "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In: USENIX Security Symposium. pp. 393–410. SSYM '21, USENIX, Virtual Conference (Aug 2021)
47. Microsoft, Corporation: Windows Hello: Can I Disable the PIN? (Jun 2026), https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/faq, as of November 19, 2026
48. Nawrath, F.: Quantitative Analysis of FIDO2 Client Support. In: Who Are You?! Adventures in Authentication Workshop. pp. 1–5. WAY '21, WAY, Virtual Conference (Aug 2021)
49. Nisenoff, A., Golla, M., Wei, M., Hainline, J., Szymanek, H., Braun, A., Hildebrandt, A., Christensen, B., Langenberg, D., Ur, B.: A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In: USENIX Security Symposium. pp. 5127–5144. SSYM '23, USENIX, Anaheim, California, USA (Aug 2023)
50. Oesch, S., Ruoti, S., Simmons, J., Gautam, A.: "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In: ACM Conference on Human Factors in Computing Systems. pp. 33:1–33:23. CHI '22, ACM, New Orleans, Louisiana, USA (Apr 2022). https://doi.org/10.1145/3491102.3517534
51. Pearman, S., Thomas, J., Naeini, P.E., Habib, H., Bauer, L., Christin, N., Cranor, L.F., Egelman, S., Forget, A.: Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In: ACM Conference on Computer and Communications Security. pp. 295–310. CCS '17, ACM, Dallas, Texas, USA (Oct 2017). https://doi.org/10.1145/3133956.3133973
52. Pearman, S., Zhang, S.A., Bauer, L., Christin, N., Cranor, L.F.: Why People (Don't) Use Password Managers Effectively. In: Symposium on Usable Privacy and Security. pp. 319–338. SOUPS '19, USENIX, Santa Clara, California, USA (Aug 2019)
53. Porter, J.: Bitwarden Begins Adding Passkey Support to Its Password Manager (Nov 2023), https://www.theverge.com/2023/11/2/23943173/, as of November 19, 2026
54. Ramat, B., Kartchner, D., Clark, M., Seamons, K.: Passkeys in the Wild: A Systematic Study of FIDO2 User Experience Consistency Across Websites. In: Symposium on Usable Privacy and Security. pp. 21–39. SOUPS '26, USENIX, Hannover, Germany (Aug 2026)
55. Ranjit, S., Bingham, S.: Convincing a Billion Users to Love Passkeys: UX Design Insights from Microsoft to Boost Adoption and Security (Dec 2024), 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/, as of November 19, 2026
56. Redmiles, E.M., Acar, Y., Fahl, S., Mazurek, M.L.: A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. Technical Report CS-TR-5055, University of Maryland (2017). https://doi.org/10.13016/M22K2W
57. Reittinger, T., Glas, M., Pernul, G.: Moving Beyond Passwords: Investigating the Effect of Digital Nudges on Passkey Adoption. In: ACM Conference on Human Factors in Computing Systems. pp. 1329:1–1329:17. CHI '26, ACM, Barcelona, Spain (Apr 2026). https://doi.org/10.1145/3772318.3791425
58. Reittinger, T., Pernul, G.: No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage. In: IEEE Symposium on Security and Privacy. pp. 3607–3626. SP '26, IEEE, San Francisco, California, USA (May 2026). https://doi.org/10.1109/SP63933.2026.00022
59. Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., Consolvo, S., Churchill, E.: "Privacy Is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In: Symposium on Usable Privacy and Security. pp. 127–142. SOUPS '18, USENIX, Baltimore, Maryland, USA (Aug 2018)

PREPRINT

60. Semenova, K.: Google Developer Blog: How KAYAK Reduced Sign in Time by 50% and Improved Security with Passkeys (Oct 2023), https://developers.googleblog.com/how-kayak-reduced-sign-in-time-by-50-and-improved-security-with-passkeys/, as of November 19, 2026
61. Sony Group Corporation: Password-Free Sign In: What Is a Passkey? (Jul 2026), https://www.playstation.com/passkey/, as of November 19, 2026
62. Spiel, K., Haimson, O.L., Lottridge, D.: How to Do Better with Gender on Surveys: A Guide for HCI Researchers. Interactions **26**(4), 62–65 (Jun 2019). https://doi.org/10.1145/3338283
63. StatCounter: Desktop Operating System Market Share Worldwide (Jul 2026), https://gs.statcounter.com/os-market-share/desktop/worldwide, as of November 19, 2026
64. Stobert, E., Biddle, R.: The Password Life Cycle: User Behaviour in Managing Passwords. In: Symposium on Usable Privacy and Security. pp. 243–255. SOUPS '14, USENIX, Menlo Park, California, USA (Jul 2014)
65. Taylor, T.E.: Users and Technology: A Closer Look at How Technology Engagement Affects Users. Computers in Human Behavior Reports **15**, 100473:1–100473:9 (Aug 2024). https://doi.org/10.1016/j.chbr.2024.100473
66. U.S. Department of Homeland Security: The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research (Aug 2012), https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of November 19, 2026
67. Wash, R., Rader, E.J., Berman, R., Wellmer, Z.: Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. In: Symposium on Usable Privacy and Security. pp. 175–188. SOUPS '16, USENIX, Denver, Colorado, USA (Jul 2016)
68. Wolf, F., Kuber, R., Aviv, A.J.: "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. In: ACM Conference on Human Factors in Computing Systems. pp. 151:1–151:12. CHI '19, ACM, Glasgow, Scotland, United Kingdom (Apr 2019). https://doi.org/10.1145/3290605.3300381