ARTIFACT EVALUATED
USENIX
AVAILABLE

"Maybe there's only one passkey?": Challenges Investigating and Remediating Adversarial Passkeys

Alaa Daffalla* *Cornell University*
Grace Myers *Cornell Tech*
Rosanna Bellini *New York University*
Thomas Ristenpart *University of Toronto*
Nicola Dell *Cornell Tech*

Abstract

Passkeys are being actively rolled out by hundreds of web services who market them as a promising passwordless authentication method. However, it remains unclear whether people understand how to manage passkeys as part of their broader account security management, particularly in the aftermath of account compromise. We conducted a qualitative lab-based study that explores how people investigate and remediate suspicious activity when passkeys are used as a vector for illicit account access on three popular, passkey-supporting services: Google, PayPal, and LinkedIn. We recruited 31 participants with diverse technical backgrounds and tasked them with: (1) investigating a potential incident of compromise involving passkeys and (2) taking steps needed to re-secure the account.

Participants struggled to manage passkeys within account security settings and on devices, even when supported by service-provided email notifications, account security interfaces (ASIs), and streamlined wizards. The design and content of notifications and ASIs were often confusing or unclear, while the service-provided wizards were incomplete or misleading. This resulted in participants missing key steps required to discover adversarial passkeys and fully secure the account to prevent continued adversarial access. We discuss design implications and opportunities for future work to improve passkey management tools in ways that better support people experiencing account compromise.

1 Introduction

The search for secure and usable alternatives to password-based authentication is ongoing [11] with passkeys [20, 56] emerging as a strong contender for reducing password use and improving security. Passkeys are a form of cryptographic credential built on public key cryptography and have been positioned as the cornerstone of a passwordless future by major service providers including Apple, Google, and Microsoft [1, 4]. Services encourage users to adopt passkeys, often via registration- or login-time suggestions to set them up, which is driving increasingly widespread use [41].

Despite this rapid adoption, it remains unclear whether people can easily adapt to using passkeys in everyday account management, particularly when investigating and remediating issues related to account compromise. A few prior studies [34, 35, 39, 59] have shown the challenges people face setting up and using passkeys, but no prior work has investigated how contemporary passkey deployments impact user experience when passkeys may, themselves, be a vector for harm.

Recently, Daffalla et al. [13] performed an abusability analysis of passkeys in the context of interpersonal violence. The study highlights the threat of adversarial passkeys, which arise when an attacker registers their own (adversarial) passkey on a victim's account. Doing so requires temporary initial access (e.g., via physical access to an unlocked device or password compromise), which is an all-too-common threat in interpersonal abuse [14, 22, 38, 54]. What the study does not explore, however, is whether users can effectively utilize service-provided account security management tools, including notifications, account security interfaces (ASIs) [14], and security wizards, to diagnose and remediate such attacks. Our study is therefore driven by two key research questions:

- How do people approach account compromise investigation and remediation when passkeys are in use?
- How do service-provided account security management tools support people experiencing account compromise, particularly when passkeys are a vector for compromise?

To answer these questions, we recruited 31 participants with diverse technical backgrounds and, in 60-minute 1:1 sessions asked them to investigate and remediate simulated account compromises involving an adversarial passkey on one or more services. To make these simulations realistic, we used three popular, passkey-supporting services: Google, PayPal, and LinkedIn. We carefully prepared these scenarios using dedicated research accounts used only for the study.

* Corresponding author: alaadaffalla@cs.cornell.edu

Our findings indicate that participants struggled with diagnosing and remediating the simulated compromise. Many participants were unable to discover the adversarial passkey without specific nudging from the researcher. This reflects in part on the difficulty of understanding how passkeys work (e.g., conflating biometrics with passkeys), but also that notifications and ASIs were challenging to interpret. As examples, LinkedIn does not send an email alert when a new passkey is added, only a re-authentication challenge via email to create a passkey, while different passkeys using the same passkey provider have almost identical labels on Google's ASI.

Most worrisome is that *no participants* were able to completely secure the account (remove the passkey, change the password, ensure adversarial sessions were terminated) on their own. Again, this is due in part to design of management tools. For example, Google's *Security Checkup* wizard does not address passkeys at all, which led many participants to a "false finish": mistakenly, but understandably, concluding they had successfully secured the account using the wizard. In addition, some participants assumed that changing the password sufficed for removing passkeys and securing the account. On the other hand, some participants took a conservative "scorched earth" approach, removing all passkeys and invalidating all sessions, including honest ones. And some design choices led a smaller number of participants to falsely believe they had not finished securing the account when, in fact, they had. For example, when removing a passkey on PayPal and LinkedIn, the services warn users to also delete the passkey from the device it is stored on—an impossible task for an adversarial passkey on an attacker-controlled device.

As the first study into the challenges people face in diagnosing and securing passkey-enabled accounts, our results surface a wide variety of open challenges. We provide a discussion of design implications, but emphasize that improvements will require much future work on diagnostic and remediation tool designs, descriptions that help users develop useful mental models for passkeys, account security, and more.

2 Background and Related Work

Passkeys are an implementation of the FIDO2/WebAuthn standards developed by the FIDO Alliance and the World Wide Web Consortium, aiming to promote passwordless, multi-device authentication across platforms [56]. While passkeys is a catch-all term for a number of related technologies, in this work, we focus on the FIDO2 implementation.

At a high level, a passkey is a cryptographic credential consisting of an asymmetric key pair for a digital signature scheme. A passkey is generated locally on a client either within an external hardware attachment (e.g., security key) or an internal authenticator (e.g., an OS-managed secure enclave or a software application like a password manager). The resulting public (verification) key is registered with a service provider and the associated secret (signing) key stored where it was generated. Subsequent authentication to the service involves using the secret key to sign a service-chosen challenge. A client device can optionally require user verification during registration and authentication (e.g., via biometric authentication (e.g., Touch ID [3]), PIN, password, etc.).

Passkeys can be synchronized across devices through cloud-based passkey providers (e.g., Apple iCloud Keychain). Unlike passwords, which are often reused, weak, or phishable, passkeys are resistant to attacks like credential stuffing and phishing because they are never shared with websites or transmitted unencrypted over the network [20]. As such, services are encouraging passkey adoption, in some cases via explicit prompts to set them up during registration and login.

However, although passkey adoption has accelerated across web services [16], the rollout has not been without challenges. Prior work has studied the security of the FIDO2 protocol [6, 7, 10, 25] and client-side and social engineering attacks [31, 29]. Research has also explored the general usability, adoption challenges, and user perceptions associated with FIDO2 credentials [35, 33, 39, 19, 59, 34], finding that while users perceive passkeys to be more secure than passwords, the added complexity around passkey use, management, and recovery pose barriers to adoption. More recent work [47] conducted a systematic analysis of the passkey user experience across more than 100 sites to analyze deployment patterns and enumerate passkey management features. However, they do not study if or how people understand the role of passkeys in account compromise situations, especially diagnosing and remediating illicit account access via adversarial passkeys.

Investigating and recovering from compromise. Beyond general usability, we were interested in how people understand their account security, particularly their ability to detect illicit access and remediate by stopping ongoing, and preventing future, illicit access. Prior research has explored how people detect and respond to account compromise. Shay et al. [53] found that 30% of surveyed users reported experiencing an account compromise, with half discovering it through suspicious activity on their account. Other studies have evaluated the effectiveness of security notifications, such as browser warnings [2] and alerts about password reuse [24].

Several works have specifically studied compromise-related notifications. Redmiles et al. [49] found that vague Facebook login alerts often failed to prompt action, as people perceived them as false positives. Markert et al. [37] observed that although people appreciated notifications of suspicious logins, they were often confused by their content and experienced fatigue from receiving too many warnings. Follow-up work showed that these warnings rarely offer actionable guidance [36]. Other works reinforce these concerns [27, 40, 51]. For example, Neil et al. [40] investigated 57 services, finding that 85% of services did not provide remediation advice. Huh et al. [27] analyzed password reset emails on LinkedIn, showing that most participants do not click on these emails.

Similarly, Sahin et al. [51] showed that although users' ability to act on notifications was essential for effective remediation, they were wary of emails that pressured them to click links.

Also relevant to our research is work by Yadav and Seamons [60] that systematizes seven local attacks on FIDO2, showing that users fail to detect these active attacks through current service-provided error messages and email notifications. We expand this literature by specifically focusing on the post-compromise investigation and remediation workflows when passkeys are used for authentication. Moreover, we go beyond studying notifications by also analyzing service-provided tools and interfaces intended to help people manage account access via passkeys. Along these lines, prior work has investigated the information available to users via account security interfaces (ASIs), such as device logs, session logs, etc. [9, 14]. For example, Daffalla et al. [14] found that although ASIs could help people to diagnose account compromise, users frequently find them confusing and struggle to understand the status of their account. Moreover, they showed that information on ASIs can be easily spoofed or otherwise obscured [14]. More recent work has demonstrated that these design and security flaws persisted across ASIs for more than 100 services [9].

In sum, no prior work has investigated users' experiences with both detecting and remediating illicit account access when passkeys are used for authentication. We contribute a qualitative study that explores actions people take to discover and remediate adversarial passkeys on three widely-used online services. We now discuss our study methods.

3 Methodology

Study overview. The goal of our study is to shed light on how the widespread adoption of passkeys impacts users' management of account security, particularly when passkeys are leveraged for illicit access. When a passkey is added to a user account, the credential's private key is stored locally on the user's device via a passkey storage provider; this enables access to the account from that device. Passkeys can also be synced across devices, enabling multi-device access [43]. Passkeys can be removed either from the user account via service ASIs, or from the passkey storage provider (e.g, iCloud Keychain). As such, passkey management fundamentally differs from pre-passkey authentication mechanisms, such as passwords or one-time codes sent to emails or phones.

We designed a simulated account compromise scenario in which an attacker who has one-time access to the victim's password uses it to register their own adversarial passkey on the victim's account, with the goal of obtaining ongoing account access. This scenario was motivated by the important context of interpersonal attackers, who have a personal relationship with the victim and exploit social proximity to bypass traditional defenses to control or surveil the victim [8, 55, 57]. This threat model is common among at-risk users [57, 8] such as intimate partner violence (IPV) survivors, where account security can be critical to their safety and well-being [22, 21].

Our simulated account compromise scenario utilizes three popular real-world services: Google (to access Gmail), LinkedIn (a professional networking service), and PayPal (a financial service). Prior literature informed our selection of these services: Daffalla et al. [13] analyzed 19 popular passkey-supporting services according to the Tranco list [46]. We utilized their analysis to weigh: Tranco list ranking; available passkey ASIs and information attributes; passkey session management options; and service type. All three selected services are in the Tranco top 200, offer passkey deletion and session termination (key to remediation), have more than four information attributes (listed in [13]), and represent disparate service types (email, finance, social networking). As such, they constitute examples of robust passkey deployments.

Our study asks participants to investigate the simulated compromise via inspection of service-provided notifications and exploration of relevant ASIs. After identifying the adversarial passkey, we anticipated three activities participants should perform to re-secure the account: removing the adversarial passkey, resetting the password, and ensuring adversarial sessions are terminated. As we'll see, participants struggled to do so without assistance.

3.1 Recruitment and Participants

We sought participants with a range of backgrounds and technical expertise. To achieve this, we recruited from three groups. First, we recruited *local residents* (R) from the neighborhood adjacent to our university's campus by posting flyers and sending emails to community listservs. Second, we recruited *technical students* (S) by posting flyers and sending emails to campus listservs. Third, we recruited *consultants* (C) from the Clinic to End Tech Abuse (CETA) that handles referrals for hundreds of IPV survivors (clients) each year [1]. Consultants help clients to investigate their account security. We recruited consultants by reaching out via clinic channels (i.e., Slack). Across groups, all flyers, emails, and messages detailed the study, eligibility, time commitment, compensation ($25 giftcard), and a signup link.

To take part, participants had to be at least 18 years old, able to attend an in-person session, and have experience managing a personal online account. Participants were told they did not need to share any confidential information about themselves or their clients. After participants filled out the signup form, we screened responses for eligibility and scheduled a session.

We recruited a total of 31 participants between 23 and 78 years old, with diverse backgrounds and technical experiences (see Figure 1). All participants had at least a Bachelors degree. Fourteen considered themselves to be highly technically skilled while another fourteen reported having taken

[1] https://ceta.tech.cornell.edu/

No. of Participants		Gender		Age		Technical Knowledge	
Local residents (R)	13	Female	22	18–29	7	Technical degree	14
Students (S)	11	Male	8	30–49	5	Some computer courses	14
Tech Consultants (C)	7	Non-binary	1	50+	6	Little/no technical background	3

First		Second	
Google	10	Google	9
LinkedIn	10	LinkedIn	10
PayPal	11	PayPal	9

Table 1: Summary of participant characteristics (left) and distribution of services across the first and second investigations (right) across study sessions. A more detailed participant table is provided in the Appendix (Figure 9).

computer courses and felt comfortable with general technical tasks (e.g., 2FA, Touch ID, etc.). Three had little or no technical background, but reported feeling comfortable with simple tasks (e.g., signing into an online account using a password). All participants reported familiarity with navigating ASIs to configure security settings (e.g., 2FA, recovery information).

3.2 Study procedure

We held 1:1, in-person, 60-minute study *sessions* in a meeting room at our university. Two consultants preferred meeting off-campus, but the protocol was otherwise identical. We first explained the study goals, emphasizing that all tasks would be performed on a lab computer using pre-configured test accounts. We obtained consent from all participants, including to audio and screen record their interactions.

After obtaining consent, we asked questions that probed participants' familiarity with and use of passkeys. For consultants, we also asked about their clients' experiences with passkeys. Participants then completed a warm-up activity: registering a passkey on a test account and logging in using the newly created passkey. The goal was to ensure a baseline familiarity with the technology and interfaces required for the main study tasks: investigating and remediating adversarial access (described in detail below). Participants then completed *investigations*, consisting of the warm-up activity and investigation and remediation tasks, for as many services as time allowed. The researcher did not intervene unless participants became stuck, at which point the researcher provided assistance, but did not complete the tasks for participants.

Finally, we asked participants to reflect on their experiences in the study and any recommendations they had around passkeys or ASIs. For consultants, we also asked what future challenges they perceive clients may have with passkeys. A condensed study protocol is provided in the Appendix.

Device setup. We used two MacOS devices for the study, both 14-inch MacBook Pros running macOS Sonoma (v14.5) and Google Chrome. Participants completed the tasks for each investigation in a separate on-device account. Thus, each device had two on-device test accounts. One was configured with the researcher's fingerprint (i.e., Touch ID) and the other was configured with only a password (i.e., no Touch ID). Across sessions and investigations, we counterbalanced the order of using these accounts, alternating Touch ID setups so participants did not always start with the same configuration.

Simulating account compromise. To simulate illicit access, we presented participants with a hypothetical scenario in which a victim's account had been compromised by an adversary who used access to the victim's password to register an adversarial passkey, enabling persistent covert access. We assume a UI-bound attacker [22] consistent with the threat model that is prevalent in interpersonal attacks [8, 57].

For student and resident participants, the victim (a friend played by a member of the research team) has asked the participant for help investigating suspicious account activity. The friend shares their account details, credentials, and discusses how they have received email notifications that suggest potential compromise. Participants were tasked with investigating the relevant account interfaces and determining whether the account had indeed been compromised. Participants were allowed to ask the friend questions (e.g., about devices, locations of access, etc.), or refer to help guides and external resources. After investigating adversarial access, participants were tasked with remediation: re-securing their friend's account to prevent future security breaches. They were also encouraged to provide security recommendations and advice.

For tech consultants, the protocol was very similar, involving the same tasks. However, instead of a hypothetical friend asking for help, we presented the scenario as a hypothetical client seeking help. This scenario is highly realistic for consultants, reflecting their routine work in the tech clinic.

Within this setting, we sought to understand how participants might recognize unauthorized account access, particularly when the victim and attacker both authenticate using passkeys. To achieve this, we set up a victim device (MacOS study device), and a new adversarial device (iPhone). During the study, participants only had access to the victim's device. New web sessions (hereafter, sessions) and passkeys for a simulated victim account were also set up, distinct from the account used for the warm-up exercise; Figure 1 shows the steps to set up the scenario. All sessions and passkeys, both legitimate and adversarial, appeared in the services' ASIs [14] (e.g., see Figures 4 and 8). Browser cookies and other state were not cleared between steps.

As shown in Figure 1, researchers created the first session on the victim device by logging in with the victim's password (*Step 1*), creating a passkey (*Step 2*), and logging out (*Step 3*). In a new session (second session), the researchers logged back in using the same newly-created passkey (*Step 4*), and

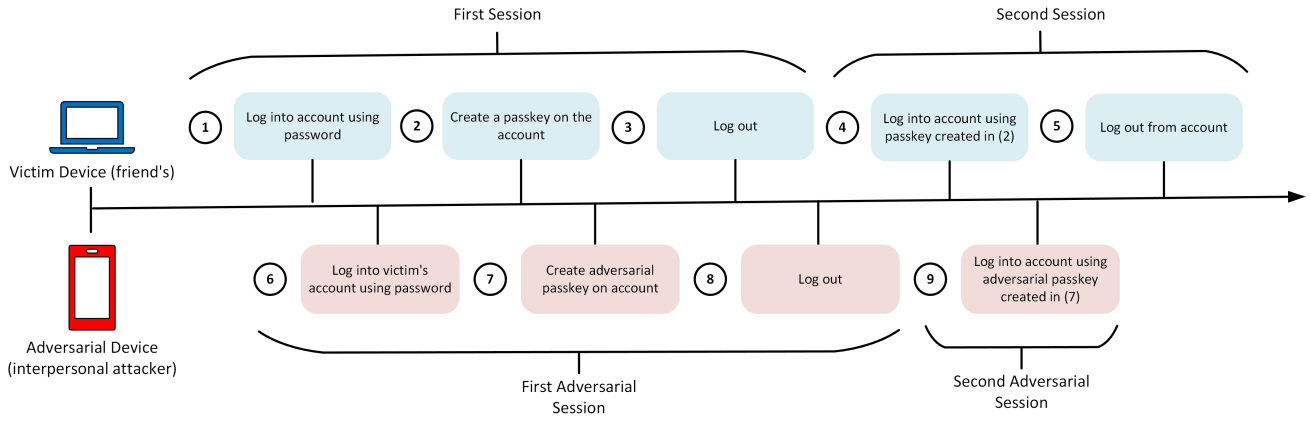

Figure 1: Steps the researchers took to setup the study scenario, showing both victim and adversarial actions to set up passkeys and sessions on the simulated victim account. All four sessions are logged on service account security interfaces. The second adversarial session is not logged out; this is because we wanted an active adversarial session, to provide participants with an opportunity to re-secure the account by terminating this session.

logged out again (*Step 5*). All passkeys were created using the default passkey provider or storage on the device (i.e., iCloud Keychain) for both the victim's and adversary's devices.

On the adversary device, the researchers created the first adversarial session by logging into the victim's account with the victim's password (*Step 6*), generating an adversarial passkey (*Step 7*), and logging out (*Step 8*). On LinkedIn, step 7 required the adversary to satisfy a re-authentication challenge sent to the victim's email; we presume the adversary has this capability (e.g., due to physical device access or the ability to log into the victim's email). To generate the second adversarial session, the researcher logged into the victim's account using the adversarial passkey and did not terminate the session (*Step 9*). We kept the second adversarial session active to see if participants would identify this session as suspicious and take steps to terminate it.

These steps generated email alerts and populated the services' ASIs. For Google and PayPal, participants were shown email notifications for both new device logins (*Step 6*) and the addition of the adversarial passkey (*Step 7*). For LinkedIn, the only notification generated was the re-authentication challenge email (*Step 7*) sent when the adversary added a passkey; LinkedIn does not send alerts about new device logins. Participants were able to inspect the notification emails via the browser on the test device, and many used them as a starting point for their investigations. However, in a few cases (n=8), technical difficulties and/or time constraints led to participants bypassing the email notifications. These participants began investigating by directly navigating to the services' ASIs using a browser on the test device (Figure 2).

We expected the information provided by services' notifications and ASIs to enable participants to identify the adversarial passkey and logins from an unknown device. We anticipated they would then take steps to secure the account by removing the passkey, changing the password, and logging out other devices. For Google, we also expected participants to identify and remediate the suspicious recovery email address, which we configured as a required step during the account creation process for the test account.

Data analysis. All sessions were audio recorded and screen captured. Recordings were transcribed using Whisper [58], an AI transcription tool with speaker diarization. We used Atlas.ti [5], a qualitative data analysis software, to analyze session transcripts and screen recordings in tandem. We applied the first stage of Kuckartz et al.'s [32] three-stage process for qualitative data analysis, namely the application of structural coding of high-level categories. We began by generating structural codes—a method of classifying large sections of data—in accordance with our research goals. After discussing and approving the structural codes, two authors applied them to relevant chunks of data across all transcripts. The first and second authors (the coding team) then applied Braun & Clarke's thematic analysis [12] to generate themes within these chunks of data. We used collaborative qualitative analysis [50] to ensure consistency by reaching agreement throughout the coding process, meeting regularly to discuss and resolve any disagreements. The coding team first independently coded a single transcript, creating separate codebooks. Then, they met to discuss, merge and group codes, generate a shared codebook, and re-code the transcript using the shared codebook. They repeated this process over an additional four sessions, meeting to discuss and iterate on the shared codebook until it stabilized and no new codes emerged. The remaining 26 transcripts were then split equally across the coding team. The final codebook contained 93 codes (11 structural codes and 82 open codes) and is provided in Figure 7 in the Appendix. Finally, the coding team clustered related codes into

overarching themes that represent our findings.

Limitations. We conducted a qualitative study with a small sample recruited from a single US city. As such, our findings may not generalize to other contexts. We also studied passkeys on three real-world services in a controlled lab setting, with participants using researcher-provided hardware and test accounts rather than their own devices and personal accounts. This may not capture the full spectrum of usability and security concerns that arise from long-term, real-world passkey use. Finally, participants received researcher assistance when they were unable to make progress; this guidance bounds our interpretation of success and failure rates, and real-world failure rates are likely higher than those we observed.

4 Findings

Our main results focus on participants' investigations into adversarial account access, and what steps they took towards compromise remediation. In total, *n=31* participants conducted *v=59* investigations (Figure 9). Recall that the study session included a scenario involving unauthorized access to a friend's or client's account. The hope was that participants would (1) identify an adversarial passkey added to the account as well as logins from another (attacker) device and, for Google, an additional adversarial recovery email; and (2) remediate the compromise by removing the passkey, changing the account password, and logging out other devices.

Overall, our findings paint a grim picture; the overwhelming majority of participants struggled to complete the study tasks without researcher assistance. This was despite the fact that 15 participants reported using or setting up passkeys in their online accounts (R=5, S=4, C=6) and 12 participants (R=3, S=2, C=7) reported personally experiencing account compromise/lockout or having a friend, family member, or client (for consultants) experience these.

Investigations. We provide an overview of how participant investigations proceeded. Figure 2 provides a graphical summary. In most investigations (49 of 59), participants started by inspecting email notifications for new passkeys and/or account logins. In the other 10 investigations, participants started by directly navigating to the ASIs.

After looking at the notifications, many participants (30 of 49 investigations) began investigating by switching to a new browser tab and navigating to service-specific ASIs. Others (19 of 49) clicked on a link in an email notification; in 15 investigations this triggered an account security wizard (wizard, hereafter) while in 4 this led to a service's ASI. A subset of participants who first went to an ASI ended up triggering a wizard from within an ASI (4 of 44 investigations). Of all those investigations that engaged a wizard (19 total), most (14 of 19) completed the wizard, which then ended back at an ASI. As we'll see, the differences in experience are primarily due to how services design their notifications.

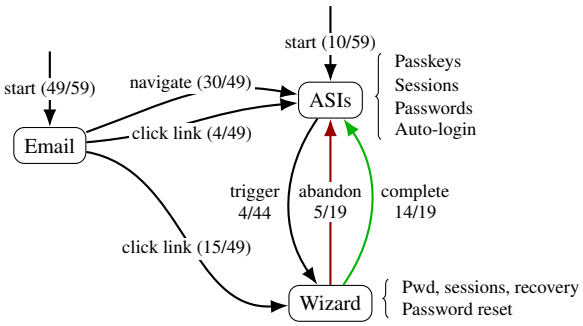

Figure 2: Investigation & remediation paths for all participants. A directed edge (→) represents a path. The red edge indicates that the wizard was abandoned, whereas the green edge indicates the wizard was completed. The labels on the edges represent the action required to transition to the node and the number of investigations in which participants took the specified path. We also show the different types of ASIs and Wizards next to the respective nodes.

In these exploration paths, participants sought to contextualize the incident and better understand how and whether the unauthorized access occurred. In most investigations participants succeeded in identifying the adversarial artifacts on the account, however not all did it without researcher assistance. More worrisome, *no participants* were able to completely secure the account (remove the passkey, change password, terminate adversarial sessions, and, for Google, remove recovery email) by themselves, and instead needed assistance. We only assisted when participants became stuck and could not proceed or missed important tasks. The assistance provided involved steering them towards ASIs or nudges to complete tasks. Without assistance, participants would not have completed the study in a reasonable timeframe. On average each participant received assistance twice during a session.

Below, we shed light on the challenges participants faced investigating and remediating compromise. We start by describing how email notifications often contained incomplete or confusing information (Section 4.1). We then discuss how participants struggled to identify adversarial activity when inspecting the different passkeys ASIs (Section 4.2) or other ASIs (Section 4.3). Finally we describe interactions with security wizards and how participants were often misled by incomplete remediation actions within the wizard (Section 4.4).

4.1 Inspecting Email Notifications

All three services sent email notifications when new passkeys were added to the account. PayPal and Google also sent emails for account logins from a new device. Most participants (n=29; v=49; see Figure 2) started at least one investigation by inspecting the email notifications, including the

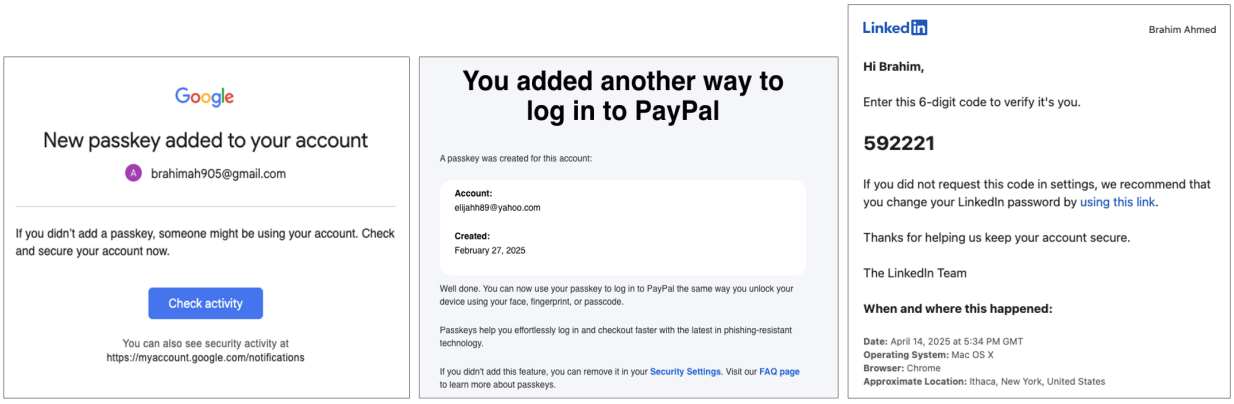

Figure 3: Email notifications received from Google, Paypal, and LinkedIn respectively. On Paypal and Google, notifications are received upon passkey creation. LinkedIn only sent a verification code required to create a passkey. Each of the notifications embed a link that either redirects to an ASI or triggers an account security wizard. Account information belongs to a test account.

header information, device and login details, and body text.

Concerns about phishing. Many participants (n=9, v =13) initial reaction to the setting was to question the veracity of the notification emails, with many explicitly expressing concern about these potentially being phishing attempts. As such, most participants first inspected the email header (sender and receiver information) to verify the authenticity of the email. For example, G13 said while inspecting the LinkedIn notification, *"I would just check the sender first . . . . . Okay, it looks like it has a legit email. But those could be spoofed."* This behavior suggests participants have adopted the lessons of prior work on phishing defense (e.g., [15, 17]), which emphasize training users to inspect email headers.

Expert participants (C3, C4) also advised (the hypothetical client) against clicking on email links even if the sender is verified. This concern was shared by other participants. G12, who considers their technical knowledge to be limited to computer courses, said: *"Okay, so I can tell you, if emails ask click here, do not do it. It could be a lot of fraud with PayPal."* Most phishing concerns arose for LinkedIn and PayPal, with only two participants concerned about Google. This perhaps suggests greater trust in Google emails being legitimate.

Understanding notifications: Google. The design of the notifications varied greatly across services, impacting participants' experiences. Google's notifications focused on the addition of a new passkey (Figure 3) and a new login. Both contained text about the potential for illicit account access, and a prominent button *Check activity* that links to a wizard. Participants would readily click on the button (recall that they did not express concern about phishing as per above). For example S10 stated that *"I would just go ahead and click on check activity because that's the most obvious thing."*

In short, the notification's design channeled participants to a wizard. However, as discussed in Section 4.4, the wizard does not actually help the user address the adversarial passkey.

Understanding notifications: PayPal, LinkedIn. Participants struggled to understand the PayPal and LinkedIn notifications, including for those participants who were concerned about phishing and verified email authenticity.

In our scenario, PayPal sent two email notifications. The first, *Stay logged in on this trusted device*, showed device, browser, and OS information. It said that PayPal recognized the device as a trusted one and if the user does not recognize it, they can *turn off the trusted device status*. Clicking on this link redirected to a *Turn off auto-login* ASI on PayPal. Most participants struggled to understand what a trusted device is or what action to take. G13 said: *"It says if this is a shared device or you don't recognize, turn off . . . Should I do it?"*

The second email, *You've changed your login settings* (Figure 3), stated that a passkey was created, with its date of creation and associated account email address. Participants had to scroll to the bottom of the email to see, in small text, text saying that if they did not add the passkey they can remove it in *Security Settings*, with a link to the *Passkeys* ASI on PayPal. Some participants missed this link; G9 said: *"So [the legitimate account owner] could not have created this. But there's nothing clickable in this part . . . I would have to go to PayPal and check the security settings there."*

LinkedIn only sent an email with a 6-digit code (Figure 3), triggered by the challenge required when the (simulated) attacker added the adversarial passkey. The email said that if the user didn't request the code they should change their password *"using this link,"* and the date, OS, browser, and location of the request. Nothing in the email mentions passkeys.

Participants found interpreting this notification challenging. C3 said: *"There's a lot of actions that would require an authorization prompt for LinkedIn or many sites. So it's not clear that this is to set up a passkey, but it does seem that somebody was trying to do something"*. G12 incorrectly thought the

email indicated a password reset: *"I started to get confused . . . so it's saying that a password had been changed."*

On PayPal and Linkedin, many participants (n=13, v=16) sought to contextualize the notifications by asking the hypothetical friend or client if they recall adding a passkey or changing configurations and also if they own an iOS device. For example, S5 said while inspecting the PayPal passkey notification: *"So the first thing I would ask them is, did you give your password to anyone else by mistake? Or did you give the device that you stored the passkey on to anyone else by mistake?"* The researcher responses (as the client/friend) were important for interpreting the notifications.

Next steps were often unclear on PayPal, LinkedIn. Unlike on Google where almost all participants simply clicked on the notification's button to engage a wizard, many participants on PayPal and LinkedIn were unsure of next steps after inspecting the notification(s). This was true even for participants who received clarification from the researcher about the notifications' context. For example, G1 said, after verifying the authenticity of the PayPal notification: *"The email is fine . . . I don't know if I would need to go onto PayPal. I might just look at the device to see if there was unusual activity."* Eventually, four participants clicked on the email links on PayPal to get to either the *Auto-login* or *Passkeys* ASI.

When participants became stuck, the researcher needed to provide assistance encouraging progress. For G1, for example, the researcher said: *"Where would you go check for unusual activity?"* G1 responded: *"I'm not sure."* For LinkedIn, most participants similarly needed assistance: only two people clicked on the notification's password reset link unprompted.

Checking email accounts for compromise. After inspecting the email notifications, a few participants (n=5) checked the email account for potential compromise, suspecting that the attacker might have access to the email. This was warranted, given that LinkedIn's verification email contained a one-time password, implying the attacker may have had email access.

On Google, the email account was the same test account for the study session (i.e., a Google account is also a Gmail account). However, on both PayPal and LinkedIn, email accounts were separate from the services' test accounts. C5 said: *"I would probably look in the Yahoo settings to see if someone unauthorized logged in to the email account, just because I'm here. And then I would go back and look at the LinkedIn account to see if there were any logins you didn't recognize."*

4.2 Investigating Passkey ASIs

All participants at some point used services' ASIs to investigate the unauthorized access (n=31, v=59). In 20 investigations, participants began with the services' passkeys ASIs; this was expected since Google's and PayPal's email alerts specifically said a new passkey was added to the account.

Participants struggled to understand passkey ASIs. All three services had ASIs for managing passkeys, such as adding, listing, and removing passkeys. These ASIs displayed each configured passkey as an entry in a list with a label, device (browser, OS) on which the passkey was created, and date of creation. Location information was only available on Google and LinkedIn. Our protocol resulted in services' passkeys ASIs containing two entries: one legitimate and one adversarial, displayed in order of registration with the service.

Many participants were confused by the passkey labels on the ASIs. For example, on Google, passkeys are labeled by the passkey provider or storage mechanism. In our scenario, both the legitimate and adversarial passkeys were labeled iCloud Keychain (see Figure 4) because we chose the default passkey storage option on both the legitimate and adversarial devices (Section 3). Participants found this confusing. G1 did not interpret the entries as two passkeys, instead believing the list showed one passkey being used across two devices: *"maybe there's only one passkey? So it shows . . . two devices. So this means that the passkey separately works for the two devices."*

More broadly, participants struggled to understand the role of passkey providers. For example, G11 told us: *"The Keychain is a thing that records what activity you've had, right? That you checked into the iCloud Keychain?"* G11 was further confused if the *delete* action next to each passkey entry referred to deleting the passkey itself or simply removing it from the iCloud Keychain: *"It's not clear if it's eliminating the passkey itself. It's just saying . . . if you want to eliminate it from the Keychain."* This confusion around passkey providers meant most participants (n=28) did not review the victim's iCloud account or Keychain app. Only a few consultants, including C6, suggested: *"We would have to check your iCloud account, because this [passkey] is what we just used to connect here. So it is associated to your iCloud account."*

Participants needed help finding the adversarial passkey. When exploring the passkeys ASIs, we expected participants to identify the adversarial passkey and take actions to secure the account. However, most participants (n=20, v=25) required assistance to correctly identify the adversarial passkey.

Consider G7, which is representative of the way passkey investigation typically went. First they expressed confusion about the passkey entries on the ASI, saying *"That's really weird, because they said there was a [passkey] that showed up."* The researcher tried to nudge them towards the information on the ASI: *"So what are you seeing?"* G7 replies, *"I'm seeing that it looks to me that there isn't a [passkey] that's been added."* The researcher again nudges them towards the passkey entries: *"What do you think those two icons are?"* Ultimately, G7 recognized the device information associated with the passkeys, and identifies the adversarial one.

Even expert participants needed assistance to complete the task. C2 struggled to identify the adversarial passkey

on Google because they incorrectly thought that resetting a password would also reset the passkey. Thus, they assumed that the passkeys listed on the ASI were created after the password reset during the session: *"The time right now is 11:42am October 2nd . . . this time is wrong though . . . If these were generated 11 hours ago, [that means] it didn't generate a new passkey when we created the new password. Yeah, it's crazy that it wouldn't wipe that away. I'm pretty clueless to be honest."* However, with researcher nudging they could finally reason about and identify the adversarial passkey: *"So you're saying you don't have an iPhone. And it's giving me context that this was done with an iPhone. So that gives me an indication, like, you didn't generate this passkey . . . so that would probably be the one of concern."*

In sum, most participants were not able to identify the adversarial passkey without assistance. While our methodology does not tell us whether, counterfactually, participants may eventually have somehow identified the passkey had we not nudged them, our data strongly suggests it to be unlikely.

Removing adversarial passkeys. After eventually discovering the adversarial passkey, most participants (n=30, v=56) removed it as part of re-securing the account. However, before removing some participants hesitated, asking the researcher if they should remove the passkey; the researcher replied they should take any actions needed to secure the account.

Removing passkeys on Google was relatively straightforward after participants found the relevant passkeys ASI. Participants clicked on the button to remove the passkey and saw a warning that they should revert to their old sign-in method if the passkey is removed; participants confirmed the revocation.

On PayPal and LinkedIn, removing the passkey triggered a warning to also remove it from the device it is stored on. In scenarios like ours, where the victim does not have access to the adversarial device, there is no way to do so. It is also not necessary to prevent access using the adversarial passkey.

Participants found the PayPal and LinkedIn warnings confusing. S7, who considers themselves to be highly technical, thought that removing the passkey on PayPal would also remove it from the adversarial device. Several participants (n=4) turned to on-service help guides or Google's search engine to attempt to understand how to remove passkeys from the adversarial device or the implications of (not) doing so. For example, S10 searched through the LinkedIn help pages to understand how to remove the passkey from the device per the instructions they received: *"It says that you should remove it from both your LinkedIn settings and the device, but the device is that of the hacker, so I'm not sure how you can do that . . . [what] happens if you only delete it from one side?"*

LinkedIn further required participants to complete a re-authentication challenge sent to the email to remove the passkey. Several participants (n=5) perceived this to be more secure; S4 said: *"there is an added benefit of utilizing the [one-time password] to add or remove a passkey. If someone is using my device, they cannot add a passkey to their phone for my account because they would need access to my email or phone number."* By contrast, S5 reasoned that if the adversary already has access to the account, then there was no added benefit to re-authentication: *"So we remove [the passkey] but if [the adversary] is already in the account, adding a [one-time password] again is not going to change that."*

Finally, we saw that most participants (n=22, v=30) preferred to not only remove the adversarial passkey but, for added safety, also removed the legitimate passkey. For example, G7 said: *"Okay, so we're going to remove all passkeys."* They then encouraged the victim to create a new passkey and further suggested registering it with their own fingerprint.

Some experts avoided removing passkeys. Several consultants (C4, C5, C6, C7) suggested not removing passkeys without first discussing safety implications with the hypothetical client. This presumably reflects consultant training that emphasizes client agency and safety [26]. Consultants pointed out that removing access may notify the adversary, possibly escalating abuse. As C6 said, *"This is what we have to caution victims. So you have two options here. You could remove it, or you could document it and store it for later. Because if you remove it, then the person logged in will be aware that they have no access. And sometimes that's not what's safe."*

Only one non-consultant participant (G11) expressed safety concerns with removing passkeys, not knowing whether removing passkeys might lock the hypothetical friend out of their account, and not realizing that authentication would fall back to passwords: *"No, I wouldn't delete it, only because I don't know what the ramifications are . . . it's not specific enough for me. So what is possible in terms of consequences of deleting? Well, not [being able to] access her account."*

Participants added new passkeys to secure account. After passkey revocation, some participants (n=10) suggested setting up a new passkey as a remediation action, often with the use of Touch ID (fingerprint). Participants perceived this would restrict access to a specific device and require a fingerprint for future logins, overlooking the fact that most passkeys are not device-bound and may be synced across devices [44]. Indeed, prior work has shown that passkey cloning is a valid abuse vector in interpersonal threat models [13]. Passkeys are also not tied to a specific user verification method. So, if Touch ID is disabled, then user verification will fall back to a password or, in some cases, no user verification.

4.3 Exploring Sessions and Password ASIs

Beyond passkeys ASIs, participants explored a range of other ASIs to investigate and remediate adversarial activity. These included sessions ASIs, which communicate which devices are logged into a user account, and password ASIs, which provide visibility into password state and changes. We now

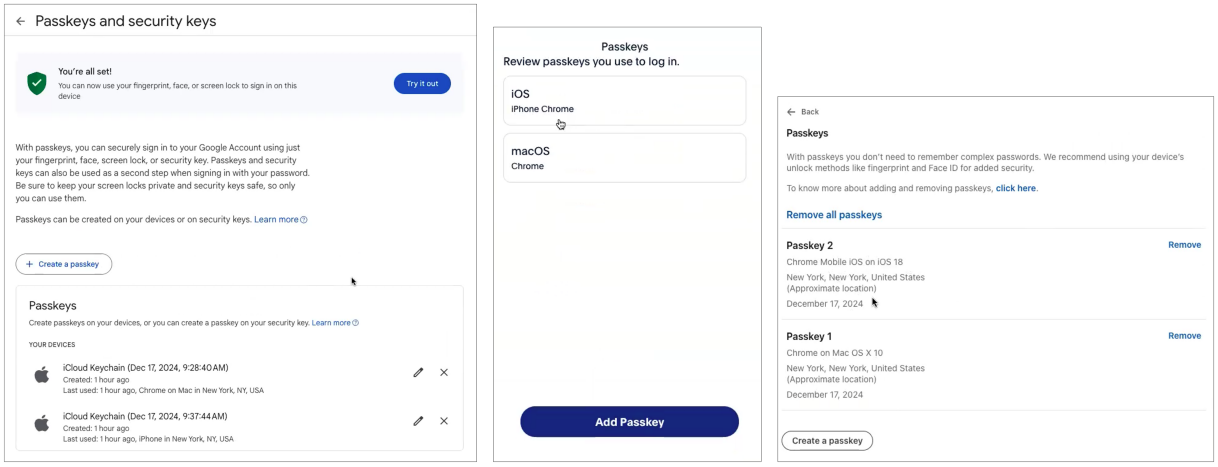

Figure 4: Passkeys ASIs across the three services: Google, PayPal, and LinkedIn respectively. Each ASI shows the simulated adversarial and legitimate passkey. All account information shown belongs to a test account.

discuss participants' experiences with these other ASIs.

Checking sessions ASIs was key to investigation. As part of the study protocol, we expected participants to identify adversarial sessions and take actions to remove adversarial access. Across all services, many participants (n=12, v=13) first navigated to the sessions ASI to review account login activity, considering it important for investigating adversarial access. As C3 said: *"I'm not familiar with LinkedIn, but at least Google can tell you recent sessions, even recently closed sessions. So what I would do with the client is say, do you have an iPhone? If not, then this is a suspicious login."*

Recall that, as part of the study setup, the second adversarial session was not logged out and remained active (Figure 1). In line with prior work [14], we saw that PayPal and LinkedIn only display active sessions, with logged out sessions not shown. As such, participants on PayPal and LinkedIn saw two sessions on the ASI: one current active session and another adversarial active session (Figure 8). By contrast, Google's ASI shows both active and past sessions. Thus, participants saw five sessions on the ASI, two adversarial (one logged out and one active) and three legitimate sessions (two logged out and one active). For logged out sessions, Google provides a clear *signed out* indicator. S9 described Google's sessions ASI: *"Okay, now I'm seeing manage all devices. So there are three sessions on my computer. So yeah, this is my current session which is on this Chrome Mac OS. And then I'm seeing that the other Google Chrome and the other iPhone that was previously signed in already logged out."*

Most participants relied primarily on the device information to identify the adversarial session(s) (i.e., MacBook vs. iPhone). Some participants also used the time of access, which they compared to when the email notification was received. For example, S7 explained their thought process around identifying adversarial sessions on PayPal with the help of device and browser information on the ASI: *"I would want to manage my logins as well. Because you've told me that she received that 11:42am email which she was not expecting. So what happened is this account was also logged into on another device. I would want to check that. So I click on Manage and I see that, other than the current Chrome [MacOS] login, there is an Apple iPhone login this morning. Multiple logins. I'm not sure I should do anything with it or not. I'd love to keep the current [MacOS] one and remove the others."*

Terminating adversarial sessions. After identifying adversarial sessions, most participants (n=21, v=31) terminated these sessions if they weren't already logged out. Participants were comfortable clicking on the relevant ASI buttons to end the session. Similar to removing passkeys, LinkedIn required completing an authentication challenge to end a session.

Rather than only terminating adversarial sessions we found that, for additional safety, most participants preferred to terminate *all* sessions other than the currently active one. Several participants (C2, C7, G13) also took a screenshot of the sessions ASI in case the information was manipulated; G13 said: *"I would probably take a screenshot first, just to get all these details . . . people can have ways of making things look like they're not, like your metadata and IP."* Prior work has indeed shown that device and location information on device and session logs can be spoofed by a technically unsophisticated adversary to hide accesses to a victim's account [14].

Similar to passkeys, expert participants often chose not to terminate sessions before discussing the implications with the hypothetical client. For example, C3 said: *"So I would tell a client . . . the person who is logged in on this account might be notified that you have ended their session. So you know, just make sure you're safe and in a position to do that."*

One participant (S1) clicked on PayPal's trusted device email notification which led to a *Turn off auto-login* ASI. S1

		Remediation actions					
		Remove passkey	Terminate session	Reset password	Remove/edit recovery info	Add new passkey	Remove saved device
ASIs	Passkeys & security keys (Google)	●	○	○	○	●	○
	Passkeys (PayPal)	●	○	○	○	●	○
	Passkeys (LinkedIn)	●	○	○	○	●	○
	Your devices (Google)	○	●	●	○	○	○
	Recent security activity (Google)	○	●	●	●	○	○
	Manage your logins (PayPal)	○	●	○	○	○	○
	Turn off auto-login (PayPal)	○	○	○	○	○	●
	Where you're signed in (LinkedIn)	○	●	○	○	○	○
Wizards	Pwd, sessions, & recovery (Google)	○	●	●	●	○	○
	Password reset (LinkedIn)	○	○	●	○	○	○

Figure 5: The set of remediation actions that can be completed on most ASIs and wizards that participants encountered during the study. We only include an action if the interface/wizard clearly describes an action can be carried out. We do not include email notifications because notifications channeled users to either an ASI or a wizard as described in Section 4.1. ● indicates that an action can be completed on the interface/wizard, whereas ○ indicates that it cannot.

confused disabling auto-login with session termination. They first inspected the email and aimed to remove the adversarial iPhone. However, as confirmed via separate experimentation, disabling auto-login does not terminate the session and they would have to do it separately on the PayPal's sessions ASI. As a result, S1 required nudging to terminate sessions.

Performing a password reset. All three services have dedicated ASIs for password reset. Six participants navigated to these as the first step for account remediation after inspecting email notifications. As C7 said: *"A good first step is to change the password."* Many participants who completed a password reset understood that doing so would also terminate sessions (we did not verify whether sessions were actually logged out after password reset). One expert participant (C5) was confused when their active session on PayPal wasn't immediately logged out after the password reset: *"That's weird . . . usually, whenever we change passwords, [clients] are logged out of any previous sessions. So it's odd that PayPal doesn't log you out when we just changed your password."*

Some participants (n=6, v=6) believed that performing a password reset would also remove the passkeys on the account. However, on these services and most others [13], password reset does *not* remove passkeys, and participants needed to be nudged to check and remove passkeys.

Other remediation actions. When asked if they would take any remediation actions beyond passkeys, sessions, and passwords, we found that participants most often returned to the central security dashboard (LinkedIn and PayPal) or security page (Google) and checked through the different options on these ASIs. As G3 said, while scrolling through Google's security page: *"So I turn on two step verification. I change my password, skip password when possible because I leave that on out of convenience. And I'd add a mobile number and recovery email. So I do the rest of these things as well."*

As part of our protocol, we expected participants to identify the adversarial account recovery information configured on the Google account (Section 3). This information was visible under the *How you sign in to Google* ASI. Of the six participants on Google who started their investigation on ASIs, three correctly identified the adversarial account recovery information and took steps to edit or remove it. The other three required nudging from the researcher to realize the adversary had configured a recovery email address. For example, in the following interaction, the researcher nudges S7 to check the recovery email configured on the account: *"Have you checked what kind of recovery information is configured on the account?"* S7 replies: *"There is a good chance that the hacker could have set it up as well. I would probably change it and add my phone number."*

4.4 Navigating Account Security Wizards

We now discuss participant interactions with security wizards: structured sequences of UI steps or screens that walk a user through reviewing or managing security-related settings. In our study, wizards were triggered when a participant clicked a link in an email notification (n=15, v=15). A small number (n=4, v=4) also triggered wizards while exploring ASIs. We came across two distinct wizards: (1) Google's password, sessions, and recovery wizard, and (2) LinkedIn's password reset wizard. Neither provided a complete view of the security settings needed for account remediation (Figure 5). PayPal did not have a wizard; notifications instead linked to ASIs.

Google's password, sessions, & recovery wizard. This wizard was triggered by clicking the *Check Activity* button in the email notification sent when a new passkey is added (Figure 6). It has multiple pages: the first page contains device and login information, the second suggests the account may be at risk, the third enables password reset, and the final page contains collapsible menu items to review other security settings. Although 17 participants triggered this wizard, only 13 completed all the steps; the other four abandoned the wizard.

Many participants who completed the wizard perceived the

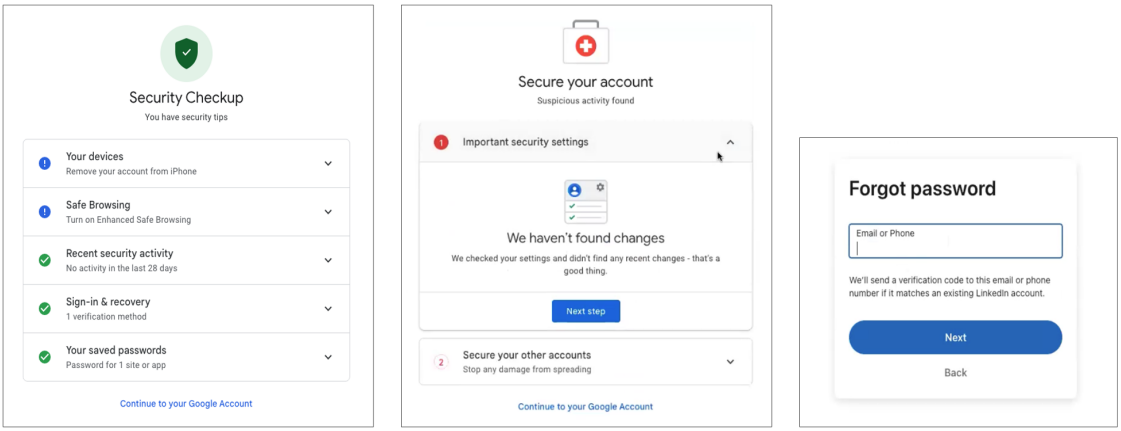

Figure 6: Screenshots of the *Security Checkup* (left) and *Secure your account* (middle) pages from Google's password, sessions, and recovery wizard, and the *Forgot password* page (right) on LinkedIn's password reset wizard.

account to then be secure and did not think they also needed to check passkeys (n=6). Only one participant (G13) noticed the wizard was incomplete and was frustrated at the lack of passkey management options: *"I would have expected an option like . . . these are your other passkeys, dropdown if you want to see them, and the option to remove all."*

Another participant (S10) who triggered the wizard via an ASI was confused that it did not include steps to remediate access from an unrecognized device, saying: *"So it's saying that this other person access your Gmail from the iPhone . . . and it's saying that there are recommended steps that can be followed. I don't see the recommended steps right now."*

For participants who abandoned the wizard (n=4), three did not want to reset the password via the wizard, wanting instead to address the new passkey notification by navigating to the passkeys ASI. After triggering the wizard, S6 said: *"Is it okay if I jump around? . . . I would go back to my Google account. It says I have two passkeys set up."* The fourth participant (G10) was concerned about phishing and preferred to not take a security critical action using the wizard. While inspecting the URL for the wizard's password reset page, G10 said: *"I'm looking at the URL. I'm trying to see if there's something fishy there . . . I wouldn't . . . change the password here."*

Although participants took the same path through the wizard, they saw one of two different pages to review account security settings: either the *Security Checkup* or the *Secure your account* page (Figure 6). We don't know what determines which page the wizard shows. In our sessions, the *Secure your account* page showed a *No recent changes* indicator under the changes to security settings even though multiple adversarial artifacts (passkey, sessions, recovery email) had been configured on the account. Some participants were misled by this; S11, while inspecting the *Secure your account* page, said: *"We haven't found any changes. This is a good thing."*

Overall, six of the 13 participants who completed the wizard required nudging to check the adversarial account recovery information because they missed it and didn't expand on the *Sign-in & recovery* item on the *Security checkup* page or because it was not shown on the *Secure your account* page.

LinkedIn's password reset wizard. This wizard was triggered when participants clicked the *change your LinkedIn password using this link* on the verification email sent during the process of adding a new passkey (Figure 3). The wizard guides users through a series of pages to reset their password. Two people triggered this wizard. G11 completed the wizard and then perceived the account to be secure; they did not attempt to check the passkeys until prompted by the researcher: *"Should your friend feel safe now that you've changed your password?"* G11 replied: *"Yeah."* The researcher replied: *"Do you want to check passkeys at all?"* to which G11 replied they *"Don't even know if it is a possibility."*

The other participant, G9, abandoned the wizard and suggested deleting the email notification. They thought the notification and wizard were for a password reset requested by the hypothetical friend: *"so clearly he wants to change the password. If that's the case, then this is not so suspicious."* When the researcher clarified that the friend did not attempt a password reset, G9 suggested deleting the notification: *"There's a possibility that somebody is pretending [and] asked for a new password. If my friend says they didn't, my advice would be . . . just delete the [email]."* This echoes findings in Section 4.1 related to participants' confusion with LinkedIn emails.

5 Discussion

We provide the first study of how people investigate and remediate adversarial passkeys. We now synthesize key takeaways and implications for passkey-enabled service design.

The challenges. Overall, we saw that participants struggled with diagnosing and remediating potential account compro-

mise. We distill these down into four main challenges participants faced: warped entry points, diagnosis difficulties, remediation mental model mismatch, and false finishes.

Warped entry points: Although services' email notifications provide a logical starting point for investigations and contain important information that can alert users to potential compromise, participants were often concerned about the authenticity of the email notifications, mostly foregoing clicking on email links to trigger remediation wizards. This echoes similar findings by Sahin et al. [51] who found that people were skeptical of clicking on email links. Some services, namely LinkedIn, do not even send a notification that a passkey was added to an account; the lack of binding between notification and actions on the account is a cause of confusion for users. Overall, participants preferred to navigate to the sites' ASIs instead, suggesting that they trusted the content of the notification, and the potential for services' ASIs to assist with remediation, but not external links.

Diagnosis difficulties: Even after navigating to ASIs, many participants were unable to discover the adversarial passkey on their own. They struggled to differentiate malicious from benign passkeys, suggesting that passkey labels and iconography were insufficient to alert users to a potential compromise. Some services labeled passkeys after the passkey provider (i.e., iCloud Keychain) which confused participants who did not understand the role of passkey providers in passkey management. Overall, our findings indicate that ASIs are not yet effectively communicating security posture to users.

Remediation mental model mismatch: Participants were also confused about what actions were necessary to re-secure the account. Some participants assumed that changing the password sufficed for full remediation, unaware that this does not automatically remove existing (adversarial) passkeys. Because participants struggle to determine which passkey was adversarial, many chose to remove all passkeys, a "scorched earth" approach. Similarly, what sessions were associated to adversarial access was opaque, and so some participants similarly default to ending all sessions.

False finishes: The mental model issue above combined with the current design of management tools often led participants to suffer from what we call the problem of "false finishes": the misunderstanding that steps the user has taken suffices to ensure security, or the misunderstanding that the user must take additional difficult or impossible actions to ensure security. As an example of the former, Google's wizard either suggested that completion of the wizard was itself sufficient for account remediation even though it was not (it ignores passkey review), or inaccurately stated that no security settings had been changed. Simliarly, LinkedIn directed users to a password reset wizard that did not address the issue of a new passkey being added to the account. Such situations dangerously lead users to a false sense of security.

As example of the other type of false finish, both LinkedIn and Paypal provided a warning that told users to delete the passkey from the device it is stored on. This is not necessary to secure the account and, in our study context, is impossible since the adversarial passkey resides on an attacker-controlled device. Such a misunderstanding leads to a false sense of insecurity, a damaging issue particularly in contexts of interpersonal abuse where it could lead to inflated views of abuser capabilities, trigger hypervigilance or other trauma stress reactions (c.f., [48]), and more.

Design implications. We now turn to implications for the design of account security management tools. We caution that while our findings surface a surfeit of challenges (as per above), these ideas below are speculative and further research will be needed to refine and validate them.

Improving email notifications: Our findings highlight opportunities for services to improve the design of their email notifications. Echoing prior work [51], the email subject line should mention the suspicious activity and why the recipient is receiving the notification. This should clearly reflect the action that was taken on the account; in our context, that a passkey was added to the account. Failing to do so, as in the case of LinkedIn in our study, leads to people being confused about why the email was sent and what actions to take.

If an email notification does provide a link (e.g., to a wizard), this should link to relevant tools and/or ASIs that guide people to take any and all actions needed to remedy the specific problem identified (e.g., an adversarial passkey was added). As our findings show, it is not sufficient to link to a general security settings page and expect people to know what steps to take on their own. At the same time, services should be cognizant of people's understandable skepticism for clicking on email links and instead design notifications that support user discovery of service ASIs, as we now discuss.

Designing pathways & ASI discovery: Since people are skeptical of email links, designers might instead foster organic navigation pathways. By this we mean moving away from reliance on a single link in an email notification, and instead displaying a security message with clear, simple instructions. For instance, the email could provide breadcrumb navigation pathways that users organically take (*"Account > Settings > Passkeys"*) to help people find remediation tools on their own. To support this self-directed approach, platforms could add contextual banners on the account landing page. If a user logs in after a security alert, a visible banner could provide a direct link to the relevant passkeys ASI. This might provide a trusted, internal path that makes it easier for users to secure their accounts without the need for using external email links.

Developing remediation processes: Our work also suggests opportunities to improve remediation processes in light of widespread passkey deployments. The FIDO Alliance's passkey design guidelines specify required patterns for enrollment, authentication, and basic management of passkeys, but provide no guidance on detecting or remediating compromise,

including cases where an adversary has registered a passkey on a victim's account [42]. Participants in our study experienced false finishes: a disconnect between their perception and the actual completeness of remediation processes.

We suggest that services maintain and communicate to users remediation checklists that enumerate the set of actions required for complete remediation and signal to users their progress and completion status. Software security checklists have been reported as a useful practice in the software development lifecycle for audits and evaluations [18, 23], and further research has shown that users' decision making process is significantly improved when using checklists [28, 52, 30]. These remediation checklists should cover all access routes to the account (e.g., passwords, passkeys, recovery emails, etc.) and explain to users the implications of each of the remediation actions (e.g., how account access changes once a passkey is removed). This is particularly acute for at-risk users navigating complex safety issues as reported by consultants, who suggested not taking action to remove passkeys before considering safety implications.

Attributing session activity: Our findings showed that when participants struggled to distinguish between adversarial and legitimate sessions or passkeys, they often simply removed all sessions or passkeys. While this may be sufficient for initial remediation, many users, such as those suffering from interpersonal violence, need to be able to diagnose compromise to navigate complex safety issues as reported by consultants and mentioned in prior work [14]. One approach is to enrich ASIs with identifying information such as device serial numbers, but the cryptographic protocols [45] needed to do so without sacrificing privacy are not currently deployed.

In the mean time, services could maintain logs that tie sessions to the authentication pathways used to establish them (e.g., password-based authentication, which passkey was used, etc.), as well as the access-related security changes made during those sessions. This information should be made available to users via ASIs (perhaps advanced ones), which would help them understand what sessions are tied to which credentials and what changes were made. Such logs can also be used during remediation, helping highlight to users which account activity that they don't recognize is likely due to the attacker.

6 Conclusion

We provided the first investigation into how people approach account compromise investigation and remediation when passkeys are in use. Via an in-lab study, we asked participants to explore realistic, but safely simulated, account compromise scenarios. We found participants struggled to use service-provided account security management tools to correctly diagnose and re-secure accounts, particularly when passkeys are a vector for compromise, and provide recommendations for how services might better ensure user safety via design of improved account security management tools.

7 Acknowledgments

We thank all our participants. This research was supported in part by NSF Awards 2452613 and 452614, and a Google Cyber Award.

Ethical Considerations

Our study was reviewed by our university's institutional review board (IRB) and was considered exempt from IRB review. Nevertheless, we took steps to safeguard participants.

We obtained both written and verbal consent from participants, including to audio and screen record sessions. We collected only what identifying information was needed to contact participants about study and scheduling information (i.e., first names and email addresses). Clinic consultants are trained to not share identifying information of their clients; none did so. We assured consultants that this was not a performance evaluation and that participation was not going to impact their standing in the clinic. We assured them that they need not share anything discomfiting, particularly given that their consultant work might be a source of vicarious trauma.

We designed a study protocol that limited participants' disclosure of their own account security behaviors and practices and only probed for familiarity with passkeys as an authentication mechanism and its use. For task completion, we did not ask participants to use their personal information, devices or accounts; instead, we used lab devices and created test accounts with synthetic information (e.g., names, recovery emails). When participants became stuck, the researcher provided gentle hints to help them make progress, helping to limit any stress or discomfort participants may feel.

At the end of the session, all participants were provided with a detailed briefing about how passkeys work in practice and concrete steps to perform account remediation in the event of a compromise to ensure that participants did not leave the session with inaccurate or incomplete security information.

We also considered researcher safety. Researchers also did not have to use any of their personal information or accounts. Moreover, although we draw on contexts of interpersonal violence, our study did not require researchers or participants to engage with traumatic or abusive content.

We also considered whether our work infringes on any of the service's terms of use. As such, we created test accounts on each of the services without causing undue network traffic and strain on the service infrastructure. We also designed our compromise scenario to simulate a standard multi-device account owner, adding passkeys and logging in on multiple devices. All study tasks were completed through the standard UI provided by services. We plan to share our findings to the three services in this study, and will make ourselves available to them for discussions.

We do not believe there is a material risk that (potential) abusers would learn new strategies from our work. The threat

of adversarial passkeys was surfaced in prior work. Our simulated adversary is basic, using standard account management tools in obvious ways. While we show mishaps in how remediation fails with security wizards, we believe that improving safety requires a frank discussion of such issues.

Open Science

All artifacts required to evaluate this work are available at: https://doi.org/10.5281/zenodo.20420527. These include the study-materials folder and the recruitment-materials folder. The study materials folder contains the codebook used for qualitative analysis, the consent form provided to participants, participant demographics, participant sheet, study protocol, and code frequency. Furthermore, the recruitment-materials folder contains the recruitment flyer, initial screening form, and demographic information form.

We also include a set of artifacts in the body of the paper and the Appendix; screenshots of email notifications (Figure 3), passkeys ASIs (Figure 4), and security wizards (Figure 6), a condensed study protocol in Section A.1, demographic information of all participants in Figure 9, and a copy of the codebook in Figure 7.

We do not release the full interview transcripts due to re-identification risks. Researchers interested in accessing the transcripts may contact the authors of this work directly.

References

[1] Heather Adkins. Passkeys, Cross-Account Protection and New Ways We're Protecting Your Accounts. https://blog.google/technology/safety-security/google-passkeys-update-april-2024/, 2024. Accessed 2026-06-10.

[2] Devdatta Akhawe and Adrienne Porter Felt. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. *USENIX Security Symposium*, pages 257–272, 2013.

[3] Apple. About the Security of Passkeys. https://support.apple.com/en-us/102195. Accessed 2026-06-10.

[4] Apple. Apple, Google, and Microsoft Commit to Expanded Support for FIDO Standard. https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/. Accessed 2026-06-10.

[5] ATLAS.ti. Qualitative Data Analysis Software. https://atlasti.com/. Accessed 2026-06-10.

[6] Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi. Provable Security Analysis of FIDO2. In *Advances in Cryptology*. Springer, 2021.

[7] Manuel Barbosa, André Cirne, and Luís Esquível. Rogue Key and Impersonation Attacks on FIDO2: From Theory to Practice. In *International Conference on Availability, Reliability & Security*, pages 1–11, 2023.

[8] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. SoK: Safer Digital-Safety Research Involving At-Risk Users. *IEEE Symposium on Security and Privacy*, 2024.

[9] Arkaprabha Bhattacharya, Alaa Daffalla, Kevin Lee, Rosanna Bellini, Nicola Dell, and Thomas Ristenpart. Inconsistent, Incomplete, and Insecure: A Survey of Account Security Interfaces. *USENIX Security Symposium*, 2026.

[10] Nina Bindel, Cas Cremers, and Mang Zhao. FIDO2, CTAP 2.1, and WebAuthn 2: Provable Security and Post-Quantum Instantiation. In *IEEE Symposium on Security and Privacy*, pages 1471–1490, 2023.

[11] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Symposium on Security and Privacy*, 2012.

[12] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[13] Alaa Daffalla, Arkaprabha Bhattacharya, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models. *USENIX Security Symposium*, 2025.

[14] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. Account Security Interfaces: Important, Unintuitive, and Untrustworthy. *USENIX Security Symposium*, pages 3601–3618, 2023.

[15] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why Phishing Works. In *ACM Human Factors in Computing Systems*, pages 581–590, 2006.

[16] Passkey Directory. https://passkeys.directory/. Accessed 2026-06-10.

[17] Julie S Downs, M Holbrook, and Lorrie Cranor. Decision Strategies & Susceptibility to Phishing. In *Symposium on Usable Privacy and Security*, 2006.

[18] Bob Duncan and Mark Whittington. Reflecting on Whether Checklists Can Tick the Box for Cloud Security. In *IEEE Cloud Computing Technology & Science*, pages 805–810, 2014.

[19] Florian M Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security*, pages 19–35, 2020.

[20] FIDO Alliance. Introduction to Passkeys. https://fidoalliance.org/passkeys/, 2024.

[21] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[22] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology. In *ACM Human Factors in Computing Systems*, 2018.

[23] David P Gilliam, Thomas L Wolfe, Joseph S Sherif, and Matt Bishop. Software Security Checklist for the Software Life Cycle. *IEEE Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2003.

[24] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *ACM Computer and Communications Security*, 2018.

[25] Jingjing Guan, Hui Li, Haisong Ye, and Ziming Zhao. A Formal Analysis of FIDO2 Protocols. *European Symposium on Research in Computer Security*, 2022.

[26] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical Computer Security for Victims of Intimate Partner Violence. *USENIX Security Symposium*, 2019.

[27] Jun Ho Huh, Hyoungshick Kim, Swathi SVP Rayala, Rakesh B Bobba, and Konstantin Beznosov. I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. In *ACM Human Factors in Computing Systems*, 2017.

[28] Anthony Jameson. Recommender Systems as Part of a Choice Architecture for HCI. In *Workshop on Decision Making and Recommender Systems*, pages 3–7, 2014.

[29] Mohammed Jubur, Prakash Shrestha, Nitesh Saxena, and Jay Prakash. Bypassing Push-Based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications. In *ACM Asia Conference on Computer & Communications Security*, 2021.

[30] Mark Keil, Lei Li, Lars Mathiassen, and Guangzhi Zheng. The Influence of Checklists and Roles on Software Practitioner Risk Perception and Decision-Making. *Journal of Systems and Software*, 81(6):908–919, 2008.

[31] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. Evaluating the Security Posture of Real-World FIDO2 Deployments. In *ACM Computer and Communications Security*, pages 2381–2395, 2023.

[32] Udo Kuckartz. Three Basic Methods of Qualitative Text Analysis. In Udo Kuckartz, editor, *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. SAGE Publications, London, 2013.

[33] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. *USENIX Security Symposium*, 2021.

[34] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. *USENIX Security Symposium*, 2024.

[35] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy*, 2020.

[36] Philipp Markert, Andrick Adhikari, and Sanchari Das. A Transcontinental Analysis of Account Remediation Protocols of Popular Websites. In *Symposium on Usable Security and Privacy (USEC)*, 2023.

[37] Philipp Markert, Leona Lassak, Maximilian Golla, and Markus Dürmuth. Understanding Users' Interaction with Login Notifications. In *ACM Human Factors in Computing Systems*, 2024.

[38] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. Stories from Survivors: Privacy & Security Practices When Coping with Intimate Partner Abuse. In *ACM Human Factors in Computing Systems*, 2017.

[39] Florian Nawrath. Quantitative Analysis of FIDO2 Client Support. *Who Are You?! Adventures in Authentication Workshop (WAY)*, 2021.

[40] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security*, pages 359–376, 2021.

[41] State of Passkeys. State of Passkey Adoption. https://state-of-passkeys.io/. Accessed 2026-06-10.

[42] Passkey Central. Design Guidelines. https://www.passkeycentral.org/design-guidelines/. Accessed 2026-06-08.

[43] Passkey Central. Glossary of Terms. https://www.passkeycentral.org/resources-and-tools/glossary-of-terms#synced-passkey. Accessed 2026-06-10.

[44] Passkey Central. Passkey Types. https://www.passkeycentral.org/introduction-to-passkeys/passkey-types. Accessed 2026-06-10.

[45] Carolina Ortega Pérez, Alaa Daffalla, and Thomas Ristenpart. Encrypted Access Logging for Online Accounts: Device Attributions without Device Tracking. *USENIX Security Symposium*, 2025.

[46] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Wouter Joosen, et al. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. *Network and Distributed System Security*, 2019.

[47] Bernhardt Ramat, Dave Kartchner, and Kent Seamons. A Systematic Analysis of the Passkey User Experience. In *Symposium on Usable Privacy and Security*, 2025.

[48] Lana Ramjit, Natalie Dolci, Francesca Rossi, Ryan Garcia, Thomas Ristenpart, and Dana Cuomo. Navigating Traumatic Stress Reactions During Computer Security Interventions. *USENIX Security Symposium*, 2024.

[49] Elissa M Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *IEEE Symposium on Security and Privacy*, 2019.

[50] K Andrew R Richards and Michael A Hemphill. A Practical Guide to Collaborative Qualitative Data Analysis. *Journal of Teaching in Physical Education*, 37(2):225–231, 2018.

[51] Sena Sahin, Burak Sahin, and Frank Li. Was This You? Investigating the Design Considerations for Suspicious Login Notifications. *Network and Distributed System Security*, 2025.

[52] Tobias Schnabel, Paul N Bennett, Susan T Dumais, and Thorsten Joachims. Using Shortlists to Support Decision Making and Improve Recommender System Performance. *World Wide Web Conference*, 2016.

[53] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. "My religious aunt asked why I was trying to sell her viagra": Experiences with Account Hijacking. In *ACM Human Factors in Computing Systems*, pages 2657–2666, 2014.

[54] Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy. In *ACM Human Factors in Computing Systems*, 2025.

[55] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *IEEE Symposium on Security and Privacy*, 2021.

[56] W3C. Web Authentication: An API for Accessing Public Key Credentials – Level 2. https://www.w3.org/TR/webauthn-2/, 2021. Accessed 2025-05-28.

[57] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A framework for unifying at-risk user research. *IEEE Symposium on Security & Privacy*, 2022.

[58] WhisperTranscribe. Transcribe your audio with Whisper AI. https://www.whispertranscribe.com/. Accessed 2026-06-09.

[59] Brandon Willis-Arnold, Paul Vickers, and James Nicholson. Are Passkeys the Key? Older Adults' Perceptions of Passwordless Authentication. In *European Symposium on Usable Security (EuroUSEC)*, 2025.

[60] Tarun Kumar Yadav and Kent Seamons. A Security and Usability Analysis of Local Attacks Against FIDO2. *Network and Distributed System Security*, 2024.

A Appendix

A.1 Condensed study protocol

We provide a condensed version of our study protocol with example questions for a single service; instructions and questions were similar for other services. Besides the initial and wrap up questions, the study procedure for local residents, students, and consultants was similar.

A.1.1 Initial questions (all participants)

Are you familiar with passkeys? Please explain.
Are you familiar with (mention services in the study)?
Have you used biometric authentication (e.g., Touch ID)?
Are you a Mac user or have been in the past?

Initial questions (consultants)
How long have you been a volunteer at (clinic)?
When serving clients, how often does account security come up?
Have passkeys come up in your client cases? Please explain.

A.1.2 Warm up activities (LinkedIn)

- Open new Chrome browser window
  Navigate to linkedin.com/login
  Sign-in to account using the credentials provided
- **Set up passkey on the account as an alternative to the password you just used to sign in**
  HINT: Do you know where to find the interface to set up a passkey on LinkedIn?
  HINT: Navigate to the profile icon on the top right
  HINT: Go to "Settings & Privacy → Sign in & security"
  HINT: Do you see the passkeys option?
  HINT: Click on "Create a passkey" and follow instructions if any to configure a passkey on the account
  HINT: Enter device password if required
- What do you think about the process of creating a passkey?
  How will you login to this account in the future?
  Was it easy/difficult completing this task?
- **Now we want to log in to the account using the created passkey instead of the password**
  Log out of your current session
  Close browser window and open new browser window
  Navigate to linkedin.com/login
  Sign-in to account using a passkey
  Can you explain what just happened?

A.1.3 Main study tasks (Google)

You have a friend/client who is trying to understand what is going on in their account and they need your help. They suspect there might be some unauthorized access where someone accessed their account without their knowledge or permission. They received email notifications indicating login alerts just like this one [show email] and this one [show alert] indicating a new passkey was added to their account. They do recall adding a passkey but don't remember when that occurred. They use a Mac computer.

- Open a new browser window; navigate to accounts.google.com
  Log in to Google account using the credentials provided
- **Investigate what might be going on**
  HINT: Do you want to take a look at the Gmail alerts?
  HINT: Is there a way to investigate these alerts further?
  HINT: Maybe go into Manage your google account → Security. Is there any info in there that can help?
  HINT: Can you tell which devices accessed the account?
  HINT: If you sign out any of these devices, would this prevent this device from logging in again?
  HINT: Can we figure out how many passkeys they have configured associated with this account?

Re-securing the account. Now we want you to ensure that the account is protected and secure from similar accesses in the future. We'd like you to reason through what actions you took before or plan to take here on this interface to secure the account.

- **Password reset**
  What does this mean?
  Do you think whoever had access to your friend's account has now lost this access following [action]?
  What about your friend, can they still access their account?
  Is this sufficient or is there anything more we can do?
  HINT: Have you checked passkeys on the account?
  HINT: Is there a way to tell who logged into the account?
  HINT: Should we check the configured recovery information?
- **Remove passkeys**
  What does this mean?
  Do you think whoever had access to your friend's account has now lost this access following [action]?
  What about your friend, can they still access their account?
  Is this sufficient or is there anything more we can do?
  HINT: Have you considered performing a password reset?
  HINT: Is there a way to tell who logged into the account?
  HINT: Should we check the configured recovery information?
- **End sessions**
  What does this mean?
  Do you think whoever had access to your friend's account has now lost this access following [action]?
  What about your friend, can they still access their account?
  Is this sufficient or is there anything more we can do?
  HINT: Have you considered performing a password reset?
  HINT: Have you checked passkeys on the account?
  HINT: Should we check the configured recovery information?
- **Recovery (Google)**
  What does this mean?
  Do you think whoever had access to your friend's account has now lost this access following [action]?
  What about your friend, can they still access their account?
  Is this sufficient or is there anything more we can do?
  HINT: Have you considered performing a password reset?
  HINT: Have you checked passkeys on the account?
  HINT: Is there a way to tell who logged into the account?

A.1.4 Wrap up (all participants)

Do you think passkeys are secure?
Would you use passkeys for your personal accounts instead of passwords? Why or why not?
What concerns do you have?
Do you have feedback about your experiences today?
Is there anything else you'd like to tell us?

Wrap up (consultants)
How similar is your experience today with the work that comes up with clients? Please explain.
What do you think are going to be the biggest challenges for clients once passkeys become more prevalent?
What would have been more helpful overall? Please explain.
What is helpful guidance & resources for consultants to help them investigate similar incidents?

Structural codes	Open codes	
lack of passkey experience	passkeys as 2FA	passkeys replacing 2FA
prior passkey experience	passkeys as biometric authentication	confusion between passkeys and 2FA
	confusion whether biometric authentication is a passkey	passkeys linking account to device
	logging in without password	platform prompts for passkey creation
	incorrect understanding of passkeys	familiarity with study device
	familiarity with biometric authentication	
lack of account security experience	use of 2FA	proactive security measures
prior account security experience		
experience setting up passkey	difficulty locating/navigating ASI	prompts for researcher help
experience logging in with a passkey	confusion about whose Touch ID to use	confusion logging in on a different device
	confusion about ASI content	decides to keep system defaults
	annoyance with security checks	incorrect study setup
	user relies on prior security behavior/understanding	suggests researching task info
	understanding of passkey creation pop-up	unsure whether biometric identification is required
	confusion signing in without any prompt	confusion about which password to input
investigating security notifications	prioritizing security tasks/actions	examine email alerts/notifications
investigating the incident	ask about friend's sign-in behavior	arousing suspicion
steps to secure account	ask about friend's password use/reuse	password reset signs out devices
overall experience with service	understanding secure your account ASI	reasoning about attacker's access
	ask whether friend's gmail account has sensitive info	turn off skip password
	understanding of skip password ASI	understanding of help screen ASI
	check phone number on account	researcher provides hints
	understanding of security checkup ASI	ask about friend's recovery info
	suggests friend adds recovery info	remove adversarial recovery info
	confusion about no passkey option on wizard	suggests reporting incident
	remove adversarial session	remove adversarial passkey
	remove all entries on ASI for safety	suggests friend changes their password
	understanding of passkeys ASI	correct understanding of passkey authentication
	reset password	suggests adding biometric to device
	suggests logging out from all accounts	suggestions for improvements
	does not identify adversarial passkey	suggests creating new passkey
	suggests turn on 2FA	lack of confidence
	suggests checking browser security	suggests checking iCloud account access
	suggests checking credentials on iCloud account	ask about abuse context
	participant references CETA guides	expresses lack of CETA guides/resources
	reason about actions/safety planning	express safety concerns
	password reset remove/reset passkey	phone number safety concerns
	forget about passkeys ASI	express concern about forgetting some actions
	express lack of familiarity/knowledge	document suspicious login/activity
overall experience with both services	comparison between services	participant prefers 2FA to passkeys
	perception of account security status	perception of usability
	perception of passkey security	challenges with passkey adoption and use
	suggestions for improvement	

Figure 7: The codebook consisting of 11 structural codes and 82 open codes used in our qualitative analysis.

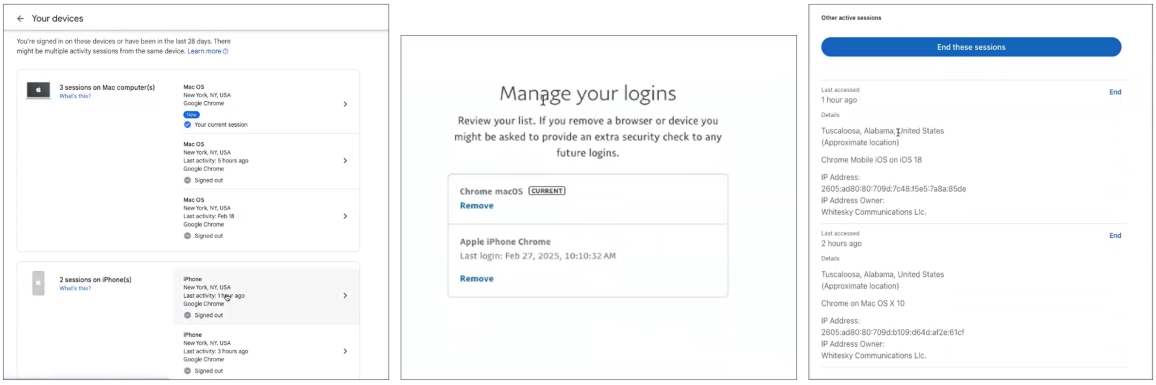

Figure 8: The sessions ASIs as shown on Google, PayPal, and LinkedIn. All account information shown belongs to a test account.

Participant	Gender	Age	Technical Knowledge	Profession	Service (1)	Service (2)
G1	Female	75–80	Little/no technical background	Social worker	Paypal	Google*
G2	Female	75–80	Little/no technical background	Physician	Paypal	LinkedIn*
G3	Male	30–34	Some computer courses	Coordinator	LinkedIn*	Google
G4	Female	65–69	Some computer courses	Retired	LinkedIn	Google*
G5	Female	40–44	Some computer courses	Finance	Paypal*	LinkedIn
G6	Male	25–29	Some computer courses	Attorney	Paypal	LinkedIn*
G7	Female	55–59	Some computer courses	Volunteer	Paypal*	LinkedIn
G8	Female	70–74	Some computer courses	Public relations	LinkedIn*	Google
G9	Female	65–69	Some computer courses	Retired	LinkedIn	PayPal*
G10	Female	45–49	Some computer courses	Business manager	Google*	PayPal
G11	Female	65–69	Some computer courses	Actor	PayPal	LinkedIn*
G12	Female	50–54	Some computer courses	Self-employed	linkedIn	PayPal*
G13	Female	30–34	Technical degree	Urban planner	LinkedIn	Google*
S1	Female	18–24	Little/no technical background	Student	Google	Paypal*
S2	Female	25–29	Some computer courses	Student	Google*	–
S3	Female	25–29	Some computer courses	Student	Paypal*	LinkedIn
S4	Male	18–24	Some computer courses	Student	Google	LinkedIn*
S5	Female	25–29	Technical degree	Student	Paypal*	LinkedIn
S6	Female	18–24	Technical degree	Student	Google	LinkedIn*
S7	Male	30–34	Technical degree	Student	Paypal	Google*
S8	Female	18–24	Technical degree	Student	LinkedIn*	Paypal
S9	Female	25–29	Technical degree	Student	Google*	Paypal
S10	Female	18–24	Technical degree	Student	Google*	LinkedIn
S11	Non-binary	25–29	Technical degree	Student	Google	Paypal*
C1	Female	20–24	Some computer courses	Student	Google	PayPal*
C2	Male	35–39	Technical degree	Student	Google	–
C3	Male	25–29	Technical degree	Research engineer	LinkedIn*	Paypal
C4	Male	25–29	Technical degree	Security engineer	LinkedIn*	Google
C5	Male	50–54	Technical degree	Program coordinator	LinkedIn*	–
C6	Female	25–29	Technical degree	Data engineer	PayPal*	Google
C7	Female	25–29	Technical degree	Student	PayPal	Google*

Figure 9: Self-reported participant demographics including participant number, gender, age, profession, technical knowledge, and the services each participant used during the study. Participants who are students are labeled as (S), those from the general population as (G), and experts/consultants as (C). An * indicates that a device configuration with Touch ID has been used to complete the tasks for the service. If absent, this indicates that the device has been configured with a password and no Touch ID.