Understanding Users' Interaction with Login Notifications

Philipp Markert
Ruhr University Bochum
philipp.markert@rub.de

Leona Lassak
Ruhr University Bochum
leona.lassak@rub.de

Maximilian Golla
CISPA Helmholtz Center for Information Security
golla@cispa.de

Markus Dürmuth
Leibniz University Hannover
markus.duermuth@itsec.uni-hannover.de

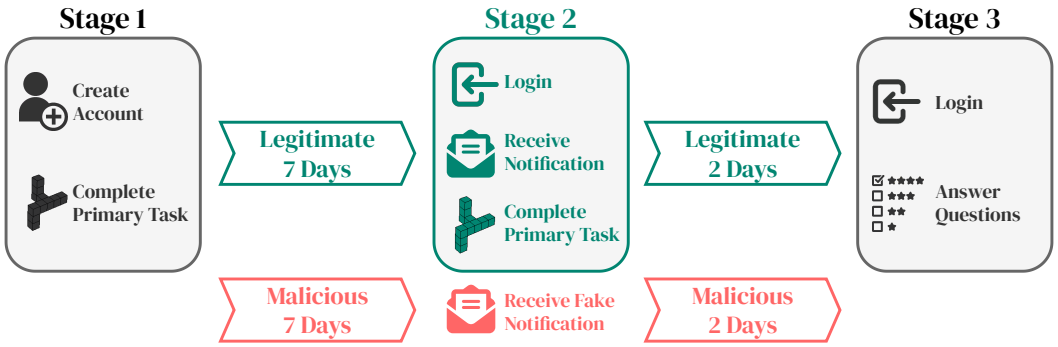


Figure 1: Structure of the user study (n = 229). After 7 days, participants in the legitimate treatment were invited to return to Stage 2 and received a notification after logging in. The malicious group received a notification without actually signing in to mimic the scenario when an unexpected login occurred. Before the final stage, we gave participants 2 days to react.

ABSTRACT

Login notifications intend to inform users about sign-ins and help them protect their accounts from unauthorized access. Notifications are usually sent if a login deviates from previous ones, potentially indicating malicious activity. They contain information like the location, date, time, and device used to sign in. Users are challenged to verify whether they recognize the login (because it was them or someone they know) or to protect their account from unwanted access. In a user study, we explore users' comprehension, reactions, and expectations of login notifications. We utilize two treatments to measure users' behavior in response to notifications sent for a login they initiated or based on a malicious actor relying on statistical sign-in information. We find that users identify legitimate logins but need more support to halt malicious sign-ins. We discuss the identified problems and give recommendations for service providers to ensure usable and secure logins for everyone.

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642823

CCS CONCEPTS

• **Security and privacy → Authentication**; **Usability in security and privacy**.

KEYWORDS

notification, email, authentication, risk-based authentication, password change

ACM Reference Format:
Philipp Markert, Leona Lassak, Maximilian Golla, and Markus Dürmuth. 2024. Understanding Users' Interaction with Login Notifications. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3613904.3642823

1 INTRODUCTION

Login notifications intend to inform users about recent sign-ins, to protect accounts from unauthorized access. Depending on the service, notifications are sent if the login occurred from an *unknown location* or *new device*, which may indicate malicious activity.

Notifications are often delivered via email and include details about the device (browser and OS), approximate location, date, and time of the sign-in. Users need to decide whether the reported login is legitimate or malicious and are recommended to change the password in case the login is unfamiliar. Logins can be confused to be malicious when users *share accounts*, and friends or family log in unknowingly. While the notification is intended to protect users and provide a feeling of security, it can also be perceived as burdening and overwhelming by requiring a decision based on technical jargon and highlighting negative consequences.

Previous work [41] focused on challenge-based notifications and studied incident-response information-seeking and mental models about attackers. In contrast, we focus on *granted access* notifications informing users about a recent sign-in and analyze users' comprehension, expectations, and reaction to the notification.

In this work, we collected and analyzed 72 login notifications sent by real-world services and developed a *baseline* notification that we employed in a user study. The structure of the study is shown in Figure 1. We disguised the study (n = 229) as a psychological test, and let users create an account they had to sign into during different stages of the study. Participants then either received a legitimate notification to their email upon signing in themselves (*Legitimate*) or unexpectedly received a notification prefilled with sign-in information a non-targeted statistical attacker would use after around one week (*Malicious*).

We sought to answer the following questions:

RQ1 *[Reaction & Comprehension] Which actions do users take in response to receiving notifications, and is resolving the situation a priority? Do users understand why they received the notification and which factors may have caused receiving it?*

We found that participants correctly understood that "a login" caused receiving the notification. However, they are unaware of or misinterpret the trigger and are thus unsure how to react appropriately, especially in the malicious case.

RQ2 *[Decision-Making & Execution] Do the state of the art notifications help users distinguish malicious and legitimate logins? Which information helps account owners with their decision, and do current notifications appropriately guide users in resolving the situation?*

Based on device and location, participants can correctly attribute notifications caused by their own logins, but they are confused when the notification is unexpected (Malicious) and struggle to identify the correct reaction even if (as it was the case in our study) all necessary information is provided by the notification.

RQ3 *[Perception & Expectation] How do login notifications make users feel? When do they expect notifications to be sent, and how does prior experience affect their decision?*

Notifications about malicious logins evoke (more) negative emotions, but participants who changed their password also felt empowered by taking action to protect their account. Interestingly, more than 90% of the participants expect services to send login notifications because it makes them feel protected.

Analyzing 72 real-world notifications revealed malformed login notifications and problematic anti-phishing advice. Our user study shows that login notifications contribute to account security, yet our results suggest room for improvement. We find that only 22% of the participants who should have changed their password to protect their account did. While participants appreciate when companies decide to monitor their accounts for incidents, services that send notifications for every, or almost every login in a "better safe than sorry" manner contribute to warning fatigue. We give clear recommendations for service providers to improve their notifications. While login notifications can help reinforce account security, protecting their accounts by identifying malicious logins should not be solely the user's responsibility.

2 RELATED WORK

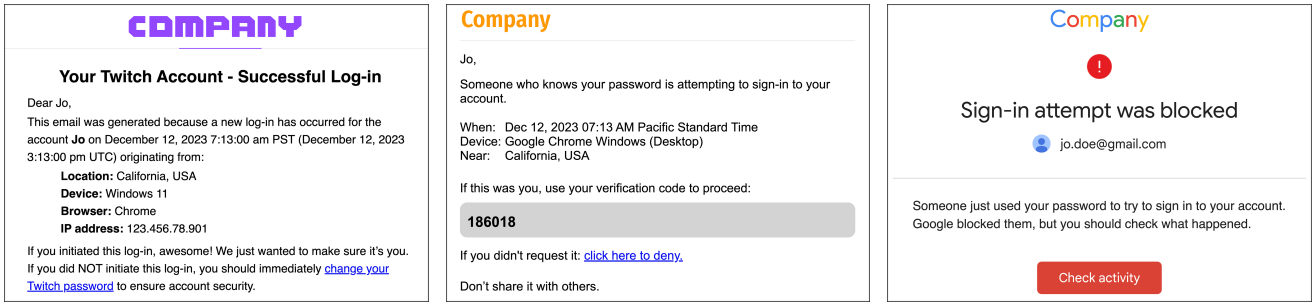
Next, we outline how our research extends related work.

2.1 Risk-Based Authentication, Login Notifications, and Account Sharing

Only few have studied login notifications in the context of risk-based authentication so far. A qualitative interview study (n = 67) by Redmiles [41] explores the account security incident response at Facebook by interviewing users who experienced a login incident. Unlike our work, Redmiles focused on "secondary authentication" notifications that prompt users to enter a code to regain access to their accounts after the account has been temporarily disabled due to suspicious account activity. Redmiles interviewed participants from 5 countries and reported on incident-response information-seeking and mental models about attackers. Regarding the notifications' effectiveness, Redmiles identified a lack of key information as problematic, e.g., the likelihood that the notification is about a legitimate threat. In contrast, our work studies a different type of login notification (see Section 3). It focuses on users' comprehension, expectations, and reaction to the notification, not on regaining access or mental models about attackers. Markert et al. [30] studied administrators' risk-based authentication (RBA) configuration. Administrators are responsible for the content of the login notifications users receive. The researchers found that the predefined notifications were often barely customized, and only a few administrators opted to disable them entirely. Also, participants lacked consensus about which information to include, indicating a knowledge gap. The administrators also wished for more context and explanation to prevent phishing attacks and pointed out the inaccuracy of IP-based location estimation. Our research helps identify key features of notifications that yield correct user comprehension. These results can help administrators align RBA configurations with users' expectations.

A study by Doerfler et al. [14] evaluated the efficacy of login challenges in preventing account takeovers, finding that up to 94% of phishing-rooted hijacking attempts and 100% of automated hijacking attempts can be prevented. This highlights the efficacy of login notifications in account protection and motivates the design of usable and understandably designed notifications. Still, Gavazzi et al. [17] found that only about 20% of popular websites employ risk-based measures. Wiefling et al. [62] showed that verification codes sent via email are the de facto standard for login challenges enforced by RBA. In a subsequent study, they demonstrated that providing this code in the subject of the notification can reduce the login time [63]. Using account login notifications, Wardle [61] measured the time it takes for leaked credentials to be abused by creating accounts on web services and intentionally leaking the credentials online. Adding to this literature, our research contributes insights on concrete user behavior, identifying key success features to deepen the understanding of the notifications' efficacy.

Shared passwords and accounts are of particular concern when it comes to login notifications. When multiple individuals access the same account, the intended account owner might find it challenging to maintain control and recognize logins. In this context, Obada-Obieh et al. [36] investigated online account sharing and found that users struggle to remember which accounts they share and with



(a) Granted Access from Twitch. **(b) Additional Challenge from Amazon.** **(c) Blocked Access from Google.**

Figure 2: Real-world examples of the three sign-in notification types (logos removed due to copyright, cropped, as of Dec. 2023).

whom. Similarly, Song et al. [49] studied account-sharing practices in the workplace and observed conflicts over simultaneous access and difficulties controlling access. While account sharing is out of scope in our research, it can have influence on users' understanding of notifications which we also address in our discussion.

2.2 Security Warning & Notification Design

There is a large body of literature on security warning design [11, 44, 59]. The most prominent applications are notifications in the context of TLS [3, 16], phishing [39], malware [4], and cookie banners under GDPR [13, 24, 35, 57], as well as warnings for developers [20] or for countering misinformation [23]. For user authentication, there is work on breach notifications [22, 64], password-reuse notifications [19, 53], notifications to promote the use of 2FA [18, 42], or FIDO2 [25], or protect users from using common PINs [29].

While considering the best practices for notification design in other domains is important, this is not the main focus of our study. However, in our notification analysis (see Section 3), we try to identify common design patterns.

3 LOGIN NOTIFICATIONS IN THE WILD

Login notifications intend to inform users about recent sign-ins and often include technical details such as the login time, used device, or approximate sign-in location. However, depending on the service, they are not sent for every login. While theoretically significant location or device changes trigger notifications, the probabilistic nature involving factors like sign-in history and user behavior makes it difficult to predict when notifications are sent. Some services sent notifications for every login; others only sent notifications in case of significant location and device changes, causing a higher risk level. For example, we noticed receiving fewer sign-in notifications if the affected account had two-factor authentication enabled. Interestingly, the cause for receiving a login notification is not always transparent to the user. We encountered multiple instances where notifications were not triggered by the account owner logging into their account. Most commonly, the phenomenon of unexpectedly receiving a login notification is related to shared accounts (i.e., Netflix or Amazon) [8] but is also known from third-party apps or services automatically signing into an account on behalf of the user [1, 40].

3.1 Notification Types

Based on the type of information they convey, notifications can be divided into three different types [30]. Examples of each of them are shown in Figure 2.

(1) **Granted Access:** The notification informs about *granted access*. Some services send such notifications for every sign-in, while others follow a risk-based approach.
(2) **Additional Challenge:** These notifications inform about a new sign-in attempt for which an *additional challenge* needs to be solved (i.e., insert a code or click a link).
(3) **Blocked Access:** The notification informs users about *blocked access*, which can happen because the risk-based authentication system ranks the sign-in as too risky.

For the remainder of this work, we focus on the first type, i.e., notifications informing the user about *granted access*. This popular notification type is deployed by well-known companies such as Alphabet [5], Amazon [6], Apple [10], Meta [31], and Microsoft [32]. Every organization can send this type, as it does not require an advanced risk assessment (i.e., basic logic and the ability to display login details are enough). Moreover, we limited our dataset to email-based notifications. While notifications can also be sent via other channels, e.g., SMS or push notifications, establishing them requires additional effort.

3.2 Analysis Method

To familiarize ourselves with the state of the art of granted access notifications, we collected over 90 login-related emails from real-world services by enumerating over 500 existing accounts. To trigger the notification, we signed in using the Tor browser, which is often classified as suspicious activity, and monitored our inbox. We also searched through account remediation pages [34] and community support forums [9] and learned about them via friends and colleagues. In both cases, we created an account on the service to obtain a notification. Our collection is limited to the top Tranco list [26] websites (as of June 2023), with about $\frac{1}{3}$ being in the top 100/1, 000/50, 000 respectively. The dataset includes popular websites from social media, streaming, shopping, finance, travel, email, and gaming services. Most of them are US-based (44) and the rest are from Europe (18) and Asia (10). The dataset is biased towards English notifications; few non-English notifications have been translated. The full list can be found in Appendix B and C.

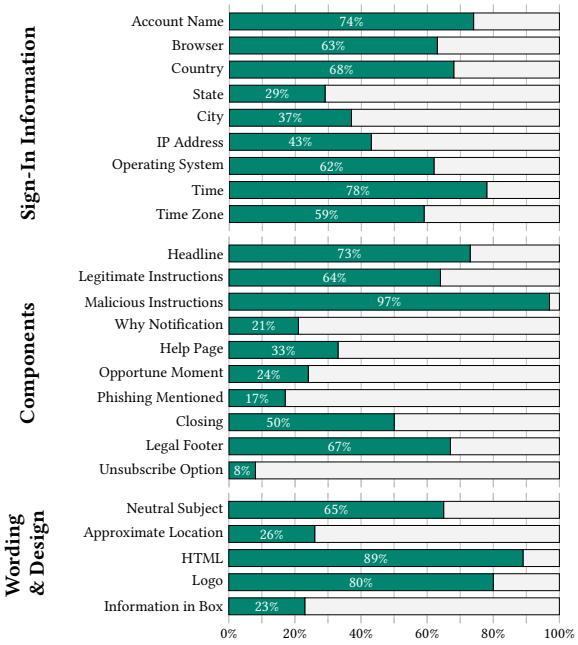


Figure 3: The information included in login notifications for granted access notifications (n = 72) sent by real-world services.

For the analysis, two authors categorized 72 emails as *granted access* notifications. The authors then independently analyzed the notifications based on a set of features derived following an iterative coding approach until no new codes and themes emerged [12, 55]. In particular, the authors checked which sign-in information the notification includes (i.e., login time, location, device), what the main components are (i.e., headline, malicious instructions), salient design and wording decisions (i.e., logo, highlighting of sign-in details, neutral language), and metadata such as sender and subject. Conflicts were resolved when they emerged by consensus discussion with a third member of the team (resulting in a hypothetical final agreement of 100%).

3.3 Findings of Notification Analysis

We summarize our findings in Figure 3. Please refer to Appendix B and C for the full details.

Sign-In Information As depicted in Figure 3, the majority of notifications included the login ❼ *Time* (78%), ❺ *Account Name* (74%), ❼ *Country* (68%), ❼ *Browser* (63%), and ❼ *Operating System* (62%). Less frequently, the notifications included the ❼ *Time Zone* (59%) or a login *IP Address* (43%). The small number of notifications, including the login *City* (37%) or *State* (29%), is explained by geographical differences between the U.S. and Europe. For our dataset, we collected notifications from different sources and observed that notifications for logins in the U.S. mostly reported the state. Notifications for logins from Europe often also included a city.

Components Most notifications made use of a ❹ *Headline* (73%) that was often (76%) different from the email subject. Another critical component were the instructions describing how users should

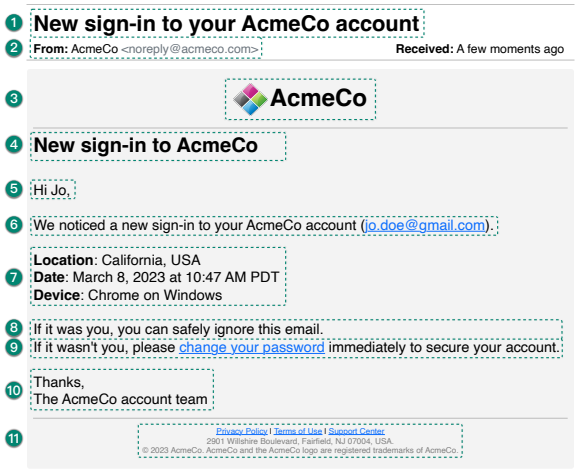


Figure 4: The *baseline* login notification, which we derived from (n = 72) real-world notifications. For our user study, we rebranded the text and the look to match the study website.

respond to the notification. While only 64% provided instructions in the ❽ *Legitimate* case, more than 97% explained how to react in the ❾ *Malicious* case if the user does not recognize the login. The large majority (66%) recommended changing the password. Fewer (high-ranked) web services included a button to report the login as malicious or legitimate on a separate web page (9%) displaying account remediation steps. Similarly, a small number (9%) suggested to visit the account activity page. Prominent among financial services was the option to contact support (4%). A dedicated *Why Notification* component was included in 21% of the notifications. It primarily creates context and explains to users why they received the notification. It often gives examples of legitimate (i.e., new device) and malicious causes ("someone unauthorized gained access") that might have triggered the notification. 33% included a link to a dedicated *Help Page* (note: *regular* support links in the email footer were not counted).

About 24% of the emails tried to use the *Opportune Moment* to tell the user about other options to secure their account (i.e., enabling 2FA). The dangers of *Phishing* and methods to double-check the legitimacy of the notification were mentioned in 17% of the emails, with the most prominent suggestion being not to click the "change password" link and instead sign in to the website by manually pasting or typing in the URL. About half of the notifications included a ❿ *Closing* (50%) text that often thanked the user and included the name of a "{service} account team." A footer with ⓫ *Legal* information was included in 68% of the emails, and an *Unsubscribe* link was present in 8% of the notifications.

Wording & Design Using affinity diagramming, we identified the wording of most email subjects as *Neutral* (65%), with a strong focus on "*New login to {service}*." In some cases, it is alarming (23%), like "*Security alert*" or a prompt (9%), like "*Please review this sign in!*." In two cases, it was a question (3%), e.g., "*Did you recently sign into {service}?*." Almost all emails (92%) referred to ❻ "your account" to emphasize the importance of the notification. A few services tried to address the inaccuracies of IP-based location estimation by

describing it as *Approximate* (26%). Most notifications (89%) were sent as *HTML* emails; the rest were sent in plaintext. For a "corporate look-and-feel," 80% of all notifications included a ❸ *Logo*, with an even split between a centered or left alignment. Interestingly, 23% of the emails displayed the sign-in information in a visually detached box, most likely to draw the user's attention to the login details.

Subject & Sender We identified three different types of email subjects: (a) The majority of email subjects (79%) did not include specific details and were relatively generic, e.g., "Your account has been logged into" (Tumblr). (b) A small fraction (15%) made use of login metadata, e.g., "New login to Twitter from {browser} on {OS}" (X, formerly Twitter). (c) Only a few (6%) included the account name, e.g., "{Name}, did you recently sign into Etsy?" (Etsy). Five services did not use an email sender name (display name).

Technical Details Throughout our analysis, we found numerous areas for improvement regarding the parsing and displaying of technical details such as location data, browser, and OS. We found incorrectly escaped HTML "Île-de-France" instead of "Île-de-France," empty placeholders, e.g., "Browser: N/A," and cryptic smartphone model numbers "SM-S908B/DS" instead of accessible names like "Samsung Galaxy S22." Operating systems were often reported with their full version number, e.g., "iOS 17.1.2." We even found four notifications that included the raw User-Agent string.

Questionable Advice Some notifications included information about phishing, which does not always align with state of the art recommendations on those topics. Questionable advice is given by X (and three other major services), which suggests that the presence of a padlock icon will "let you know a site is secure" and that users should check for the presence of "https://" and "{domain}" in the hyperlink. Similarly, Amazon suggests better copying and pasting the "It wasn't me"-link into a browser "just to be safe." Spotify advises users to verify that the email was sent from "@spotify.com," which is only expedient if the email server and DNS are configured correctly. In line with the latest research, PayPal's advice [38] explicitly mentions to "not rely on the padlock symbol and the 's' in HTTPS". Interestingly, LinkedIn added a security footer message [28] to their login notification that includes the affected account name and corresponding profession to authenticate official emails.

3.4 Selecting a Representative Notification

For our user study (see Section 4), we aimed to use a notification that closely resembles the state of the art of real-world login notifications. Our data-driven *baseline* (see Figure 4) includes all components used by at least 50% of the analyzed notifications, leading to 11 components comprising the notification: It uses a neutral subject and a slightly modified headline. We adjusted the email sender, opted for an HTML email, and included a logo. We also mentioned the affected account name and referred to "your account." We listed the most popular sign-in details and legitimate and malicious instructions with actions for users to take after receiving the notification. Our study sample was U.S.-based, so we included the ❼ *State* in the sign-in details. The email also had a closing and footer with fictional legal information.

By deriving a representative notification, we could test users' general understanding , their reaction, and their perceptions. While the majority of the 72 collected notifications included slightly fewer components (57% include at least 9 components) we still decided to include all 11 components in the *baseline* to be able to make a statement about each components' usefulness in an idealized scenario. Components omitted in real-world notifications most often were the ❺ *Account Name*, e.g., "Hi {Account Name}," and the ❿ *Closing*, e.g., "Thanks, The AcmeCo account team."

4 METHOD

The following section outlines the protocol, treatments, recruitment, ethics, and limitations of our user study.

4.1 Study Protocol

Participants in this study should receive a notification for a concrete account. To resemble a real-world setting, the protocol had to fulfill four criteria: (1) A *real account* gets created, (2) participants are *unaware* that the study is about login notifications, (3) participants receive the notification in their *personal email account*, (4) and reactions to login notifications are *measurable*.

For this, we invited participants to take part in a multi-stage study about changes in the cognitive ability of mental rotation over time [48, 58]. This framing allowed us to inform people about the length of the commitment without revealing our interest and justified the account creation on our website. The task was also a strong cognitive distractor that prevented participants from paying too much attention to the notification and authentication task.

We used two treatments, and the baseline notification (see Figure 4) was adapted to the branding of our study's website: The legitimate group (n = 110) received a notification only after they logged in. The location, date, and device in the notification were derived from the metadata of their login. The malicious group (n = 119) received a notification unexpectedly at a time when they had not interacted with the account for multiple days. This resembled a login attempt by a malicious actor. The location ("California, USA") and device ("Chrome on Windows") were selected to have the highest statistical chance of matching any user in our U.S.-based sample [50, 51, 56]. Trawling (untargeted) attackers would likely use a similar configuration when signing into the account, to minimize the risk of being detected by RBA systems [14]. Because the details are intentionally chosen to closely align with common user configurations – just like in real life – some participants in our study (10 of 119) also matched these details, making it more challenging for them to recognize that the notification is a result of a malicious login. We did not allow mobile devices and recorded if the email was opened via a small self-hosted image, which itself was invisible in the email.

Stage 1: The first page on the study's website explained the mental rotation test. To ensure participants regularly check their email and understand the value of the account, they saw a privacy notice after giving their consent, which highlighted the importance of the account as it would be used to store the study data and email address. It also explained that the email would be used to send invitations to subsequent stages, and the compensation would be in the form of Amazon gift cards. After the account creation, participants solved 5 mental rotation tests and provided demographic information (**MD1**–**MD4**). At the end, participants in the legitimate treatment

were informed that invitations to Stage 2 would be sent in approx. 7 days; in the malicious group, the note said 14 days.

Stage 2: After 7 days, participants in the legitimate group received an email inviting them to return to our website for another mental rotation test. To do so, they had to log into their account, which triggered a notification. Participants in the malicious group expected their next email after 14 days. However, to imitate a malicious login, we sent them an (unexpected) login notification filled with our statistical sign-in data 7 days after they completed the first stage.

Stage 3: For the legitimate group, invitations to the final Stage 3 were sent 48 hours after they completed Stage 2; in the malicious group, 48 hours after they received a notification for a login they did not initiate. We chose this time frame to give participants enough time to react. After logging into Stage 3, participants were debriefed and told about the purpose of the study. This was followed by our questionnaire (see Appendix A). From then on, the notification we sent was shown on the left side of their screen for reference.

(1) *Email:* First, we asked if participants remember receiving the notification (**MQ0**); if not, they were forwarded to a different section (see Appendix A). Participants for whom we received a read receipt or who changed their password skipped this question.
(2) *I-PANAS-SF:* To learn about the feelings and emotions in reaction to the notification, in **MP** we utilized the Positive and Negative Affect Schedule (I-PANAS-SF) [54].
(3) *Reaction:* Next, we asked how thoroughly participants read the notification (**MQ1**) and how and why they chose to react to it (**MQ2a**–**MQ3a**). Participants who changed their password were specifically asked about any other actions (**MQ2b**–**MQ3b**).
(4) *Content & Design:* To better understand the reactions, **MQ4** asked about influencing factors like metadata, content, and design. **MQ5** specifically asked about the helpfulness of the account name, location, date, and device.
(5) *Time & Location:* **MQ6**–**MQ10** investigated the time when and location where the notification was read. With **MQ7**, we verified if the location, which had been derived automatically, was actually accurate or could have led to confusion, and **MAC2** was an attention check.
(6) *Comprehension & Expectation:* With **MQ11**, we captured if participants understood why they received the notification. **MQ12** and **MQ13** asked participants when they expect real companies to send notifications.
(7) *Prior Experience:* We concluded with three questions covering negative experiences with security incidents (**MQ14**), as well as their opinion on regular (**MQ15**) and event-driven password changes (**MQ16**).

4.2 Recruitment & Demographics

We used the panel provider Cint for the recruitment of the study. They are a comparable platform to larger providers such as Respondi and Kantar, operating numerous sub-panels for different locations across the globe. Criteria for participation were being 18 or older, being willing to participate in deception studies, and being US-based. For Stage 1, we recruited 625 participants, about 3 times more than the desired number of completions as recommended by the panel provider. Our a priori power analysis determined the minimum sample size to be $N = 100$ per group - in order to achieve 80% power for detecting a medium effect (Cohen's $d = .4$), at a significance criterion of $\alpha = .05$. After filtering 12 participants who failed the attention check (**MAC1**), 613 participants remained. At the end of Stage 3, we had 252 completions. This high number of dropouts is almost exclusively attributed to participants who did not return after the first stage of the study. Lastly, we removed 23 participants who provided unrelated answers or failed the second attention check (**MAC2**) for a final number of $n = 229$. Stage 1 took, on average, 2.5 minutes and was compensated with $3.00 USD. Stage 3 took, on average, 6 minutes and was compensated with $4.00 USD. Participants in the legitimate group received an additional $1.00 USD for the completion of Stage 2, which took 2 minutes on average. Table 1 shows the participants' demographics. Regarding the demographics, we observe a shift towards male-identifying participants (65%). The age distribution is diverse, ranging from 14% to 21% for all age groups between 25 and 74. Most participants had a high school (33%), Bachelor's (26%), or trade degree (23%) and did not have a technical background (82%).

Table 1: Participants' demographics.

	Male		Female		Other		Total	
	No.	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
Age	149	65	79	34	1	0	229	100
18–24	4	2	6	3	0	0	10	4
25–34	17	7	15	7	0	0	32	14
35–44	27	12	17	7	0	0	44	19
45–54	24	10	15	7	0	0	39	17
55–64	35	15	13	6	0	0	48	21
65–74	31	14	11	5	0	0	42	18
75+	11	5	2	1	1	0	14	6
Education	149	65	79	34	1	0	229	100
High School	47	21	31	14	0	0	78	34
Trade	39	17	12	5	1	0	52	23
Bachelor's	34	15	24	10	0	0	58	25
Master's	23	10	10	4	0	0	33	14
Doctorate	4	2	2	1	0	0	6	3
Prefer not to say	2	1	0	0	0	0	2	1
Background	149	65	79	34	1	0	229	100
Technical	10	4	25	11	0	0	35	15
Non-Technical	134	59	53	23	1	0	188	82
Prefer not to say	5	2	1	0	0	0	6	3

4.3 Ethical Considerations

At the time we conducted the study, none of the authors worked at an institution with an IRB. However, we carefully followed the guidelines provided in the Menlo Report, including a risk-benefit evaluation, developing the protocol with peers familiar with conducting user studies and following the legal requirements. The study included deception and sent a login notification to participants' personal email accounts, which could have caused more anxiety than just imagining to have received a login notification.

To protect participants from unnecessary risks, we implemented several safeguards: i) Our panel provider offered the study only to

participants who agreed to studies that might involve deception. ii) The affected spatial reasoning account had no subjective value to the participants and only allowed to access the email address. Participants might have been concerned about their answers to the questionnaire, which, in their impression, were also tied to the same account. However, at the time the malicious login notification was sent, participants had not been asked any sensitive or personal questions yet. iii) All participants (including those who decided to withdraw early or drop out) have been debriefed. In particular, we told them about the true purpose of the study, and in case they belonged to the *malicious* treatment that "This sign-in did not take place; at no time was your account at risk," and asked them whether they prefer to leave the study early (while being fully compensated), which nobody did. iv) We provided an optional contact address and feedback form that we closely monitored (we have not received any complaints). v) We shared a website (also accessible from outside the study) that participants could visit and share to learn more about login notifications and related account security measures. vi) We created a distinct email account for sending notifications that applied all state of the art email security features, which can prevent email spoofing attacks. We also allowed participants to reply to the notification and ask for assistance. Finally, all email addresses were only stored encrypted, separated from the study responses, and were deleted after the study in accordance with progressive data protection laws like GDPR and CCPA.

4.4 Limitations

For this study, we relied on a controllable artificial account setting, which might lack ecological validity. However, only 7 participants mentioned the non-real-world setting as a reason for not reacting to the notification. We expect more participants to change their password if the notification was sent for an account with a higher subjective value. We did not control for VPN usage, which might also slightly influence results in real-world settings. Like many human-subject studies, there is the potential for a bias in question-wording. To circumvent this, we piloted the study and tried to keep the questions short and clear. The full survey instrument can be found in Appendix A. Lastly, we only recruited US-based participants, which can have culture-based influences on the results.

5 RESULTS

Next, we present the results of the study. The qualitative coding was done by two of the researchers, who started by separately coding 10% of the answers. Afterward, they agreed on a joint codebook (see Tables 4–6 in Appendix D) and used it to code the remaining 90%. The agreement between the two coders was high ($\kappa = 0.77$). When quoting individual participants, e.g., L61-N, one can derive their treatment (***L****egitimate* or ***M****alicious*) and password change behavior (***N****o Change* or ***C****hange*). Similarly, we use color codes like A *Was Me* corresponding to Figure 5 within the text when referring to participants' explanations.

5.1 RQ1: Reaction & Comprehension

Reaction General Out of the total 229 participants, 48 participants, 23 in the legitimate and 25 in the malicious treatment, F cannot remember the notification. Still, for 26 of them, we received a read receipt, so they must have at least opened the notification. Among

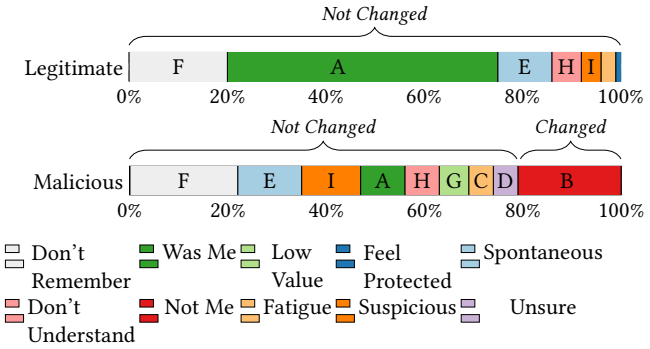


Figure 5: Breakdown of treatments into participants who *have* or *have not* changed their password and their reasoning.

the large majority of participants who saw the notification (181; 79%), it was very rare that they completely ignored its content. In response to **MQ1**, just 6% said that they only read the subject. About 90% read the notification completely or at least skimmed the body.

Reaction Legitimate No participant in the legitimate treatment changed their password. As shown in Figure 5, the majority of participants (60; 55%) explained their reaction in response to **MQ3b** by saying A it was their own login. Another 12, i.e., 11%, described it as a E *spontaneous* reaction, e.g., M42-N: "I just didn't think much of it." We also see that some participants do not understand what the notification is saying, which was the driving reason for H 6% (6) to ignore it. Finally, we recorded themes of participants who were I *suspicious* about the legitimacy of the notification (4; 4%), felt C *fatigued* (3; 3%), or J *protected* (3; 3%).

Reaction Malicious In the malicious group, only 26 of the 119 participants, i.e., 22%, changed their password; all of them correctly saying B it was not them logging in. The reasons given by the other 78% (93) in response to **MQ3b** for not changing their password mostly overlapped with responses given by participants in the legitimate treatment: E *spontaneous* reaction (15; 13%), notification looked I *suspicious* (14; 12%), or was H *not understood* (8; 7%), C being *fatigued* (6; 5%) or D *unsure* how to react (6; 5%). Finally, there are two justifications that are owed to the study design: participants describing they A logged in themselves although they did not (11; 9%), likely an example of social desirability, and those who assigned a G low value to the account (7; 6%):

"*This account has no value, it was not a streaming or banking account or amazon account*" (M74-N)

This justification can be reasonable, but users need to keep in mind that an attacker can also target other accounts that verbatim or partially reused the compromised password [37].

Comprehension When asked why they have received the notification (**MQ11**), 85% (93) in the legitimate and 79% (94) of the participants in the malicious treatment realized that a new login happened. Very few who gave a different explanation believed it was a phishing attempt (3; 1%), most simply did not understand what has happened at all (39; 17%):

"*I had no idea, which is why I deleted it.*" (M93-N)

Those in the legitimate treatment who mapped the notification to a new login usually perceived it as a simple info email (42; 38%),

followed by those who saw it as a prompt to review the login (28; 26%). Fewer responses (15; 13%) explicitly mention that the login must have been abnormal. In the malicious treatment, most participants who understood that a new login happened described that they were (potentially) compromised (46; 36%). Another 19% (22) perceived it as an informative but non-critical email. The remainder (13; 11% each) either mentioned that the system rated the login as unusual or wants them to review the login.

We observed a low comprehension of what might have caused the notification, especially in the malicious group. One explanation might be the temporal connection between logging in and receiving the notification. From **MQ6**, we know that about two-thirds read it immediately, and most of the others within a few hours. Hence, participants in the legitimate treatment had indeed a connection, and their understanding was substantially better. This influence of contextual factors was already observed by prior work on warning design [20, 44] and could be achieved by including a *Why Notification* section. Some websites already do (see Section 3), and we will elaborate on this in the discussion.

Summary About 80% saw the notification. Participants in the legitimate treatment who triggered it themselves understood what it was telling them and reacted accordingly. In the malicious treatment where participants did not have this context, only 22% changed their password, and they had more difficulties explaining the circumstances. Hence, the number of password changes in the malicious treatment is substantially lower than expected.

5.2 RQ2: Decision-Making & Execution

We now focus on the decision-making process to understand if participants struggle with determining whether it was them or not, especially for malicious logins.

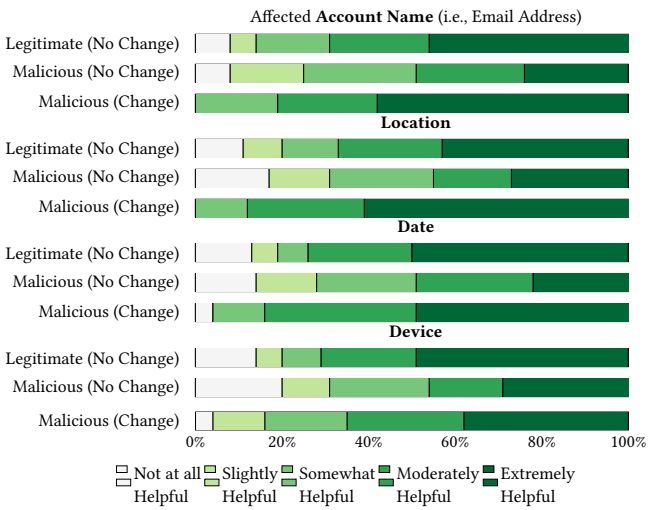


Figure 6: Helpfulness of the details for deciding (MQ5).

Helpfulness of Login Information Foremost, we wanted to get insights into the helpfulness of the displayed login information (**MQ5**). In Figure 6, we can see that for those in the *Legitimate* and *Malicious (Change)* group, all information is about equally helpful: 22–35% find the different types *moderately* and 38–62% even *extremely* helpful. Participants in the *Malicious (No Change)* group, in contrast, appear to have a less distinct opinion as ratings are more equally distributed, ranging from 8–30%. A Kruskal-Wallis test also showed significant differences for all types of information when comparing *Malicious (No Change)* to *Legitimate* and *Malicious (Change)*, respectively. This uncertainty of participants in the *Malicious (No Change)* group regarding the displayed information aligns with the previous section, where we found that those participants misattributed or did not understand the cause of the notification.

Effect of Other Factors In addition to the already-known influence of the login information, we were also interested in the effect of other exogenous and endogenous factors (**MQ4**). Figure 7 gives an overview. Generally speaking, the content (e.g., provided information, instructions, wording) and prior experience in dealing with such notifications had the highest effect on participants' reactions, with 42% expressing a *moderate* or *major effect* on average. Followed by that is the metadata (e.g., sender, subject, time of arrival) with 29%. All other factors seemed to have a weaker influence, with only 18% (appeared to be phishing) to 23% (was expected) of the participants reporting a *moderate* or *major effect*.

When comparing groups, *Legitimate* is the one where most participants reported a factor having no effect. The *Malicious (Change)* group, on the other hand, is the one where participants describe the strongest influences of the factors. Using a Kruskal-Wallis test with Bonferroni-correction for pairwise comparisons, we found that metadata had a significantly higher effect for *Malicious (Change)* participants compared to *Malicious (No Change)* participants ($\chi^2(2) = 6.65, p < 0.05$). The same is true for the email content ($\chi^2(2) = 7.73, p < 0.05$). Thus, to nudge more users to change their password upon receiving potentially malicious login notifications, focusing on designing the content and metadata is vital.

Influence of Negative Experiences Overall, 30% of participants described falling victim to a security breach within the last two years (**MQ14**). In the malicious treatment, 42% of those who changed their password reported prior negative experiences. Only 32% of those who did not change their password said so. The difference is not statistically significant, $\chi^2(2) = 2.61, p = 0.271$, but suggests that prior breach experience increases the likelihood of users changing their password upon receiving a notification.

Summary When comparing login information side-by-side, we can conclude that all factors are equally essential. We also observed that the helpfulness of the information for the *Malicious (No Change)* participants is significantly lower, which further explains the issues of this group when determining what happened. Regarding other factors, the content of the notification, its metadata, and prior experience in dealing with it had the highest effect across all treatments. Negative experience tends to influence the reaction as well; other aspects appeared to be less crucial.

5.3 RQ3: Perception & Expectation

Perception The PANAS (**MP**) reveals that participants who changed their password feel more positive but also more negative. The average positive *affect* of the *Malicious (Change)* group is 15.0 (SD: 4.5) but only 11.6 (SD: 5.0) and 12.6 (SD: 5.6) for the *Malicious (No Change)* and *Legitimate*, respectively. Using a Kruskal-Wallis test (Bonferroni corrected), we were also able to confirm the significance between the two malicious groups, $\chi^2(2) = 8.29, p < 0.05$. For the negative *affect*, *Malicious (Change)* averages 9.8 (SD: 4.1), *Malicious (No Change)* 8.1 (SD: 4.3), and *Legitimate* 5.7 (SD: 1.6). Again, Kruskal-Wallis was used yielding significance between both malicious groups and *Legitimate* ($p < 0.01$); the comparison between the two malicious groups nearly did, $\chi^2(2) = 5.26, p = 0.0654$.

Expectation So far, the study showed that there is a substantial number of participants who have not changed their password although they should, some of them mentioning that it was a spontaneous reaction, which this fatigue may also explain. Hence, we used **MQ12** to learn when users expect to receive notifications. A majority of participants (151; 66%) expressed they want to receive notifications after suspicious account activity. On average, 60% want to be notified if a login takes place from a new device, 47% for logins from a new location, 31% if they have not logged in for a while, and 22% for logins that take place at an unusual time of the day. Only 9% want to receive a login for *every* login, and even fewer (9; 3%) do not want to receive login notifications at all.

Summary We can conclude that participants who changed their password felt both more positively and negatively, probably because they assumed some form of compromise but also had a sense of achievement after preventing it by changing the password. The other groups had lower scores, aligning with them not expecting any harm. We showed that participants expect services to send login notifications and can further specify this by saying that participants want to be notified after suspicious logins, logins from new devices, and logins from new locations. Fewer participants expect to receive notifications based on temporal deviations.

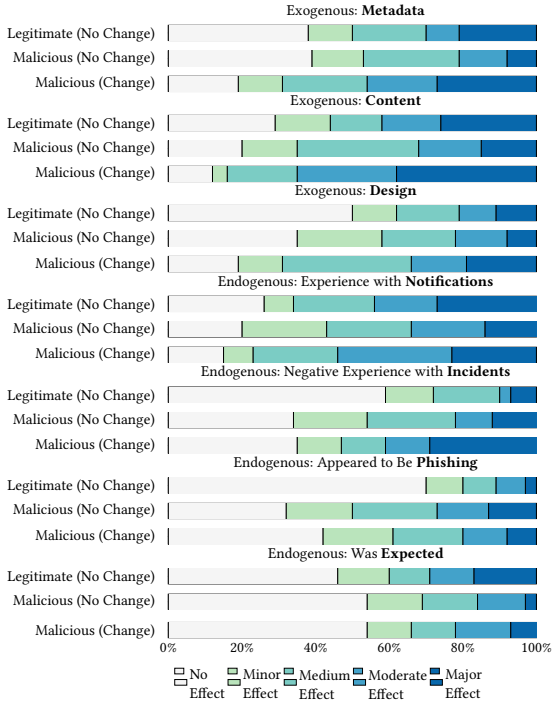


Figure 7: Influence of factors on participants reaction (MQ4).

6 DISCUSSION

Next, we discuss the takeaways and give recommendations.

6.1 Effectiveness of Login Notifications

We wondered if login notifications that many services use daily, achieve their goal of increasing the security of online accounts.

Effectiveness Depends on Trigger According to our findings, the notifications achieve what they intend—at least to a certain extent. In the malicious login case, we saw that only about 20% of the users in the study reacted to our *baseline* notification and changed their password. Hence, we conclude that login notifications can improve account security partially, as every password change can help to stop a malicious actor. However, at the same time, 80% of the participants in the malicious group who should have changed their password did not. While some participants might have decided not to change their password due to the study accounts' low value, it is still a high number, questioning the overall cost-benefit trade-off of the notifications.

Arguments against Notifications On the cost side of things, we found several participants being *annoyed*, which is in line with research on fatigue in the context of security warnings and notifications [3, 7]. Another argument against the notifications is that they shift the responsibility for account security away from the service provider onto the user. In a sense, such notifications can be perceived as *burdening and blaming* [21, 46]. If service providers which hold exhaustive records about a user's login history are uncertain, why should the user be able to determine the legitimacy of a login? It is fair to say that in some cases users may know better whether i.e., their location has changed. However, in real life with shared accounts [8], third-party apps and services that automatically sign in to an account [1, 40], or simply on busy days only few of us can realistically remember which accounts they used (note that we did not explicitly test these factors in our study). Thus expecting users to determine the legitimacy of a login better than a service provider is unfair. From a service provider's perspective, allowing logins and hedging them with a notification rather than blocking them makes sense; for them, it is the easiest "solution" to the problem. On a conceptual level, it all boils down to whether users should be made responsible for damages or if it should rather be the service provider's duty to implement robust security measures [27].

Arguments for Notifications Contrary to concerns about burdening users, it can be argued that users took the appropriate action in the legitimate case—namely, ignoring the notification. Our study showed that most *participants correctly followed the instructions* when prompted by a legitimate login notification and our qualitative results proved that they even correctly understand its meaning and cause. Additionally, some users *felt more protected*

and satisfied when receiving such notifications. According to their qualitative feedback, such notifications' reassurance contributes to a positive user experience and reinforces trust in the service.

6.2 Refining Notifications

As indicated before, research and development should focus on refining notification systems to ensure their maximum effectiveness and usability. Past examples in the warning design space, i.e., TLS warnings, have demonstrated how improved warning designs can increase comprehension and adherence and decrease click-through rates [16]. One approach to facilitate appropriate reactions may be to align notifications' implementations with users' understanding. As shown in Section 5, participants appear to expect and need contextual factors to determine what caused a notification. Especially, we saw significant differences in the helpfulness ratings of information between those in the malicious group, who changed their password, and those who did not.

While future research needs to investigate the exact root cause for this difference, we can certainly say that the information provided and users' ability to understand it correlates with their behavior in terms of password change. Malicious (No Change) participants, in particular, often misattributed or did not understand the cause of the notification—indicating that this information needs to be refined. Services could address this and adhere to users' expectations by including a distinct *Why Notification* component, e.g., by explicitly saying that a login happened from a previously unseen device. Our initial analysis of real-world notifications only found this contextualizing section in about 20% of the real-world notifications. Moreover, from a security standpoint, services need to provide more help than just suggesting to change the password. While password change is a first line of defense upon account compromise, it is by far not sufficient to ensure that the compromised account and other accounts are safe. Service providers should thus initiate a thorough remediation process, including expiring all sessions, reviewing third-party access, enabling 2FA, suggesting using a password manager, and checking related accounts [33, 60].

6.3 Expectation vs. Fatigue

Besides the correct reaction and understanding of notifications—user satisfaction with notifications is equally important. Fortunately, we found that more than 95% of the participants expect services to send login notifications, and only 3% do not want notifications to be sent at all, underlining an overall positive assessment. However, it is crucial to find a balance between sending them too often and too rarely. For service providers, sending notifications following a "better safe than sorry"-mentality may be tempting. Yet, for users, this leads to security warning fatigue [3, 15, 52]. This fatigue is most likely caused by unnecessary login notifications, i.e., those that do not convey a real risk teach users that all notifications are unimportant. The situation is aggravated by services like Etsy, GitLab, Mozilla, Tumblr, and others that send notifications for each and every login. We saw that over 90% did not want to receive a notification on every login, and 15% even explicitly expressed "fatigue." Thus, we strongly dissuade sending notifications on every login. Instead, they should only be sent if the service suspects malicious account activity. Concretely, the majority of the participants wants to be notified when a login takes place from a new device or location, and especially if a login appears "suspicious." Service providers can accomplish this with advanced logic provided by risk-based algorithms [62, 63]. Time-related notifications (i.e., a login after a long or at an unusual time) are less demanded. In favor of sparsity, time-related notifications should be omitted unless there is a concrete reason for suspecting malicious account activity.

6.4 Good Intentions & Questionable Advice

In the study, about 8% of the participants questioned the legitimacy of the notification or referred to it as phishing. Prior work explains how to best advise users on this topic [47], yet most of the 10 real-world notifications that include information about phishing do not follow the recommendations. While contradicting security advice, as well as no consensus among security experts about its prioritization, is nothing new in the community [43, 45], for us, it was surprising how potentially dangerous and obsolete some of the given advice is (see Section 3.3). For example, many large services like X (Twitter), Spotify, and Amazon portrayed the padlock icon of the browser as a type of trust and legitimacy indicator. While this is not only false, in early September 2023, Google removed the padlock icon with Chrome 117, as HTTPS should be considered the default state [2].

6.5 Recommendations

Based on our findings, we give some recommendations for service providers below.

Notify about Devices, Locations, and Suspicious Logins We advise against sending notifications after every login, mainly because some of our participants reported being annoyed by the frequency of real-world services sending notifications (see Section 5.2). Instead, we recommend that services send login notifications when a login takes place from a new device or location, and especially if a login appears "suspicious."

Describe What Happened What triggers a notification, e.g., an "unusual login," is often unclear to participants (see Section 5.1). Services could easily address this issue by explaining what triggered the notification, yet only 21% of the evaluated emails currently provide examples of common triggers (see Section 3.3). Explaining the circumstances would also help to create context, which is especially important when users receive unexpected notifications and struggle to assess the situation correctly.

Include Information in Metadata We found that the metadata is an influential factor, and 75% of the participants paid attention to the email subject (see Section 5.2). Hence, in addition to the most important information, the email subject should already provide context for deciding how to react. Currently, only 15% of our analyzed notifications make use of subjects like "New login to Instagram from {browser} on {OS}" (see Section 3.3). Similarly, websites should make use of the email sender's name so that recipients can quickly parse the information about the sender.

Specify Instructions Based on the findings of our email analysis (see Section 3.3), notifications should include instructions for both outcomes, i.e., legitimate and malicious logins. For the legitimate case, most services suggest to ignore the message. For malicious logins, the recommendation needs to prompt users to visit the

website and change or reset the password or, even better, initiate a thorough remediation process. Most services facilitate this by including a link, which is a controversial practice. However, 8% of the participants were suspicious, some of them due to the presence of a link, and did not change their password.

Provide Comprehensible Details We found that all types of information (account name, location, time, and device) have a positive influence (see Section 5.2). Still, services need to be careful when it comes to parsing and displaying technical details such as location data, browser, and OS (see Section 3.3). Here, special care and testing are required, as a badly parsed or displayed detail could impact the overall perceived legitimacy of the notification.

By addressing the identified areas, service providers can continue to strengthen account security and foster user trust.

7 CONCLUSION

We explored users' comprehension, reactions, and expectations of login notifications that are sent by services to help users protect their accounts from unauthorized access.

In a three-stages user study ($n = 229$), we evaluated a *baseline* notification that was created by collecting and analyzing 72 notifications sent by real-world services. To prevent participants from spending most of their attention on the notification and authentication task, we introduced a strong cognitive distractor by implementing a mental rotation test. We split participants into two treatments: a) The legitimate group received a notification only after they logged in, using metadata derived from their login information. b) The malicious group received a notification unexpectedly at a time when they had not interacted with the study website for multiple days using a generic location ("California, USA") and device ("Chrome on Windows") with the highest statistical chance of matching any user in our U.S.-based sample.

Overall, we find that login notifications achieve their goal of increasing account security. However, the tested notification failed to convince the majority of participants to change their password. Participants expressed the need for more contextual factors to help determine what caused the notification. Thus, instead of talking about an "unusual login," services need to explain what triggered the notification to assist users who received the notification unexpectedly. Even though some participants expressed feeling more protected and satisfied after receiving a notification, we argue that the service and not the user must be held accountable for implementing robust account protection measures. Interestingly, we find that more than 90% of the participants expect services to send login notifications when a login takes place from a new device or location, and especially if a login appears "suspicious." However, participants also expressed that they do not want to be notified for every login, highlighting the importance of finding the right balance between sending notifications too often or too rarely.

ACKNOWLEDGMENTS

This research was supported by the research training group "Human Centered Systems Security" sponsored by the state of North Rhine-Westphalia and funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

REFERENCES

[1] 1Password Community Member. 2022. 1Password "New Login" E-Mail Notification. https://1password.community/discussion/comment/643758/, as of February 22, 2024.
[2] David Adrian, Serena Chen, Joe DeBlasio, Emily Stark, and Emanuel von Zezschwitz. 2023. Chromium Blog: An Update on the Lock Icon. https://blog.chromium.org/2023/05/an-update-on-lock-icon.html, as of February 22, 2024.
[3] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *USENIX Security Symposium (SSYM '13)*. USENIX, Washington, District of Columbia, USA, 257–272.
[4] Hazim Almuhimedi, Adrienne Porter Felt, Robert W. Reeder, and Sunny Consolvo. 2014. Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning. In *Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX, Menlo Park, California, USA, 113–128.
[5] Alphabet, Inc. 2024. Respond to Security Alerts: When You'll Get an Alert. https://support.google.com/accounts/answer/2590353, as of February 22, 2024.
[6] Amazon.com, Inc. 2024. If You Get a Security Alert about Activity You Don't Recognize. https://www.amazon.com/gp/help/customer/display.html?nodeId=GLXNK37D6R3WGXKW, as of February 22, 2024.
[7] Ammar Amran, Zarul Fitri Zaaba, and Manmeet Kaur Mahinderjit Singh. 2018. Habituation Effects in Computer Security Warning. *Information Security Journal: A Global Perspective* 27, 4 (Oct. 2018), 192–204.
[8] Francesca Angelini. 2023. Do You Know Who's Logging into Your Netflix Account? https://www.thetimes.co.uk/article/do-you-know-whos-logging-into-your-netflix-account-m728z3678, as of February 22, 2024.
[9] Apple, Inc. 2022. Apple Support Community: Notification of Sign In with Apple ID. https://discussions.apple.com/thread/253581666, as of February 22, 2024.
[10] Apple, Inc. 2024. Signs That Your Apple ID Has Been Compromised. https://support.apple.com/en-us/102560, as of February 22, 2024.
[11] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. 2013. *Warning Design Guidelines*. Technical Report CMU-CyLab-13-002. Carnegie Mellon University.
[12] Melanie Birks and Jane Mills. 2022. *Grounded Theory: A Practical Guide* (3 ed.). SAGE Publications, Ltd., Thousand Oaks, California, USA.
[13] Tom Biselli, Laura Utz, and Christian Reuter. 2024. Supporting Informed Choices about Browser Cookies: The Impact of Personalised Cookie Banners. In *Privacy Enhancing Technologies Symposium (PETS '24)*. PoPETS, Bristol, United Kingdom, 171–191.
[14] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. 2019. Evaluating Login Challenges as a Defense Against Account Takeover. In *The World Wide Web Conference (WWW '19)*. ACM, San Francisco, California, USA, 372–382.
[15] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *ACM Conference on Human Factors in Computing Systems (CHI '08)*. ACM, Florence, Italy, 1065–1074.
[16] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2893–2902.
[17] Anthony Gavazzi, Ryan Williams, Engin Kirda, Long Lu, Andre King, Andy Davis, and Tim Leek. 2023. A Study of Multi-Factor and Risk-Based Authentication Availability. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 2043–2060.
[18] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M. Redmiles. 2021. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 109–126.
[19] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. 2018. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *ACM Conference on Computer and Communications Security (CCS '18)*. ACM, Toronto, Ontario, Canada, 1549–1566.
[20] Peter Leo Gorski, Yasemin Acar, Luigi Lo Iacono, and Sascha Fahl. 2020. Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs. In *ACM Conference on Human Factors in Computing Systems (CHI '20)*. ACM, Honolulu, Hawaii, USA, 1–13.
[21] Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *New Security Paradigms Workshop (NSPW '09)*. ACM, Oxford, United Kingdom, 133–144.
[22] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. 2017. I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. In *ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, Colorado, USA, 387–391.

[23] Ben Kaiser, Jerry Wei, Elena Lucherini, Kevin Lee, J. Nathan Matias, and Jonathan Mayer. 2021. Adapting Security Warnings to Counter Online Disinformation. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 1163–1180.

[24] Chiara Krisam, Heike Dietmann, Melanie Volkamer, and Oksana Kulyk. 2021. Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. In *European Workshop on Usable Security (EuroUSEC '21)*. ACM, Virtual Conference, 1–8.

[25] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 91–108.

[26] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Symposium on Network and Distributed System Security (NDSS '19)*. ISOC, San Diego, California, USA.

[27] Xu Lin, Panagiotis Ilia, Saumya Solanki, and Jason Polakis. 2022. Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting. In *USENIX Security Symposium (SSYM '22)*. USENIX, Boston, Massachusetts, USA, 1651–1668.

[28] LinkedIn, Inc. 2023. Security Footer Message in LinkedIn Emails. https://www.linkedin.com/help/linkedin/answer/a1339250, as of February 22, 2024.

[29] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security* 24, 4 (Sept. 2021), 30:1–30:36.

[30] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. 2022. "As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication. In *Symposium on Usable Privacy and Security (SOUPS '22)*. USENIX, Boston, Massachusetts, USA, 483–501.

[31] Meta Platforms, Inc. 2024. Get Alerts about Unrecognized Logins to Facebook. https://www.facebook.com/help/162968940433354, as of February 22, 2024.

[32] Microsoft, Corporation. 2024. What Happens If There's an Unusual Sign-in to Your Account. https://support.microsoft.com/en-us/account-billing/what-happens-if-there-s-an-unusual-sign-in-to-your-account-eba43e04-d348-b914-1e95-fb5052d3d8f0, as of February 22, 2024.

[33] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. 2021. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 359–376.

[34] Netflix, Inc. 2023. I Received an Email Stating There Was a New Sign-in to My Account. https://help.netflix.com/en/node/100775, as of February 22, 2024.

[35] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *ACM Conference on Human Factors in Computing Systems (CHI '20)*. ACM, Honolulu, Hawaii, USA, 1–13.

[36] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. 2020. The Burden of Ending Online Account Sharing. In *ACM Conference on Human Factors in Computing Systems (CHI '20)*. ACM, Honolulu, Hawaii, USA, 503:1–503:13.

[37] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. 2019. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. In *IEEE Symposium on Security and Privacy (SP '19)*. IEEE, San Francisco, California, USA, 866–883.

[38] PayPal, Inc. 2023. PayPal Security Center: How to Identify Fake Messages. https://www.paypal.com/us/security/learn-about-fake-messages, as of February 22, 2024.

[39] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *ACM Conference on Human Factors in Computing Systems (CHI '19)*. ACM, Glasgow, Scotland, United Kingdom, 518:1–518:15.

[40] RedFox Community Member. 2022. Netflix Email Message: "A new device is using your account". https://forum.redfox.bz/threads/netflix-email-message-a-new-device-is-using-your-account.86205/, as of February 22, 2024.

[41] Elissa M. Redmiles. 2019. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *IEEE Symposium on Security and Privacy (SP '19)*. IEEE, San Francisco, California, USA, 920–934.

[42] Elissa M. Redmiles, Everest Liu, and Michelle L. Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In *Who Are You?! Adventures in Authentication Workshop (WAY '17)*. USENIX, Santa Clara, California, USA, 1–5.

[43] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *USENIX Security Symposium (SSYM '20)*. USENIX, Virtual Conference, 89–108.

[44] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *ACM Conference on Human Factors in Computing Systems (CHI '18)*. ACM, Montreal, Quebec, Canada, 512:1–512:13.

[45] Robert W. Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy* 15, 5 (Oct. 2017), 55–64.

[46] Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy* 13, 3 (May 2015), 80–83.

[47] SECUSO Research Group, KIT. 2022. How to Detect Fraudulent and Phishing Messages. https://secuso.aifb.kit.edu/betr-nachrichten-flyer2EN, as of February 22, 2024.

[48] Roger N. Shepard and Jacqueline Metzler. 1971. Mental Rotation of Three-Dimensional Objects. *Science* 171, 3972 (Feb. 1971), 701–703.

[49] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '19)*. ACM, Austin, Texas, USA, 83:1–83:25.

[50] StatCounter. 2023. Desktop Browser Market Share Worldwide – June 2023. https://gs.statcounter.com/browser-market-share/desktop/worldwide, as of February 22, 2024.

[51] StatCounter. 2023. Desktop Operating System Market Share Worldwide – June 2023. https://gs.statcounter.com/os-market-share/desktop/worldwide, as of February 22, 2024.

[52] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium (SSYM '09)*. USENIX, San Diego, California, USA, 399–416.

[53] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, and Elie Bursztein. 2019. Protecting Accounts from Credential Stuffing with Password Breach Alerting. In *USENIX Security Symposium (SSYM '19)*. USENIX, Santa Clara, California, USA, 1556–1571.

[54] Edmund R. Thompson. 2007. Development and Validation of an Internationally Reliable Short-Form of the Positive and Negative Affect Schedule. *Journal of Cross-Cultural Psychology* 38, 2 (March 2007), 227–242.

[55] Cathy Urquhart. 2013. *Grounded Theory for Qualitative Research: A Practical Guide* (1 ed.). SAGE Publications, Ltd., Thousand Oaks, California, USA.

[56] U.S. Census Bureau. 2023. U.S. and World Population Clock. https://www.census.gov/popclock/, as of February 22, 2024.

[57] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *ACM Conference on Computer and Communications Security (CCS '19)*. ACM, London, United Kingdom, 973–990.

[58] Steven G. Vandenberg and Allan R. Kuse. 1978. Mental Rotations, a Group Test of Three-Dimensional Spatial Visualization. *Perceptual and Motor Skills* 47, 2 (Oct. 1978), 599–604.

[59] Meridel Walkington. 2019. Designing Better Security Warnings. https://blog.mozilla.org/ux/2019/03/designing-better-security-warnings/, as of February 22, 2024.

[60] Kathryn Walsh, Faiza Tazi, Philipp Markert, and Sanchari Das. 2021. My Account Is Compromised – What Do I Do? Towards an Intercultural Analysis of Account Remediation for Websites. In *Workshop on Inclusive Privacy and Security (WIPS '21)*. SSRN Electronic Journal, Virtual Conference, 1–6.

[61] David Wardle. 2019. *How Long Does It Take To Get Owned?* Technical Report RHUL–ISG–2019–4. Royal Holloway University of London.

[62] Stephan Wiefling, Luigi Lo Iacono, and Markus Dürmuth. 2019. Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In *International Conference on ICT Systems Security and Privacy Protection (IFIP SEC '19)*. IFIP, Lisbon, Portugal, 134–148.

[63] Stephan Wiefling, Tanvi Patil, Markus Dürmuth, and Luigi Lo Iacono. 2020. Evaluation of Risk-based Re-Authentication Methods. In *International Conference on ICT Systems Security and Privacy Protection (IFIP SEC '20)*. IFIP, Virtual Conference, 280–294.

[64] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *ACM Conference on Human Factors in Computing Systems (CHI '19)*. ACM, Glasgow, Scotland, United Kingdom, 194:1–194:14.

A SURVEY INSTRUMENT

Stage 1: Enrollment

Landing Page

This study is used to measure the spatial reasoning ability by letting participants decide whether two displayed objects have the same shape and size. Since there is no detailed information about changes in this ability over time, you can help us to close this gap by participating in this multi-stage study. What do you have to do?

- Create an account. This allows us to observe changes over time.
- Assess your spatial reasoning ability by completing the five rounds.
- Participate in the additionally payed recall stages to enable us to analyze how your abilities change over time.

If you want to learn more about spatial reasoning or the study itself, visit the About page. In case you have any questions, please do not hesitate to contact us via our email address. A typical reply is within 24 hours, or sooner.

Consent Form

Please indicate, in the boxes below, that you are at least 18 years old, have read and understood this consent form and agree to participate in this study.

- ☐ I am at least 18 years old.
- ☐ I have read and understood this consent form.
- ☐ I voluntarily agree to participate in this study.

The full consent form is left out for space reasons.

Privacy Note

On the next page, you are asked to create an account. Make sure to use an email address you frequently check, as we will use it to send you the invitations to the subsequent stages. At the end of the study, we will delete your email address. Please use a secure and unique password to prevent others from accessing your personal information during the study. We recommend treating this account like other important accounts you have, e.g., your email account.

- ☐ I understand this is an important account, and I am responsible for it.

Account Creation

Please create an account by providing the data in the fields below.
Email: _____
Password: _____
Confirm Password: _____

Email Address Confirmation

Confirm your email address by providing the code or clicking the link we just sent you via email to: *{participant's email address}*
If you need to change the email address, you can go back to the previous step.

Explanation

On the following five pages you will see pairs of perspective line drawings. Please decide for each pair whether the two drawings portray objects with the **same** shape and size, i.e., are congruent with respect to three-dimensional shape, or depict objects of **different** three-dimensional shapes.

The following page was shown 5 times

***{No.}* Perspective Line Pair**

Please decide for each pair whether the two drawings portray objects with the **same** shape and size, i.e., are congruent with respect to three-dimensional shape, or depict objects of **different** three-dimensional shapes.

Demography

To improve the quality of our research, we kindly ask you to provide some demographic information in the form below.

MD1 What is your age range?
○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65–74 ○ 75+
○ Prefer not to answer

MD2 Which of these best describes your current gender identity?
○ Woman ○ Man ○ Non-binary ○ Prefer to self-describe: _____
○ Prefer not to answer

MD3 What is the highest degree or level of school you have completed?
○ No schooling completed ○ Some high school, no diploma
○ High school graduate, diploma, or equivalent ○ Some college
○ Trade, technical, or vocational training ○ Associate's degree
○ Bachelor's degree ○ Master's degree ○ Professional degree ○ Doctorate
○ Prefer not to answer

MAC1 Please select 'Agree' as the answer to this question.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree ○ Agree
○ Strongly agree

MD4 Which of the following best describes your educational background or job field?
○ I have an education in, or work in, the field of computer science, computer engineering or IT.
○ I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT.
○ Prefer not to answer

Thank you for taking the survey!

The invitation for the second stage will be sent in **2 weeks**. You can now close this window.

Stage 2 was only completed by participants in the legitimate group

Stage 2: Recall

Landing Page

This study is used to measure the spatial reasoning ability by letting participants decide whether two displayed objects have the same shape and size. Since there is no detailed information about changes in this ability over time, you can help us to close this gap by participating in this multi-stage study. What do you have to do?

- Log in with your account that you created at the beginning of stage one.
- Assess your spatial reasoning ability by completing the five rounds which enables us to analyze how your ability has changed over time.

If you want to learn more about spatial reasoning or the study itself, visit the About page. In case you have any questions, please do not hesitate to contact us via our email address. A typical reply is within 24 hours, or sooner.

Sign In

Please sign in with the account you created for this study.
Email: _____
Password: _____

Explanation

On the following five pages you will see pairs of perspective line drawings. Please decide for each pair whether the two drawings portray objects with the **same** shape and size, i.e., are congruent with respect to three-dimensional shape, or depict objects of **different** three-dimensional shapes.

The following page was shown 5 times

***{No.}* Perspective Line Pair**

Please decide for each pair whether the two drawings portray objects with the **same** shape and size, i.e., are congruent with respect to three-dimensional shape, or depict objects of **different** three-dimensional shapes.

Thank you for taking the survey!

We will send you the compensation for completing the second stage of this study shortly. In **2 days**, we will send the invitation for the third and final stage, for which an **additional $4.00** is paid. You can now close this window.

Stage 3: Questionnaire

Landing Page

This study is used to measure the spatial reasoning ability by letting participants decide whether two displayed objects have the same shape and size. Since there is no detailed information about changes in this ability over time, you can help us to close this gap by participating in this multi-stage study. What do you have to do?

- Log in with your account that you created at the beginning of stage one.
- Assess your spatial reasoning ability by completing the five rounds which enables us to analyze how your ability has changed over time.

If you want to learn more about spatial reasoning or the study itself, visit the About page. In case you have any questions, please do not hesitate to contact us via our email address. A typical reply is within 24 hours, or sooner.

Sign In

Please sign in with the account you created for this study.
Email: _____
Password: _____

Debriefing

The main part of the research that is relevant for us starts on the next page.
Please do not close the browser window yet.

What are we trying to learn in this research?

Unlike initially explained, the goal of this study is to better understand the effectiveness of **sign-in emails**. Our only interest surrounds your interaction with the **sign-in email** you received for your account during this study. The spatial reasoning task's only purpose was giving the study a meaningful primary task that does not hint at the true purpose of our study. Your answers in the spatial reasoning task have been stored, and may be analyzed, but are not of primary interest for our research.

What data was collected?

As part of this study, we collected usage data about the sign-in emails, including whether users changed their password and how long it took them to react to the sign-in email. All your responses are only stored anonymously **using a random identifier**. Moreover, we separated all your survey responses from your email address, to **prevent any chance of re-identification**. All collected data was **encrypted**, and all identifiable data (such as your email addresses) **will be deleted** at the end of the study.

Why is this important to scientists or the general public?

Our work is concerned with designing systems to help users keep their accounts secure. Part of designing good security systems is usability: if people cannot use a system, they will not be able to keep their accounts secure. By better understanding the usability and effectiveness of sign-in emails, we will be able to create systems that are usable and secure.

What if I have question later?

If you have any remaining concerns, questions, or comments about the experiment, please feel free to contact us. To continue in the study, please continue to the next page. If you do not want to participate anymore you can click here.

Email

The individual login notification we sent to the participant is displayed for later reference (see Figure 4, but re-branded to match the SRS study).
If participant has not changed their password.

MQ0 Do you **remember** receiving **this email**?
○ Yes ○ No

*Participants who selected 'No' in **MQ0** were forwarded to **MQ10**.*

MP I-PANAS-SF

Now we would like to know how you felt in reaction to the email. The list below consists of a number of words that describe different feelings and emotions. Read each item and then mark the appropriate answer on the list. **Indicate to what extent you felt this way when you noticed the email**.

	Very slightly or not at all (1)	A little (2)	Moderately (3)	Quite a bit (4)	Extremely (5)
Upset	◯	◯	◯	◯	◯
Hostile	◯	◯	◯	◯	◯
Alert	◯	◯	◯	◯	◯
Ashamed	◯	◯	◯	◯	◯
Inspired	◯	◯	◯	◯	◯
Nervous	◯	◯	◯	◯	◯
Determined	◯	◯	◯	◯	◯
Attentive	◯	◯	◯	◯	◯
Afraid	◯	◯	◯	◯	◯
Active	◯	◯	◯	◯	◯

Reaction

MQ1 Did you **read** this **email** when you received it? (email as shown on the left)
○ I did not read it at all ○ I only read the subject but not the body
○ I read the subject and skimmed the body ○ I fully read it

MQ2a In reaction to this email, you decided to change your password.
Please **describe** any **other actions** you took.
Answer: _____

MQ3a **Why** did you react this way, i.e., change your password and take the other actions you described.
Answer: _____

If participant has not changed their password.

MQ2b **What** did you do **in reaction** to it?
Answer: _____

MQ3b **Why** did you react this way?
Answer: _____

Content & Design

MQ4 How much did the following **factors influence** your **reaction**?
Answer choice per item: No effect (1) – Major effect (5).
⋈ Email metadata (e.g., sender, subject, time of arrival)
⋈ Email content (e.g., information, instructions, wording)
⋈ Email design (e.g., structure, color, font size)
⋈ Experience in dealing with such emails
⋈ Negative experience with security and privacy incidents (e.g., data breach, identity theft)
⋈ Email appeared to be phishing
⋈ Expected to receive such an email
⋈ Other: _____
Answer choices were randomly ordered.

MQ5 Please rate how **helpful** the following **information** was for **deciding how to react** to this email?
Answer choice per item: Not at all helpful (1) – Extremely helpful (5).
⋈ Affected account name (i.e., email address) ⋈ Location ⋈ Date ⋈ Device

Time & Location

MQ6 **When** did you read the email?
○ I never read it ○ Immediately after I noticed it
○ Less than 1 hour after I noticed it ○ A few hours after I noticed it
○ One day after I noticed it ○ More than one day after I noticed it
○ I do not remember

*If participant has not selected "Never" in **MQ6**:*

MQ7 **In which US state** have you been when you **read** the **email**?
Dropdown with all 50 US states + District of Columbia.
If somewhere outside the USA: _____

MQ8 **Where** did you read the email?
○ At home ○ At work ○ On the go ○ Somewhere else: _____
○ I do not remember

MAC2 Please select 'Agree' as the **answer** to this question.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree ○ Agree
○ Strongly agree

MQ9 In case you received the email at a **different location or different time**, would your **reaction** to it been any **different**?
○ Yes ○ No ○ Do not know

*If participant selected "Yes" in **MQ8**:*

MQ10 **What** would you have **done differently**, if you had received the email at a **different location or different time**?
Answer: _____

Comprehension

MQ11 In your opinion, **why** have you **received** this email?
Answer: _____

Expectation

MQ12 In your opinion, **when** should real companies **send emails** like this one? (Select all that apply)
□ Never
□ After every detected sign-in which suggests that something is suspicious or wrong
□ After every detected sign-in when I have not signed in for a while
□ After every detected sign-in from a new device
□ After every detected sign-in at an unusual time of the day (e.g., in the middle of the night)
□ After every detected sign-in from a new location
□ After every detected sign-in
□ Other: _____

*If participant selected "Never" in **MQ12**:*

MQ13 In your opinion, **why** do you think real companies should **never send emails** like this one?
Answer: _____

Prior Experience

MQ14 Have you had any **negative experiences** with a **security or privacy** incident within the **last two years** (e.g., data breach, identity theft)?
○ Yes ○ No

MQ15 **Regularly changing** my **password** (e.g., every 90 days) **increases** the **security** of my account.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree ○ Agree
○ Strongly agree

MQ16 **Changing** my **password** after it **has been breached increases** the **security** of my account.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree ○ Agree
○ Strongly agree

One More Thing

Please indicate if you've honestly participated in this survey and followed instructions completely. You will not be penalized/rejected for indicating 'No' but your data may not be included in the analysis:
○ Yes ○ No

Thank you for taking the survey!

We will send you the compensation for completing the final stage of this study shortly. You can now close this window.

Only for participants in the malicious group:
*Note, as part of this research, we have sent you an email about a new sign-in. This sign-in did not take place; **at no time was your account at risk**.*

If you want to learn more about sign-in emails, feel free to visit: {link} There we have created some information material for you. The info website will stay online even after the end of this study, so feel free to save the link or share it.

B REAL-WORLD NOTIFICATIONS: EMAIL METADATA

Table 2: Sender, email address, and subject of the notifications sent by real-world services.

Rank	Domain	Display Name	Email Address	Subject
1	google.com	Google	no-reply@accounts.google.com	Security alert
	workspace.google.com	Google Workspace Alerts	google-workspace-alerts-noreply@google.com	Alert: Suspicious login
2	facebook.com	noreply	noreply@facebookmail.com	Did you use Facebook from somewhere new?
6	microsoft.com	Microsoft account team	account-security-noreply@ . . . microsoft.com	Microsoft account unusual sign-in activity
7	twitter.com	Twitter	verify@twitter.com	New login to Twitter from {browser} on {OS}
9	instagram.com	Instagram	security@mail.instagram.com	New login to Instagram from {browser} on {OS}
10	cloudflare.com	Cloudflare	noreply@notify.cloudflare.com	Your Cloudflare account has been accessed from a new IP Address
13	apple.com	Apple	noreply@email.apple.com	Your Apple ID was used to sign in to iCloud on a {device}
14	linkedin.com	LinkedIn	security-noreply@linkedin.com	{Name}, please verify your new device
15	netflix.com	Netflix	info@mailer.netflix.com	A new device is using your account
17	wikipedia.org	Wikipedia	wiki@wikimedia.org	Login to Wikipedia as {account name} from a device you have not recently used
20	amazon.com	amazon.com	account-update@amazon.com	amazon.com, action needed: Sign-in
25	yahoo.com	Yahoo	no-reply@cc.yahoo-inc.com	Unexpected sign-in attempt
32	github.com	GitHub	noreply@github.com	[GitHub] Please review this sign in
36	pinterest.com	Pinterest	noreply@account.pinterest.com	New login on your Pinterest account
63	vk.com	VK	admin@notify.vk.com	Someone has accessed your account from {OS} through {browser}, {country}
65	tiktok.com	TikTok	noreply@account.tiktok.com	New device login detected
72	mozilla.org	Firefox Accounts	accounts@firefox.com	New sign-in to Firefox
80	spotify.com	Spotify	no-reply@spotify.com	New login to Spotify
82	tumblr.com	Tumblr	no-reply@tumblr.com	Your account has been logged into.
83	paypal.com	service@paypal.com	service@paypal.com	Login from a new device
97	ebay.com	eBay	ebay@ebay.com	A new device is using your account
99	dropbox.com	Dropbox	no-reply@dropbox.com	We noticed a new sign in to your Dropbox
103	csdn.net	CSDN	service@register.csdn.net	[CSDN] Notification of remote login
104	imdb.com	imdb.com	account-update@imdb.com	imdb.com, action needed: Sign-in
125	soundcloud.com	SoundCloud Login	no-reply@login.soundcloud.com	SoundCloud sign-in detected from a new device
155	twitch.tv	Twitch	no-reply@twitch.tv	Your Twitch Account - Successful Log-in
157	etsy.com	Etsy	noreply@mail.etsy.com	{Name}, did you recently sign into Etsy?
164	booking.com	-	noreply@booking.com	New sign in to your account
171	sourceforge.net	SourceForge	noreply@sourceforge.net	Foreign login to your SourceForge.net account
179	researchgate.net	ResearchGate	no-reply@researchgatemail.net	New login from {browser} on {OS}
180	oracle.com	Oracle	no-reply@oracle.com	New Device Login Detected with Your Account
186	slack.com	Slack	feedback@slack.com	Slack account sign in from a new device
206	weebly.com	-	noreply@messaging.squareup.com	New login from {browser} on {OS}
236	samsung.com	Samsung Account	sa.noreply@samsung-mail.com	New sign in to your Samsung account
322	grammarly.com	Grammarly	hello@info.grammarly.com	New Login to Grammarly
328	fiverr.com	Fiverr	noreply@e.fiverr.com	New login on your Fiverr account
344	snapchat.com	Team Snapchat	no_reply@snapchat.com	New Snapchat Login
381	yelp.com	Yelp	no-reply@yelp.com	New login to your Yelp account ({account name})
392	binance.com	Binance	do-not-reply@ses.binance.com	[Binance] Login Attempted from New IP address {IP} - {time}({timezone})
524	netease.com	NetEase Account Center	passport@service.netease.com	NetEase mailbox account abnormal login reminder
541	gitlab.com	GitLab	gitlab@mg.gitlab.com	gitlab.com sign-in from new location
545	atlassian.com	Atlassian	noreply@am.atlassian.com	Unusual login attempts on your Atlassian account
563	uber.com	Uber	noreply@uber.com	New device sign-in
753	airbnb.com	Airbnb	automated@airbnb.com	Account activity: New login from {browser}
885	nintendo.com	-	no-reply@accounts.nintendo.com	[Nintendo Account] New sign-in
924	xing.com	XING	mailrobot@mail.xing.com	New login on XING: {browser} {OS}
1205	wayfair.com	Wayfair	noreply@wayfair.com	New device sign-in
1327	deezer.com	Deezer Security Team	securityteam@deezer.com	Login troubles?
1387	lyft.com	Lyft	noreply@lyftmail.com	New Login
1413	battle.net	Blizzard Entertainment	noreply@blizzard.com	Help us keep your Blizzard Account safe with a security check
1576	agoda.com	Agoda	no-reply@security.agoda.com	New Login to Your Agoda-Account
2476	1password.com	1Password	hello@1password.com	New 1Password sign-in from {browser}
2645	porkbun.com	Porkbun Support	support@porkbun.com	porkbun.com | account security notice - successful login
2705	synology.com	Synology Account	noreply@synologynotification.com	Synology Account - Security alert
3179	faceit.com	FACEIT	no-reply@faceit.com	Login from a new IP
3210	bitwarden.com	Bitwarden	no-reply@bitwarden.com	New Device Logged In From {browser}
3605	plex.tv	Plex	noreply@plex.tv	New sign-in to your Plex account
4189	dhl.de	-	noreply.kundenkonto@dhl.de	Successful login to your DHL account with a new device or browser
4250	dashlane.com	Dashlane	no-reply@dashlane.com	New device added to Dashlane
5383	logmein.com	LogMeIn.com Auto-Mailer	do-not-reply@logmein.com	LogMeIn Audit Notification - Login from an unfamiliar location
8544	maxmind.com	-	support@maxmind.com	MaxMind Notification: Unrecognized Device Login
10625	check24.com	CHECK24 Accounts	customeraccount@check24.com	New Login to Your Customer Account
16460	myunidays.com	UNiDAYS	no-reply@myunidays.com	Important: UNiDAYS Log-in Notification
16993	n26.com	N26	noreply@n26.com	Action needed: Unusual login to your N26 account
19535	neteller.com	NETELLER	no-reply@emails.neteller.com	New device has been detected
25667	splitwise.com	Splitwise	hello@splitwise.com	New sign-in to your Splitwise account
27539	decathlon.com	DECATHLON Service	noreply@services.decathlon.com	DECATHLON: New login to your account
31988	netatmo.com	Legrand - Netatmo - Bticino	do-not-reply@netatmo.com	Someone has logged into your account
40161	stacksocial.com	StackSocial	shop@email.stackcommerce.com	Account Activity Notification
46969	kinguin.net	Kinguin	help@kinguin.net	New browser login detected
48031	traderepublic.com	Trade Republic	service@traderepublic.com	Registration from a new device

C REAL-WORLD NOTIFICATIONS: FEATURES

Table 3: Information contained in notifications sent by real-world services.

Rank	Domain	Account Name	Browser	Country	State	City	IP	OS	Time	Time Zone	Instructions Legitimate	Instructions Malicious
1	google.com	●	○	○	○	○	○	●	○	○	●	●
	workspace.google.com	●	○	○	○	○	●	○	○	○	○	○
2	facebook.com	●	●	●	○	●	○	●	●	●	●	●
6	microsoft.com	●	●	●	○	○	●	●	●	●	●	●
7	twitter.com	●	●	●	●	●	○	●	○	○	●	●
9	instagram.com	●	●	●	○	●	○	●	●	●	●	●
10	cloudflare.com	●	●	○	○	○	●	●	●	●	●	●
13	apple.com	●	○	○	○	○	○	●	●	●	●	●
14	linkedin.com	●	●	●	●	●	○	●	●	●	○	●
15	netflix.com	●	○	●	●	○	○	○	●	●	●	●
17	wikipedia.org	○	○	○	○	○	○	○	○	●	●	●
20	amazon.com	○	●	●	●	○	○	●	●	●	●	●
25	yahoo.com	●	●	●	○	○	●	●	●	○	●	●
32	github.com	●	○	○	○	○	○	○	○	○	●	●
36	pinterest.com	○	●	○	○	○	○	●	○	●	●	●
63	vk.com	○	●	○	○	○	○	○	●	○	○	●
65	tiktok.com	●	○	○	●	○	○	○	●	●	●	●
72	mozilla.org	○	○	●	●	●	●	○	●	●	○	●
80	spotify.com	○	○	●	○	○	○	○	●	●	●	●
82	tumblr.com	○	●	●	●	○	●	●	●	○	●	●
83	paypal.com	●	●	●	●	●	○	●	●	●	●	●
97	ebay.com	●	●	●	●	●	○	●	●	●	●	●
99	dropbox.com	●	●	○	○	○	○	●	●	●	●	●
103	csdn.net	●	○	●	○	○	●	○	●	○	○	●
104	imdb.com	●	●	●	●	○	○	●	●	●	●	●
125	soundcloud.com	●	●	●	○	●	●	●	●	●	●	●
155	twitch.tv	●	●	●	●	●	●	●	●	●	●	●
157	etsy.com	●	●	●	●	●	●	●	○	●	●	●
164	booking.com	○	●	●	○	●	○	●	●	●	●	●
171	sourceforge.net	●	●	●	○	○	○	●	●	●	○	●
179	researchgate.net	●	●	●	○	○	○	●	●	○	○	●
180	oracle.com	●	●	●	●	●	●	●	●	●	●	●
186	slack.com	○	●	●	○	○	●	○	●	○	●	●
206	weebly.com	●	●	●	●	●	○	●	●	●	●	●
236	samsung.com	●	○	●	○	○	○	○	●	●	○	●
322	grammarly.com	●	●	●	○	●	●	●	●	●	○	●
328	fiverr.com	●	●	●	○	●	○	●	●	●	○	●
344	snapchat.com	●	○	●	○	●	●	○	●	●	●	●
381	yelp.com	●	●	○	○	○	○	●	●	●	●	●
392	binance.com	●	○	○	○	○	●	○	●	●	○	●
524	netease.com	●	○	●	○	○	●	○	●	○	○	●
541	gitlab.com	●	○	○	○	○	●	○	●	●	●	●
545	atlassian.com	●	●	●	●	●	●	●	●	●	●	●
563	uber.com	○	●	●	○	●	●	●	●	●	○	●
753	airbnb.com	○	●	●	●	○	○	●	●	●	●	●
885	nintendo.com	●	●	●	○	○	○	○	●	○	○	●
924	xing.com	●	●	●	○	○	○	●	●	○	●	●
1205	wayfair.com	●	○	○	○	○	○	●	●	●	●	●
1327	deezer.com	○	●	●	○	●	○	○	●	●	●	●
1387	lyft.com	●	●	●	●	●	○	○	●	○	●	●
1413	battle.net	●	○	○	○	○	○	○	○	●	○	●
1573	agoda.com	●	●	●	○	○	○	●	●	●	●	●
2476	1password.com	○	●	●	●	○	●	○	●	●	○	○
2645	porkbun.com	●	○	○	○	○	●	○	○	●	○	●
2705	synology.com	●	●	●	○	○	●	●	●	●	●	●
3210	bitwarden.com	○	●	○	○	○	●	○	●	●	○	○
3179	faceit.com	○	○	●	○	○	●	○	○	○	●	●
3605	plex.tv	●	○	●	●	●	●	○	○	●	○	●
4189	dhl.de	○	○	○	○	○	○	○	○	●	○	●
4250	dashlane.com	○	●	●	○	○	●	●	○	●	○	●
5383	logmein.com	●	●	●	●	●	●	●	●	○	○	●
8544	maxmind.com	○	○	●	●	●	●	○	●	●	●	●
10625	check24.com	●	●	●	○	○	○	●	●	●	○	●
16460	myunidays.com	●	○	○	○	○	●	○	●	●	○	●
16993	n26.com	●	●	●	○	●	●	●	●	●	●	●
19535	neteller.com	●	●	○	○	○	○	●	●	●	●	●
25667	splitwise.com	●	●	○	○	○	○	●	○	●	●	●
27539	decathlon.com	○	●	●	○	○	○	●	●	●	●	●
31988	netatmo.com	●	○	●	○	●	●	●	●	○	●	●
40161	stacksocial.com	●	○	○	○	○	○	○	●	●	●	●
46969	kinguin.net	●	●	○	○	○	●	●	●	●	○	●
48031	traderepublic.com	●	○	○	○	○	○	●	○	○	○	●

D CODEBOOK

Table 4: Codebook for MQ2a, MQ2b, MQ3a, MQ3b, and MQ11 used in Section 5.1 RQ1: Reaction & Comprehension.

Code	Freq.	Description	Example
MQ2a: In reaction to this email, you decided to change your password. Please describe any other actions you took. **MQ2b**: What did you do in reaction to it?			
Nothing	121	Participant did nothing.	*"After I read it, I didn't do anything as it was me who signed in."* (L17-N)
Change PW	26	Participant changed the password.	*"I took no other actions than to change my password as directed because I had not signed in."* (M71-C)
Check Details	10	Participant checked the login details in the notification.	*"I just made sure it was my device, and on the day I accessed"* (L69-N)
Reaction Unclear	10	Participant did not know how to react.	*"I was confused and decided to wait and see."* (M93-N)
Archive Email	6	Participant archived the notification.	*"save it in my personal files in gmail"* (M8-N)
Mark as Spam	4	Participant marked the notification as spam.	*"Put it in my spam folder"* (M25-N)
Understand	4	Participant tried to understand the notification.	*"I thought about it for a couple of minutes and then deleted it."* (M105-N)
MQ3a: Why did you react this way, i.e., change your password and take the other actions you described. **MQ3b**: Why did you react this way?			
Was Me	71	Participant described the own login being the reason.	*"because it was me that logged in"* (L10-N)
Spontaneous	27	Participant reacted spontaneously.	*"I just didn't think much of it"* (M51-N)
Not Me	26	Participant was not the one signing in.	*"Because the wrong state especially the opposite coast is a huge red flag."* (M77-C)
Suspicious	18	Participant questioned the legitimacy the notification.	*"I hadn't logged in and the location was California so I was afraid it was a phishing attempt."* (M107-N)
Don't Understand	14	Participant did not understand the notification.	*"Wasn't sure what it was for"* (L30-N)
Fatigue	9	Participant felt fatigued by seeing the notification.	*"it's good for security but I get these all the time."* (M74-N)
Low Value	7	Account has a low value for the participant.	*"Why should I care if someone accesses my SRS survey?"* (M70-N)
Unsure	6	Participant did not know how to react.	*"I unsure it was me why I received it"* (L40-N)
Feel Protected	3	Participant felt protected by receiving the notification.	*"I was glad that they sent me this in case there was anything out of the ordinary going on."* (L17-N)
MQ11: In your opinion, why have you received this email?			
Inform About Login	64	Notification informed about a new login.	*"Because your system recognized that a device signed into my account."* (L47-N)
Check Login	41	Notification was a prompt to check the login that just happened.	*"To make sure that it was in fact you who had signed in to the account."* (M104-N)
(Potential) Compromise	46	Notification informed about an actual or a potential compromise.	*"My reaction was that someone from California somehow got into my account."* (M116-C)
Don't Know	39	Participant did not know why the notification was sent.	*"I had no idea, which is why I deleted it."* (M93-N)
Unusual Login	28	Notification informed about a login that was somehow unusual.	*"It sounded like someone other than my typical device had logged into my account."* (M45-N)
Security	8	Notification was sent for security reasons.	*"Security purposes."* (L9-N)
Phishing	3	Notification was phishing.	*"I thought it was phishing"* (L30-N)

Table 5: Codebook for MQ10 used in Section 5.2 RQ2: Decision-Making & Execution.

Code	Freq.	Description	Example
MQ10: What would you have done differently, if you had received the email at a different location or different time?			
Pay More Attention	12	Participant would have payed more attention to the email.	*"I might have taken a closer look at it."* (L56-N)
Change PW	6	Participant would have changed the password.	*"I would have done as the email said and changed my password "* (L104-N)
Contact Support	4	Participant would have contacted the support.	*"Read it very carefully. If anything didn't look right I'd have contacted your organization"* (L19-N)
Panic	2	Participant would have panicked because then someone else would have been signing in.	*"If i was outside I might panic a bit more, or if the email came at a weird or random time"* (L69-N)

Table 6: Codebook for MQ13 used in Section 5.3 RQ3: Perception & Expectation.

Code	Freq.	Description	Example
MQ13: In your opinion, why do you think real companies should never send emails like this one?			
Feels Like Scam	4	Email notification in the current form feels like scam.	*"I got very concern, since include a link in the email instead of suggesting go to the website."* (M10-N)
Annoying	2	Receiving the email notifications is annoying.	*"They take too much time"* (M107-N)