"*I Knew It Was Me*": Understanding Users' Interaction with Login Notifications (Extended Version)

Philipp Markert, Leona Lassak, Maximilian Golla*, Markus Dürmuth‡
*Ruhr University Bochum, * Max Plank Institute for Security and Privacy, ‡ Leibniz University Hannover*

***Abstract*—Login notifications are intended to inform users about recent sign-ins and help them protect their accounts from unauthorized access. The notifications are usually sent if a login occurs from a new location or device, which could indicate malicious activity. They mostly contain information such as the location, date, time, and device used to sign in. Users are challenged to verify whether they recognize the login (because it has been them or someone they know) or to proactively protect their account from unwanted access by changing their password. In two user studies, we explore users' comprehension, reactions, and expectations of login notifications. We utilize two treatments to measure users' behavior in response to login notifications sent for a login they initiated themselves or based on a malicious actor relying on statistical sign-in information. Users feel relatively confident identifying legitimate logins but demonstrate various risky and insecure behaviors when it comes to malicious sign-ins. We discuss the identified problems and give recommendations for service providers to ensure usable and secure logins for everyone.**

***Index Terms*—notification, security warning, login, risk-based authentication, password change, sign in, unauthorized access**

1. Introduction

To protect accounts from unauthorized access, login notifications are intended to inform users about recent sign-ins. Depending on the service, the notifications are only sent if the login occurred from an *unknown location* or *new device*, which could 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 [24] 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 67 login notifications sent by real-world services and developed a *baseline* notification that we employed in two user studies. In the first study ($n = 220$), we asked participants to imagine having an account they recently have or have *not* signed in to (depending on their treatment) and then showed participants a login notification that either contained their current *real* sign-in information or was prefilled with information from an attacker relying on statistical data (i.e., California, USA; Chrome on Windows). The second study ($n = 229$), disguised as a psychological test, let users create an account they had to sign in to during the multi-stage study. Participants then either received a legitimate login notification to their email upon signing in themselves (*Legit*) or unexpectedly received a notification prefilled with statistical sign-in information after around one week (*Malicious*). We sought to answer the following research questions:

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

We find that participants correctly understand that "a login" caused receiving the notification. However, they are unaware of or misinterpret the trigger and are thus unsure how to react appropriately. Unique to Study 1, participants either claim they would change the password (Legit) or report they would mistakenly ignore the notification (Malicious). Comparing both studies, we find a large gap between participants' intended and actual behavior regarding password changes.

RQ2 *[Decision-Making & Execution] Do the currently employed 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.

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 perception and 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.

Our results suggest that login notifications are not, *per se*, a net positive for online account security. We find only $\frac{1}{5}$ of the participants who should have changed their password to protect their account actually did. While participants appreciate when companies decide to monitor their accounts for incidents, services that send notifications for every login can cause warning fatigue. We find malformed login notifications and current anti-phishing advice problematic and give clear recommendations for service providers to improve their notifications. While login notifications can help to reinforce account security, we think that protecting their accounts by identifying malicious logins should not be the sole responsibility of the user and highlight the need for better notifications.

2. Related Work

Next, we outline how our research extends related work.

2.1. Login Notifications & Challenges

Related to our work is a qualitative interview study ($n = 67$) by Redmiles [24]. It explores the account security incident response at Facebook by interviewing users who experienced a login incident. Different from our work, Redmiles focused on "secondary authentication" notifications that prompt users to enter a code to access their accounts. Redmiles interviewed participants from 5 countries and reported on incident-response information-seeking and mental models about attackers. Regarding the effectiveness of notifications, Redmiles identified a lack of key information, like the likelihood that the notification is about a legitimate threat, to be problematic. In contrast, our work studies a different kind of notification (see Section 3) and focuses on users' comprehension, expectations, and reaction to the notification and not on regaining access or mental models about attackers. Markert et al. [17] studied administrators' configuration of risk-based authentication (RBA). The predefined notifications were slightly customized by the administrators, and only few opted to disable them completely. Administrators lacked consensus about which information to include. Further aspects were the need for more context and explanation to prevent phishing attacks and to mention the inaccuracy of IP-based location estimation. Wardle [40] measured the time it takes for leaked credentials to be abused. For this, Wardle created accounts on web services, intentionally leaked them online, and then used login notifications, among other signals, to measure the time between the leak of the credentials and their first malicious abuse. A study by Doerfler et al. [4] 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. Wiefling et al. [41] 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 can reduce the login time [42]. Jubur et al. [11] presented an attack to bypass push-based two-factor authentication (2FA) notifications.

2.2. Security Warning & Notification Design

There is a large body of literature on security warning design [3], [26], [38]. The most prominent applications are notifications in the context of TLS [1], [6], phishing [22], and malware [2], as well as domains like warnings for developers [9] or countering misinformation [12]. For user authentication, there is work on breach notifications [10], [43], password-reuse notifications [8], [33], notifications to promote the use of 2FA [7], [25], or FIDO2 [13], or protect users from using common PINs [16].

While certain design patterns discussed in these works, like the use of opinionated design, proved to be effective for certain applications [6], we did not observe such patterns in login notifications. This is likely owed to the uncertainty of whether a true threat is present. Similarly, the use of alarming language or wording highlighting urgency was low. Interestingly, only a handful of notifications in our analysis (see Section 3) tried to explain why the notification is sent and attempted to address contextual misunderstandings [17], [26]. Personalization was the only best practice strictly applied [7] by referring to "your account" and including the account name to create trust and direct the notification.

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, 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 actually sent. Some services sent notifications for every login, others only 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.

3.1. Notification Types

Based on the type of information that is conveyed about a sign-in, one can distinguish three different notifications that are commonly sent by online services:

(1) **Granted Access:** These notifications inform about a *granted access*. Some services send such notifications for every sign-in, while others follow a risk-based approach (sending only if one or multiple aspects of a sign-in differ from prior observations).
(2) **Additional Challenge:** These notifications inform about a new sign-in attempt for which an *additional challenge* needs to be solved to complete the sign-in (i.e., insert a code or click a link).
(3) **Blocked Access:** The notification informs users about a *blocked access*, which can happen because the risk-based authentication system ranks the sign-in as too risky or because a challenge was not solved successfully.

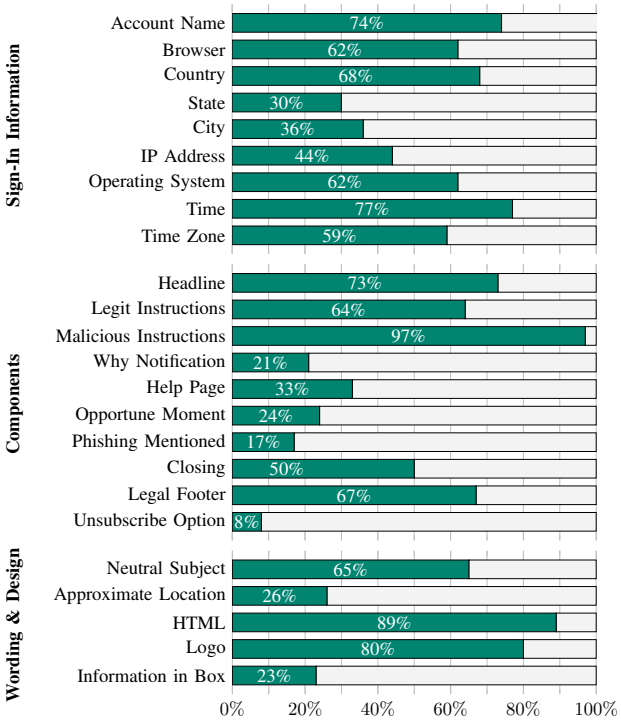

Figure 1. The information included in login notifications for a granted access ($n = 67$) sent by real-world services.

For the remainder of this work, we focus on the first type, i.e., notifications informing the user about a *granted access*. Granted access notifications are by far the most widespread notifications. Sending this type can be done by every organization, as it does not require an advanced risk assessment (i.e., basic logic and the ability to display login details are enough). While notifications can be sent via different channels (i.e., email, SMS, or push notifications), we limited our dataset to the most prominent type, which is email-based notifications.

3.2. Analysis

To find a representative *baseline* notification, we collected more than 80 login-related emails sent by real-world services by actively enumerating over 500 existing accounts we had on various websites. For this, we signed in using the Tor browser, which is often classified as suspicious activity, and monitored our inbox for notifications. Our collection is limited to the top Tranco list [14] websites (as of November 2022), with about $\frac{1}{3}$ being in the top 100, top 1000, and top 50,000 respectively. The dataset is biased towards English language websites (few non-English notifications have been translated). For analysis, two authors categorized 67 of the emails as *granted access* notifications. They then independently analyzed various aspects including: which sign-in information the notifications includes (i.e., login time, location, device), what the main components are (i.e., headline, malicious instructions), salient design and

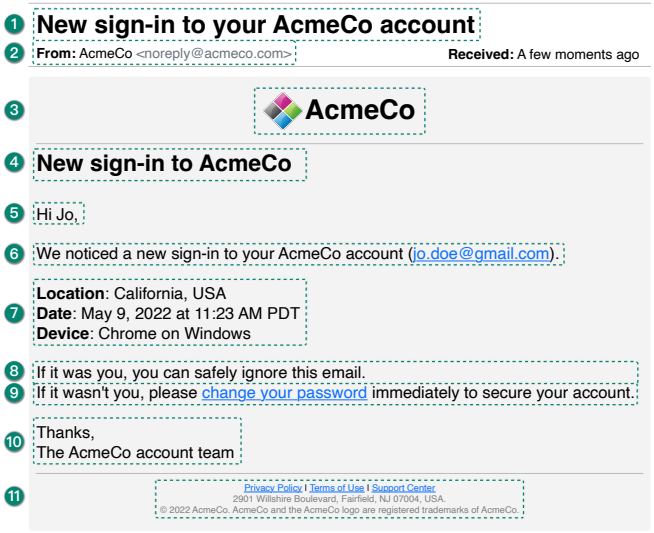

Figure 2. The *baseline* login notification, as used in our user studies, is derived from ($n = 66$) real-world notifications.

wording decisions (i.e., logo, highlighting of sign-in details, neutral language), and metadata such as sender and subject. We summarize our findings in Figure 1. Please refer to Appendix C for full details. Appendix D shows an in-depth analysis of the email sender and subject.

Sign-In Information. As depicted in Figure 1, the majority of notifications included the login 7 *Time* (77%), 5 *Account Name* (74%), 7 *Country* (68%), 7 *Browser* (62%), and 7 *Operating System* (62%). Less frequently, the notifications also included the 7 *Time Zone* (59%) or a login *IP Address* (44%). The small number of notifications including the login *City* (36%) or *State* (30%), is explained by geographical differences between the U.S. and Europe. Notifications about logins in the U.S. mostly focused on states; European notifications often focused on cities.

Components. Throughout all notifications, we noted the presence of a 4 *Headline* (73%) that was often (76%) different from the email subject. Another key component is the instructions describing how users should react in response to receiving the notification. While only 64% provided instructions in the 8 *Legitimate* case, more than 97% explained how to react in the 9 *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 legit on a separate web page (9%) displaying account remediation steps. Similarly, a small number (9%) suggested to visit the account activity page and reviewing all active sessions and devices. 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 computer/smartphone, new physi-

cal location, and private browsing) and malicious causes ("someone else/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 to not 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 10 *Closing* (50%) text that often thanked the user and included the name of a "{service} account team." A footer with 11 *Legal* information was included in 67% of the emails, and an *Unsubscribe* link was present in 8% of the notifications.

Wording & Design. The wording of the email subject was often *Neutral* (65%), with a strong focus on "*New login to* {*service*}," in some cases also alarming (23%), like "*Security alert*" or a prompt (9%), like "*Please review this sign in!*," and in two cases a question (3%), like "*Did you recently sign into* {*service*}?" Almost all (92%) emails referred to 6 "your account" to emphasize the importance of the notification. A few services tried to address the inaccuracies of IP-based geographic location estimation by describing it as *Approximate Location* (26%). The majority (89%) of the notifications were sent as *HTML* emails. Very few sent only plaintext emails. For a "corporate look-and-feel," 80% of all notifications included a 3 *Logo*, with an even split between a centered or left-aligned placement. Interestingly, 23% of the emails opted to display the sign-in information in a visually detached box, most likely to draw the user's attention to the login details.

Selecting a Representative Login Notification. Our data-driven *baseline* login notification (see Figure 2) includes all components used by at least 50% of the notifications. It uses a neutral subject and a slightly modified headline. We adjusted our email sender, opted for an HTML email, and included a logo. Also, we included the affected account name and referred to "your account." We included the most popular sign-in details, as well as legitimate and malicious instructions for users to take after receiving the notification. As our study sample was U.S.-based, we included the 7 *State* in the sign-in details. The email also included a closing and footer with fictional legal information.

4. Baseline Study: Method

This section describes our baseline studies' methodology. We first explain the study structure and treatments. Next, we describe the recruitment process and demographics, before concluding limitations and ethical considerations.

4.1. Study Protocol

We ran a quantitative online study with the following structure utilizing our baseline notification (see Section 3).

(1) *Consent:* In line with ethical best practices, we briefed participants about the research project and their participation at the beginning of the study. To start the study, participants had to consent.
(2) *Scenario:* Followed by the consent form, we described the scenario for the study telling participants to imagine that they are Jo Doe (jo.doe@gmail.com) and have an account with the company AcmeCo which is "like other accounts you may have, such as for online shopping or social media." Based on their (randomly) assigned treatment (see Section 4.2), we told participants on a subsequent page to imagine that they recently signed into this AcmeCo account (*Legit*) or have not signed into the account for a while (*Malicious*).
(3) *Notification:* After describing the circumstances, participants saw a login notification sent by AcmeCo (Figure 2). The login information depicted in the notification was either derived from the currently used system (*Legit*) or showed a login from California using Chrome on Windows (*Malicious*). From now on, up to the questions about prior experiences, the survey website used a two-column layout that displayed the login notification on the left and the questions on the right-hand side.
(4) *Reaction:* To understand how participants felt in reaction to being exposed to the login notification, we used the international short-form of the Positive and Negative Affect Schedule (I-PANAS-SF) [34]. Afterward, we asked participants to list three actions they would take after receiving the notification (**BQ1**), how concerned they would feel (**BQ2–BQ3**), and their priority of taking action (**BQ4–BQ5**).
(5) *Understanding:* Questions **BQ6–BQ9** were asked to investigate if participants understand what the notification is telling them, why they received it, and whether it appropriately guides them in resolving the situation (e.g., changing their password).
(6) *Expectation:* Next, we intended to learn what participants think would be the consequence of ignoring the notification (**BQ10–BQ11**) and if they expect real companies to send similar emails (**BQ12–BQ13**). This set of questions also contained an attention check **BAC**.
(7) *Prior Experience:* If participants described having received similar login notifications in the past (**BQ14**), we asked if and why they decided to read them (**BQ15–BQ16**) and situations where such notifications helped them to identify an unrecognized login (**BQ17–BQ18**).
(8) *Demography:* Next, we asked for demographics, including their age, gender identity, education, and any technical background (**BD1–BD4**).
(9) *Feedback:* At the end of the study, we asked participants if they participated honestly and whether they wanted to share any (optional) feedback regarding the study.

4.2. Treatments

We used two treatments to cover the cases that can trigger a notification: a *Legit* and a *Malicious* login. While a legit login is initiated by the user (or anyone who was intentionally given access), a malicious login is initiated by an attacker who got hold of the password, e.g., via a breach.

Legit ($n = 110$): To mimic a legit login, participants in this treatment should imagine that they recently logged into their AcmeCo account. The login details for the notification were obtained from the current session, i.e., their operating system and browser (based on the HTTP User-Agent string), as well as state and country derived from the IP address.

Malicious ($n = 110$): Participants in this treatment were told to imagine they had not logged into their AcmeCo account for a while and were all shown a notification for a login from California using Chrome on Windows. These login details were selected as we expect an attacker to know the victim resides in the USA. Logging in from the state with the highest population [35], as well as the browser and operating system with the highest market share [30], [31] minimizes the risk of being detected. We consider more sophisticated attacks [4], [18] that involve relaying login details and spoofing the user's sign-in information out of scope, as it makes recognizing such logins very difficult.

4.3. Recruitment and Demographics

For the baseline study, we recruited $n = 220$ participants, 110 for each treatment. We required participants to be over the age of 18 and reside in the U.S. to fulfill the assumption of the attacker in the malicious treatment. We did not exclude any participants as all of them passed the attention check (**BAC**) and indicated to have answered honestly; we also did not identify any inconsistencies. The baseline study was compensated with $2.50 USD and took participants, on average, 12 minutes to complete.

The demographics for the baseline study are depicted in Table 1. Participants split equally between male- and female-identifying participants; seven identified as non-binary, and four preferred not to disclose their gender. In terms of age and education, 49% of the participants were younger than 35 years, and 50% had a Bachelor's or Master's degree. Lastly, 73% of the participants stated not to have a technical background.

TABLE 1. DEMOGRAPHICS OF THE BASELINE STUDY.

	Male		Female		Other		Total	
	No.	%	No.	%	No.	%	No.	%
Age	105	48	104	47	11	5	220	100
18–24	16	7	9	4	2	1	27	12
25–34	37	17	39	18	6	3	82	37
35–44	25	11	29	13	1	0	55	25
45–54	14	6	14	6	1	0	29	13
55–64	10	5	6	3	0	0	16	7
65–74	2	1	6	3	0	0	8	4
75+	1	0	1	0	0	0	2	1
Education	105	48	104	47	11	5	220	100
High School	14	6	11	5	1	0	26	12
Some College	19	9	20	9	2	1	41	19
Trade	4	2	5	2	0	0	9	4
Associate's	10	5	8	4	2	1	20	9
Bachelor's	36	16	40	18	2	1	78	35
Master's	17	8	14	6	2	1	33	15
Professional	3	1	2	1	0	0	5	2
Doctorate	1	0	4	2	1	0	6	3
Background	105	48	104	47	11	5	220	100
Technical	10	5	39	18	1	0	50	23
Non-Technical	92	42	61	28	8	4	161	73
Prefer not to say	3	1	4	2	2	1	9	4

4.4. Limitations

Although we carefully considered various aspects of the study, it has its limitations which we will outline in the following. First, we conducted an online study and asked participants to describe their behavior, opinion, and perception based on a fictitious scenario. Hence, we cannot determine if this reflects reality even if none of the participants indicated to have answered dishonestly at the end of the study. To draw our conclusion based on measured instead of intended behavior and experienced situations, we only used this study as a preliminary and conducted a subsequent study to delve further into the topic. Second, the baseline study's sample was comprised of younger and higher-educated participants, which is typical for Prolific or other crowdsourcing platforms. We note that results may change for different populations, which should be investigated in succeeding studies. Third, results may suffer from self-report biases (e.g., social desirability). To mitigate this, we did not explain that this was a study about usability or security. Fourth, 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. Fifth, we only recruited US-based participants, which can have culture-based influences on the results.

4.5. Ethical Considerations

When the baseline study was conducted, none of the authors worked at an institution with an Institutional Review Board (IRB) that could oversee it. We followed the principles of the Menlo Report [36] "Respect for Persons," "Beneficence," and "Justice." We designed the study to minimize any potential harm while maximizing benefits. At the beginning of the study, we described the study procedure carefully, including all risks, and asked participants for their consent. Participants could withdraw from the study at any point without risking losing their compensation. All collected data were stored and processed in accordance with the General Data Protection Regulation (GDPR).

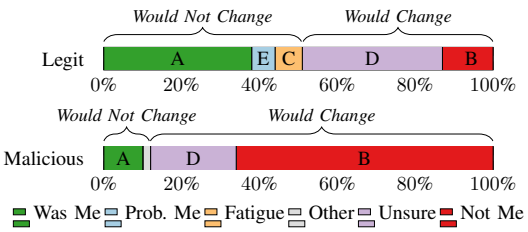

Figure 3. Breakdown of participants (based on **BQ1**), into those respondents who reported they *would* or *would not* change their password.

5. Baseline Study: Results

Next, we present the results of our baseline study focusing on our three research questions (see Section 1). The coding of qualitative answers was done by two members of the research team, who started by separately coding 10% of the answers. Afterward, they agreed on a joint code book and used it to code the remaining 90%. The agreement between the two coders was high ($\kappa = 0.82$). When applying statistics, we first checked for normality using D'Agostino's K^2 test, followed by Levene's test to check the variance. Based on the outcome, we applied the corresponding test for significance using Bonferroni correction for all pairwise tests. When quoting individual participants, e.g., L61-N, one can derive their treatment (***Legit*** or ***Malicious***) and password change behavior (*Would **Not** Change* or *Would **Change***).

5.1. RQ1: Comprehension & Reaction

Comprehension. Questions **BQ6** and **BQ7** asked participants to describe what the notification is telling them and why they may have received it. On the one hand, all 220 participants correctly described that a new login happened, yet, 63 (29%), 40 in the legit and 23 in the malicious group, assumed that the login must have been abnormal. Some respondents speculated that the device (38; 17%) or the location is unknown (15; 7%). Missing cookies, e.g., when using private browsing, were brought up by 3 participants, and only 1 person mentioned an unusual login time as a reason. However, all of those deviations may trigger a notification, and each service can implement its own logic. We further discuss this discrepancy between users' understanding and the actual implementation in Section 8.

Reaction Legit. The legit group splits equally between participants who would ignore the notification (56; 51%) and those who would change their password (54; 49%) (**BQ1**).

The majority of participants who would ignore it argued that they A definitely (42; 75%) or E probably (6; 11%) received it because they logged in themselves:

"*I live in Texas, use Chrome on Windows, and have just logged into this account. It's probably me.*" (L61-N)

Another 8 participants (14%) thought it was them causing the notification, but also explicitly mentioned C fatigue:

"*Delete the email because I know I am the person who signed in, [...] I unsubscribe from Acme entirely because I am tired of receiving these emails constantly.*" (L80-N)

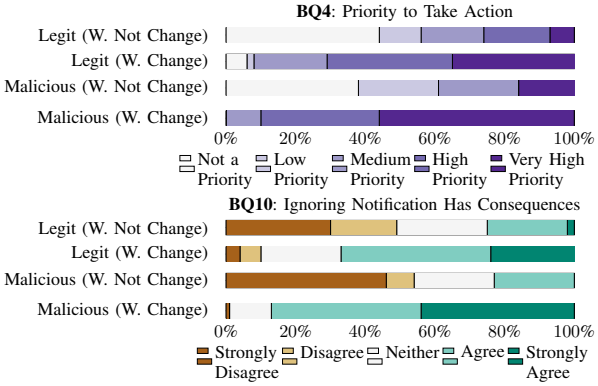

Figure 4. Responses to **BQ4** (Priority) and **BQ10** (Ignoring Consequences) as discussed in Section 5.1.

Of participants who said they would change their password (unnecessarily), 40 (74%) were D unsure whether it was them logging in. They said they would change the password to eliminate the possibility of someone having access:

"*It looks like someone else logged in. [...] Even if I'm not sure, might do this just in case.*" (L87-C)

The remaining B 14 (26%) do not describe being uncertain that someone else knows their password:

"*I would think my password was compromised.*" (L56-C)

Taking action (see Figure 4) has a significantly higher priority for participants who said that they would change their password than for those who do not ($\chi^2(2) = 31.3, p < 0.001$): 39, i.e., 72% describe the priority to be *high* or *very high* which aligns with their assumption of being compromised. Likewise, their agreement to **BQ10** saying "that ignoring this email from AcmeCo would have consequences" is also significantly higher ($\chi^2(2) = 29.0, p < 0.001$): 67% *agree* or *strongly agree* compared to only 25% for participants who stated they would ignore the notification. Generally, the ratings of participants who reported that they would change their password in the legit group are more similar to those participants in the malicious group who reported that they would change their password, which highlights the strong influence of a misinterpreted notification.

Reaction Malicious. In the malicious group, the majority (97; 88%) described that they would change their password, and 13 (12%) said they would ignore it. Of the prior, B 73 (75%) justified their reaction by saying that someone else just logged into their account:

"*Someone else got into my account, so I need to change the password right away.*" (M56-C)

Again, there are also D participants who expressed some form of uncertainty (24; 25%), yet, in contrast to the legit group, they mostly questioned the legitimacy of the email:

"*I would hover over the email to ensure it wasn't a phishing email [...] after ensuring it was legit and safe, I would change my password*" (M87-C)

Of the 13 participants in the malicious group who said they would ignore it, A 11 described that it must have been them logging in, misinterpreting the situation:

"*It is safe to assume that my account is not compromised. [. . .] It is good to see that my safety is a concern.*" (M92-N)

Only F 2 participants argued differently: M25-N mentions phishing, similar to many other participants, but would "send the email to spam" and not do anything else. M51-N, on the other hand, would "ignore it. It is my business, not theirs."

Similar to the legit treatment, the intend to take action in response to the notification was of significantly higher priority for participants who supposed to be compromised than those who did not ($\chi^2(2) = 23.4, p < 0.001$). Likewise, of those who intended to change their password, 87% *agreed* or *strongly agreed* that ignoring the notification would have consequences compared to only 23% among those who said they would not change it ($\chi^2(2) = 24.9, p < 0.001$).

Summary. While users understand that the notification informs them about a new login, their comprehension of potential triggers deviates from what can be actual reasons. We find a tendency to misinterpret the notification: participants either stated they would unnecessarily change the password (*Legit*) or they would mistakenly ignore the notification (*Malicious*). Note this study is limited to self-reported, hypothetical reactions. Thus, we further investigate these findings in the subsequent study (see Section 6).

5.2. RQ2: Decision-Making & Execution

Decision-Making. To identify the type of information (*location*, *date*, *device*) participants based their decision on, we specifically checked the open responses. Most participants (122; 55%) consider the device as a factor (explicitly the browser or operating system). However, percentages vary noticeably between the 4 groups. While 79% in the *Legit (Would Not Change)* group mentioned the device when describing how they made their decision, only 67% did in the *Legit (Would Change)* group. Participants in the malicious treatment mentioned the device less, 46% of the time by those who would not change their password and only 37% by those who stated they would.

Although one might think that the *location* is the easiest, hence, most popular factor to put into context, it is only the second most frequent one mentioned by 87 participants across all groups (40%). Again, participants in the legit treatment who reported they would not change their password included it most often (31; 55%), followed by *Legit (Would Change)* (21; 39%). In the malicious treatment, the differences are only marginal: 31% vs. 32% when contrasting the *Would Not Change* and *Would Change* groups.

Lastly, 49 participants (22%) mentioned the *date* and/or *time* in their responses. When comparing the groups, ratios range from 10% for the *Malicious (Would Change)* group to 43% for the *Legit (Would Not Change)* group, which fits the overall picture: participants in the legit group who expressed not to change their password refer to the login factors the most, followed by the *Legit (Would Change)* and the *Malicious (Would Not Change)* group. The participants who refer to any of the 3 types of information the least are those in the *Malicious (Would Change)* group.

A second view on this is given by **BQ18**, where we asked participants if they ever had a real-world situation in which they learned about an unrecognized login through such a notification. Of those who did (134; 61%), 51% described that the *location* was the determining factor. Only 13% say that the stated information about the *device* helped them, and only twice it was the *time*.

Execution. Question **BQ8** asked participants if the notification explained how to resolve the situation. The majority across all groups *agrees* or *strongly agrees*, ranging from 81% (*Legit (Would Change)*) to 89% (*Legit (Would Not Change)*). When explaining their answer (**BQ9**), most participants (61%; 133) focus on the information on how to resolve the situation for a malicious login, even if they do not intend to change their password:

"*It gave me steps to take if this was not me.*" (L41-N)

Another 25% (53) explicitly mention both outcomes:

"*It explains to ignore the email if it was me, and change my password if it wasn't.*" (L101-N)

Participants who criticize the notification report that they miss information in some form (15%; 33):

"*Changing my password is the very first line of defense, but I wish there was more information about what steps to take, or further assistance from AcmeCo.*" (M26-C)

This highlights an important aspect, as account remediation usually consists of more steps than just changing the password. Related work similarly observed a lack of advice provided by websites [19], [39]. In Section 8, we further discuss the risk that arises from this lack of information and the opportunity of the moment.

Lastly, 32 participants referred to the *change your password* link, which is provided in the notification. On the one hand, 22 (10%) noted it positively:

"*The steps to take were very clear and easy to follow. It also provided a link to make it easy to change my password if I needed to.*" (L42-C)

In contrast, 10 participants (5%) mention the link negatively, saying that they do not trust it and describe it as bad practice:

"*It shouldn't be suggesting that I click the link in the email as this is a trick often used by scammers.*" (M35-C)

Both positions provide reasonable arguments which come down to a weighting of usability and security. We further contrast both perspectives in Section 8.

Summary. Based on the open-ended questions, the *device* and the *location* appear to be influential types of information when participants make their decision. The *Legit (Would Not Change)* group generally refers to login information the most, *Malicious (Would Change)* participants the least. As we identified differences between responses regarding the study and real-world experiences, we will employ the second study to investigate to what extent the different types drive their decision processes. In terms of the execution, most participants, irrespective of the treatment and the described action, agree that the notification provides them with sufficient information. Participants who commented negatively mentioned a lack of information or disliked the *change your password* link.

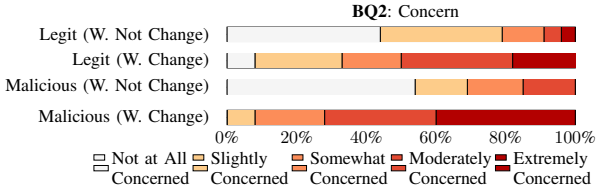

Figure 5. Responses to **BQ2** (Concern) as discussed in Section 5.3.

5.3. RQ3: Perception & Expectation

Perception. Using the PANAS, we investigated how the notifications make participants feel and also asked them about their concern (**BQ2**). Participants in the *Malicious (Would Change)* group feel the most positive, averaging 15.6 (SD: 3.2), followed by *Legit (Would Change)* with a mean of 14.6 (SD: 4.2). *Malicious (Would Not Change)*, 13.0 (SD: 4.6), and *Legit (Would Not Change)*, 11.8 (SD: 3.9), rank the lowest. Differences within the treatments, i.e., *Would Not Change* vs. *Would Change*, are also significant (*Legit*: $F_{55,53} = 13.0, p < 0.05$, *Malicious*: $F_{96,12} = 42.6, p < 0.001$), which shows that participants feel more positive if they do something in reaction to the notification. This may explain why participants (*Legit*) would tend to change their password even if it may not be necessary.

The situation for the negative *affect* is more distinct. The mean for participants in the malicious group who described to change their password, 12.7 (SD: 4.1), is significantly higher than for all other groups ($p < 0.001$). This stark contrast may be explained by the fact that 75% of them report being hacked in the scenario, while only 26% in the *Legit (Would Change)* have a similar assumption and all others just try to "better be safe than sorry." Scores of the *Legit (Would Not Change)*, 6.8 (SD: 3.0), and *Malicious (Would Not Change)* group, 6.7 (SD: 2.3), are significantly lower, even compared to *Legit (Would Change)*, $\chi^2(2) = 21.7, p < 0.001$ and $\chi^2(2) = 7.94, p < 0.05$, respectively. This aligns with the participant's understanding of the notification as information about their own login.

Participants' responses regarding the concern (**BQ2**–**BQ3**) match the previous observations. As can be seen in Figure 5, the *Malicious (Would Change)* group has the highest concern level, with 72% being *moderately* or *extremely concerned*. This is significantly higher compared to *Legit (Would Change)* ($\chi^2(2) = 1702.0, p < 0.001$), where 31% are *moderately*, and 20% are *extremely concerned*. The lowest concern is reported by participants who described not to change their password; 81% (*Legit (Would Not Change)*) and 69% (*Malicious (Would Not Change)*) are only *slightly* or *not at all concerned*.

Expectation. In response to **BQ12**, nearly all participants *agree* or *strongly agree* that login notifications should be sent by real companies. They feel that the notifications *protect accounts* (111; 51%), *alert customers* (95; 43%), and show that companies are invested in security (15; 7%). The only negative aspect mentioned was *annoyance*:

"*People who log into the site a lot are going to get spammed. It would be better if they only sent you a notification when they detect a strange login.* " (L32-N)

Still, this is only reported by 10 participants (5%). Likewise, only 9% (20) report to receive such notifications *regularly* (**BQ14**). More than three times as many (74; 33%) said they get them *many times*, and the largest portion (93; 42%) described to receive them *occasionally*. Similarly, 63% say they read them *always*, 17% *often*, 13% *sometimes*. Hence, there appears to be some decline which could be explained by participants differentiating between *expected* and a *unexpected* notifications:

"*If I signed in from a second device and then received the email, I knew it was me, so I would ignore it. But when I didn't sign in, I would pay attention and read the email.*" (L16-N)

Summary. Participants who would change their password have a higher positive *affect*, which may be explained by them securing their accounts. Yet, those that assumed to be hacked, also felt the most negative. If participants reported they would not change their password, their reaction was significantly more indifferent. We use Study 2 to observe participants' feelings when confronted with a real notification. More than 90% of the participants expect services to send login notifications, leaving them feel protected. They claimed to always read them or at least when the notification arrives unexpectedly. About 10% reported being annoyed by such notifications.

6. Measurement Study: Method

In the second study, we expand on the self-reported results from our baseline study by measuring user behavior. The following outlines the study protocol, treatments, recruitment, ethical considerations, and limitations.

6.1. Study Protocol

In contrast to Study 1, participants in this study received a notification for an account they created. 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) reactions to login notifications are *measurable*.

To achieve this, we invited participants to take part in a multi-stage study about changes in the cognitive ability of mental rotation over time [29], [37]. Framing the study this way allowed us to inform people about the length of the commitment without revealing our interest and justified the necessity of creating an account. The task also was a strong cognitive distractor that prevented participants from drawing too much attention to the authentication task.

Similar to Study 1, we used two treatments: The legit group ($n = 110$) received a notification only after they logged in themselves. The location, date, and device information 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 from "California, USA" using "Chrome on Windows." Location and device were selected to have the highest statistical chance of matching any user in our U.S.-based sample [30], [31], [35]. We did not allow mobile devices. Next, we detail the study procedure.

Stage 1: The study started by explaining the mental rotation test. To ensure participants would regularly check their email and understand the value of the account, after giving their consent, they saw a privacy notice, which highlighted the importance of the account as it would be used to store the study data, name, and email address. It also explained that the email would be used to send invitations to subsequent stages, and the compensation in 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 legit 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 legit group received an email inviting them to conduct another mental rotation test. To do so, they had to log into their account, which triggered a login 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 legit 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 to the notification. After logging into Stage 3, participants were debriefed and told about the actual purpose of the study. This was followed by our questionnaire (see Appendix B). From then on, the notification we sent to the participant was shown on the left side of their screen for reference.

(1) *Email:* First, we asked participants if they remember receiving the notification (**MQ0**); if not, they were forwarded to a different section (see Appendix B). Participants who triggered the tracking pixel in the notification or who changed their password skipped this question.
(2) *I-PANAS-SF:* To learn about the feelings and emotions in reaction to the notification, we again utilized the Positive and Negative Affect Schedule (I-PANAS-SF) [34].
(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.

TABLE 2. DEMOGRAPHICS OF THE MEASUREMENT STUDY.

	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

(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**).

6.2. Recruitment & Demographics

We recruited 625 participants for Stage 1. After filtering 12 participants who failed the attention check (**MAC1**), 613 participants remained. At the end of Stage 3, we had 252 completions. However, we removed 23 as they provided unrelated answers or failed the second attention check (**MAC2**). The final number of participants was $n = 229$. The relatively high number of dropouts is not owed to the login notification, as the participants already left the study before any notification was sent (before the login at Stage 2). Instead, it is primarily owed to the fact that it was a multi-stage study, and dropout rates like ours are within our panel provider's expected range. 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 legit group received an additional $1.00 USD for the completion of Stage 2, which took 2 minutes on average.

Table 2 shows the participants' demographics. While 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%).

6.3. Ethical Considerations

As with our baseline study, at the time we conducted the measurement study, none of the authors worked at an institution with an IRB. However, as discussed in Section 4.5, we carefully followed the guidelines provided in the Menlo Report, including a risk-benefit evaluation, following the legal requirements of the GDPR, and discussed and tested the protocol with peers familiar with conducting user studies. 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. We actively tried to avoid this situation by conducting our baseline study first. However, motivated by its results, i.e., 49% stated they would (unnecessarily) change their password, we decided to verify this potentially user-burdening behavior by conducting a second study.

To protect participants from unnecessary risks, we implemented several safeguards: i) Our panel provider offered the study only to participants that 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 name and email address. iii) All participants have been debriefed (also the ones that decided to withdraw early or drop out). 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 of the study), that participants could visit and share with their friends to learn more about login notifications and related account security measures. vi) We created a distinct email account for sending the 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 GDPR.

6.4. Limitations

In addition to the limitations from Study 1, we relied on a controllable artificial account setting for this study which might lack ecological validity. However, only 7 participants mention 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.

7. Measurement Study: Results

Next, we present the results of the measurement study. We have applied the same structure, coding methods, and statistical testing as with our baseline study (see Section 5).

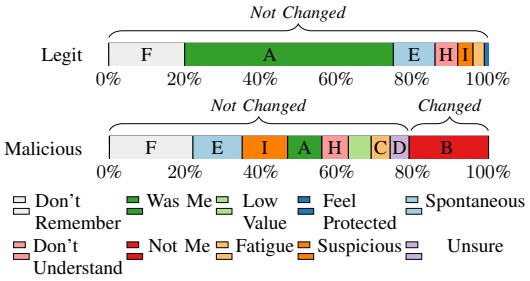

Figure 6. Breakdown of participants (measured), into those participants who *have* or *have not* changed their password.

7.1. RQ1: Comprehension & Reaction

Comprehension. When asked to describe why they have received the notification (**MQ11**), 85% (93) of the participants in the legit and 79% (94) in the malicious treatment realized that a new login happened to their account. Very few participants 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 legit 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.

In contrast to the first study, we observed a lower 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, most of the others within one or multiple hours. Hence, participants in the legit treatment had indeed a connection, and their understanding was substantially better. Similarly, we did not observe differences between treatments in the baseline study, where both had identical circumstances. This influence of contextual factors was already observed by related work on security warning design [9], [26] and could be achieved by including a *Why Notification* section. Some websites already do (see Section 3), and we will further elaborate on this in the discussion.

Reaction General. Out of the total 229 participants, 48 participants, 23 in the legit and 25 in the malicious treatment, F cannot remember the notification. Still, 26 of them triggered the tracking pixel, so they must have at least opened the notification. Among the large majority of participants who saw the login 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.

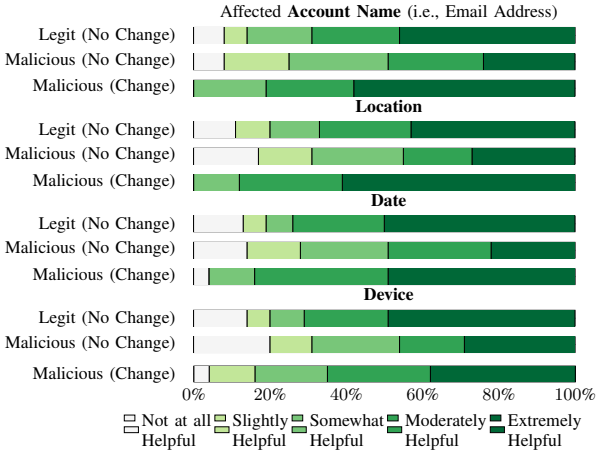

Figure 7. Helpfulness of the login details for deciding how to react (**MQ5**).

Reaction Legit. Unlike the baseline study suggested, where 49% of participants in legit treatment said they would change their password (see Section 5.1), none in the measurement study actually did. As shown in Figure 6, the majority of participants (60; 55%) explained their reaction 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." Previously, we saw 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 aligning with the findings from the baseline study with participants who were I *suspicious* about the legitimacy of the notification (4; 4%), felt C *fatigued* (3; 3%), or G *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 but someone else logging in. The reasons given by the other 78% (93) for not changing their password have mostly been given by participants in the legit 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 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 [20].

Summary. About 80% saw the notification. Participants in the legit 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, while we could not prove the tendency to unnecessary password changes.

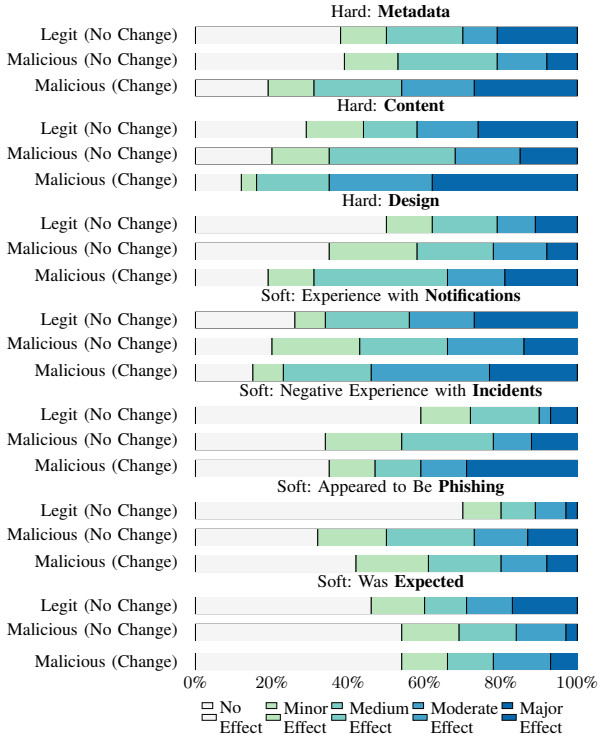

Figure 8. Influence of factors on participants chosen reaction (**MQ4**).

7.2. RQ2: Decision-Making & Execution

Participants in the baseline study reported that the notification tells them how to resolve the situation, irrespective of their assigned treatment and described reaction. Hence, we did not further test the execution and focused on the decision-making process instead, as participants seem to struggle when determining whether it was them or not, especially in case of a malicious login.

Helpfulness of Login Information. Foremost, we wanted to get more insights into the helpfulness of the displayed login information. We know from the baseline study that information about the *device* and *location* are considered by participants when deciding how to react to a login notification. In Figure 7, we can see that for those in the *Legit* 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 *Legit* 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 hard and soft factors. Figure 8 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 less distinct influence, with 18% (appeared to be phishing) to 23% (was expected) of the participants reporting a *moderate* or *major effect*.

When comparing the groups, *Legit* 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 the 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 ($\chi^2(2) = 7.73, p < 0.05$). These findings suggest that to nudge more users to change their password upon receiving potentially malicious login notifications, focusing on properly 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. Based on the first study, we assumed the device and location to be more helpful than the account name and the date. However, when compared side-by-side, we can conclude that all factors are equally essential. What we did observe is 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.

7.3. RQ3: Perception & Expectation

Perception. In the baseline study, the PANAS revealed that participants who would change their password felt significantly more positive (M: 15.6, SD: 3.2) but also more negative (M: 12.7, SD: 4.1). Participants who described ignoring the notification scored the lowest. The second study backs up both findings. 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 *Legit*, 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)* (M: 8.1, SD: 4.3), and *Legit* (M: 5.7, SD: 1.6). Again, Kruskal-Wallis was used yielding significance between both malicious groups and *Legit* ($p < 0.01$); the comparison between the two malicious groups nearly did, $\chi^2(2) = 5.26, p = 0.0654$.

Expectation. More than 90% of the participants in the baseline study expect real-world services to send login notifications. Participants who expressed disagreement reported receiving them constantly and being annoyed. Moreover, the second study showed so far 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 further understand when users expect to receive login 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 less (9, 3%) do not want to receive login notifications at all.

Summary. We can confirm 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.

The baseline study showed that participants expect services to send login notifications. With the new findings, we 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.

8. Discussion & Recommendations

Next, we discuss the takeaways of our analyses of 67 notifications and the main findings of our two subsequent user studies and give recommendations for service providers.

8.1. Best Practice

Overall, the baseline notification we developed achieved its primary goal: informing participants about a new login. Yet, understanding the trigger and correctly assessing the situation remained an issue. Below, we describe best practice based on what we learned for each of the components.

Metadata. We found that the metadata is an influential factor, and 75% of the participants paid attention to the subject. Hence, in addition to the most important information, the subject should already provide context for deciding how to react. Generic clauses, e.g., "Your account has been logged into." as used by Tumblr, do not achieve this, which is why email subjects like "New login to Twitter from {browser} on {OS}" are preferable. Similarly, websites should make use of the email sender's name so that recipients can quickly parse the information about the sender; in our initial analysis, we found 5 services that did not.

What Happened. What triggers a notification, e.g., an "unusual login" is often unclear to participants. Services could easily address this issue by explaining what triggered the notification, yet, only 12% of the evaluated emails currently provide examples of common triggers. 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.

Login Information. We found that all types of information (account name, location, time, and device) have a positive influence. IP addresses are a technical detail, not mentioned by any of the participants when referring to prior experiences. Tech-savvy users may argue being able to derive information from it, yet, the shift to IPv6 mostly eliminates this argument. Thus, we dissuade displaying it.

For the location, one needs to keep in mind that IP-based localization can be inaccurate, and potential issues like the reporting of default locations [23] were already noted by prior work [17]. To circumvent this problem, some services add notes or an "Approximate" to the location. Another approach would be to only report the location on a country or state level, as none of the participants mentioned cases where a login from a different city attracted their attention; it was always a different state, country, or continent.

When the date is reported, the month should be spelled out, as we found multiple examples where the DD/MM vs. MM/DD representation caused confusion. Similarly, the login time should follow the user's local conventions to prevent confusion due to the 12/24-hour clock format. Finally, it is important to include the timezone. Concerningly, we found 26 services that did not report any timezone.

Including the browser and operating system proved to be helpful. To fully benefit, services should avoid technical details, as most services already do for browsers, when they list them with just their name. Negative examples are sign-ins on smartphones displayed using the model number instead of the device name, e.g., "SM-S908B/DS" instead of "Samsung Galaxy S22." Operating systems are also usually reported with their full version number, e.g., "iOS 16.0.1." The least recommendable example is the inclusion of the raw HTTP User-Agent string, which we found in 4 emails.

Instructions. Notifications need to include instructions for both outcomes, i.e., legit and malicious logins. For the legit case, most services describe to ignore the message. For malicious logins, the recommendation needs to prompt users to visit the website and change or reset the password. Most services facilitate this by including a link which is a controversial practice. Of course, it simplifies the process, and 10% in our study explicitly appreciated the shortcut. However, also 10% of the participants were suspicious due to the presence of a link and did not change their password. Hence, services should carefully evaluate including a link.

Avoidable Pitfalls. Throughout our analysis of real-world notifications, we found numerous shortcomings that can make legit notifications appear suspicious. We saw that assessing a notification as suspicious can make the difference between changing the password and ignoring the notification. Luckily, all of the identified issues are easily avoidable, so services should make sure to thoroughly test their implementation. Examples we found include: incorrect, e.g., "<b>If you did not do this<b\>" or escaped HTML "Île-de-France" instead of "Île-de-France," and missing placeholders, e.g., "Browser: N/A."

Privacy. The vast majority of services employed tracking technologies in their emails like tracking pixels, URL parameters, and third-party redirects. Some participants reported to be concerned about this and wondered "what else they're tracking." The only exception to this are the 7 plaintext notifications we received from services like Cloudflare, GitHub, and Nintendo.

8.2. Expectations & Fatigue

More than 90% of the participants expect services to send login notifications, and finding a balance between sending them too often and too rarely is crucial. We found that participants want to be notified when a login takes place from a new device or location, but also if a login appears "suspicious," which can be accomplished with advanced logic provided by risk-based algorithms [41], [42]. Time-related notifications (i.e., login after a long or at an unusual time) are less demanded.

For service providers, sending notifications more often than necessary, following a "better safe than sorry"- mentality may be tempting. Yet, for users, this leads to a well-documented phenomenon in the area of security warnings: fatigue [1], [5], [32]. This fatigue, which affects all services, 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 further aggravated by services like Mozilla, Tumblr, Etsy, and others that send notifications for every single login.

8.3. Phishing Warning & Questionable Advice

Throughout both studies, about 15% of the participants questioned the legitimacy of the notification or referred to it as phishing. Related work showed how to best advice users [27], yet, most of the 10 notifications that include some information about phishing, do not follow it.

For example, questionable advice is given by Twitter (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 to better copy and paste the "It wasn't me"-link into a browser, "just to be safe." Spotify advises users to verify the email was sent from "@spotify.com," which is only expedient, if the email server and DNS are configured correctly. Related work demonstrated how vulnerable this email ecosystem is [28].

A good example is some of PayPal's advice [21] that explicitly mentions to "not rely on the padlock symbol and the 's' in https." Interestingly, LinkedIn opted to add a security footer message [15] to their login notification that includes the name and profession of the affected user in order to authenticate official emails.

References

[1] D. Akhawe and A. P. Felt, "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness," in *USENIX Security Symposium*, ser. SSYM '13. Washington, District of Columbia, USA: USENIX, Jul. 2013, pp. 257–272.

[2] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo, "Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning," in *Symposium on Usable Privacy and Security*, ser. SOUPS '14. Menlo Park, California, USA: USENIX, Jul. 2014, pp. 113–128.

[3] L. Bauer, C. Bravo-Lillo, L. Cranor, and E. Fragkaki, "Warning Design Guidelines," Carnegie Mellon University, Technical Report CMU-CyLab-13-002, Feb. 2013.

[4] P. Doerfler, K. Thomas, M. Marincenko, J. Ranieri, Y. Jiang, A. Moscicki, and D. McCoy, "Evaluating Login Challenges as a Defense Against Account Takeover," in *The World Wide Web Conference*, ser. WWW '19. San Francisco, California, USA: ACM, May 2019, pp. 372–382.

[5] S. Egelman, L. F. Cranor, and J. Hong, "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '08. Florence, Italy: ACM, Apr. 2008, pp. 1065–1074.

[6] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving SSL Warnings: Comprehension and Adherence," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. Seoul, Republic of Korea: ACM, Apr. 2015, pp. 2893–2902.

[7] M. Golla, G. Ho, M. Lohmus, M. Pulluri, and E. M. Redmiles, "Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 109–126.

[8] M. Golla, M. Wei, J. Hainline, L. Filipe, M. Dürmuth, E. Redmiles, and B. Ur, ""What was that site doing with my Facebook password?" Designing Password-Reuse Notifications," in *ACM Conference on Computer and Communications Security*, ser. CCS '18. Toronto, Ontario, Canada: ACM, Oct. 2018, pp. 1549–1566.

[9] P. L. Gorski, Y. Acar, L. Lo Iacono, and S. Fahl, "Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '20. Honolulu, Hawaii, USA: ACM, Apr. 2020, pp. 1–13.

[10] J. H. Huh, H. Kim, S. S. Rayala, R. B. Bobba, and K. Beznosov, "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*, ser. CHI '17. Denver, Colorado, USA: ACM, May 2017, pp. 387–391.

[11] M. Jubur, P. Shrestha, N. Saxena, and J. Prakash, "Bypassing Push-Based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications," in *ACM Asia Conference on Computer and Communications Security*, ser. ASIA CCS '21. Virtual Conference: ACM, May 2021, pp. 447–461.

[12] B. Kaiser, J. Wei, E. Lucherini, K. Lee, J. N. Matias, and J. Mayer, "Adapting Security Warnings to Counter Online Disinformation," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 1163–1180.

[13] L. Lassak, A. Hildebrandt, M. Golla, and B. Ur, ""It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 91–108.

[14] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," in *Symposium on Network and Distributed System Security*, ser. NDSS '19. San Diego, California, USA: ISOC, Feb. 2019.

[15] LinkedIn, Inc., "Security Footer Message in LinkedIn Emails," Nov. 2022, https://www.linkedin.com/help/linkedin/answer/a1339250, as of December 2, 2022.

[16] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth, and A. J. Aviv, "On the Security of Smartphone Unlock PINs," *ACM Transactions on Privacy and Security*, vol. 24, no. 4, pp. 30:1–30:36, Sep. 2021.

[17] P. Markert, T. Schnitzler, M. Golla, and M. Dürmuth, ""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*, ser. SOUPS '22. Boston, Massachusetts, USA: USENIX, Aug. 2022, pp. 483–501.

[18] A. Mirian, J. DeBlasio, S. Savage, G. M. Voelker, and K. Thomas, "Hack for Hire: Exploring the Emerging Market for Account Hijacking," in *The World Wide Web Conference*, ser. WWW '19. San Francisco, California, USA: ACM, May 2019, pp. 1279–1289.

[19] L. Neil, E. Bouma-Sims, E. Lafontaine, Y. Acar, and B. Reaves, "Investigating Web Service Account Remediation Advice," in *Symposium on Usable Privacy and Security*, ser. SOUPS '21. Virtual Conference: USENIX, Aug. 2021, pp. 359–376.

[20] B. Pal, T. Daniel, R. Chatterjee, and T. Ristenpart, "Beyond Credential Stuffing: Password Similarity Models using Neural Networks," in *IEEE Symposium on Security and Privacy*, ser. SP '19. San Francisco, California, USA: IEEE, May 2019, pp. 866–883.

[21] PayPal, Inc., "PayPal Security Center: How to Identify Fake Messages," Dec. 2022, https://www.paypal.com/us/security/learn-about-fake-messages, as of December 2, 2022.

[22] J. Petelka, Y. Zou, and F. Schaub, "Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '19. Glasgow, Scotland, United Kingdom: ACM, May 2019, pp. 518:1–518:15.

[23] K. Rawlinson, "U.S. Couple Sues IP-Mapping Firm," Aug. 2016, https://www.bbc.com/news/technology-37048521, as of December 2, 2022.

[24] E. M. Redmiles, ""Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response," in *IEEE Symposium on Security and Privacy*, ser. SP '19. San Francisco, California, USA: IEEE, May 2019, pp. 920–934.

[25] E. M. Redmiles, E. Liu, and M. L. Mazurek, "You Want Me To Do What? A Design Study of Two-Factor Authentication Messages," in *Who Are You?! Adventures in Authentication Workshop*, ser. WAY '17, Santa Clara, California, USA, Aug. 2017, pp. 1–5.

[26] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An Experience Sampling Study of User Reactions to Browser Warnings in the Field," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '18. Montreal, Quebec, Canada: ACM, Apr. 2018, pp. 512:1–512:13.

[27] SECUSO Research Group, KIT, "How to Detect Fraudulent and Phishing Messages," Mar. 2022, https://secuso.aifb.kit.edu/betr-nachrichten-flyer2EN, as of December 2, 2022.

[28] K. Shen, C. Wang, M. Guo, X. Zheng, C. Lu, B. Liu, Y. Zhao, S. Hao, H. Duan, Q. Pan, and M. Yang, "Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 3201–3217.

[29] R. N. Shepard and J. Metzler, "Mental Rotation of Three-Dimensional Objects," *Science*, vol. 171, no. 3972, pp. 701–703, Feb. 1971.

[30] StatCounter, "Desktop Browser Market Share Worldwide: Dec 2021 – Dec 2022," Dec. 2022, https://gs.statcounter.com/browser-market-share/desktop/worldwide, as of December 2, 2022.

[31] ——, "Desktop Operating System Market Share Worldwide: Dec 2021 – Dec 2022," Dec. 2022, https://gs.statcounter.com/os-market-share/desktop/worldwide, as of December 2, 2022.

[32] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: An Empirical Study of SSL Warning Effectiveness," in *USENIX Security Symposium*, ser. SSYM '09. San Diego, California, USA: USENIX, Jun. 2009, pp. 399–416.

[33] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting Accounts From Credential Stuffing With Password Breach Alerting," in *USENIX Security Symposium*, ser. SSYM '19. Santa Clara, California, USA: USENIX, Aug. 2019, pp. 1556–1571.

[34] E. R. Thompson, "Development and Validation of an Internationally Reliable Short-Form of the Positive and Negative Affect Schedule," *Journal of Cross-Cultural Psychology*, vol. 38, no. 2, pp. 227–242, Mar. 2007.

[35] U.S. Census Bureau, "U.S. and World Population Clock," Dec. 2022, https://www.census.gov/popclock/, as of December 2, 2022.

[36] U.S. Department of Homeland Security, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," Aug. 2012, https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of December 2, 2022.

[37] S. G. Vandenberg and A. R. Kuse, "Mental Rotations, a Group Test of Three-Dimensional Spatial Visualization," *Perceptual and Motor Skills*, vol. 47, no. 2, pp. 599–604, Oct. 1978.

[38] M. Walkington, "Designing Better Security Warnings," Mar. 2019, https://blog.mozilla.org/ux/2019/03/designing-better-security-warnings/, as of December 2, 2022.

[39] K. Walsh, F. Tazi, P. Markert, and S. Das, "My Account Is Compromised – What Do I Do? Towards an Intercultural Analysis of Account Remediation for Websites," in *Workshop on Inclusive Privacy and Security*, ser. WIPS '21, Virtual Conference, Aug. 2021, pp. 1–6.

[40] D. Wardle, "How Long Does It Take To Get Owned?" Royal Holloway University of London, Technical Report RHUL–ISG–2019–4, Mar. 2019.

[41] S. Wiefling, L. L. Iacono, and M. Dürmuth, "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*, ser. IFIP SEC '19. Lisbon, Portugal: IFIP, Jun. 2019, pp. 134–148.

[42] S. Wiefling, T. Patil, M. Dürmuth, and L. Lo Iacono, "Evaluation of Risk-based Re-Authentication Methods," in *International Conference on ICT Systems Security and Privacy Protection*, ser. IFIP SEC '20. Virtual Conference: IFIP, Sep. 2020, pp. 280–294.

[43] Y. Zou, S. Danino, K. Sun, and F. Schaub, "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*, ser. CHI '19. Glasgow, Scotland, United Kingdom: ACM, May 2019, pp. 194:1–194:14.

Appendix

1. Baseline Study: Survey Instrument

Scenario Description
In the following survey, you will be asked to imagine that your name is **Jo Doe** (jo.doe@gmail.com). You have an online account with a major company called **AcmeCo** which you **regularly access with all the devices you own**. Imagine that **this account is important to you**, and that it is like other accounts you may have, such as for online shopping or social media.

A Notification from AcmeCo
Imagine, you {**recently signed into** your AcmeCo account. / **have not signed into** your AcmeCo account for a while.}
In your inbox, you see the following email.

Notification

We displayed an interactive mockup email interface with our baseline notification shown in Figure 2.

I-PANAS-SF
Now we would like to know **how you feel in reaction to the email** shown on the left. 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 feel this way right now, that is, at the present moment.

	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

BQ1 **Please list 3 actions** you might take after receiving this email **and explain why** you might take those actions.
1 Action: _____
Explanation: _____
2 Action: _____
Explanation: _____
3 Action: _____
Explanation: _____

BQ2 I would **feel** _____ **about receiving** this email from AcmeCo.
○ Not at all concerned ○ Slightly concerned
○ Somewhat concerned ○ Moderately concerned
○ Extremely concerned

BQ3 Why?
Answer: _____

BQ4 For me, **taking action in response** to this email from AcmeCo **would be**
○ Not a priority ○ Low priority ○ Medium priority ○ High priority ○ Very high priority

BQ5 Why?
Answer: _____

Understanding

BQ6 In your own words, please **describe what this email is telling** you.
Answer: _____

BQ7 In your own words, please **describe all of the factors that may have caused you to receive this email**.
Answer: _____

BQ8 I feel that this email from AcmeCo explained to me **how to resolve the situation**.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree
○ Agree ○ Strongly agree

BQ9 Why?
Answer: _____

Expectation

BQ10 I feel that **ignoring this email** from AcmeCo **would have consequences**.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree
○ Agree ○ Strongly agree

BQ11 Why?
Answer: _____

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

BQ12 I think **real companies should send emails like this one** when necessary.
○ Strongly disagree ○ Disagree ○ Neither agree or disagree
○ Agree ○ Strongly agree

BQ13 Why?
Answer: _____

Prior Experience

BQ14 **I have received emails similar to this one** in the past.
○ Never ○ A few times ○ Occasionally ○ Many times
○ Regularly

*If participant stated to have received similar notifications in **BQ14**:*
We will now ask you about **your personal experiences with similar emails** you have received in the past. **Based on these experiences**, please answer the questions below:

BQ15 I _____ read them.
○ Never ○ Rarely ○ Sometimes ○ Often ○ Always

BQ16 Why?
Answer: _____

BQ17 Have you **ever received a similar email** that helped you to **learn about an unrecognized sign-in**? For example, a sign-in that concerned you.
○ Yes ○ No ○ Don't know

*If participant answered 'Yes' in **BQ17**:*

BQ18 Referring to the situation where a similar email helped you to learn about an unrecognized sign-in. Please **describe the situation**, how you knew that something was wrong, and **how you solved it**.
Answer: _____

Demography

BD1 Select your age.
○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65–74
○ 75+ ○ Prefer not to answer

BD2 Which of these best describes your current gender identity?
○ Woman ○ Men ○ Non-binary
○ Prefer to self-describe: _____
○ Prefer not to answer

BD3 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

BD4 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

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

2. Measurement Study: Survey Instrument

Stage 1: Enrollment

Participants solved 5x spatial reasoning tests.

Demography

MD1 Select your age.
○ 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 ○ Men ○ 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

Stage 2: Recall

Participants solved 5x spatial reasoning tests.

Stage 3: Questionnaire

Debriefing

Participants were debriefed and told about the actual purpose of the study.

Email

The individual login notification we sent to the participant is displayed for later reference (see Figure 2, 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**.*

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**.

We asked I-PANAS-SF from the Baseline Study again.

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?
Ans. 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

3. 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 Legit	Instructions Malicious
1	google.com	●	○	○	○	○	○	●	○	○	●	●
	workspace.google.com	●	○	○	○	○	●	○	○	○	○	○
4	facebook.com	●	●	●	○	●	○	●	●	●	●	●
6	microsoft.com	●	●	●	○	○	●	●	●	●	●	●
7	netflix.com	●	○	●	●	○	○	○	●	●	●	●
8	twitter.com	●	●	●	●	●	○	●	○	○	●	●
9	instagram.com	●	●	●	○	●	○	●	●	●	●	●
12	apple.com	●	○	○	○	○	○	●	●	●	●	●
13	linkedin.com	●	●	●	●	●	○	●	●	●	○	●
14	cloudflare.com	●	●	○	○	○	●	●	●	●	●	●
16	wikipedia.org	○	○	○	○	○	○	○	○	●	●	●
17	yahoo.com	●	●	●	○	○	●	●	●	○	●	●
21	amazon.com	○	●	●	●	○	○	●	●	●	●	●
32	pinterest.com	○	●	○	○	○	○	●	○	●	●	●
33	github.com	●	○	○	○	○	○	○	○	○	●	●
67	vk.com	○	●	○	○	○	○	○	●	○	○	●
71	mozilla.org	○	○	●	●	●	●	○	●	●	○	●
74	csdn.net	●	○	●	○	○	●	○	●	○	○	●
84	tumblr.com	○	●	●	●	○	●	●	●	○	●	●
87	spotify.com	○	○	●	○	○	○	○	●	●	●	●
89	paypal.com	●	●	●	●	●	○	●	●	●	●	●
98	dropbox.com	●	●	○	○	○	○	●	●	●	●	●
112	ebay.com	●	●	●	●	●	○	●	●	●	●	●
116	imdb.com	●	●	●	●	○	○	●	●	●	●	●
119	soundcloud.com	●	●	●	○	●	●	●	●	●	●	●
153	twitch.tv	●	●	●	●	●	●	●	●	●	●	●
157	sourceforge.net	●	●	●	○	○	○	●	●	●	○	●
169	etsy.com	●	●	●	●	●	●	●	○	●	●	●
182	researchgate.net	●	●	●	○	○	○	●	●	○	○	●
188	weebly.com	●	●	●	●	●	○	●	●	●	●	●
199	oracle.com	●	●	●	●	●	●	●	●	●	●	●
212	booking.com	○	●	●	○	●	○	●	●	●	●	●
230	samsung.com	●	○	●	○	○	○	○	●	●	○	●
279	slack.com	○	●	●	○	○	●	○	●	○	●	●
318	snapchat.com	●	○	●	○	●	●	○	●	●	●	●
345	grammarly.com	●	●	●	○	●	●	●	●	●	○	●
359	yelp.com	●	●	○	○	○	○	●	●	●	●	●
361	fiverr.com	●	●	●	○	●	○	●	●	●	○	●
457	netease.com	●	○	●	○	○	●	○	●	○	○	●
465	binance.com	●	○	○	○	○	●	○	●	●	○	●
617	atlassian.com	●	●	●	●	●	●	●	●	●	●	●
691	gitlab.com	●	○	○	○	○	●	○	●	●	●	●
760	battle.net	●	○	○	○	○	○	○	○	●	○	●
786	airbnb.com	○	●	●	●	○	○	●	●	●	●	●
829	uber.com	○	●	●	○	●	●	●	●	●	○	●
904	xing.com	●	●	●	○	○	○	●	●	○	●	●
1102	nintendo.com	●	●	●	○	○	○	○	●	○	○	●
1273	wayfair.com	●	○	○	○	○	○	●	●	●	●	●
1318	deezer.com	○	●	●	○	●	○	○	●	●	●	●
2716	plex.tv	●	○	●	●	●	●	○	○	●	○	●
3322	1password.com	○	●	●	●	○	●	○	●	●	○	○
3386	lyft.com	●	●	●	●	●	○	○	●	○	●	●
4146	dhl.de	○	○	○	○	○	○	○	○	●	○	●
4416	dashlane.com	○	●	●	○	○	●	●	○	●	○	●
4738	porkbun.com	●	○	○	○	○	●	○	○	●	○	●
5325	logmein.com	●	●	●	●	●	●	●	●	○	○	●
7067	check24.com	●	●	●	○	○	○	●	●	●	○	●
10644	maxmind.com	○	○	●	●	●	●	○	●	●	●	●
11953	faceit.com	○	○	●	○	○	●	○	○	○	●	●
14822	myunidays.com	●	○	○	○	○	●	○	●	●	○	●
20163	n26.com	●	●	●	○	●	●	●	●	●	●	●
22898	neteller.com	●	●	○	○	○	○	●	●	●	●	●
30613	traderepublic.com	●	○	○	○	○	○	●	○	○	○	●
33584	stacksocial.com	●	○	○	○	○	○	○	●	●	●	●
38229	netatmo.com	●	○	●	○	●	●	●	●	○	●	●
42238	splitwise.com	●	●	○	○	○	○	●	○	●	●	●
43757	decathlon.com	○	●	●	○	○	○	●	●	●	●	●

4. Real-World Notifications: Email Metadata

TABLE 4. 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
4	facebook.com	noreply	noreply@facebookmail.com	Did you use Facebook from somewhere new?
6	microsoft.com	Microsoft account team	account-security-noreply@accountprotection.microsoft.com	Microsoft account unusual sign-in activity
7	netflix.com	Netflix	info@mailer.netflix.com	A new device is using your account
8	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}
12	apple.com	Apple	noreply@email.apple.com	Your Apple ID was used to sign in to iCloud on a {device}
13	linkedin.com	LinkedIn	security-noreply@linkedin.com	{Name}, please verify your new device
14	cloudflare.com	Cloudflare	noreply@notify.cloudflare.com	Your Cloudflare account has been accessed from a new IP Address
16	wikipedia.org	Wikipedia	wiki@wikimedia.org	Login to Wikipedia as {account name} from a device you have not recently used
17	yahoo.com	Yahoo	no-reply@cc.yahoo-inc.com	Unexpected sign-in attempt
21	amazon.com	amazon.com	account-update@amazon.com	amazon.com, action needed: Sign-in
32	pinterest.com	Pinterest	noreply@account.pinterest.com	New login on your Pinterest account
33	github.com	GitHub	noreply@github.com	[GitHub] Please review this sign in
67	vk.com	VK	admin@notify.vk.com	Someone has accessed your account from {OS} through {browser}, {country}
71	mozilla.org	Firefox Accounts	accounts@firefox.com	New sign-in to Firefox
74	csdn.net	CSDN	service@register.csdn.net	[CSDN] Notification of remote login
84	tumblr.com	Tumblr	no-reply@tumblr.com	Your account has been logged into.
87	spotify.com	Spotify	no-reply@spotify.com	New login to Spotify
89	paypal.com	service@paypal.com	service@paypal.com	Login from a new device
98	dropbox.com	Dropbox	no-reply@dropbox.com	We noticed a new sign in to your Dropbox
112	ebay.com	eBay	ebay@ebay.com	A new device is using your account
116	imdb.com	imdb.com	account-update@imdb.com	imdb.com, action needed: Sign-in
119	soundcloud.com	SoundCloud Login	no-reply@login.soundcloud.com	SoundCloud sign-in detected from a new device
153	twitch.tv	Twitch	no-reply@twitch.tv	Your Twitch Account - Successful Log-in
157	sourceforge.net	SourceForge	noreply@sourceforge.net	Foreign login to your SourceForge.net account
169	etsy.com	Etsy	noreply@mail.etsy.com	{Name}, did you recently sign into Etsy?
182	researchgate.net	ResearchGate	no-reply@researchgatemail.net	New login from {browser} on {OS}
188	weebly.com	-	noreply@messaging.squareup.com	New login from {browser} on {OS}
199	oracle.com	Oracle	no-reply@oracle.com	New Device Login Detected with Your Account
212	booking.com	-	noreply@booking.com	New sign in to your account
230	samsung.com	Samsung Account	sa.noreply@samsung-mail.com	New sign in to your Samsung account
279	slack.com	Slack	feedback@slack.com	Slack account sign in from a new device
318	snapchat.com	Team Snapchat	no_reply@snapchat.com	New Snapchat Login
345	grammarly.com	Grammarly Security	info@security.grammarly.com	New Login to Grammarly
359	yelp.com	Yelp	no-reply@yelp.com	New login to your Yelp account ({account name})
361	fiverr.com	Fiverr	noreply@e.fiverr.com	New login on your Fiverr account
457	netease.com	NetEase Account Center	passport@service.netease.com	NetEase mailbox account abnormal login reminder
465	binance.com	Binance	do-not-reply@ses.binance.com	[Binance] Login Attempted from New IP address {IP} - {time}({timezone})
617	atlassian.com	Atlassian	noreply@am.atlassian.com	Unusual login attempts on your Atlassian account
691	gitlab.com	GitLab	gitlab@mg.gitlab.com	gitlab.com sign-in from new location
760	battle.net	Blizzard Entertainment	noreply@blizzard.com	Help us keep your Blizzard Account safe with a security check
786	airbnb.com	Airbnb	automated@airbnb.com	Account activity: New login from {browser}
829	uber.com	Uber	noreply@uber.com	New device sign-in
904	xing.com	XING	mailrobot@mail.xing.com	New login on XING: {browser} {OS}
1102	nintendo.com	-	no-reply@accounts.nintendo.com	[Nintendo Account] New sign-in
1273	wayfair.com	Wayfair	noreply@wayfair.com	New device sign-in
1318	deezer.com	-	securityteam@deezer.com	Access from new PC
2716	plex.tv	Plex	noreply@plex.tv	New sign-in to your Plex account
3322	1password.com	1Password	hello@1password.com	New 1Password sign-in from {browser}
3386	lyft.com	Lyft	noreply@lyftmail.com	New Login
4146	dhl.de	-	noreply.kundenkonto@dhl.de	Successful login to your DHL account with a new device or browser
4416	dashlane.com	Dashlane	no-reply@dashlane.com	New device added to Dashlane
4738	porkbun.com	Porkbun Support	support@porkbun.com	porkbun.com | account security notice - successful login
5325	logmein.com	LogMeIn.com Auto-Mailer	do-not-reply@logmein.com	LogMeIn Audit Notification - Login from an unfamiliar location
7067	check24.com	CHECK24 Accounts	customeraccount@check24.com	New Login to Your Customer Account
10644	maxmind.com	-	support@maxmind.com	MaxMind Notification: Unrecognized Device Login
11953	faceit.com	FACEIT	no-reply@faceit.com	Login from a new IP
14822	myunidays.com	UNiDAYS	no-reply@myunidays.com	Important: UNiDAYS Log-in Notification
20163	n26.com	N26	noreply@n26.com	Action needed: Unusual login to your N26 account
22898	neteller.com	NETELLER	no-reply@emails.neteller.com	New device has been detected
30613	traderepublic.com	Trade Republic	service@traderepublic.com	Registration from a new device
33584	stacksocial.com	StackSocial	shop@email.stackcommerce.com	Account Activity Notification
38229	netatmo.com	Legrand - Netatmo - Bticino	do-not-reply@netatmo.com	Someone has logged into your account
42238	splitwise.com	Splitwise	hello@splitwise.com	New sign-in to your Splitwise account
43757	decathlon.com	DECATHLON Service	noreply@services.decathlon.com	DECATHLON: New login to your account

5. Codebook

TABLE 5. CODEBOOK FOR **BQ1**, **BQ5**, AND **BQ6** USED IN SECTION 5.1 RQ1: COMPREHENSION & REACTION.

Code	Freq.	Description	Example
BQ1: Please list 3 actions you might take after receiving this email and explain why you might take those actions.			
Change PW	151	Participant would change the password.	*"Someone else got into my account, so I need to change the password right away."* (M56-C)
Ignore	69	Participant would ignore the email.	*"Ignore the email. It was me that signed in."* (L78-N)
Contact AcmeCo	64	Participant would contact AcmeCo.	*"I would try and contact them and get a solution to this urgent problem."* (M54-C)
Review Activity	59	Participant would check what has been done with the account.	*"I would look for strange activity on the account."* (M47-C)
Review Details	37	Participant would check the shown login information.	*"Check location, date, device. If it is my own location, date, and device, then I can safely ignore this message."* (L12-N)
Prevent Phishing	33	Participant would check the legitimacy of the notification.	*"Check the sender of the email. I would want to be sure the email was legitimate."* (M16-C)
Change Other PWs	25	Participant would change passwords of other accounts.	*"Change passwords for other important accounts as well"* (M87-C)
Check Other Accounts	22	Participant would check the other accounts.	*"I would look to see if other accounts of mine had been compromised."* (M28-C)
Add Additional Security	19	Participant would try to add security measures.	*"Look for additional security options e.g. 2FA"* (L8-C)
Ask Family/Friends	12	Participant would ask family and/or friends if they have used the account.	*"Ask my husband if he signed in."* (L42-C)
Delete Account	10	Participant would consider deleting the account.	*"My account has been taken over, and might as well make a new account and terminate this account."* (M7-C)
Log Out (All) Devices	10	Participant would try to end the session of some or all devices.	*"I would logout all devices if the option is available."* (M61-C)
Remember Recent Logins	9	Participant would try to recall past actions.	*"I will do my best to remember whether I have login recently."* (L71-C)
Verify Old PW	7	Participant would log in to check if the password still works.	*"Check to see if my login still works to see if my password's been changed."* (M16-C)
BQ5: Why? (***BQ4****: For me, taking action in response to this email from AcmeCo would be [Priority Level]*)			
Secure Account	105	Participant would want to secure the account.	*"To make my information secure if it wasn't me logging in."* (M46-C)
It Was Me	37	Participant would know why it was sent.	*"It wouldn't be a priority if I recognize the device, data, and location."* (L1-N)
Serious Consequences	31	Participant would assume that an attacker could cause serious damage.	*"It could have serious consequences."* (M53-C)
Security Is Important	11	Behaving securely is generally important to the participant.	*"Protecting my accounts is important"* (M31-C)
Just Info	8	Participant would see the notification as a heads-up.	*"I assume it's simply a courtesy email."* (L95-N)
Account Is Important	9	The account is important to the participant.	*"This account is important to me, so I want to make sure it's not compromised."* (M83-C)
Annoyed by Notification	4	Participant would be annoyed by the notification.	*"I will not waste my time pursuing something that is not a real security threat to my account."* (L83-N)
Identify Damage	4	Participant would want to understand what happened.	*"I would need to get to the bottom of the notification"* (L37-C)
BQ6: In your own words, please describe what this email is telling you.			
New Login	157	Participant describes that there was a new login.	*"It's alerting me that my account has been signed into."* (L61-N)
Abnormal Login	63	Participant describes that there was a new login which deviates from previous ones.	*"The main factor is a security issue associated with an unknown login to my account."* (L72-N)
Abnormal Login: Device	38	Participant describes that there was a new login from an unusual device.	*"There was a sign in to my account not recognized as me or one of my devices"* (L6-N)
Abnormal Login: Location	15	Participant describes that there was a new login from an unusual location.	*"someone signed in from California and I'm not normally in that area"* (M91-N)
Abnormal Login: Cookies	3	Participant describes that there was a new login without cookies.	*"I just logged in after not logging in for a while, so the cached session was probably expired, and it thought I was a new login."* (M87-N)
Abnormal Login: Time	1	Participant describes that there was a new login at an unusual time.	*"A new sign-in from a different location or a different time signing in."* (L91-N)

TABLE 6. CODEBOOK FOR **BQ7** AND **BQ11** USED IN SECTION 5.1 RQ1: COMPREHENSION & REACTION.

Code	Freq.	Description	Example
BQ7: In your own words, please describe all of the factors that may have caused you to receive this email.			
Hack	134	An unauthorized person logged into the account.	*"There could have been a breach into my account and jeopardized my security."* (M54-C)
New Device	90	Login with a new device.	*"Signing in on a different device than normally used"* (L40-N)
It Was Me	53	Participant logged in.	*"I logged in and triggered the email."* (L20-C)
New Location	32	Login from a new location.	*"Because someone signed into my account from a new location."* (M38-C)
Account Inactivity	12	Login after a longer period of inactivity.	*"I logged in to an account that I haven't tried in a long time and it wanted to give me notice"* (M62-N)
Deleted Cookies	11	Previously set cookies were deleted.	*"I probably have cleared all of my cookies so the site didn't recognize this device and though it was a new device."* (L28-N)
Phishing	11	Notification is a phishing attempt.	*"It is a phishing email... they probably just got a list of everyone who has AcmeCo emails and sent it out to all of them to try to get passwords."* (M25-N)
Unknown Login	9	An unknown login happened	*"The main factor is a security issue associated with an unknown login to my account."* (L72-C)
Shared Account	9	Someone who the account is shared with logged in.	*"If it wasn't me, then it might have been a loved one with my account access."* (L93-C)
Error	8	An error occurred on AcmeCo's side.	*"It could be an error, the email may have been sent to me by a glitch in the system."* (M57-C)
Notifications Enabled	8	The participant opted in to receive such notifications.	*"I have alerts set up to send this notice to me automatically every time my AcmeCo account is accessed (even if it's me who logged in)"* (L41-N)
BQ11: Why? (***BQ10**: I feel that ignoring this email from AcmeCo would have consequences. [Agreement Level]*)			
Someone Has Access	115	An attacker has access to the account.	*"Someone potentially may have hacked my account"* (L6-C)
It Was Me	37	It was the participant logging in.	*"There would be no consequences of ignoring it if the sign-in was me."* (L1-N)
Identity Compromised	36	Own identity could be compromised.	*"My personal info could be stolen and used for nefarious purposes."* (M7-C)
Depends	27	It depends on whether the login was legit or malicious.	*"It depends on whether this was me or not."* (L90-N)
Unclear	9	Participant has no clear opinion on the consequences of ignoring.	*"There is no telling what is happening."* (M94-C)
Compromise Other Accounts	7	Ignoring the notification could also compromise other accounts.	*"Someone else has my account and can use it to steal other accounts associated with this email."* (M11-C)
Lock Out	7	Access to the account could be lost entirely.	*"I feel that someone could get me locked out of my account."* (M28-C)
Just Info	6	Notification is just a heads-up.	*"It is a courtesy email."* (L95-N)
Check Login	5	Login needs to be checked.	*"I should at least ensure there was no fraud."* (L55-C)

TABLE 7. CODEBOOK FOR **BQ9** AND **BQ18** USED IN SECTION 5.2 RQ2: DECISION-MAKING & EXECUTION.

Code	Freq.	Description	Example
BQ9: Why? (***BQ8**: I feel that this email from AcmeCo explained to me how to resolve the situation. [Agreement Level]*)			
Explains Malicious	133	Participant appreciates that instructions for the malicious case are explained.	*"It gives me the option to change my password."* (L41-N)
Explains Both	53	Participant appreciates that instructions for the legit and malicious case are explained.	*"It explains to ignore the email if it was me, and change my password if it wasn't."* (L101-N)
Missing	33	Participant misses information or advice.	*"Changing my password is the very first line of defense, but I wish there was more information about what steps to take, or further assistance from AcmeCo."* (M26-C)
Provides Link	22	Participant appreciates that a link is provided to change the password.	*"The steps to take were very clear and easy to follow. It also provided a link to make it easy to change my password if I needed to."* (L42-C)
Notification Untrusted	10	Participant describes the notification to be untrustworthy.	*"It shouldn't be suggesting that I click the link in the email as this is a trick often used by scammers."* (M35-C)
BQ18: Referring to the situation where a similar email helped you to learn about an unrecognized sign-in. Please describe the situation, how you knew that something was wrong, and how you solved it.			
Malicious	134	It was not the participant signing in.	*"I changed my password for my email once because someone got a hold of it somehow."* (L42-C)
Location	68	Login took place at an unknown location.	*"I knew it because the login happened from a place I did not even visit and immediately changed my password."* (L43-C)
Location: Continent	19	Login took place on a different continent.	*"I received a notification that someone from another continent logged into my account and I immediately knew this was not me."* (L50-C)
Location: Country	17	Login took place in a different country.	*"I received an email that someone logged into my account from another country so I changed my password"* (L69-N)
Location: State	8	Login took place in a different state.	*"I had a login notification from California when I live in Texas. Immediately I knew someone hacked into my account."* (M61-C)
Unexpected	32	Notification came unexpected.	*"I knew something was wrong because I received a sign-in attempt notification from a website I hadn't used in a while, and hadn't even tried signing in to lately."* (M95-N)
Device	17	Login was done with an unknown device.	*"It was my instagram account, I hadn't logged in on that device they described, I changed my password"* (M20-C)
Account Sharing	10	Login was done by someone who the account is shared.	*"My kids sometimes use my accounts - Amazon, Netflix, Disney plus - I ask them to confirm it was them signing in - which is fine."* (L89-C)
It Was Me	10	It was actually the participant logging in.	*"I received a similar email from Amazon about a new sign in. It turned out that I used a new device that it didn't recognize."* (L10-C)
Time	2	Login took place at an unusual time.	*"I knew it was me because the sign in came at a time, and from a location, which did not at all correlate to my real world location, and I dealt with the situation as described in this study - I changed my password and ensured that 2FA was enabled."* (M27-C)

TABLE 8. CODEBOOK FOR **BQ3**, **BQ13** AND **BQ16** USED IN SECTION 5.3 RQ3: PERCEPTION & EXPECTATION.

Code	Freq.	Description	Example
BQ3: Why? (***BQ2**: I would feel [Concern Level] about receiving this email from AcmeCo.*)			
Someone Has Access	99	The account is accessed by someone else.	*"Cause someone else is using my account"* (M60-C)
It Was Me	41	Participant knows why it was sent.	*"Because I already know that I just signed in"* (L90-N)
Privacy Invasion	28	Participant mentions the private information which may be saved on the account.	*"i don't want someone to have access to my personal info"* (M39-C)
PW Exposed	13	Participant refers to the risk of an exposed password.	*"Someone is logging into my account which means they have my login info"* (M31-C)
Someone Tried	12	Participant focuses on someone trying to sign into the account.	*"Somebody else tried to log in to my account"* (L85-C)
Only Information	8	Participant sees the notification as a heads-up.	*"It seems like a normal security warning"* (L56-N)
Feeling of Security	5	Participant appreciates the information.	*"Because I like the added security function and appreciate the notice."* (L28-N)
Annoyed	5	Participant is annoyed by the notification.	*"It's not a problem. It is just annoying."* (L32-N)
Phishing	4	Participant sees the notification as phishing.	*"I would feel moderately concerned because it is a phishing email."* (M25-N)
BQ13: Why? (***BQ12**:I think real companies should send emails like this one when necessary. [Agreement Level]*)			
Protect Accounts	111	Notifications are a form of protection.	*"It's helpful and protects the persons data."* (M45-C)
Alert Users	95	Notifications alert users to unknown logins.	*"To alert customers about possible security breach"* (M67-C)
Show Protection	15	Sending notifications shows that companies are security conscious.	*"It shows that they care about users security."* (L22-C)
Annoying	10	Notifications are annoying.	*"These emails are incredibly annoying."* (L90-N)
Quick Action	9	Notifications allow to take a quick action in case something unauthorized happens.	*"You can immediately stop access to your account from people who exhibit criminal behavior"* (M91-C)
BQ16: Why? (***BQ15**: I [Frequency Level] read them.*)			
Account Security	110	Reading the notification assure that the account is secure.	*"Because it keeps my accounts safe and protected by monitoring this."* (L82-C)
Know Sign-in	33	Reading the notification depends on whether the login is known.	*"If I signed in from a second device and then received the email, I knew it was me, so I would ignore it. But when I didn't sign in, I would pay attention and read the email."* (L16-N)
Important	46	Reading the notifications is important.	*"I read them, cos they are important."* (M36C)
Check Details	36	Notification is read to check the login details.	*"Just in case it wasn't me. I look at the date, location, and time to determine."* (L20-N)

TABLE 9. CODEBOOK FOR **MQ2A**, **MQ2B**, **MQ3A**, **MQ3B**, AND **MQ11** USED IN SECTION 7.1 RQ1: COMPREHENSION & REACTION.

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 is 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)
BQ11: 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 10. CODEBOOK FOR **MQ10** USED IN SECTION 7.2 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 11. CODEBOOK FOR **MQ13** USED IN SECTION 7.3 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)