

# Was This You? Investigating the Design Considerations for Suspicious Login Notifications

Sena Sahin  
Georgia Institute of Technology  
ssahin8@gatech.edu

Burak Sahin  
Georgia Institute of Technology  
buraksahin@gatech.edu

Frank Li  
Georgia Institute of Technology  
frankli@gatech.edu

**Abstract**—Many online platforms monitor the account login activities of their users to detect unauthorized login attempts. Upon detecting anomalous activity, these platforms send suspicious login notifications to their users. These notifications serve to inform users about the login activity in sufficient detail for them to ascertain its legitimacy and take remedial actions if necessary. Despite the prevalence of these notifications, limited research has explored how users engage with them and how they can be effectively designed.

In this paper, we examine user engagement with email-based suspicious login notifications, focusing on real-world practices. We collect and analyze notifications currently in use to establish an empirical foundation for common design elements. We focus our study on designs used by online platforms rather than exploring all possible design options. Thus, these design options are likely supported by real-world online platforms based on the login data they can realistically provide. Then, we investigate how these design elements influence users to read the notification, validate its authenticity, diagnose the login attempt, and determine appropriate remedial steps. By conducting online semi-structured interviews with 20 US-based participants, we investigate their past experiences and present them with design elements employed by top online platforms to identify what design elements work best. Our findings highlight the practical design options that enhance users' understanding and engagement, providing recommendations for deploying effective notifications and identifying future directions for the security community.

## I. INTRODUCTION

Login notifications are integral elements of online account security, serving as a defense against unauthorized access. Suspicious login notifications are typically triggered by login abnormalities, including logins from a new device, geographical location, or irregular time. The primary purpose of these alerts is to facilitate immediate user awareness of potentially unauthorized access, thereby enabling rapid intervention.

In practice, existing login notifications exhibit significant diversity in designs, with different websites implementing varied combinations of notification components. This variability underscores a lack of clarity on the most effective ways to employ these notifications and poses challenges in directly assessing user preferences across a wide range of designs. Prior

security warning studies have largely focused on improving browser warnings, phishing alerts, malware notifications, and phishing trainings to keep users safe [1]–[15], leaving a gap in our understanding of user engagement with suspicious login notifications specifically. The context, user engagement, and necessary responses make login notifications unique, necessitating tailored design and communication strategies rather than directly applying lessons from other types of warnings.

Our study addresses this gap by focusing on user-driven design considerations to better align login notifications with user expectations. Through a structured co-design process, we not only explore user perspectives on individual notification components but also provide actionable insights into which design elements resonate most effectively with users and why. This approach allows us to move beyond prior work, such as Markert et al. [16], which focused on a single design, by engaging users in designing their own notifications and evaluating how different elements influence their trust and decision-making process.

Specifically, our work investigates the design considerations of email-based suspicious login notifications in real-world settings. We constrain our study to designs currently used by actual websites, as these are supported by the login data they can realistically provide. Additionally, the observed diversity in these designs makes identifying effective approaches among existing options particularly valuable. To address these challenges, we focus on four core research questions regarding notification email components:

**RQ1.** How do components capture user attention for engaging with the notification content?

**RQ2.** How do components facilitate user understanding about notification authenticity?

**RQ3.** How do components enable users to assess the legitimacy of the login event?

**RQ4.** How do components provide guidance to users about remedial actions, if necessary?

To answer these research questions, we first collected the suspicious login notifications used by real-world websites in order to analyze the design elements common in existing notifications. Our preliminary analysis reveals a wide diversity in notification components, indicating a lack of standardization around notification design. Grounded in our real-world observations, we then conducted an online semi-structured interview with 20 participants. In the first part of the inter-

view, we investigate participants' past experiences with login notifications. In the second part of the interview, participants were then presented with the notification design components observed from real-world notifications and tasked with constructing their preferred notifications. Through this multi-part interview, we identify how notification components engage, inform, and guide users in responding to unusual login events. We additionally determine what design components that our participants prefer, shedding light on how such notifications should be designed in practice.

Our study revealed that participants can utilize diverse information for evaluating login notifications and classifying the associated login events, highlighting the importance of nuanced notification design. We identified elements that help foster user trust and engagement with the notification, including recognizable senders, personalization, legitimacy warnings, and legal disclaimers. We also found that the notification's tone impacts user perception and response, with participants favoring language that raises the alarm without pressuring immediate action. Additionally, providing varied telemetry about the login attempt, as well as suggested actions, helped facilitate user response.

Ultimately, our study expands upon prior work on security notifications, not only informing the design of login notifications specifically but more broadly providing further insights into effective communication about security incidents. As an outcome of our work, we provide two primary contributions. First, our study offers empirical grounding on how different components of these notifications capture user attention, enhance understanding of their authenticity, assist in assessing the legitimacy of login events, and guide users in taking remedial actions. Second, drawing from our findings, we make grounded recommendations for improving suspicious login notification design and suggest directions for improving online authentication practices in the future.

## II. RELATED WORK

In this section, we discuss previous studies that have explored login notifications, particularly highlighting challenges, as well as the design of warning notifications.

**Login Notification Responses and Challenges.** Only a few prior studies have focused on login notifications. Redmiles [17], involving 67 participants from 5 countries, concentrated on Facebook login issues related to account security incidents and users' responses to secondary authentication (e.g., 2-FA) notifications. The study delved into users' mental models regarding their feelings and information-seeking behaviors during security incidents. Redmiles identified a lack of key information in notifications, such as whether the notification was about a legitimate login, as problematic. The context here is that the notification itself is not inherently suspicious but becomes so if the user did not generate it. In contrast, our work focuses on informative login notifications. We emphasize users' engagement, understanding of email legitimacy, comprehension of login legitimacy, and reactions to the notifications. Redmiles's scope was limited to Facebook

and secondary authentication, which reduces its overall generalizability across platforms and user contexts.

Markert et al. [18] studied administrators' configuration of risk-based authentication (RBA). RBA includes configuring notifications when the login is considered risky. The study found that notifications were often predefined or slightly customized, with a few administrators disabling them entirely. There was no consensus among administrators on what information to include in the notifications, and many struggled with the configuration interface. Administrators expressed a desire for more context and explanations to prevent phishing attacks and highlighted the inaccuracy of IP-based location estimation. Additionally, Wiefling et al. [19], [20] analyzed RBA solution designs, suggesting a need for more research in notification design. Those prior works highlight the need for guidance on notification design, which motivates our work.

The most similar study to ours was conducted by Markert et al. [16], which involved 229 participants and focused on their comprehension, reactions, and expectations regarding login notifications. They created one representative notification using 72 notification examples to understand how people reacted to this specific design and how they understood it. Their findings showed that while users could identify legitimate logins, they struggled with malicious ones and often did not know what actions to take. In contrast, our work explores more of the design space by examining various notification design options. Using real-world data, we created multiple notification options and provided these to participants, allowing them to design their own suspicious login notifications. While Markert et al. focused on one design and observed reactions to it, our work provides a more comprehensive and user-centered approach, exploring how users react to different elements of notifications and offering specific design recommendations based on user preferences and behaviors. Despite different methodologies, both studies converge on similar notification structuring approaches, enhancing scientific confidence. Our study advances further by offering specific, actionable recommendations for each notification section. While previous research suggests including instructions, we specify precise types, such as recommending password changes, two-factor authentication, and email legitimacy warnings. This granularity addresses practical implementation concerns, guiding users on immediate problem resolution and overall security enhancement.

**Security Warning Notification Designs.** Effective communication of security risks through warning notifications is a crucial aspect of modern platforms. Research in this domain, spanning notifications about browser security [3]–[6], [9], [21]–[23], phishing [1], [2], [24], malware [25], [26], data breaches [27]–[30], and two-factor authentication [31]–[33], has studied user perceptions, mental models, and preferences for such warnings. These studies have emphasized the significance of clear, comprehensible warnings, as well as the influence of user familiarity and historical context on warning receptions. Our research uniquely concentrates on suspicious login notifications from the end-user perspective. Suspicious login notifications are distinct from other security warning

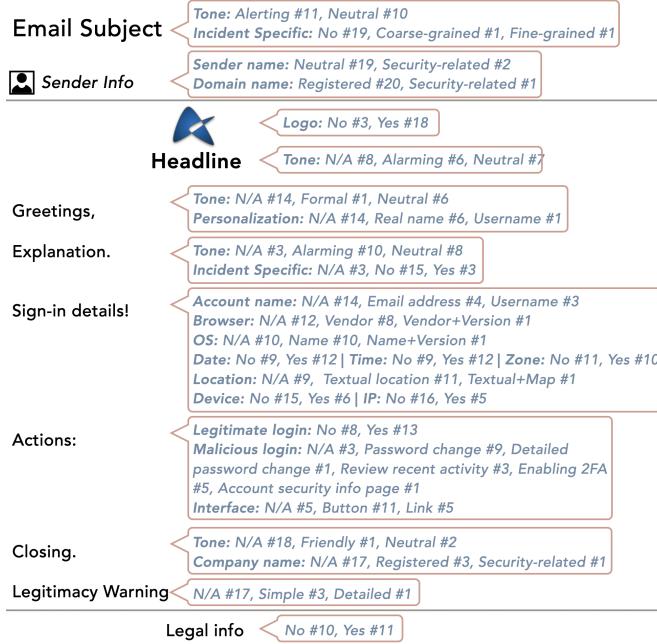


Fig. 1: Visualization of the notification components observed in our measurement of real-world notifications, and the design dimensions for each component. The numbers indicate the number of domains whose notification contained a component using a specific design dimension.

notifications. Firstly, login notifications alert users to potential unauthorized access to their accounts, requiring a different level of urgency and action than general security warnings. Unlike phishing and malware alerts, which often instruct users to avoid certain actions or websites, login notifications typically require users to verify their identity and secure their accounts immediately. The context, user engagement, and necessary responses make login notifications unique, necessitating tailored design strategies rather than directly applying lessons from other warnings.

### III. MEASUREMENT OF REAL-WORLD LOGIN NOTIFICATION DESIGNS

Here, we collect the login notifications used by real-world websites, in order to analyze the design elements common in existing notifications. This analysis then informs our investigation of effective notification design in subsequent sections.

#### A. Notification Collection Method

To ground our understanding of real-world suspicious login notifications, we attempted to collect email-based notifications from the top 100 websites as ranked by Tranco [34] in March, 2023. Our strategy was to create a test account on these sites and execute a suspicious login to solicit the login notification. For the top 100 domains, we manually found site-specific account login pages for 63 domains that were suitable for investigation. For the remaining sites, we opted not to include them because we either could not find a public login page,

the site’s login used a third-party service (e.g., single sign-on), or the site was excluded as our team was not comfortable evaluating an account on that site (i.e., adult sites).

Across these 63 websites, we followed a consistent manual method to attempt to trigger suspicious login notifications. First, we created an account on each site using a specific network and device, registering an email account under our control. For 13 domains, we were unable to create an account because the site did not provide public registration or required payment. For the 50 sites where we could create an account, we then logged into these accounts every two days, spending a few minutes interacting with the site, all while using the same network and device as during account creation. Our aim with this activity was to build a consistent user behavior profile on these accounts. After two weeks, we logged into the account from a new location, seeking to trigger a notification from this unusual login. Using a VPN set to a Lithuanian proxy<sup>1</sup>, we logged into the accounts using a new device and browser, distinct from the ones used for all previous logins.

From this process, we collected suspicious login notifications from 34 domains, demonstrating that such notifications are widely used. However, we observed that several domains were for the same organization and produced the same login notification (e.g., Google and Microsoft domains). Thus, in total, we gathered distinct login notifications across 21 websites. While we did not receive login notifications from the remaining 16 domains, they may still employ such notifications, and we simply failed to trigger them.

#### B. Design Analysis

To analyze the design of collected notifications, two researchers independently examined all notifications, categorized their components, and classified design decision variations for each component across notifications. Subsequently, they convened to discuss and compare their individual categorizations and classifications, converging upon the final design characterizations for notification components. From this analysis, we observed common notification components, but diversity in design decisions, as discussed below.

**Email Subject.** We observed several design variations in email subject. One observed design decision was the subject tone, varying between a neutral/informative tone (10/21 notifications) vs. an alarming one (11/21). We also observed variation in the amount of information provided in the subject line, from a generic subject (1) to an user/incident-specific one (1).

**Notification Sender.** We identified different strategies in the email sender’s information (username and domain). Sender usernames were either neutral (19/21), such as no-reply, or security-related (2/21). Meanwhile, email domains were primarily the site’s registered domain (20/21), but one site used a security-related subdomain.

**Logo.** We observed that the majority of notifications contained a site/company logo (18/21).

<sup>1</sup>We used a NordVPN proxy that we manually verified was IP geolocated to Lithuania.

**Headline.** In the notification bodies, we observed that 13 (21) started with a headline summarizing the notification content. For headlines, we observed similar design decisions as with the subject: 7 had a neutral tone while 6 had an alarming tone. **Greeting.** We observed that 8 (out of 21) notifications started the notification message with a greeting. These ranged from the presence or absence of a greeting to variations in tone, from neutral to formal. Specifically, six of them used a neutral *Hi* as the greeting, while one opted for a more formal approach using *Dear*. Additionally, the greetings differed in their use of personalization, with some using the user's real name (6/8) and others opting for usernames (1/8). One email used only the user's real name as a greeting.

**Explanation.** In notification bodies, we observed that most (18/21) contained text explaining the notification cause (while the others simply relied on the subject or headline as explanation). For these explanations, we classified two main design decisions. The first was a variation in the tone between a neutral/factual explanation (8/21) versus an alarming explanation (10/21). The second was varying specificity of the information, between only indicating that an unusual login had occurred (15/18) to specifying that the login was unusual because of the device or location used (3/18).

**Login Attempt Details.** The notification bodies varied widely in the types of login attempt details they provided. Five emails omitted login attempt details entirely, while sixteen emails presented various information. Seven emails included an account name; specifically four included an email address and three featured usernames. Browser information was present in nine emails, with one specifying the browser version. Operating system details were present in 11 emails, two of which provided version information. Date details were included in 12 notifications, with varying levels of specificity. Time was specified in 12 emails, mainly in a 12-hour format along with the time zone (one lacked a time zone). Location data was present in 11 emails and varied from country-only to city-level information, including a map in one case. IP address information was provided in five emails in IPv4 format.

**Suggested Actions.** Thirteen (out of 21) notification bodies included instructions if the login was legitimate, while 18 provided instructions for potentially malicious login attempts. The instructions in the notifications fell into several categories: changing the password (9/18), changing the password with an automatic logout of all active sessions (1/18), reviewing recent account activity (3/18), using a button to change the password or notify the company (10/18), enabling two-factor authentication (2FA) (5/18), and providing comprehensive account security advice (1/18).

**Closing.** Five notifications contained a closing statement. We identified two distinct design dimensions: the tone of the closing and the type of name used. The tone varied between neutral and friendly, while the name type was either the company's general name or a security-specific team. Two featured a neutral tone, using *Thanks* and one used a friendly tone, signing off as *Your Friends*. Three emails opted for the company's general name, and another concluded with only a

security-specific team name.

**Email Legitimacy Warning.** We observed that 4 out of 21 notifications contained text warnings about email legitimacy. Notably, these warnings fell into two distinct categories: brief cautionary statements advising against clicking on links for more information, and comprehensive advisories that highlighted security protocols and offered detailed guidelines for verifying links.

**Legal Disclaimer.** We note that 11 of 21 notifications contained legal disclaimers at the bottom of the email.

#### IV. USER STUDY METHOD

After analyzing real-world notifications, we next investigate end-user perceptions regarding the constituent design elements featured in email notifications for suspicious login events, derived from the components and design decision observed in our empirical measurement (in Section III). Our exploration is organized around four core research questions about email notification components.

**RQ1.** How do components capture user attention for engaging with the notification content?

**RQ2.** How do components facilitate user understanding about notification authenticity?

**RQ3.** How do components enable users to assess the legitimacy of the login event?

**RQ4.** How do components provide guidance to users about remedial actions, if necessary?

To address our research questions, we conducted a qualitative study involving end-users. Specifically, we conducted semi-structured interviews with 20 end-users where we asked participants to construct a suspicious login notification email. Subsequent interview questions probed their design choices, evaluative criteria, and previous encounters with suspicious login notifications. This approach granted us deep insights into user perceptions of each design element. Designing notifications through interviews allows us to identify the specific components that facilitate user engagement with an email, determine the email's legitimacy, assess the nature of the login attempt, and understand the remedial actions if required.

##### A. Recruitment

We recruited participants through the Prolific platform, focusing on U.S. residents over 18 years old. Participants were compensated \$10, based on an hourly wage of \$15 (aligning with general standards for research participation) for the 40-minute interviews. We launched the study on Prolific and awaited participants to join the interviews. Before joining, participants completed a brief survey to provide details such as age, location information, gender, education, and their CS/IT-related experience. Our analysis of the collected interview data achieves thematic saturation, indicating our data collection was conducted at an appropriate scale.

##### B. Semi-Structured Interviews

We conducted semi-structured interviews to examine user perceptions of various design elements in suspicious login

notifications (Appendix A lists our interview instrument). First, we asked about participants' prior experiences with such notifications. Specifically, we aimed to understand the content of these emails, the types of information and recommendations they offered, and the actions that participants subsequently took. We also asked how participants verified the legitimacy of these notifications and whether they could distinguish between alerts related to their own login activities and potentially malicious attempts. Additionally, we inquired about the overall utility of such notifications, asking whether participants found them to be helpful.

We then further examined participants' workflows upon receiving suspicious login notifications. We inquired about how participants decide to open such an email, criteria for determining the email's legitimacy, and methods for assessing whether the login activity was legitimate or malicious. We also asked about their decision-making process for taking corrective actions in the event of a malicious login, as well as the specific actions they would opt for. These questions were designed to provide us with a nuanced understanding of participants' general perceptions and decision-making strategies when faced with a suspicious login alert.

Finally, we sought participant input on designing effective notifications. We presented introductory information about suspicious login notifications, including showing an example notification for a dummy website. Additionally, we provided a narrative scenario in which participants were to assume they had an account with the dummy website. For this hypothetical scenario, we supplied them with assumed usernames and email addresses to be used for account registration. This setup was intended to ground participants in a realistic context, facilitating the creation of their own suspicious login notifications for the designated website.

We then presented participants with a blank notification template that only listed the names of potential notification components. Next, we showed them design options for each notification component, where the design options were formulated based on our real-world suspicious login notifications<sup>2</sup> (from Section III). Participants were then asked to design their own notifications by selecting from the available options under different components. Throughout the interview, we reminded participants that they were not obliged to include every listed component or to choose an option under each component. They were also informed that they could create a component entirely different from our pre-established options if desired. For each of their selections, we asked participants to articulate why they chose to include or exclude a particular component and why they preferred specific design options for each specific component. The detailed contextual insights gained from this study can help us to model how these

<sup>2</sup>For the notification greeting, we observed that personalization was a design dimension. While we did not observe this design dimension for the email subject and notification headline, we opted to test a personalized variant of these as well, as they can naturally contain personalization. All other components and design options that we used in our study were observed in our collected notifications.

preferences might manifest in everyday actions. Therefore, even though there's a possibility of discrepancies, the depth and richness of data from this study are invaluable for making informed suggestions.

To avoid participants' responses being biased by our pre-defined options, we first asked them to recall their past experiences with notification emails. This approach allowed us to gather their raw experiences and understand their natural reactions to various aspects of email notifications, such as what prompts them to open an email, how they assess its legitimacy and the authenticity of the login, and what influences their decision to take action. By collecting this unguided feedback first, we better understood their personal preferences and experiences. Only after acquiring this data did we present our options to the participants.

After participants had completed their designs, we engaged them in a reflective discussion about their choices. We asked them to compare their custom-designed notifications with the original example provided, specifically noting what they liked and disliked about each. We also inquired whether, should they receive their own designed notifications in the future, there were additional elements they would want included that were not among the options we had provided. Lastly, we asked them to assess the completeness of their designs and identify anything missing.

Ultimately, our multi-part interview assessed participant interactions with suspicious login notifications from different angles, providing a more comprehensive characterization of the human factors at play. From June to August 2023, we conducted our interviews with 20 participants. The first three interviews served as a pilot study. From these pilot participants, we validated that our interview instrument was providing the insights and answers desired for our research questions, and thus we did not significantly modify our interview instrument beyond removing a few redundant questions. We include the pilot participants' data in our final results, as their interview questions are a superset of subsequent ones. To maintain consistency, all interviews were led by one researcher. The interviews were conducted via the Zoom video conferencing platform and had an average duration of 42 minutes.

### C. Data Analysis

All interview recordings were transcribed and subjected to iterative open coding analysis [35]. In the initial stage, two researchers worked independently to identify coding schemes for each segment of the interview questions, drawing from the responses of all participants. These researchers subsequently convened to integrate their individual coding schemes into a unified codebook. Using this finalized codebook as a reference, each researcher independently coded the collected responses from the participants. To evaluate the consistency of the coding process, we computed the Kupper-Hafner inter-rater reliability scores [36], yielding an average agreement of 0.93. This score indicates highly consistent coding between the coder pairs. Subsequently, the two researchers met to discuss the final codes assigned to each participant's response. Throughout

TABLE I: Demographics of our participants. We had 11 females and 8 males (1 indicating other). Only 3 participants had IT job experience. Our participants had diverse educational backgrounds and spanned multiple age ranges.

ID	Age	Edu	Gender	IT Job Exp.
P1	30-49	B.S.	M	No
P2	30-49	B.S.	O	No
P3	30-49	M.S.	F	No
P4	30-49	High School	F	No
P5	18-29	B.S.	F	No
P6	50-69	M.S.	F	No
P7	30-49	B.S.	F	No
P8	30-49	B.S.	F	Yes
P9	50-69	Some College	F	No
P10	50-69	M.S	M	No
P11	30-49	Assoc. Degree	M	No
P12	30-49	Some College	M	-
P13	30-49	Some College	F	Yes
P14	18-29	High School	F	No
P15	18-29	M.S.	M	No
P16	30-49	B.S.	F	No
P17	50-69	B.S.	M	No
P18	30-49	Assoc. Degree	M	No
P19	18-29	Some College	M	Yes
P20	18-29	M.S.	F	No

this iterative process, all research team members engaged in periodic discussions to resolve disagreements and validate that the identified themes, which are elaborated upon in the paper, accurately represent the team’s collective data interpretation.

#### D. Participants

As listed in Table I, our 20 participants were diverse across education level and gender. The majority of our participants don’t have IT job experience. Our participants are from different age groups, allowing us to observe the different perspectives of young adults and elderly people.

#### E. Limitations

Our study shares inherent limitations common with interview-based qualitative research methodologies, including social desirability bias, wherein participants may provide responses they perceive as more socially acceptable, particularly in the sensitive domains of security and privacy. To mitigate those biases, we employed strategies including ensuring anonymity in responses, creating a non-judgmental environment during sessions, and emphasizing that all feedback about suspicious login notifications, whether positive or negative, was valuable. These measures were designed to encourage honest and uninhibited input from participants.

Additionally, our study acknowledges potential recall bias, where participants might not accurately remember details of their past experiences. However, the qualitative nature of our exploratory research primarily sought to uncover diverse user perspectives and behaviors rather than accurately characterize past events.

Furthermore, the scale and scope of our participant pool, primarily restricted to individuals within the United States, may not provide a comprehensive view of global end-user experiences. While this limitation impacts the generalizability

of our findings, it is suitable for our study’s exploratory objectives. Future research could extend to more diverse populations and potentially involve a larger-scale quantitative analysis of real-world user behavior.

We also note that our participants largely lacked expertise in security or design. This deliberate selection aligns with participatory and co-design methodologies, which prioritize the involvement of end-users as experts in their own experiences, fostering a collaborative environment with technical experts [37]. To facilitate the co-design process, we provided participants with a template for a suspicious login notification along with various design options. While participants were encouraged to design freely based on their personal preferences, the use of our template and pre-defined options may have constrained creativity or biased participants toward considering only those elements presented. We note that some participants did go beyond the template, although these additions only involved a couple minor design considerations (discussed in Section VII-B), suggesting that our template captured common design options.

Finally, the ideas generated were primarily conceptual, serving as a lens through which we synthesized design implications, rather than definitive recommendations. Nonetheless, our findings lay the groundwork for defining the design space for suspicious login notifications. Future research, such as by industry stakeholders with access to a large user base, could expand and refine this investigation.

#### F. Ethical Considerations

This research was reviewed and approved by our university’s Institutional Review Board (IRB). We acquired informed consent from all participants. They were explicitly notified that they reserved the right to abstain from answering any questions that made them uncomfortable and could halt their participation at any point. Prior to conducting the interviews, we also secured permission from the participants to record the sessions. All gathered data underwent anonymization procedures and has been securely stored, with access restricted to our research team members.

## V. PAST EXPERIENCES WITH LOGIN NOTIFICATIONS

In this section, we consider participants’ past experiences and their general perception of suspicious login notifications, providing initial insights towards our research questions. To do so, we asked participants about various aspects of their most recent experience with suspicious login notifications. Specifically, we asked what was the content of the notification email they previously received, what information and suggestions it provided, what actions they took upon receiving it, how they verified the legitimacy of the email, and whether they were able to discern if the login attempt was their own or potentially malicious. Additionally, we sought to understand which notification features helped or hindered them in making these determinations. These inquiries were designed to trigger participants’ memories, thereby preparing them to design a notification email informed by their own experiences.

**No Experience.** Two participants reported a lack of prior experience with suspicious login notifications, indicating that not all users may encounter such notifications regularly or recognize them when they do.

**Legitimate Login.** Eight participants received suspicious login notifications triggered by their own logins. P12 noted that these notifications were “instantaneously triggered automatically,” reinforcing the immediate correlation between their login activity and the received alert. This timing led all participants to attribute the notification to their own actions correctly. Moreover, participants indicated awareness of specific conditions that tended to prompt these suspicious login notifications, including logging in from a device or location other than their regular ones.

**Malicious Login.** Twelve participants reported experiences with malicious login attempts. They were able to clearly identify the logins as unauthorized, primarily because the notifications highlighted discrepancies such as foreign locations, unfamiliar devices, or new IP addresses. These alerts often informed participants about their login activity and provided a link suggesting a password change as a precaution. While all participants claimed to have changed their passwords following such an incident, a notable majority (10/12) refrained from using the email-provided link for this purpose. Rather, they visited the official website to change their passwords via the account security page. P16 exemplified this cautious behavior, expressing hesitation to click on email links and stating, “I don’t click on the email links because this seems suspicious, and I don’t quite know if they’re real or if they’re spam, like trying to trick me into clicking on those links.”

**Provided Information.** Participants indicated that the notification emails provided them with an array of information, including location, device, IP address, date, time, browser, and recommended actions like changing their password in cases of unrecognized logins. However, P3 noted that some notification emails included vague details. Of note, eight out of 20 participants indicated that they share their accounts with family or friends, and occasionally receive notifications triggered by these known users’ activities. In such instances, they investigated the location and device data to determine the legitimacy of the login. P6 further elaborated that they were able to identify a malicious login through the “recent activity” section of their Facebook account after receiving a suspicious login notification.

**Notification Usefulness.** All participants expressed that suspicious login notifications are useful. They considered these notifications crucial for alerting them to potential malicious activity, prompting them to take preventive measures such as changing their passwords. Even in cases where the notification originated from their own login activities, participants viewed it as advantageous. They considered these notifications to serve as a form of verification, confirming not only successful login but also the up-to-date nature of their contact details with the respective site. P3 emphasized the importance of detailed, rather than vague, information within the notifications, stating, “I think if it doesn’t have a lot of information, that’s when it

tends not to be as helpful.”

Participants stressed the importance of timely notifications. For instance, P15 noted, “It usually tells you immediately so you can resolve it before anything happens.” P16 also highlighted this significance. Despite receiving an immediate alert, their account had already been compromised by the time they attempted to resecure it. The attacker had altered substantial information, necessitating contact with customer support to regain access and change the account password. The timeliness of the notification, however, enabled them to limit the extent of unauthorized changes. Similarly, P9 described an incident involving a malicious login to their internet service account. The timely notification allowed them to immediately expel the unauthorized user. Despite also receiving notifications for legitimate logins, P9 expressed a sense of enhanced security from receiving such alerts. P14, however, emphasized that the notifications must be professionally crafted, considering the serious nature of potential security incidents. Poorly written emails, P14 warned, could be easily mistaken for spam, thereby undermining their effectiveness.

Participants have and continue to find suspicious login notifications useful, particularly when they are timely, informative, and well-crafted to avoid suspicions of phishing/spam.

## VI. WORKFLOW FOR PROCESSING LOGIN NOTIFICATIONS

In this section, we further examine our core research questions through investigating the workflows and decision-making processes that users employ for processing login notifications. Specifically, as part of our interview, we asked our participants questions about their process for deciding to open the notification email, determining the email’s legitimacy, assessing the legitimacy of the login attempt, and identifying remedial actions. This portion of our study reveals the step-by-step workflows of our participants, complementing our investigation of their past experiences (in Section V) and how they engage with individual notification design components (in Section VII).

### A. Deciding to open the notification email (RQ1)

In this section, we consider our first research question (RQ1) on how notification components capture user attention and encourage engagement with the content. Specifically, we examine three core factors that influence participants’ decisions to open notification emails: 1) evaluation of sender information, 2) assessment of the subject line, and 3) contextual relevance of the email.

**Sender Information Assessment.** Almost all participants (19/20) indicated that the sender’s information is one of the details they examine before deciding to open an email. This examination involves looking for red flags such as random strings or numbers in the sender’s email address, unfamiliar names, or incongruent domain names. Participants actively compare the sender’s domain name against the authentic website’s domain to assess legitimacy. For instance, P7 stated, “If the sender’s

information includes random capitalized letters and numbers, I'm less likely to open the email. However, if it starts with 'noreply' followed by a familiar domain name, I feel more secure in opening it." Furthermore, in cases of unfamiliar senders, P18 reported using an online service to perform a security check on the email sender. If the sender passed these checks, they would consider opening it; otherwise, they would opt to block the sender and delete the email.

**Subject Line Evaluation.** Another factor mentioned by most participants (12/17) was its subject line. Our participants showed a preference for subject lines that directly indicate the email's content, particularly if it pertains to security issues such as suspicious account activity or unusual logins. However, subject lines with urgent phrasing, such as "Urgent" or "Attention," were generally met with skepticism. Also, participants checked the grammar of the subject line. P16 mentioned that any discrepancies in subject matter or misspellings of their name or username would lead them to dismiss the email as untrustworthy.

**Additional Factors.** The placement of an email within the inbox influenced some participants' trust levels; emails found in the main inbox were typically considered more trustworthy than those relegated to other folders. Additionally, the context in which an email was received also played a critical role in its perceived legitimacy. P4 noted, "I wouldn't think it would say 'suspicious' unless it wasn't me," highlighting the trust users place in the security measures of reputable platforms.

Before opening the notification, participants primarily evaluated the legitimacy of the notification sender, as well as the content of the email subject.

#### B. Assessing the legitimacy of the email (RQ2)

Here, we tackle our second research question (RQ2) on how participants assess the legitimacy of emails. This section introduces new factors participants consider, such as the quality of the written language, the presence of links, and other visual and content-related cues.

**Evaluation of Email Content Quality.** A significant portion of participants (15/20) considered the quality of the email's written language as a critical factor in assessing its legitimacy. This includes examining the email for typos, grammatical errors, and the overall coherence of the written language. P12 pointed out that "sloppy typos and grammar are typical of low-end hackers," suggesting a correlation between email content quality and the perceived sophistication of the sender. Conversely, P14 highlighted a counterintuitive strategy where some hackers might intentionally include errors to filter out savvier recipients.

**Skepticism Towards Links.** Ten participants expressed skepticism towards emails that required clicking a link within the body text, preferring to visit a known website to manually take any necessary actions. P7 said, "The fewer links you need to click in the email, the better." Eight participants examined hyperlinks to confirm they were directed to a legitimate site.

**Additional Legitimacy Indicators.** Other considerations included the presence of a company logo (9/20), contact information (6/20), and attachments, which P2 considered a red flag. Six participants cross-verified the notification with alerts on the actual website, while five participants conducted Google searches to check for phishing schemes. P17 also analyzed the email's visual quality, noting that "repeated copying can make text look grainy," while P18 considered the presence of cc'd recipients as a phishing indicator.

Overall, participants carefully evaluated the authenticity of email notifications, weighing multiple factors before taking any actions. This showed that such login notifications prompt a lot of scrutiny from our participants.

Most participants evaluate the legitimacy of an email by considering the quality of the written language, the nature of any provided links, and company-specific details.

#### C. Assessing the legitimacy of the login (RQ3)

This section considers our third research question (RQ3), focusing on how users determine the legitimacy of login events. Participants employed a nuanced, multi-faceted approach, relying primarily on location information, device details, and the timing of login attempts as key assessment criteria.

**Location Information as a Primary Indicator.** Most participants (16/20) cited location information as one of the most critical factors in determining the legitimacy of a login attempt. When the location specified in the notification email differed from the participant's actual location, this discrepancy significantly increased suspicions of malicious activity. This finding underscores the importance of accurate and detailed location data in security notifications.

**Device Information.** Following location information, device details were the other most frequently (11/20) cited factor, as crucial in assessing login legitimacy. The type of device purportedly used for the login provided participants with a context to judge whether the login attempt was genuine. P14 noted that, due to residing in a location poorly indexed by services, they relied more heavily on device information and the timing of the login attempt.

**Timestamps.** The timestamp of the login attempt was analyzed by seven participants, who identified unusual times, such as early morning hours, as particularly indicative of suspicious activity.

**The Role of Notification Timing.** Ten participants mentioned that the timing of the notification was an essential aspect of the notification's effectiveness. Timely notifications, particularly those received in close proximity to the participant's own login activities, allowed for immediate verification of the legitimacy of the alert. This immediate feedback loop was crucial in enabling participants to confidently assess the relevancy of the login notification.

**Additional Considerations.** A few participants also looked at the IP address, although these were not as prominently highlighted as location, device, and time information.

Participants assessed login legitimacy through various factors, particularly the login location and device. Notifications closely following legitimate logins was another valuable signal.

#### D. Deciding to take an action (RQ4)

In this section, we address our fourth research question (RQ4), which examines how components guide users in taking remedial actions in response to login notifications. Specifically, we explore the types of actions users are prompted to take and the factors influencing their decision-making.

**Password Change as a Primary Action.** All participants stated that changing their passwords was their immediate course of action upon suspecting a malicious login attempt. This consensus underscores the perceived effectiveness of password updates as a fundamental security measure.

**Reviewing Email Options.** Twelve participants disclosed that they reviewed the options suggested within the email notifications before taking any action. This approach suggests a balanced consideration of the advised security measures, indicating a level of trust in the notification's content to guide their response effectively.

**Avoidance of Email Links.** Ten participants expressed a cautious approach to the links provided within the notification emails. To avoid potential phishing traps, these participants preferred to manually visit the website and change their passwords through the site's security settings.

**Seeking Further Assistance.** For cases where the account was already compromised or where participants encountered difficulties in recovering their accounts, six participants reported that contacting customer support was their next step.

**Reactions to Legitimate Login.** When participants deemed the login attempt to be legitimate, they generally did not take further action, treating the notification as informational.

**Specific Considerations for Non-Critical Accounts.** One participant highlighted a nuanced consideration for accounts deemed non-critical, such as a gaming account with no private information or monetary value. In this case, the participant chose not to respond to the malicious login attempt, indicating a calculated decision to not invest in protective measures for accounts of lesser importance.

Most participants took guidance on next steps from notifications, but were particularly wary of links.

## VII. LOGIN NOTIFICATION DESIGN CONSIDERATIONS

Here, we investigate the design considerations of suspicious login notifications, evaluating the notification components and design options observed in real-world notifications (from Section III) through our designing with interviews approach.

### A. Design Options

We first investigate users' understanding and preferences concerning the various components of suspicious login notifications. Our objective is to clarify how each element of the

notification—ranging from the email sender and subject line to the detailed information within the email body—affects users' perceptions. By examining these specific aspects, we aim to shed light on the cognitive processes that guide user interactions with suspicious login notifications, and offer insights for enhancing the notification effectiveness, further addressing our four research questions. For each component, we indicate which research questions are addressed through its evaluation.

We identified the components and design decisions for suspicious login notifications from our analysis of real-world notifications (from Section III). During our interview study, we presented these components and design options to the participants, who then crafted their own suspicious login notification emails. We also note that participants observed the full notification design template throughout the interview; thus, they were cognizant of different design elements rather than narrowly only viewing one design element at a time. As a result, they could make design decisions for one element based on their decision for another (e.g., avoiding redundant/repeating information).

**1) Email Subject (RQ1):** We categorized the email subject along three dimensions: 1) personalization (name or username) in the subject, 2) the tone of language used (alarming vs neutral), and 3) the level of information specificity.

**Personalization.** We observed that personalization was one subject line design element that many of our participants preferred. Overall, 11 out of 20 participants chose to add their usernames (8) or names (3) in the subject line, mentioning various reasons centered around specificity, legitimacy, and security. For example, P8 and P9 associated the presence of the username with increased legitimacy, as it serves as an additional layer of verification. P13 emphasized the value of the username for instant account identification. Overall, more participants preferred username over name as they felt username was more identifying. For example, P14 argued that usernames are less likely to be known to attackers.

The remaining 9 participants chose not to include personalized information in the subject. For these participants, the necessary details would be in the email body. Five participants noted that they are used to generic/standardized notifications, so they did not expect personalization. We note these participants did not express opposition to personalization though.

**Tone.** Most participants (15/20) preferred an alarming tone in the email subject to highlight the urgency of a suspicious login event, with seven participants mentioning that a neutral-toned subject might be overlooked or dismissed. For instance, P15 mentioned that "Aggressive tone seems more urgent. If it just says new login, I could be thinking that I logged in at first". Seven participants also noted that they are already familiar with real-world notifications using alarming tones. Conversely, five participants selected a neutral tone, citing concerns such as anxiety or false positives. For instance, P11 expressed skepticism about the authenticity of suspicious login claims, arguing that what is flagged as suspicious might simply be a legitimate login from a different device.

**Incident Specific.** Our participants were divided on the

information specificity in the subject. While nine advocated for some specific alert information to enhance credibility and prompt action (similar to personalization) and four advocated for vague descriptors, seven opted for a straightforward subject, reserving details for the email body.

Most participants preferred an aggressive-toned subject with incident-specific information.

2) *Notification Sender (RQ1 & RQ2)*: We consider two parts of the sender email address: username and domain name.

**Email Username.** Thirteen participants preferred a neutral sender name for its perceived legitimacy. For example, P7 mentioned that sender names like no-reply discourage interaction and signal legitimacy. Conversely, seven participants selected security-related sender names for their professionalism and enhanced security feel. P11 noted that modern systems often allow replies, making “account security team” a more reliable sender name, although no-reply might have been more relevant in the past.

**Domain name.** Fourteen participants picked using the registered domain name as it was more recognizable. For example, P4 noted that these domains are less suspicious and easier to read, defending against phishing. Meanwhile, the remaining six participants chose a security-related subdomain (we did not test a totally distinct name, which is often used for phishing and hence not recommended) for additional context on the notification sender.

Most participants preferred the notification be sent by an email address with a neutral username and the registered domain name.

3) *Logo (RQ2)*: Nearly all participants (19/20) preferred including the logo to enhance legitimacy and professionalism. For example, P11 said that logos “look more official”. However, several acknowledged that logos alone do not guarantee legitimacy as they can be easily copied. P4 chose not to include logos due to a personal preference for design simplicity.

Nearly all participants preferred notifications with the company/website logo (although this alone does not guarantee legitimacy).

4) *Headline (RQ2)*: Five participants found it unnecessary to include a headline, arguing that the email subject already contains the required information. “The subject line already tells me what the email is about,” said P13. For the remaining participants, we categorized their headline preferences along two dimensions: personalization and tone. The options for each category were as follows: real name vs. username for personalization, and neutral vs. alarming for tone.

**Personalization.** Six participants preferred a username as a stronger identification indicator. For instance, P14 said, “It’s what I identify with the site.” Three other participants selected using their real name, as it felt more personal and professional. P12 opined, “Being addressed by my first name is more

personal than by an impersonal username.” The remaining six participants included headline without any personalization, stating that it made the email seem more standard and in line with what they had seen before.

**Tone.** Eight participants preferred an alarming tone for its eye-catching and unambiguous nature, encouraging immediate action. For example, P7 said “‘You have signed in’ can kind of imply that it’s fine and you don’t need to worry about it because it’s you.” In contrast, seven participants chose a neutral tone, arguing it aligns with established services and avoids unnecessary panic. P11 emphasized that the email’s role is to inform, not alarm, given the system’s inability to verify user identity. P16 advised against exaggerated language, suggesting it could be linked to spam, and recommended straightforward terms like “new sign-in” for clarity.

Most participants preferred having a notification headline. For those that did, most favored including personalization but were split on the headline tone.

5) *Greeting (RQ2)*: Ten participants found greeting unnecessary, and that a greeting in automated or urgent notifications might be redundant and could diminish the message’s urgency or gravity. For the remaining 10 participants, we categorized their preferences into Personalization (name or username) and Tone (casual vs formal).

**Personalization.** Eight participants indicated that using their real name added a layer of personalization and credibility. For example, P16 mentioned that using their real name indicated private knowledge, enhancing the email’s legitimacy. Two participants selected usernames as they were more specific to their account.

**Tone.** Most participants (8/10) selected a causal greeting *Hi* for its friendly nature and wide acceptance. Several participants associated the formal greeting *Dear* with scam emails, thereby viewing it as less trustworthy. In contrast, the two participants who chose *Dear* did so because they felt it added formality and legitimacy.

Participants were split on including greetings. If included, they preferred casual greetings with the user’s real name.

6) *Explanation (RQ2 & RQ3)*: All participants included an explanation. These explanations were categorized along two dimensions: Tone (Neutral vs Alarming) and Information (Incident Specific).

**Tone.** Most participants (15/20) preferred an alarming tone, to draw immediate attention to potential unauthorized activity. Participants largely agreed that assumed or generalized statements like “you recently signed in” should be avoided. P16 even stated that the email should explicitly communicate that something appears to be abnormal, prompting the recipient to investigate further.

In contrast, five participants preferred a neutral tone, arguing that the email should avoid making assumptions about who initiated the login. They believe that a neutral tone enables

them to better assess the situation.

**Incident Specific.** Most participants (17/20) included the incident-specific reason for receiving the notification, such as login from “a new device” or “location,” arguing that this extra information provides valuable context and insights into the login event. For instance, many felt that specifying the reason for receiving the email would enhance their understanding. P13 clarified that the alert should explicitly state why it was triggered, allowing the user to determine whether the activity was indeed unauthorized. In contrast, three participants chose generic explanations for conciseness.

All participants preferred including an explanation in the notification body, with most preferring an aggressive tone while including incident-specific information.

7) *Login Attempt Details (RQ3):* We showed participants with multiple sign-in information variables, each with different options. Participants selected the options they believed would most effectively help them distinguish between legitimate and malicious login attempts.

**Account Name:** We investigated participants’ preferences for listing the login account’s username and email address. Eight participants opted to include both, arguing that this combination adds a layer of reliability to the email. P19 noted that having both details helps users with multiple accounts identify which one might be compromised. Five participants chose to include only the email address, mentioning it helps distinguish between multiple accounts, while another five felt that just the username was sufficient for account identification since it’s the primary login credential. P15 noted that repeating the email address was redundant as the notification email was already sent to that address. Two participants opted for neither, arguing that such details would not help in identifying an illegitimate login, and preferred a more concise notification.

**Browser.** We examined whether participants would like to include browser vendor and version information. Participants (17/20) opted to include browser details, with ten focusing solely on the browser vendor, stating it helps quickly identify if the login was authentic. They excluded version numbers largely due to unfamiliarity, as P10 explained, “Version would mean nothing to me.” The remaining 7 participants included both browser vendor and version, believing that this could help tech-savvy individuals verify the activity more accurately. P14 noted, “I’ll definitely be seen off if it’s an older version for what I’m currently using.”

**Device:** We investigated participants’ preferences regarding including device information—specifically the brand, model, and version—in login notifications. All 20 participants opted to include device information. Ten participants preferred including only the brand and model, arguing these details are more recognizable and help quickly spot unauthorized logins. The other ten included version information, arguing it offers a more nuanced understanding of login activity, especially when multiple users have similar devices. They suggested that version details could also indicate the device’s age, providing

an extra layer of verification.

**Operating System.** We further explored participants’ opinions on including operating system (OS) name, version, and minor version. Only 12 participants opted to include OS information, with the remaining 8 considering it non-essential (e.g., P16 said they would not know what to do with such information). Five participants included only the OS name, two added the version, and five opted for comprehensive OS details, believing more information was better.

**Date.** Participants had the option to include the date of the login with different information: day, month, year, and day of the week. All participants included the date (day, month, year) of the login, with only five adding the day of the week.

**Time.** Participants could also include the time of the login, either under as 12-hour or 24-hour time format. All participants included the time, with 16 choosing the 12-hour format familiar in the U.S., as P18 noted, so people in other geographic regions may prefer the format common in their locale. Four participants preferred the 24-hour format for personal or professional reasons (e.g., military background).

**Time Zone.** Every participant included time zone details, with 12 preferring the timezone of their usual login location for easier time conversion, even if a suspicious login occurs from a different timezone. Eight participants wanted the timezone of the actual login to flag suspicious activity.

**Location.** Participants were given the option to include location information, either in a text format specifying the city, state, and country or via a visual representation using a map with either a pinpoint or a circular marker. All participants included textual location data. Nine participants found this sufficient and preferred to look up unfamiliar locations independently. Ten participants added a pinpoint map for more specific visual data, and one chose a circular marker, questioning the accuracy of pinpointing an exact login location. Participants also pointed out the inaccuracy of IP-based location estimation.

**IP Address.** We presented participants with the option of including IP address information, in either IPv4 or IPv6 format. Six participants deemed it unnecessary due to unfamiliarity, as expressed by P4, “I wouldn’t know what to do with it.” However, 14 participants wanted the IP address included for deeper investigation or reporting to authorities. Among those, all preferred the IPv4 format due to its familiarity and shorter length. (We note though that in practice, the login attempt could be over IPv4 or IPv6, so this is not a configurable parameter by the online service. None of the participants mentioned this caveat though.)

Our participants strongly preferred extensive, detailed login diagnostics. These include account name, browser vendor, device brand, date in month/day/year format, time in a 12-hour format, time zone, location in text format, and the IP address in IPv4 format.

8) *Suggested Actions (RQ2 & RQ4):* We presented participants with the option to include suggested action items for

both legitimate and malicious login cases. The legitimate login category had one option, while the malicious login category offered seven different options (as outlined in Section III), aiming to guide users on appropriate actions to take in the event of a malicious login.

**Legitimate Login.** Most participants (19/20) favored including an action explanation for legitimate logins to avoid unnecessary actions like password changes. For example, P15 considered it as a reassuring message that the account has not been locked and no further steps is needed. Only P7 found the extra explanation redundant, arguing that the notification itself should be sufficient.

**Malicious Login.** First, participants had two options for linking to a password change page: a direct link and a link noting that changing the password would result in logging out all active sessions. All participants chose the second option, appreciating the added security detail. P14 highlighted the urgency of the situation, saying, “In a situation like this, you want to act as quickly as possible. Having that extra layer of protection is really nice”, while P15 found the logout feature reassuring for account safety.

We also allowed participants to include instructions to review account activities, preferred by 12 participants. Some participants valued its thoroughness, while P10 warned that technical terms might confuse some users. P11 highlighted its usefulness for establishing a timeline of events.

Additionally, 13 participants opted to add instructions for enabling two-factor authentication (2FA), viewing it as crucial for preventing unauthorized access. P10 emphasized the importance of a step-by-step guide for enabling 2FA.

Finally, we offered participants the option to add instruction to a general security guide page, included by 11 participants. They appreciated the educational aspect of this feature for preventing future unauthorized logins. P11 noted that such a link could also ease customer support workload, as users might consult these resources before seeking further assistance.

**Interface.** To direct users to external websites, we offered both links and buttons. Most participants (16/20) opposed including buttons as it was less clear where the buttons would direct to. The remaining 4 were open to including buttons but would want to first check the associated hyperlink for legitimacy. Thus, we conclude that links are still preferred, particularly when showing the destination URL. We note though that nearly all participants commented on how instructions should not require users to click links, and rather offer links for convenience.

Participants all preferred detailed instructions for both legitimate and malicious login cases, emphasizing the importance of clear guidelines and immediate actions like password changes and 2FA activation. To direct users to external webpages, they preferred links showing the destination URLs, so long as the instructions did not require users to click the links.

9) *Closing (RQ2):* We evaluate both the closing phrase (Friendly vs Neutral) and the closing name (Company Name vs Security-specific Name). Five participants chose to omit the closing phrase, arguing that this made the email more straightforward. Some emphasized that since these emails are automated, a closing was unnecessary.

**Tone.** Most participants (12/15) chose a neutral tone for email closings, emphasizing its formality and professionalism. For example, P5 noted that *Thanks* is more appropriate than *Your Friends* in a corporate context. Only three participants preferred a friendly tone for its personal touch.

**Closing Name.** Twelve participants chose a security-related team name for the closing name, arguing it added credibility. For instance, P15 said, “I like to know who’s sending the email, and I feel like that kind of makes it seem more legitimate to know who exactly sent it.” On the other hand, six participants opted for the original company name as the sender, considering it a clear indicator of the email’s legitimacy.

Most participants favored including a closing, preferring a neutral phrase and a security-related closing name.

10) *Email Legitimacy Warning (RQ2):* At the bottom of the notification, participants were offered the option to include a warning about email legitimacy. The two options provided were 1) a brief warning with a hyperlink for additional information, urging users to confirm the email’s origin, and 2) a comprehensive warning that cautioned against clicking embedded links and emphasized the website’s security protocols, also providing guidelines on link verification and a hyperlink to further resources.

Nearly all participants (19/20) added detailed email legitimacy warnings, seeing them as offering assurance and a sign of genuine communication. Participants valued these warnings for offering verification suggestions and enhancing user control. For example, P15 emphasized the informative value of the detailed warning, saying, “It says they won’t ask you for personal information, so if somebody does from a different email, then it wouldn’t be them. It just explains more about their security precautions.” 12 participants claimed such detail was unlikely in phishing attempts. However, P14 argued that only phishing emails focused on proving legitimacy and providing detailed information to deceive users.

Nearly all participants favored including a detailed legitimacy warning.

11) *Legal Disclaimer (RQ2):* We asked participants about their preference for including legal information. All participants agreed on the importance of including legal information at the end of emails for cross-referencing and verifying legitimacy. For example, P6 mentioned that they would “Google the address to confirm its authenticity”. Many participants mentioned it added an extra layer of legitimacy, giving users the option for further verification if needed.

All participants preferred including legal information in the notification content.

### B. Evaluation of Final Design

After the semi-structured interviews, we asked participants to reflect on their final notification design. This review process allowed them to consider adjustments when viewing the notification holistically, helping us understand if insights on individual components might differ when seen as a whole. No significant changes were noted during this reflection process.

**Comparison with Reference Design.** We asked our participants to compare their design with our reference one, and discuss whether they felt it served the login notification purpose better. All participants felt their designs were superior, mainly criticizing the example's lack of detail and actionable steps. For instance, P13 noted the reference was concise but lacked the specifics necessary to assess situations adequately. Despite the potential for the email to be shorter, many participants believed each element in their design was essential and should not be removed.

**Design Completeness.** We asked our participants if they felt their final design included all the information they would want, or if there was any missing information/design element that we did not offer. Eight participants wanted to see contact information, like a customer service number, for immediate assistance when needed. A few participants suggested adding social media handles for customer support, enhancing accessibility for users preferring those channels. No further design additions were suggested to include, which we argue indicates that our study's design was largely comprehensive.

**Design Length.** We asked our participants whether they felt their notification design could be overly long or complicated, and if so, whether they would like to remove any components. Most participants (16/20) stated that a comprehensive notification email was crucial, fearing a shorter version might seem ineffective or spam-like. Some participants stressed the importance of detailed information for user reassurance. Conversely, 4 participants chose to slightly streamline their emails. For instance, P15 suggested omitting the username since it is already included elsewhere. However, we note that overall the number of components removed from the notifications were limited, suggesting that participants in general felt that detailed notifications were warranted, and that their opinions on their prior component decisions were largely unchanged.

Participants preferred more detailed and informative notifications, even if emails are lengthy.

## VIII. CONCLUDING DISCUSSION

In this study, we investigated user mental models, workflows, and preferences for suspicious login notifications through semi-structured interviews with 20 participants. We explored and characterized how different notification components influence user engagement, understanding, and action. This section summarizes our key findings and distills

the insights gained, offering grounded recommendations for both web platform developers and the security community to explore potential future directions.

### A. Findings Summary and Recommendations

From our measurement of real-world suspicious login notifications, we uncovered a wide array of notification designs, signaling a lack of community consensus on how best to employ such notifications. Here, we summarize our study's core findings to distill recommendations on the design of suspicious login notifications.

**Initial Engagement.** We recommend a neutral email username and a recognized domain name, as these elements are perceived as more legitimate and easily recognizable (Sections VI-A, VII-A2). Subject lines highlighting suspicious activity and including the reason for receiving the notification can enhance capturing user attention and understanding (Sections VI-A, VII-A1).

**Assessing Email Legitimacy.** Including an email explanation, a detailed legitimacy warning (which very few of the collected notifications contained), a neutral closing phrase paired with a security-related closing name (which was also rare amongst real-world notifications), and a legal disclaimer can help users evaluate notification authenticity (Sections VII-A6, VII-A10, VII-A9, VII-A11). Participants expressed discomfort with emails pressuring users to click on links, which they often associated with phishing risks (Sections VI-B, VII-A8). Based on this feedback, we suggest limiting notifications to a small number of highly relevant links that show the destination URLs. Furthermore, the notification instructions should not require that users click on the links. Rather, a notification should clearly describe the actions required such that users can do so without visiting the links directly, and the links should be offered as an optional and convenient way to reach relevant webpages. This approach balances the value of providing useful resources with users' concerns about email legitimacy.

Even though our findings suggest adopting an aggressive tone with emphasizing the reason for the alert for notification explanation, it is important to note that using an aggressive tone contradicts the principles of trauma-informed security notifications. Therefore, the design should be tested with a wide range of user groups, including at-risk users, to ensure that it is truly inclusive and does not inadvertently cause distress or anxiety.

**Understanding Login Details.** Including comprehensive details such as username, device brand and model, and login timing helps users quickly verify the authenticity of the activity (Section VII-A7). Also, including the user's typical timezone, textual location details, and IP address further aids in distinguishing legitimate from suspicious activities (Section VII-A7). While there is a potential concern for information overload, the specificity of these details is crucial, empowering users to make informed decisions. This balance of thoroughness and usability caters to the realistic capabilities of users to effectively engage with login notifications. However,

including certain details will depend on the nature of the website and user interaction, such as using a username or logging in through an app instead of a browser.

**Deciding Actions.** For legitimate logins, we recommend adding instructions that help avoid unnecessary actions like password changes (Section VII-A8). For malicious logins, we recommend including instructions on how to change passwords and activate 2FA, while offering relevant URL links only for convenience, rather than requiring users to visit those links in the instructions (Section VII-A8). We also suggest adding a statement about logging out of all active sessions, so users are aware (which only one of our collected real-world notifications contained).

**Suggested Design.** Appendix Figure 2 shows a suggested notification design grounded in our results. We excluded the greeting, which was not widely preferred. Although participants preferred personalization, they emphasized avoiding redundant details. Thus we chose to personalize only the email explanation (note, both usernames and real names can be used for personalization). We highlight that elements such as the company logo and legal disclaimer, while not proof of email legitimacy by themselves, are valuable additions as they are familiar to users and enhance perceived legitimacy.

Our suggested design includes an email subject with an alarming tone and incident-specific information. While half of the real-world notifications we analyzed used an alarming tone, only one contained incident-specific details. For the sender’s email address, we used a neutral username paired with a registered domain name, aligning with most of the real-world notifications. Unlike real-world examples, our design combines an alarming tone with comprehensive incident-specific details for email explanation.

Additionally, we included detailed login information such as the username, date, time, timezone, location (city, state, country), device (vendor and version), and IP address. Most real-world notifications lack this level of detail and comprehensiveness. Our design also suggests clear and actionable steps, such as detailed guidance on changing passwords, explaining what happens after the password change, and recommending two-factor authentication. While half of the real-world notifications suggested a password change, only one provided detailed instructions, and very few recommended enabling 2FA.

Unlike real-world examples, which often include buttons for user actions (featured in half of the notifications we analyzed), our design avoids buttons and instead provides clear, non-coercive, URL links to take action. We also included an email legitimacy warning, a feature all our participants deemed important, but one that only a single real-world notification contained. Finally, we incorporated both legal information and a logo. While the majority of real-world notifications included a logo, only half provided legal information.

Note that our research replicates the high-level findings of previous work [16] in the notification design domain, reinforcing our results’ validity. Despite employing different methodologies, both studies converge on similar approaches for structuring notifications. This enhances scientific confi-

dence in our outcomes. However, our study advances beyond prior work by providing specific, actionable recommendations for each notification section. For example, while previous research suggests including instructions, we delineate precise types of instructions, such as recommending password changes or two-factor authentication, as well as email legitimacy warnings. This granularity addresses practical implementation concerns, guiding users on both immediate problem resolution and enhancing overall security.

### B. Lessons Learned and Future Directions

Finally, we discuss lessons learned for the research community and directions for future work.

**Quantifying Notification Effectiveness.** Our study identified how users engage with login notifications, providing insights on security communications. However, an inherent limitation of using a qualitative approach is that user preferences may not reflect real user behavior. Thus, further work can evaluate different notification designs experimentally, ideally at a larger scale.

Additionally, participants (Section VII) from small towns noted that their locations aren’t indexed correctly, making location indicators less trustworthy. In such cases, notifications must be designed thoughtfully so that the provided information supports each other when one element is inaccurate. Future studies could test which components can complement each other by presenting different combinations to users.

**Notifications vs Phishing/Spam.** A reoccurring theme from our study’s participants was the need to differentiate legitimate notifications from phishing/spam emails. Participants mental models and workflows were heavily shaped by their past experiences with malicious emails. While our work proposes recommendations for more effective login notifications, we do recognize that many such suggestions could be adopted by miscreants to craft more convincing malicious messages. Thus, this cat-and-mouse ecosystem could shift such that legitimacy signals we have identified no longer serve such a purpose. Further research is still needed on the challenging problem of establishing user trust in a notification.

**Importance of Notification Language.** Our study highlights the importance of notification language, tone, and framing. Certain languages can incentivize user engagement and action, while another language may unintentionally result in users misinterpreting the security situation. For example, as mentioned in Section VII, when websites send notifications stating “you signed in,” this makes some users believe that they indeed accessed their accounts, even in cases where they do not recall doing so. This misplaced understanding indicates the importance of composing notification language that is both clear and unambiguous. Thus, notifications must be carefully crafted, and while our study provides some initial insights into effective language, more research is needed to optimize it to align with user trust and maintain communication clarity.

**User Context Dependent Notifications.** Our findings suggest that user context can influence responses to login notifications. For instance, users preferred the time format com-

monly used in their locale. We also saw diversity in user preferences for notification designs, indicating that there are no one-size-fits-all solution. Notably, several participants in our study expressed concern that the technical terminology used in notifications could be challenging for elderly individuals to comprehend. To ensure accessibility, it is imperative that these technical terms be clearly defined or simplified for such subgroups. Moreover, considering other demographics like children, who are increasingly engaging with digital platforms, it is crucial to tailor the complexity of language in notifications to accommodate their level of understanding. A valuable direction for future research would be to investigate the design of age-appropriate notifications that are both clear and educational, thereby enhancing security awareness across all age groups. This aligns with the broader need to examine how cross-cultural factors influence user preferences in security notification designs.

**Standardized Notifications.** Our study showed that user preferences align with familiar prior experiences. Thus, consistent and recognizable notification designs could enhance user comprehension of notifications. Yet today, websites employ widely varying notifications. We argue that establishing a standardized design (or a set of designs for different subpopulations) would enhance notification effectiveness.

#### ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation award CNS-2055549. The opinions expressed in this paper may not reflect those of the research sponsors.

#### REFERENCES

- [1] 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 CHI Conference on Human Factors in Computing Systems (CHI)*, 2008.
- [2] J. Petelka, Y. Zou, and F. Schaub, “Put your warning where your link is: Improving and evaluating email phishing warnings,” in *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2019.
- [3] D. Akhawe and A. P. Felt, “Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness,” in *USENIX Security Symposium*, 2013.
- [4] L. Bauer, C. Bravo-Lillo, L. Cranor, and E. Fragnani, “Warning Design Guidelines,” CyLab, Carnegie Mellon University, Tech. Rep. CMU-CyLab-13-002, Feb. 2013. [Online]. Available: [https://www.cylab.cmu.edu/research/techreports/2013/tr\\_cylab13002.html](https://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13002.html)
- [5] R. 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 CHI Conference on Human Factors in Computing Systems (CHI)*, 2018.
- [6] M. Harbach, S. Fahl, P. Yakovleva, and M. Smith, “Sorry, I Don’t Get It: An Analysis of Warning Message Texts,” in *Proceedings of the 17th International Conference on Financial Cryptography and Data Security (FC)*, Vol. 7859. Lecture Notes in Computer Science (LNCS), 2013.
- [7] B. Anderson, A. Vance, B. Kirwan, D. Eargle, and S. Howard, “Users Aren’t (Necessarily) Lazy: Using NeuroIS to Explain Habituation to Security Warnings,” in *International Conference on Information Systems (ICIS)*, 2014.
- [8] M. Kauer, T. Pfeiffer, M. Volkamer, H. Theuerling, and R. Bruder, *It is not about the design—it is about the content! Making warnings more efficient by communicating risks appropriately*. Gesellschaft für Informatik eV, 2012.
- [9] 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*, 2009.
- [10] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, “Your attention please: Designing security-decision UIs to make genuine risks harder to ignore,” in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2013.
- [11] R. Wash and M. M. Cooper, “Who Provides Phishing Training?: Facts, Stories, and People Like Me,” in *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2018.
- [12] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, “Protecting people from phishing: the design and evaluation of an embedded training email system,” in *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2007.
- [13] N. A. G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” *Computers in Human Behavior*, vol. 29, no. 3, pp. 706–714, 2013.
- [14] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Teaching Johnny not to fall for phish,” *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, pp. 1–31, 2010.
- [15] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish,” in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2007.
- [16] P. Markert, L. Lassak, M. Golla, and M. Dürmuth, “Understanding Users’ Interaction with Login Notifications,” in *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2024.
- [17] E. M. Redmiles, “Should I Worry?” A Cross-Cultural Examination of Account Security Incident Response,” in *IEEE Symposium on Security and Privacy (S&P)*, 2019.
- [18] 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 *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2022.
- [19] S. Wiefling, L. Lo Iacono, and M. Dürmuth, “Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild,” in *IFIP SEC*, 2019.
- [20] S. Wiefling, T. Patil, M. Dürmuth, and L. Lo Iacono, “Evaluation of Risk-based Re-authentication Methods,” in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2020, pp. 280–294.

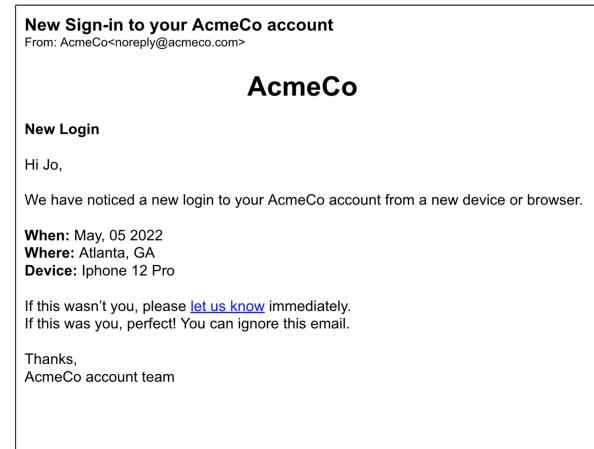
- [21] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving SSL Warnings: Comprehension and Adherence," in *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, 2015.
- [22] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the Gap in Computer Security Warnings: A Mental Model Approach," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 18–26, 2010.
- [23] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings," in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2011.
- [24] S. Egelman and S. Schechter, "The Importance of Being Earnest [in Security Warnings]," in *Financial Cryptography and Data Security*, 2013.
- [25] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo, "Your Reputation Precedes you: History, Reputation, and the Chrome Malware Warning," in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2014.
- [26] K. Krol, M. Moroz, and M. A. Sasse, "Don't work. Can't work? Why it's time to rethink security warnings," in *7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2012.
- [27] 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 CHI Conference on Human Factors in Computing Systems (CHI)*, 2017.
- [28] 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 CHI Conference on Human Factors in Computing Systems (CHI)*, 2019.
- [29] 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 (CCS)*, 2018.
- [30] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Ivernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh et al., "Protecting Accounts from Credential Stuffing with Password Breach Alerting," in *USENIX Security Symposium*, 2019.
- [31] 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*, 2021.
- [32] E. M. Redmiles, E. Liu, and M. L. Mazurek, "You Want Me To Do What? A Design Study of Two-Factor Authentication Messages," in *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017.
- [33] 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*, 2021.
- [34] V. L. Pochat, T. Van Goethem, S. Tajalizadehkhooob, M. Korczyński, and W. Joosen, "Tranco: A Research-oriented Top Sites Ranking Hardened against Manipulation," in *Network and Distributed System Security Symposium (NDSS)*, 2019.
- [35] J. Corbin and A. Strauss, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage Publications, 2014.
- [36] L. L. Kupper and K. B. Hafner, "On Assessing Interrater Agreement for Multiple Attribute Responses," *Biometrics*, vol. 45, no. 3, pp. 957–967, 1989.
- [37] M. Steen, M. Manschot, and N. De Koning, "Benefits of co-design in service design projects," *International Journal of Design*, vol. 5, no. 2, 2011.

## APPENDIX

### A. Interview Instrument

#### Introduction

Websites monitor their user accounts, and if they detect suspicious/unusual logins that might not be from the real user (such as a login from an unusual location or time), they often send a notification to the user's email about the suspicious login (such as the example notification shown below), so that the user can check the security of their account. Ideally, these notifications provide enough information so the users can clearly determine whether they made the login and if not, take action to re-secure their account as needed.



Now, imagine that your name is Jo Doe. You have an online account with a popular website called AcmeCo, which is like other accounts you may have, such as for online shopping or social media. Your account uses your email jo.doe@mail.com and your account username is jodox123. Imagine you will receive a suspicious login notification email for your account.

#### Design Options

##### Email Subject

- Category 1
  - a) Jo
  - b) Jo123
- Category 2
  - a) New login to your account
  - b) Suspicious login to your account
- Category 3
  - a) from AcmeCo in Atlanta/Chrome on Mac
  - b) from AcmeCo at an unusual location/device

##### Sender Information

- Category 1
  - a) noreply
  - b) account\_security\_team
- Category 2
  - a) @acmeco.com
  - b) @accountprotection.acmeco.com

##### Logo

- Category 1



a)

b) No logo

#### *Headline*

- Category 1
  - a) Jo
  - b) Jo123
- Category 2
  - a) New sign-in
  - b) Unusual sign-in activity

#### *Greeting*

- Category 1
  - a) Hi
  - b) Dear
- Category 2
  - a) Jo
  - b) Jo123

#### *Explanation*

- Category 1
  - a) It looks like you recently signed in to your AcmeCo account
  - b) We detected a suspicious login to your AcmeCo account
- Category 2
  - a) from a new device or location

#### *Closing*

- Category 1
  - a) Thanks
  - b) Your friends at
- Category 2
  - a) AcmeCo
  - b) AcmeCo Security Team

#### *Email Legitimacy Warning*

- Category 1
  - a) Make sure this email is from AcmeCo: support.acmeco.com/article/suspicious-email/
- Category 2
  - a) Check before you click! AcmeCo will never ask you for personal information in an email. When you click on a link the address should always contain "acmeco.com/" Visit the security.acmeco.com/phishing FAQ site to learn more

#### *Legal Info*

- Category 1
  - a) AcmeCo, Inc. 1453 Legend Street, Suite 610 San Francisco, CA 90101

#### *Sign-in Info Variables*

- Account name
  - Account name: jodoe123
  - Email Address: jodoe@mail.com
- Browser
  - Vendor: Google Chrome
  - Version: 109.0.5414.119
- Device
  - Brand: Apple
  - Model: Macbook Pro
  - Version: M1

- Operating System
  - OS: macOS
  - Version: Catalina
  - Minor version: 10.15.7
- Device
  - Month: June
  - Day: 6
  - Year: 2023
  - The name of the day: Tuesday
- Time
  - 12-hour (AM/PM): 1 pm
  - 24-hour: 13:00

- Time Zone
  - Daylight Saving Time: EDT
  - Standard Time: EST
  - Universal Time: UTC
  - Mean Time: GMT
- Location
  - City: Atlanta
  - State: Georgia
  - Country: USA
- IP Address
  - IPv4: 192.168.1.1
  - IPv6: 2001:db8:333:4444:CCCC:DDDD:EEEE:FFFF

#### *Legitimate login*

- Category1
  - If this was you, there's no need to take any action right now.

#### *Malicious login*

- Category1
  - If this was not you,
- Category1
  - Visit <https://acmeco.com/settings/security> and change your password.
- Category2
  - Visit <https://acmeco.com/settings/security> and change your password. You'll be logged out of all your active AcmeCo sessions except the one you're using at this time.
- Category3
  - Review recent activity at <http://myaccount.acmeco.com/notifications>
- Category4
  - Secure your account (button)
- Category5
  - We recommend that you enable two-factor authentication to secure your account.
- Category6
  - To learn more about how to keep your account secure, you can visit <https://acmeco.com/security>
- Category7
  - Let us know (button)

#### *Demographic Questions*

- 1) Please specify the gender with which you most closely identify.

- a) Male b) Female c) Other d) Prefer not to say
- 2) Please specify your age.  
a) 18-29 b) 30-49 c) 50-69 d) >70 e) Prefer not to say
- 3) Please specify the highest degree or level of education that you have completed.  
a) Less than high school b) High school graduate c) Some college d) 2-year degree e) 4-year degree f) Professional degree g) Doctorate h) Prefer not to say
- 4) Do you work in the fields of computer science, computer engineering, or information technology (IT)?  
a) Yes b) No c) Prefer not to say

### Interview Questions

- 1) Have you recently received a suspicious login notification email?  
a) If so, please think about the most recent incident. Please tell us what the notification email was about, and what information and suggestions it provided.
- b) What actions did you take, if any? Why?
- c) How did you determine whether the notification email was sent by a legitimate website?
- d) Were you able to identify whether the notification was about your login or a potentially malicious login? If so, which aspects of the notification helped you to identify that? If not, what was challenging about identifying whether the notification was about your login or a potentially malicious login?
- e) Do you remember what was helpful or unhelpful about that notification?
- 2) Do you think suspicious login notification emails are useful/helpful? Why/why not?
- 3) What factors influence your decision to open an email regarding a suspicious login?
- 4) How do you determine the legitimacy of the email?
- 5) How do you determine whether a login attempt is legitimate (by you) or malicious (by someone else)?
- 6) How do you decide to take action if the login is malicious, and what actions to take?
- 7) During/after drawing the notification, for each notification part:  
a) If the section is optional: Why did you include/not include this section?  
b) If the section has multiple options: Why did you pick this/these options for this section over other choices?
- 8) Please look at the following notification example from earlier. What do you (a) like and (b) dislike about it compared to your design?
- 9) Imagine that you receive the suspicious login notification email that you designed in the future. Would there be other things that you'd want in a notification that we didn't give you an option for? Please discuss why you need this additional information in the notification.
- 10) Does that design look complete for you? Are there any other design aspects we should talk about?

Email Subject. Suspicious login to your account from AcmeCo using Chrome on Mac

Sender Info. noreply@acmeco.com



**Explanation.** Jo, We detected a suspicious login to your AcmeCo account from a new device.

**Sign-in details.** Account name: jo123  
When: May, 05 2023 3pm EST  
Where: Atlanta, GA, USA  
Device: iPhone 12  
IPv4:192.168.1.1

**Actions.** If this was you, there's no need to take any action right now. If this was not you, visit your account's security settings to change your password (also available at <https://acmeco.com/settings/security>). You'll be logged out of all your active AcmeCo sessions except the one you're using at this time. We recommend that you enable two-factor authentication to secure your account.

**Closing.** Thanks AcmeCo Security Team

**Legitimacy Warning.** Check before you click!  
AcmeCo will never ask you for personal information in an email.  
When you click on a link the address should always contain "acmeco.com/". Visit the security.acmeco.com/phishing FAQ site to learn more.

Legal info. AcmeCo, Inc. 1453 Legend Street, Suite 610 San Francisco, CA 90101

Fig. 2: A recommended notification design grounded in our study's results.