"Who is Trying to Access My Account?" Exploring User Perceptions and Reactions to Risk-based Authentication Notifications

Tongxin Wei, Ding Wang, Yutong Li, Yuehuan Wang
College of Cyber Science, Nankai University, Tianjin 300350, China; wangding@nankai.edu.cn
Key Laboratory of Data and Intelligent System Security (NKU), Ministry of Education, Tianjin 300350, China
Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China

***Abstract*—Risk-based authentication (RBA) is gaining popularity and RBA notifications promptly alert users to protect their accounts from unauthorized access. Recent research indicates that users can identify legitimate login notifications triggered by themselves. However, little attention has been paid to *whether RBA notifications triggered by non-account holders can effectively raise users' awareness of crises and prevent potential attacks*. In this paper, we invite 258 online participants and 15 offline participants to explore users' perceptions, reactions, and expectations for three types of RBA notifications (i.e., RBA notifications triggered by correct passwords, incorrect passwords, and password resets).**

The results show that over 90% of participants consider RBA notifications important. Users do not show significant differences in their feelings and behaviors towards the three types of RBA notifications, but they have distinct expectations for each type. Most participants feel suspicious, nervous, and anxious upon receiving the three types of RBA notifications not triggered by themselves. Consequently, users immediately review the full content of the notification. 46% of users suspect that RBA notifications might be phishing attempts, while categorizing them as potential phishing attacks or spam may lead to ineffective account protection. Despite these suspicions, 65% of users still log into their accounts to check for suspicious activities and take no further action if no abnormalities are found. Additionally, the current format of RBA notifications fails to gain users' trust and meet their expectations. Our findings indicate that RBA notifications need to provide more detailed information about suspicious access, offer additional security measures, and clearly explain the risks involved. Finally, we offer five design recommendations for RBA notifications to better mitigate potential risks and enhance account security.

I. Introduction

Passwords remain the mainstream method of identity authentication, and are widely used in financial transactions [7] and email services [22], and they are more unlikely to be replaced in the foreseeable [3]. However, using a single password for identity authentication is vulnerable if the password has been somehow obtained by attackers (e.g., guessing [48], [49], [58] and leakage [36]). Consequently, website administrators are compelled to adopt more robust authentication methods (e.g., Two-Factor Authentication (2FA) [11], [50], Risk-based Authentication (RBA) [8], [60] and Single Sign-On (SSO) [10], [17]) to safeguard user accounts. Despite the security benefits of 2FA, it has struggled to gain popularity due to its operational complexity [11], [30]. 2FA adds inconvenience and dependency during login, e.g., lost devices or expired identity bindings can obstruct access [14]. On the other hand, SSO creates a single point of failure, which, if compromised, could impact all connected systems [10]. Furthermore, the centralized management of login information in SSO systems also raises privacy and security concerns [9].

To enhance the security of single-password authentication and improve the usability of 2FA, major online services have introduced RBA [44], [52], [54], [55]. An RBA notification is a security alert specifically designed to inform users about potential abnormal activities or security threats concerning their accounts [53]. When the security system detects login attempts or account actions that deviate from the user's historical login records, it promptly sends an RBA notification to the account holder. RBA triggers secondary authentication only when a risk is detected, making it more acceptable than constant 2FA and increasing user acceptance [52], [55]. When anomalies are detected during sign-ins, RBA records login details, e.g., IP addresses and devices [55]. A security system sends RBA notifications and demands additional verification to protect the account from unauthorized access [8], [16].

A. Motivations

Besides, users often receive various forms of identity verification codes, some of which may not originate from their actions, leading to confusion among users [57], [60]. Current RBA notification designs lack uniform standards in style and content, resulting in many RBA notifications missing detailed information about suspicious access (e.g., IP address and time, see Fig. 7 in Appendix A). Additionally, there is inconsistency in how RBA notifications describe the security status of accounts and guide remedial actions (e.g., some notifications advise, "If this was not you, ignore this message," while others say, "If this was not you, contact the help center immediately"). Besides, some phishing attackers exploit user trust by crafting phishing emails that mimic RBA notifications, thereby deceiving users [25]. This raises concerns about the effectiveness of genuine RBA notifications in preventing account attacks and promptly alerting users to unauthorized account logins. Furthermore, Li et al. [24] indicated that 81.1% of accounts can complete authentication through linked email addresses by

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.240133
www.ndss-symposium.org

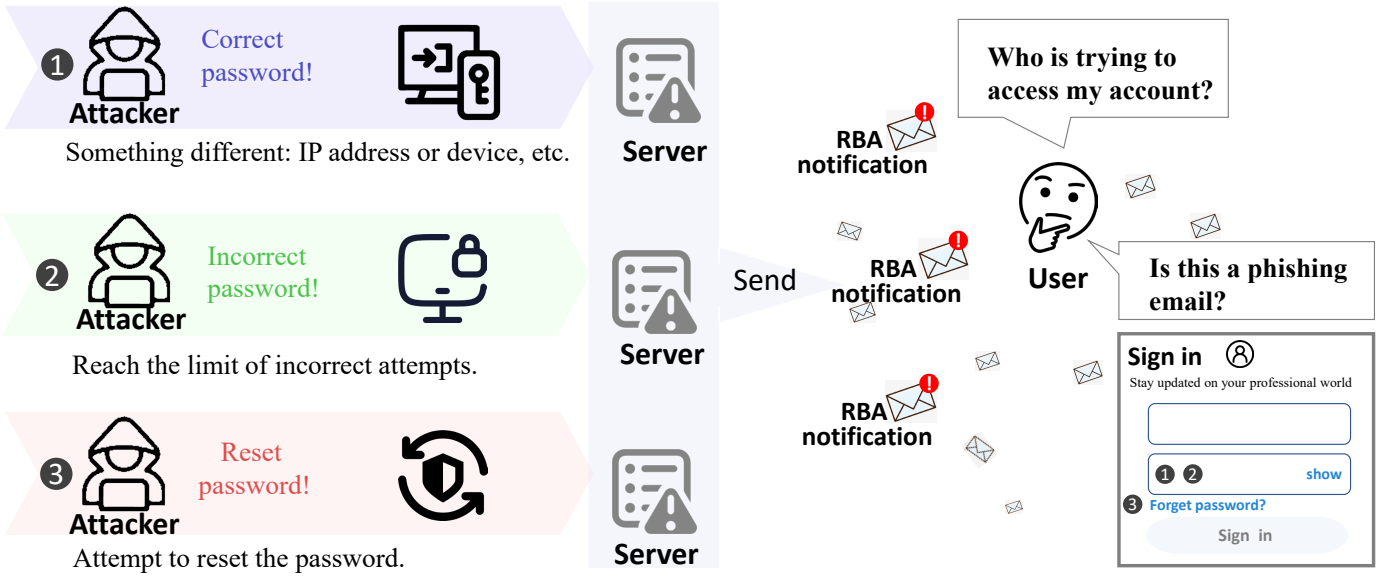


Fig. 1. Three types of suspicious access that trigger a Risk-based Authentication (RBA) notification: ❶. **Correct password trigger for RBA notification**: When an attacker uses the correct password but logs in from an unrecognized device or IP, it triggers an RBA notification due to inconsistencies with historical data. ❷. **Failed login attempts**: When an attacker attempts to crack an account's password and reaches the maximum number of incorrect attempts allowed by the website, it triggers an RBA notification for the account. ❸. **Clicking "Forget Password" triggers an RBA notification**: When an attacker attempts to log into an account by resetting the password through the associated email or other third-party applications, it triggers the website's RBA notification.

the forget password button. We aim to explore user perceptions and reactions to Risk-based Authentication (RBA) notifications triggered by non-account holders in three scenarios: correct password, incorrect password, and the forget password button.

Some priori research (e.g., [11], [29], [52]) has conducted user studies on Two-Factor authentication (2FA) and RBA, yet they mainly focus on the acceptance of 2FAs. Relatively little attention has been given to investigating the effectiveness of RBA notifications. As far as we know, Markert et al.'s work [28] at CHI'24 may be the closest to our paper: They conducted a user study on login notifications of authorized access (i.e., legitimate and malicious). However, our work has the following five differences: (1) We explore three types (e.g., correct password, incorrect password, and password reset) pre-login RBA notifications, while CHI'24 [28] considers post-login alerts. RBA notifications aim to prevent access before it occurs, offering stronger security than post-login responses. (2) Unlike CHI'24 [28] that examines post-login scenarios, we send participants real-world simulated RBA notifications disguised as official communications to capture genuine user reactions. We aim to clarify *how individuals interpret and react to RBA alerts about unauthorized access*; (3) We invite participants to score and express their expectations regarding various RBA notifications, which were not explored in [11], [28], [52]; (4) We find that 46% of users mistake RBA notifications for phishing attempts, which greatly contrasts with the 1% in CHI'24 who viewed login notifications as phishing. It is an issue that has not been highlighted in prior works (e.g., [11], [28], [29]); (5) We offer new insights beyond (e.g., [8], [28], [29]), focusing on the importance of recognizable design features and official identifiers in RBA notifications, an aspect not explored in [28].

B. Our study

In this work, we investigate 251 popular websites from the Tranco top 5K list [38], aiming to activate their RBA to receive the RBA notifications. We trigger RBA through three distinct methods: using correct passwords, incorrect passwords, and the password recovery process (see Fig. 1). We analyze the RBA notifications sent by these services and develop a baseline notification for our user survey (see Sec. III-A). We recruit 258 U.S. participants from Prolific, an online study, to collect data on their feelings, understanding, and behaviors in response to receiving these notifications. Additionally, we conduct semi-structured interviews with 15 offline participants to gather insights into their perceptions and expectations regarding RBA notifications. We aim to answer the following key questions:

RQ1: [Feelings and Awareness] *What are users' attitudes and feelings towards receiving RBA notifications that are not triggered by themselves? Do these RBA notifications raise users' awareness of potential security risks?*

In our online survey, most participants feel suspicious (82%), nervous (62%), and anxious (60%) receiving the three types of RBA notifications. Over 57% of participants perceive their account security as being at risk or under threat.

RQ2: [Reactions and Understanding] *Is addressing these notifications a priority for them? What actions do users take upon receiving RBA notifications? What do users perceive as the sources of these notifications?*

We find that 76% of participants immediately check RBA notifications. 71% read the notification in its entirety. 65% attempt to log into their accounts to verify security; if they detect suspicious activities, they change their passwords; otherwise, they take no further action. 56% of participants indicate they would activate two-factor authentication, and 33% consider updating the security information for linked accounts. Overall, 65% of participants believe that RBA notifications are provided by their service provider, while 46% suspect that these notifications might be part of a phishing attack.

RQ3: [Perceptions and Expectations] *What factors can influ-*

ence users' perceptions and reactions? What key information do participants expect to be included in an RBA notification? Do current RBA notifications meet users' expectations?

Most users think that the importance of the account (84%), the risk warning (77%), and the reasons for triggering the RBA (76%) can encourage their protective actions. Users expect RBA notifications to include the following elements: the reason for triggering the RBA (79%), the name of the account (77%), a risk warning (72%), the status of the account (71%), and detailed information about the triggering event (69%). Currently, over 75% of RBA notifications do not meet these user expectations.

C. Our contributions

The key contributions of this work are as follows:

- **New issues revealed**. Our study, for the first time, marks an effort to delve into users' perceptions and reactions to three types (i.e., correct password, incorrect password, and forget password button) of RBA notifications. Our user survey reveals a critical issue: 46% of participants perceive RBA notifications as phishing or spam, a stark contrast to the 1% reported in [28] for login notifications. This distrust of RBA notifications hinders their effectiveness. Moreover, as identified in [8], RBA notifications not only serve as identity verification tools but primarily function as alerts for unusual login risks, thereby placing more responsibility on users for account security. Our results also show that 36% of participants are unsure how to respond to RBA notifications. As a result, RBA notifications that only serve as alerts, without the second authentication, may lose their effectiveness in protecting user accounts.
- **New design gap identified**. We conduct an empirical study on RBA notifications across 251 websites, categorizing and summarizing the current RBA notifications. Building on this foundation, we carry out an online survey and offline semi-structured interviews to gauge users' perceptions and expectations regarding RBA notifications. In the interviews, we implement two innovative designs: (1) We simulate official RBA notification emails to test users' authentic reactions when receiving non-self-triggered RBA notifications. (2) We group different RBA notifications and invite users to participate in a score task, gaining deeper insights into their expectations for RBA notifications.
- **New insights**. Drawing from our website survey and user study, we find that users who perceive RBA notifications as beneficial are more likely to engage with them, emphasizing the need for user education in enhancing security. In our interview, users view long URLs as suspicious. Additionally, 89% of users check emails on mobile, yet some websites do not optimize RBA notifications for mobile devices, leading to usability problems. Furthermore, we find that 56% of users prefer enabling 2FA rather than just changing passwords (34.4%) when receiving RBA notifications. This inspires us to further explore expanding options to enhance account security for users who may not want to change their passwords.

II. Related work

In this section, we briefly introduce research related to Risk-based Authentication (RBA) and warning notification.

A. Risk-based authentication

RBA is a dynamic security method that adjusts authentication requirements based on the perceived risk of a user's access attempt, using factors like location and device [52], [53]. Wiefling et al. [53] developed an automated framework to assess the availability of RBA by logging into and interacting with eight popular sites over a two-month period. They identified the sites that utilize RBA, the features employed for user identification, and the relative importance assigned to each feature. Lin et al. [25] tested 300 sites from the Alexa top 20K to identify sites with RBA. Their RBA-detection methodology relies solely on the "remember this device" option on the login page as the trigger for enabling RBA protections. They found that only 16 sites implemented RBA, mostly in the banking and tax-preparation sectors. Thus, their results do not provide a comprehensive overview of RBA prevalence online.

RBA notifications are indispensable for assessing account security risks [51]. Overlooking RBA notifications can result in severe security breaches [60]. They encompass verification alerts triggered by correct password inputs [54], risk warnings from erroneous password attempts [43], and security advisories due to reset password actions [24]. In 2018, Li et al. [24] analyzed the account authentication and recovery protocols of 239 popular sites, categorizing them into six types based on their recovery methods. The study revealed that 81.1% of the sites could be compromised by knowing only the email password without requiring any additional credentials or contextual authentication. They noted the vulnerabilities of using email to change passwords but ignored the security and usability of this process, which was further explored in [20].

In 2020, Wiefling et al. [52] found that RBA provides better security than password-only methods and superior usability compared to 2FA. They found that users' acceptance of RBA varied by website type and device, with RBA using phone numbers for identity verification being less favored. The study focuses on user acceptance of 2FA based on device-based identity verification, overlooking the reminder forms. They found that 86% of participants prefer receiving RBA notifications via email. In 2021, Golla et al. [11] tested three reminder forms (i.e., personalization, interstitials, and opinionated reminders) on user adoption rates of 2FA. While they mentioned that the loss of mobile devices could impact users' adoption of 2FA, they did not further investigate how devices affected users' experiences and interactions with 2FA notifications. In 2022, Markert et al. [29] indicated that users' acceptance of MFA may increase in response to account risks, though this finding is based on 28 administrators, not users. Users are unsure how to handle different RBA notifications, requiring risk-level guidance and related security measures, which is confirmed by our study.

This raises questions about how users react to RBA notifications sent via email that are triggered by unauthorized attempts. Specifically, our research aims to ascertain whether participants follow the email instructions to ignore such notifications or to actively check their account's security details. We conduct a controlled experiment to assess the influence of these email instructions on user behavior. This study helps illuminate how

TABLE I. RELATED WORK ON RISK-BASED AUTHENTICATION (RBA) NOTIFICATIONS.

	Focus	**Objects**
Huh et al. (2017) [15]	Users' response to password reset notifications	249 LinkedIn users
Key findings	Only about 46% of participants who received password reset notifications reset their passwords (we confirm this finding in **RQ2**), with an average delay of 26.3 days, indicating significant hesitation to take action.	
Unique contributions	This highlights the need for more effective persuasive measures to encourage timely password resets and mitigate associated risks.	
Li et al. (2018) [24]	Risks in email-based account recovery	239 traffic-heavy websites
Key findings	Most websites rely on email for account recovery, but many email service providers have inadequate security measures, leaving accounts vulnerable to compromise and recovery attacks.	
Unique contributions	The study identified risks in email-based account recovery and proposed Secure Email Account Recovery to enhance security.	
Wiefling et al. (2019) [53]	Test the features that trigger RBA	8 popular online services
Key findings	The study identified useful features and classifiers in RBA, highlighting variations in user interface design.	
Unique contributions	The study created a framework and methodology for measuring RBA in real-world applications, providing insights into its practical use.	
Wiefling et al. (2020) [52]	Compare the security and usability of password-only, RBA, and 2FA	Lab study (n = 65)
Key findings	RBA provides better security than password-only methods and superior usability compared to 2FA. 86% prefer receiving RBA notifications via email (we confirm this finding in **RQ2**).	
Unique contributions	They found that users' acceptance of RBA varied by website type and device.	
Golla et al. (2021) [11]	User acceptance of 2FA	622,419 Facebook users
Key findings	Users' motivations and concerns effectively boost 2FA adoption.	
Unique contributions	They mentioned that the loss of mobile devices could impact users' adoption of 2FA.	
Wiefling et al. (2021) [44]	The influence of features that trigger RBA on user behavior	General public (n = 780)
Key findings	RBA must be tailored to each service; small configuration changes significantly affect security and usability.	
Unique contributions	They conducted a behavior analysis of RBA implementations, established a benchmark for suitable features, introduced a new feature, and identified factors affecting performance.	
Markert et al. (2022) [29]	RBA systems based on login risk scores	28 system administrators
Key findings	Administrators highlighted the importance of default settings and noted some confusing terms. Users were unsure how to handle different RBA notifications, require risk-level guidance and related security measures (we confirm this finding in **RQ3**).	
Unique contributions	Required the system to set different alerts or blocks for varying RBA risk levels.	
Gavazzi et al. (2023) [8]	The availability of MFA and RBA on the web	208 popular sites
Key findings	42.31% of sites that implemented multi-factor authentication (MFA), only 22.12% blocked suspicious actions, while the remaining RBA notifications merely as alerts and reminders for user account security.	
Unique contributions	Most SSO providers with MFA or RBA are major third-party trackers, creating a privacy trade-off when improving login security.	
Markert et al. (2024) [28]	User interaction with login notifications	72 login notifications Three-stage user study (n = 229)
Key findings	Users felt negative when receiving RBA notifications (We confirm this finding in **RQ1**). Login notifications improved account security but failed to convince most participants to change their passwords; users wanted more contextual information to understand the triggers. Most users fully read the RBA notifications (we confirm this finding in **RQ2**). 22% of participants changed their password after receiving RBA notifications (we confirm this finding in **RQ2**). Only 1% of participants believed RBA notifications might be phishing attacks (we contradict this finding in **RQ2**).	
Unique contributions	They emphasized the need for services to clarify the reasons behind login notifications and stressed that accountability for robust account protection rests with service providers.	
Our study	User practices and expectations for three types of RBA notifications	161 RBA notifications Online Survey(n = 258) Task+User Interviews (n = 15)
Key findings	Users' feelings toward the three types (e.g., correct, incorrect password and password reset) of RBA notifications do not differ significantly. Over 57% of participants perceive their account security to be at risk. The time, location, and device used to receive RBA notifications may affect how users respond to the notifications. 93% of participants believe RBA notifications indicate successful unauthorized access. 46% of users suspect that RBA notifications might be phishing attempts, and categorizing them as potential phishing attacks or spam leads to ineffective protection of account security. Users view long URLs as suspicious.	
Unique contributions	We identify the need for RBA notifications to assure users that these alerts are legitimate account risk notifications, not phishing emails, and to prompt them to take security measures before their accounts are compromised, thereby enhancing the notifications' effectiveness.	

communication strategies can impact users' security actions in a digital environment.

In 2023, Gavazzi et al. [8] showed that among the 42.31% of sites that implemented multi-factor authentication (MFA), only 22.12% blocked suspicious actions, while the remaining RBA notifications merely as alerts and reminders for user account security. This undoubtedly shifts more responsibility for account security onto the users. Users are often regarded as the weakest link in the security chain [42]. However, Gavazzi et al.'s study [8] does not invite users to validate the security and usability of RBA notifications. Additionally, they overlooked other methods (e.g., a certain number of incorrect password attempts) for triggering RBA.

To address the questions mentioned above, we test users' understanding and behavior across three types of RBA notifications (e.g., correct password, incorrect password, and reset password). Our findings indicate that 36% of participants are uncertain about how to respond to RBA notifications, which should raise significant concerns for service providers.

At CHI'24, Markert et al. [28] demonstrated that while users grasped the notifications triggered by logins, they found only 22% opting to change their passwords (32% in [15] and 43.3% (45/104) in our study). Users felt negative when receiving RBA notifications. Besides, we find that users' feelings toward the three types of RBA notifications (e.g., correct password, incorrect password, and password reset) do not differ significantly. Markert et al. [28] pointed out that only 1% of participants believed RBA notifications might be phishing attacks (compared to 46% in our study). Notably, Markert et al.'s study [28] did not provide participants with a range of security measures to consider, focusing instead on open-ended questions. Moreover, they neglected to include a component inviting users to critique the content and layout of the login notifications. Additionally, they overlooked how the importance of accounts affected users' reception of notifications. Their findings mainly focused on the effects of unauthorized login events, rather than login notifications.

To address the unresolved issues left in [8], [28], we design a scoring task to further investigate users' evaluations and expectations regarding the design elements of RBA notifications. We summarize the above work related to RBA notifications in terms of focus, research subjects, key findings, and unique contributions (see Table I).

B. Security warning & notification design

Extensive research has been conducted on user security authentication notifications, covering areas e.g., breach notifications [15], [59], password-reuse notifications [12], [45], and the promotion of advanced authentication methods like 2FA [11] and FIDO2 [21], as well as discouraging the use of common PINs [27]. However, other studies highlight an emerging trend known as warning fatigue, where users become increasingly desensitized to frequent alerts, often resulting in a disregard for these critical security messages [4], [32], [40]. It's important to note that the reasons behind the triggering of an RBA notification are not always clear to the user [52]. This phenomenon underscores the significant challenge in crafting effective notifications that not only capture user attention but also actively engage and motivate adherence to essential cybersecurity practices. The design of such notifications requires a deep understanding of user behavior and psychology to counteract the tendency to overlook important security warnings. This sparks our interest in how users perceive and react to RBA notifications.

III. RBA NOTIFICATIONS IN THE WILD

RBA notifications are designed to alert users about suspicious logins to their accounts. They typically include details, e.g., a verification code, the time of the login attempt, the device used, and the login location. These notifications are triggered only when suspicious activity meets the service provider's security thresholds, e.g., logins from unknown IPs or devices, or when incorrect password attempts exceed the site's limits. Due to the wide variation in the format and content of RBA notifications across different websites, in this section, we conduct an empirical measurement of RBA notifications, summarizing and categorizing various types to provide essential material for user research. We present more detailed results of our website survey in the full version.

A. Types of RBA notification

We categorize the RBA notifications based on three types of non-account holder activations. Fig. 7 in Appendix A show RBA notification examples for each of the three types used in our study. More examples can be found in our full version.

(1) **Correct password:** When someone uses the correct password to log into a user's account from an unfamiliar device, it triggers an RBA notification.

(2) **Incorrect password:** When someone repeatedly uses incorrect passwords and exceeds the website's limit of failed attempts, it triggers an RBA notification.

(3) **Reset password:** Someone attempts to access an account by clicking the "reset password" button to reset the password [24], triggering an RBA notification.

To explore the design and response of RBA notifications, we conduct tests on websites ranked in the top 5,000 by Tranco as of December 2023 [38]. We attempt 251 websites using correct and incorrect passwords and through the "reset password" option across various devices and IP addresses. We create accounts linked to emails and phone numbers to receive RBA notifications, covering categories like social media, shopping, financial transactions, travel, email, and gaming.

B. Analysis of RBA notification

In this study, four researchers first classify 161 emails as notifications related to account access, then independently analyzed various features within these emails using an iterative coding method [2]. These features included main components (e.g., headline and purpose of the email, recommended actions), access information (e.g., verification status, login time, location, device), risk warning (e.g., warning labels or text), design and words (e.g., logos, highlighting of request details), etc. The analysis continued until data saturation was reached, and any disagreements were resolved with a third team member, achieving 100% consistency in all hypotheses.

We summarize the results of RBA notifications under different RBA-triggering features. We then redesign the text and appearance of RBA notifications to align with the focus of our research (see Fig. 2). We select several RBA notifications for our user study (see Fig. 7 in Appendix A).

RBA details. The RBA notification triggered by the correct password contains comprehensive information, which we detail here. As shown in Fig. 2, most RBA notifications include the

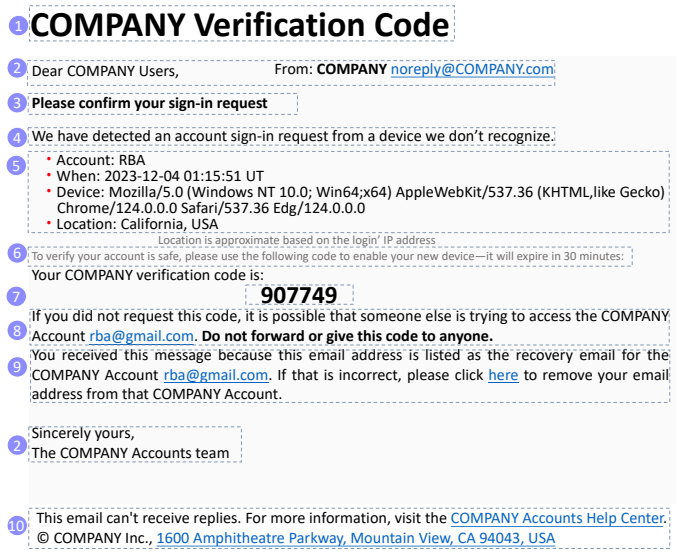


Fig. 2. The baseline RBA notification, which we derived from 57 real-world examples. We rebranded the content and design to match the study website.

❶ *title* (67%), ❷ *sender* (86%) and a closing statement, ❸ a request of login (39%), ❹ the *reason* for authentication request (37%), ❺ *account name* (34%), ❺ *time* (29%), ❺ access *operate system* (27%), and ❺ *location* (22%).

Risk warning. Some notifications include ❻ the *validity period* of the authentication, ❼ the authentication *code* (62%), ❽ *risk warnings* (45%), and ❾ *other* security measures (e.g., remove an incorrect email binding).

Design & words. Additionally, RBA notifications incorporate several key elements: *a sequential listing* includes the detailed information about the RBA; key information e.g., the email's title and the authentication code, is *highlighted in bold*; and some conclude with ❿ information about the help center.

IV. METHOD

In this section, we explore users' perceptions and reactions to Risk-based Authentication (RBA) notifications, aiming to answer the three key questions (see Sec. I). First, we provide a comprehensive overview of our research methodology, detailing the designs of both our online study (see Sec. IV-A) and offline semi-structured interviews (see Sec. IV-B). Second, we show the recruitment of participants for our user study. We then present information about the volunteers who participated in the online and offline study (see Sec. IV-C). We employ a mixed-methods approach, integrating both quantitative and qualitative techniques, to ensure a comprehensive analysis of participant data (see Sec. IV-D). Both our online study and offline interviews are approved by our Institutional Review Board (IRB) (see Sec. IV-E). Furthermore, we acknowledge the limitations of our user study (see Sec. IV-F), which help us identify potential constraints and guide future research efforts. We provide additional details about our online study and offline interview in Appendix A and Appendix B.

A. Online survey

In our online study, we evaluate three real RBA notifications. To collect such notifications, four members of our research team explore major online account providers for RBA notifications triggered by correct passwords, incorrect passwords, and clicking on the "reset password (i.e., forget password)" option. These notifications can be found online or on social media. Participants may have biases towards the companies initially sending these notifications. To minimize potential confusion from visual layouts, we rename all notifications visually as "COMPANY Name". Fig. 2 describes the renamed RBA notification. Before launching the user survey, we conduct internal discussions and exchanges among researchers to refine the wording and ensure the questions are comprehensible.

The survey starts with questions about how users describe and perceive RBA notifications (Q1). Then, we ask users if they have ever received such notifications and inquire about their behavior and response at that time (Q2).

Part 1: Feelings and Awareness. This section of the questionnaire focuses on two main questions: (1) whether participants perceive receiving RBA notifications as a threat to the security of their accounts, and (2) whether participants consider RBA notifications as important and beneficial to them. Firstly, we inquire about participants' perceptions of their account security being threatened when they receive RBA notifications triggered by someone else (Q3). Next, we present participants with three scenarios where RBA notifications are triggered by someone other than themselves. We then ask them to describe their feelings towards these notifications and explain their responses (Q4). Furthermore, we investigate the perceived benefits and drawbacks of RBA notifications (Q5, Q6). Following this, we assess the importance of RBA notifications to the participants (Q7). Lastly, we ask participants if they have difficulty understanding the content of RBA notifications (Q8).

Part 2: Understanding and Reactions. In this section, we begin by asking participants about the possible reasons they receive RBA notifications (Q9). We then inquire about the source of these RBA notifications (Q10). We offer participants a list of potential email-sending organizations to simplify the response process. Additionally, we provide open-ended responses, e.g., "Other_____" and "Don't know" options for participants. Next, we explore the timing of users typically checking RBA notifications and the specific content they read (Q11, Q12). Finally, We collect data on how participants handle RBA notifications and their reasons for doing so (Q13). We consistently emphasize the importance of participants selecting their actual practices rather than the correct actions.

Part 3: Perceptions and Expectations. Before proceeding to collect user expectations, we inquire about several environmental factors related to dealing with RBA notifications (Q16). These factors include the device, time, and location in which participants receive RBA notifications, as well as the channel (e.g., email and SMS) receiving them. We also measure the impact of these factors on participants' handling of RBA notifications (Q17, Q18). Furthermore, we examine other factors that influence user behavior, e.g., the importance of their accounts, the usage status of their accounts, and the type of risks involved. Additionally, we consider factors related to the content and design of RBA notifications. Next, we categorize the elements of RBA notification emails (as discussed in Sec. III-B) and invite participants to evaluate their necessity and level of demand (Q19). Following this, we collect participants' personal information (Q20∼Q24) and encourage users to share their questions and suggestions (Q25).

B. Offline interview

We conduct offline interviews to further explore users' genuine experiences and behaviors when RBA is triggered by someone else, as well as their expectations regarding the design and content of RBA notifications. Our volunteers are recruited at a campus market under the theme of web design testing. Once we have gathered the volunteers, we inform them about the interview process, risks, benefits, and their right to withdraw. With the participants' informed consent, we collect their contact information (e.g., phone number and email) and personal details (e.g., gender, age, major, familiarity with computer security). We employ a semi-structured interview to gather more insights and information about the participants' experiences and behaviors. The offline interviews take place between May 24th and June 10th, 2024, in a reserved classroom on our university campus. We conduct the interviews offline to ensure consistency in the experimental setting (e.g., scores) and device usage. Thus, this approach helps us avoid inconsistencies in interface and effects that might otherwise arise from using different devices. We strictly adhere to the participants' privacy protection guidelines, and the collected participant information is used solely for this experiment. The interview consists of the following three parts:

Part 1: Preparation. After obtaining the participants' interview consent, we schedule the interviews for one week. During the seven days leading up to the interviews, we impersonate the Google Security Team and send RBA notification emails to the participants. Since Google is the most popular and most visited website in the world [38], we ask users if they have a Google account when collecting user information. We exclude volunteers who do not have a Google account. We send these fake RBA notifications on the seventh day before the interview, the third day before the interview, and on the day of the interview itself. In particular, we choose to send the emails at approximately 10 AM, around 12 PM noon, and around 8 PM in the evening. Our sender uses a profile picture, name, and email address that mimics the Google Security Team by Emkei's Fake Mailer (`https://emkei.cz/`), aiming to test the participants' actual response.

Part 2: Interview. Seven days after the successful registration of participants, we schedule semi-structured interviews to be conducted in a classroom within the college building. The purpose of these interviews is to gather users' authentic experiences and expectations based on their recent interactions.

Firstly, we inquire whether the participants received any security-related email notifications in the past week and whether they clicked to view them. This helps us gauge the participants' level of attention and concern towards RBA notification (email). Next, we ask the participants about their reasons for viewing or not viewing the notifications. To further understand the participants' level of concern, we inquire about the approximate time they generally check RBA notifications and the content they encounter. We invite the participants to open up and express their feelings about the relevant email notifications. Subsequently, we invite the participants to describe the purpose of these email notifications and how they would respond to them. Furthermore, we inquire about the difficulties encountered by the participants and their expectations or suggestions regarding RBA notifications. Specifically, we inquire whether they would take any security measures mentioned in the emails, e.g., changing passwords, enabling two-factor authentication, or unlinking accounts.

Part 3: Scores-I. In this part, we show users nine RBA notification emails on both mobile phones and laptops and invite them to rate them. The RBA notifications selected for this part are a collection of various designs and elements triggered by 161 websites during our web research (see Sec. III-B). Specifically, we use a five-point rating scale to invite users to rate the design and content of RBA notifications. The RBA notifications are divided into three groups, each corresponding to three types of trigger methods. We use a unit-weighted model [44] with equal weights for each component. The composition of each notification is determined and explained based on Fig. 2 and (Q19). The scores for each component are calculated separately in three different scenarios (e.g., correct password, incorrect password, and "forget" password). Then, we extract Groups A (i.e., correct password), B (i.e., incorrect password), and C (i.e., "forget" password) from the RBA notifications' results in three different ways for this experiment. Users rate the email's subject, sender, risk warning, and handling suggestions for each group of RBA notifications. Additionally, during the experiment, if any participants feel uncomfortable, e.g., not wanting to open the email on the spot or evaluate the RBA notifications, they can pause the experiment at any time.

Scores-II. Based on Scores-I, we enhance the design, content, and intricate details of RBA notifications to precisely align with user expectations and specific requirements. Consistent with the above offline interview process, we show RBA notifications that meet user expectations to collect their feelings and reactions (see Figs.13-15 in our full version).

C. Recruitment and demographics

Online survey. We conduct an online survey and recruit 258 participants from the United States through the online research platform, Prolific. Prolific[1] is an open recruitment platform with strong capabilities for quick and efficient data collection [1], [35]. Each participant is allowed to respond to the survey only once. To ensure the quality of the survey, we reject 5 participants who complete the survey in less than 5 minutes. Additionally, 35 participants abandon the survey midway, and 22 exceed the time limit of 45 minutes. On average, it takes participants 15.7 minutes to complete the survey. Based on the local income level, each participant receives a compensation of 5 U.S. dollars for their time and effort. The survey is conducted from February 2024 to June 2024.

We use the built-in research inclusion criteria in Prolific for purposeful sampling of our target population. This criteria allows researchers to pre-screen the target population based on the research objectives to ensure the availability of the sample. Since the questionnaire is in English, we specifically select native English speakers as participants. Additionally, we strive to maintain balance in our sample by considering factors e.g., gender, major, and age. To gather more meaningful insights, particularly a conservative understanding of RBA notification issues, we exclude participants unfamiliar with computer security, as they often misunderstand and ignore RBA notifications (Chi-square test, $p<0.01$). Participants are allowed to use computers, tablets, or smartphones to complete the survey. Detailed information about the participants is displayed in Table II.

[1]Prolific: https://www.prolific.com/

TABLE II. DEMOGRAPHICS OF ONLINE PARTICIPANTS (N = 258).

Gender	n	%	Age	n	%	Education	n	%	Major	n	%	Background	n	%
Male	103	40	18-25	71	28	High school	87	34	Natural Sciences	16	6	Basic	19	7
Female	146	57	26-35	63	24	Bachelor's	103	40	Humanities	23	9	Familiar	200	78
Non-binary	5	2	36-45	70	27	Master's	47	18	Social Science	33	13	Developer/Professional	37	14
Prefer not to say	4	2	46-55	31	12	Doctorate	5	2	Engineering and Technology	33	13	Not familiar	0	0
			56-65	13	5	Others	12	5	Business and Management	24	9	Prefer not to say	2	1
			66 or older	8	3	Prefer not to say	4	2	Health Sciences and Education	25	10			
			Prefer not to say	2	1				Others	38	15			
									Prefer not to say	66	26			

*We round to the nearest whole number when dealing with percentages, which may lead to the sum of percentages not equaling 100%.

TABLE III. OFFLINE INTERVIEWEE'S PERSONAL INFORMATION.

No.	Gender	Age	Education	Proficiency
010	Female	19	Bachelor	Basic
012	Female	23	Master	Basic
020	Male	25	Master	Developer
021	Female	20	Bachelor	Familiar
022	Female	25	Bachelor	Familiar
023	Female	24	Bachelor	Basic
024	Female	22	Bachelor	Basic
025	Female	19	Bachelor	Familiar
026	Female	20	Bachelor	Familiar
027	Male	24	Master	Basic
028	Female	21	Bachelor	Familiar
029	Female	21	Bachelor	Familiar
030	Male	23	Master	Developer
031	Male	24	Master	Developer
032	Male	25	Doctor	Familiar

Offline interview. Our offline interviews recruit 15 participants. We advertise our volunteer recruitment information at the campus market, an internal forum, and trading venues. Any interested students can sign up to participate. To facilitate the subsequent experiments, we only inform participants that it is an evaluation interview about web design, with an estimated duration of 20 minutes. The actual average response time is 18.6 minutes. Based on the local income level, we compensate each participant with 6 U.S. dollars for their time and effort. The interview dates are scheduled one week after registration. The venue is a meeting room in the computer building. Before the interview begins, we request participants to provide their personal information, including phone number, email address, gender, age, education level, major, and familiarity with computer security. Participants are also informed of their informed consent: agreeing to the described procedures, risks, benefits, and the right to withdraw [37].

Most participants are between the ages of 18 and 24 and are pursuing undergraduate degrees. The gender ratio is 2:1. Over half of the participants are undergraduate students, with the remainder being master's students. All participants can use computers and access the Internet, and one-third have computer security backgrounds (see Table III).

D. Data analysis

We adopt a mixed-method approach that combines quantitative and qualitative data analysis methods.

Quantitative Analysis. We perform Likert-scale tests to assess users' feelings and perceptions towards RBA notification designs. When the expected frequency of the sample is greater than 5, we use Pearson's chi-square test to analyze the associations between different variables quantitatively. If the expected frequency is less than or equal to 5, we employ Fisher's exact test (FET) with a significance level of α=0.05.

Qualitative Analysis. We use the method of inductive coding [41] to analyze the content of participants' responses to open-ended questions (Q1, Q4, Q13, Q16) in the questionnaire and interviews. It is a common qualitative data analysis approach that categorizes and summarizes real-life situations, offering a comprehensive understanding of themes and categories. Two researchers are involved in the coding process. Initially, a primary coder creates an initial codebook based on the responses to the interview and questionnaire questions, coding them according to the questions. Then, a secondary codebook is created, coding 20% of the sub-sample for each theme. The results of the secondary coder are iterated with the primary coder until the inter-coder agreement, measured by Cohen's κ, exceeds 0.87. We follow the practices of other studies [13], [26], [31] and resolve any coding conflicts through extensive group discussions among the coders. The detailed codebook can be found in Appendix E of our full version.

E. Ethical considerations

We ensure that our research's design, purpose, and sample size comply with the local laws and regulations and adhere to general ethical principles. We disclose the associated risks and benefits before commencing the experiment. More specifically, to capture genuine user reactions, we do not inform participants about RBA notifications in advance. However, we do ask participants if they have received any other risk emails or notifications before recruiting them. Our follow-up with participants and efforts to minimize harm during the study include: (1) only retaining participants who explicitly consent to user studies involving potentially fake information; (2) simulating typical, non-alarming official Google RBA notifications to reduce stress; (3) allowing participants to withdraw at any time without penalty; (4) inviting participants to review the fake RBA notifications within a week to confirm no actual harm occurred, and explaining the purpose of our research to gain their understanding; and (5) closely monitoring participants throughout the study, with no participant reporting significant harm or distress. Finally, 4 out of 15 participants express just a little confusion and skepticism regarding the notifications, indicating that the risks are minimal and acceptable. We use structured note-taking and detailed text to record the interview process. In compliance with the GDPR and CCPA, all email addresses are encrypted, stored separately from research responses, and deleted after the study concludes.

F. Limitations

Like most research [12], [28] in privacy and security, our study results are also subject to the potential influence of self-reporting and social desirability biases. Participants' responses may differ from their actual reactions when they receive notifications in real-life situations [46]. To minimize these biases, we employ softened language in sensitive questions to gather responses from participants with different comfort levels [39]. While there may be inherent biases, related studies

demonstrate that survey responses regarding security information closely align with real-world reactions [18]. Therefore, we interpret our results as trends in user behavior rather than precise frequency estimates.

However, it is important to note that there is little difference in the sender's email address between the simulated RBA notifications sent through unofficial websites and the actual RBA notifications sent through official websites. Despite this, the subtle differences could potentially lead very attentive participants with a high level of security awareness to respond differently than they would to real RBA notifications.

Additionally, we acknowledge that the language used in the questionnaire and the influence of the RBA notification examples may influence our participant pool. We actively recruited participants who are native English speakers from the United States, which creates cultural biases in the results.

V. Results

In this section, we primarily focus on our three key research questions. First, we introduce the survey results concerning users' feelings and security awareness when receiving RBA notifications not triggered by themselves (**RQ1**, see Sec. V-A). Second, we present how users handle and understand RBA notifications (**RQ2**, see Sec. V-B). Third, we also investigate the correlation between some factors related to how users view and handle RBA notifications, and highlight users' expectations regarding RBA notifications (**RQ3**, see Sec. V-C).

A. RQ1: Feelings and Awareness

We find that 40.3% (104/258) of participants have received RBA notifications not triggered by themselves (Q2). Among them, 43.3% (45/104) changed their passwords, and 26.9% (28/104) checked the status of their accounts; However, 8.7% (9/104) of the participants did not respond in any manner, thereby compromising the security of their accounts.

Since experience is not always available to every user, we use a Chi-square test to examine the relationship between users' experiences (Q2) and their *feelings* (Q4) and *behaviors* (Q13). Our findings indicate that there is no significant correlation with behaviors (Q13) ($p = 0.133$). The Pearson coefficient of -0.162 further reflects this relationship. Given that not all users have experience, insights from both *experienced* and *inexperienced* users are crucial for understanding user behavior, as perception can shape behavior even in the absence of prior experience. However, there is a significant correlation between users' experiences (Q2) and feelings (Q4) ($p<0.01$). Users' feelings (suspicious, angry, anxious, nervous) show a significant correlation with their experience of receiving RBA notifications ($p<0.01$). Participants who have not experienced RBA are more likely to be angry (inexperienced: 38.98%, experienced: 32%) and skeptical (inexperienced: 62.7%, experienced: 60%). Participants who experience RBA are more likely to be anxious (experienced: 40%, inexperienced: 35.59%) and nervous (experienced: 36%, inexperienced: 33.9%).

Participants' perceptions of risk vary across three different types of RBA notifications. We first ask participants about their understanding of RBA notifications, which might include a detailed description of the notification's content (Q1). Among the participants, 40.3% (104/258) believe that receiving an authentication code indicates their account is under attack. Additionally, 29.8% (77/258) of the participants think their account is about to be accessed following an incorrect password attempt. Meanwhile, 15.5% (40/258) of the participants believe they need to change their password upon receiving a password reset request. Among the notifications triggered by correct passwords, 70.2% (181/258) of the participants believe that their accounts might be at risk of an attack. For notifications triggered by resetting passwords, 60.9% (157/258) of the participants think their accounts could be threatened. Lastly, for notifications triggered by incorrect password attempts, 58.9% (152/258) of the participants consider their accounts might be at risk of an attack (Q3).

RBA notifications not triggered by users often elicit negative emotions, with no significant differences in feelings toward the three types (e.g., correct password, incorrect password, and password reset). Among the twelve emotions reported by participants, suspicion (81.8%, 211/258), anxiety (60.5%, 156/258), nervousness (61.6%, 159/258), and surprise (53.1%, 137/258) are the users' feelings to receiving uninitiated RBA notifications (Q4). Fig. 3 illustrates the feelings of 258 respondents upon receiving three types of RBA notifications (using NRC EmoLex [33]). Conversely, some positive feelings, e.g., calm (10.5%, 27/258). Since the notifications convey potential risks to the participants, it is reasonable that the overall emotional response is negative. In our study, participants feel nervous and anxious, which leads them to immediately check the RBA notifications. Pearson's chi-square test results indicate that anxiety and nervousness prompt users to check RBA notifications and pay attention to account security ($p<0.05$).

Among the three types of RBA notifications, most respondents indicate that they feel suspicious after receiving an RBA notification. R65[2] explains, *"I would be suspicious as it indicates that someone may be trying to sign in to my account from an unknown device. I would be anxious about this and not happy at all."* Additionally, many participants express feelings of anxiety. *"I would be anxious and angry that an attack had begun on my account, and I would be racing to secure my account. I would also be suspicious, wanting to know where the attack is coming from." (R78)* In cases triggered by incorrect password attempts, R86 states, *"This really affects me, maybe even somewhat traumatic. To know someone is trying to compromise my most private data, and I am locked out for 10 minutes. This makes me ballistic."* Participants indicate that they are more concerned about RBA notifications attempting to change their passwords than those triggered by incorrect attempts. R157 says, *"It is scary and frustrating to have something which holds so much personal information at potential compromise."*

Most participants value RBA notifications for security, though frequent, non-self-triggered alerts are perceived as annoying, and personal experiences with fraud influence individuals' judgments of RBA notifications. 90.3% (233/258) of participants believe that RBA notifications are important (Q7), and 73.3% (189/258) of participants indicate that they can benefit and gain protection from these RBA notifications (Q5). However, if they frequently receive RBA notifications not triggered by themselves, 44.2% (114/258) of the participants express annoyance and feel bothered by this (Q6). Nevertheless, in our interviews, participants express

[2]R represents online users, and P represents offline participants.

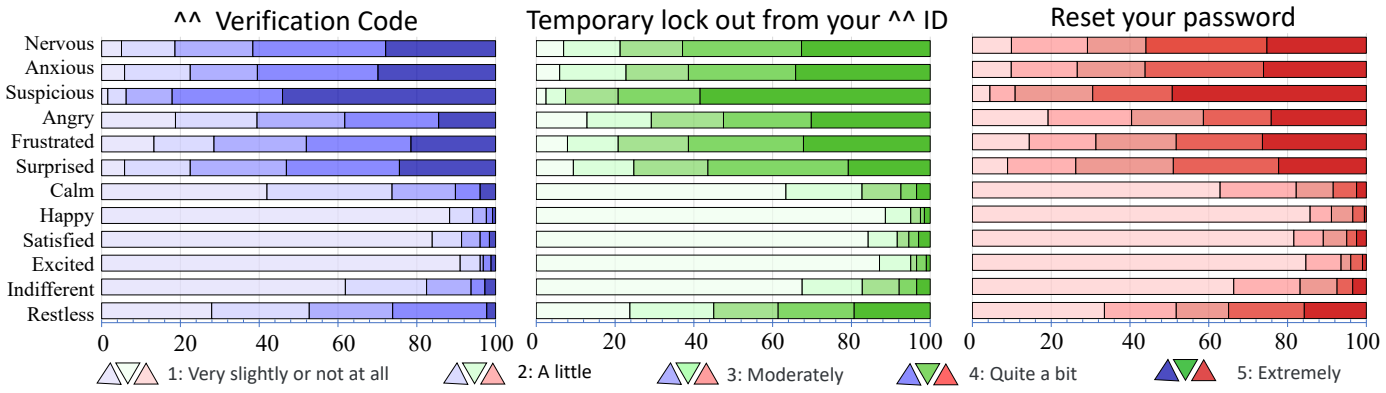


Fig. 3. The results regarding users' feelings upon receiving RBA notifications not initiated by themselves (Q4). Note: We use ^^to represent the account name.

completely different views. For instance, participant P010 states, "*I never check these emails that are not triggered by myself; these notifications are irrelevant to me unless my account is actually attacked or compromised, which might raise my awareness of a crisis.*" In contrast, another participant, P012, talks about her experience with a telecom scam, which significantly reduces her sensitivity and trust towards these emails. She says, "*These emails make me skeptical. I open and read the emails, but I do not completely trust their content. Instead, I verify the situation by logging into the official website of the account.*"

Participants believe RBA notifications mainly stem from unauthorized access and phishing, and they often ignore these alerts due to suspicions of potential attacks. 92.6% (239/258) of participants believe that unauthorized access triggers an RBA notification, followed by 53.9% (139/258) of participants who think that these notifications come from phishing attacks (Q9). Additionally, we invite participants to choose the sender of the email (Q10). 65% of participants believe that the service provider sends the RBA notifications. Surprisingly, approximately 46% of participants think that RBA notifications are phishing links sent by attackers. In our interview, P012 states, "*I do not respond to any RBA notifications that I did not trigger myself, as I am concerned that my account might be subjected to phishing attacks.*"

B. RQ2: Reactions and Understanding

We find that despite the widespread perceptions that receiving an RBA notification signals a security threat, 13.2% (34/258) of the participants tend to ignore notifications not initiated by themselves (Q12). Moreover, 25.2% (65/258) only read the titles, primarily because they believe that notifications not triggered by their own actions do not require attention. We confirm that the design of RBA notifications on websites, often perceived as user-unfriendly [56], prevents 36% (93/258) of participants from thoroughly reading and responding to these notifications (Q8). Additionally, our findings show that participants who have previously experienced account attacks are more likely to read and act on RBA notifications; however, most commonly, they do not understand or trust the system's warnings about security risks.

Most participants immediately read RBA notifications in full, especially if they view RBA notifications as beneficial. Participants are initially asked whether they unexpectedly receive RBA notifications and how they handle these notifications (Q2). Additionally, we present three types of RBA notifications to participants and inquire about their response times. The results reveal that 76% (196/258) of the participants address the RBA notifications immediately. Subsequently, 12% (31/258) participants respond within three hours, 5% (13/258) within 24 hours, and 7% (18/258) indicate that they never check these emails (Q11). Q12 shows that 10.9% (28/258) of participants only look at the notification title or skim through the content of the emails. Additionally, 20.9% (54/258) of participants tend to read only the purpose and verification information in the email, ignoring other details. Encouragingly, 70.9% (183/258) of participants report that they read the entire RBA notification. In Pearson's chi-square test (Q5, Q12), we find a significant correlation between *users' perceptions of RBA notifications as beneficial and their tendency to read the contents of these notifications (PCC: r=0.25, p<0.01).*

Most participants prefer viewing RBA notifications sent via email on their smartphones. We list the common devices currently used for receiving information. Among these, 89% of participants prefer to use their smartphones to view RBA notifications. Following this, 43% use laptops, and 25% use desktop computers (Q14). Less than 3% of participants use tablets or smartwatches to view RBA notifications. 86% of participants indicate a preference for receiving RBA notifications via email, while 51% favor SMS (Q15). 7% of the participants prefer to receive notifications through third-party apps. Fig. 4 shows the times, content viewed, devices used, and methods of viewing RBA notifications by the participants. In the Chi-square test, we do not find a significant correlation between the time users view RBA notifications and the devices they use (Q11, Q14).

The time, location, and device used to receive RBA notifications may affect how users respond to them. Q16 shows that 32.6% (84/258) users believe that the location influences their ways of handling RBA notifications. 32.2% (83/258) participants think that different devices impact their actions, and 31% (80/258) believe that the timing of receiving an RBA notification affects how they handle it. When asked about the impact of different locations, participants express concerns that public network data transmission could threaten their account security. R49 mentions that location does affect her behaviors, *"Yes - when you move from a safe environment (home encryption) to holiday hotel Wi-Fi or an unsafe Wi-Fi connection - you don't know who can access your data."* Additionally, when discussing the impact of receiving an RBA

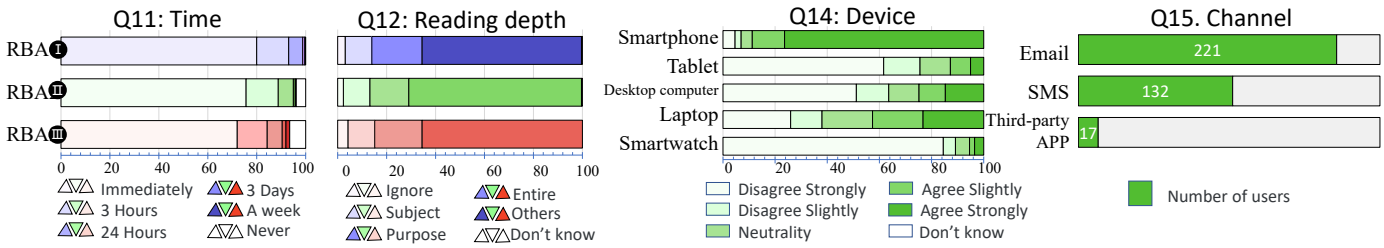


Fig. 4. The results detail how users handle RBA notifications, focusing on processing time (Q11), content read (Q12), device used (Q14), and channel (Q15). The types of RBA notifications include RBA1: Verification code, RBA2: Temporary lockout from your ID, and RBA3: Reset your password.

notification at different times, R65 explains, *"No, I'm still going to be irritated no matter the time of day."* R172 shares the same opinion, *"Time doesn't matter."*

Participants take other security measures upon receiving an RBA notification, not just changing their password. We find that when encountering RBA notifications triggered by the correct password, 65% of participants attempt to log into the account to verify the activity information of the account. If there are any suspicious activities, they attempt to change the account's password; Otherwise, they take no action. Next, 63% of participants indicate that they check for any abnormalities in the account. Additionally, 56% of participants mention that they enable two-factor authentication. It is reassuring that 55% of participants say they proactively change passwords that have been compromised. 37% of participants express that they change the passwords and information of important, key associated accounts. Meanwhile, 33% say they change passwords for other accounts that use the same password. Furthermore, 28% of participants indicate that they try using a password manager. 24% of the participants say they reset security questions. Concerningly, 31% of the participants express that they continue using the original password. Unexpectedly, 11% of participants say they deactivate unimportant accounts. 16% of the participants mention they seek official help. 8% of the participants click to unsubscribe from notifications and no longer receive related RBA notifications. Participants respond to notifications triggered by incorrect passwords in a manner similar to those triggered by correct passwords (see Fig. 5).

RBA notifications triggered by forgotten passwords are more likely to be ignored by users. However, under the "Forgot Password" button leading to RBA notifications, we find that 31% of participants attempt to change security questions, which is more than those triggered by correct passwords (15<49). Additionally, 17% of participants indicate they deactivate their accounts with correct password triggers, while 24% seek help from the support center. Participant R71 explains her reaction to RBA notifications triggered by password reset attempts, stating, *"I usually ignore these as they are just bots spamming email lists."* In contrast, participant R75 says, *"I would change my password as I feel they have been seriously attempting to gain access to my account."*

Users cannot effectively deal with RBA notifications. In our interview, most users say they don't know the risk level of their account and are unsure about which security measures to take to mitigate these risks or whether to do nothing at all. In the online study, 42% of participants state that they are capable of managing the notifications. 36% of participants do not know how to respond. Additionally, 19% of participants suggest that they might not know how to proceed (Q8).

Most participants follow the instructions in RBA notifications, but distrust and skepticism still persist. In our semi-structured interviews, participants select certain RBA notification expressions or descriptions that trigger their sense of urgency. The RBA notifications are extracted from Sec. III and some misleading descriptions we intentionally created. Most participants indicate that the following words (e.g., someone, lock, etc.) could raise their awareness of potential risks. In our interviews, 40% of the participants say they follow the instructions in the RBA notifications to perform security operations on their accounts. A key factor influencing user responses is their misunderstanding or mistrust of the received RBA notifications. For example, 54% of the participants believe that these RBA notifications are sent by phishing attackers or are just spam, and thus, they think their accounts are not threatened. Additionally, 13% of participants indicate that they do not read these RBA notifications thoroughly.

In our interview, 9/15 participants check the RBA notifications after a long time. 6 participants view the email subject or briefly scan the email and classify it as spam. Two report that their emails automatically filter these notifications. Another two review the email but deem it irrelevant, believing it is not triggered by their actions and that a verification code is necessary for successful login. One participant directly deletes the email, suspecting it might be a phishing attempt and advising that neither the content nor any included links should be trusted. During this period, 13 participants use their mobile phones to check the email notifications, while 2 use a computer. One participant (P024) believes that an RBA notification triggered by an incorrect password input is legitimate and anxiously asks, *"Have you really frozen my account?"* We inform her that the email is fabricated and no actual attack has occurred. Another participant (P022) states, *" I saw the email which includes a RBA notification, and tried to log into my account, but unfortunately, everything seemed normal. I think the email is just spam."*

Finally, one participant (P032) says *"When I see a 'reset password' message, I mistakenly think someone else has accessed my account, which leads to immediate concern about losing control of my account. As a result, I promptly log in and change my password."* Additionally, two users mention that they do not check their emails frequently, causing them to miss these RBA notifications. Another participant mentions that for accounts she considers unimportant (e.g., accounts without financial or social connections), she would choose to abandon the use of the account if it were compromised.

Some websites' security regulations may prevent users from changing their passwords. In our RBA notification study, we find that acting on some RBA notifications can

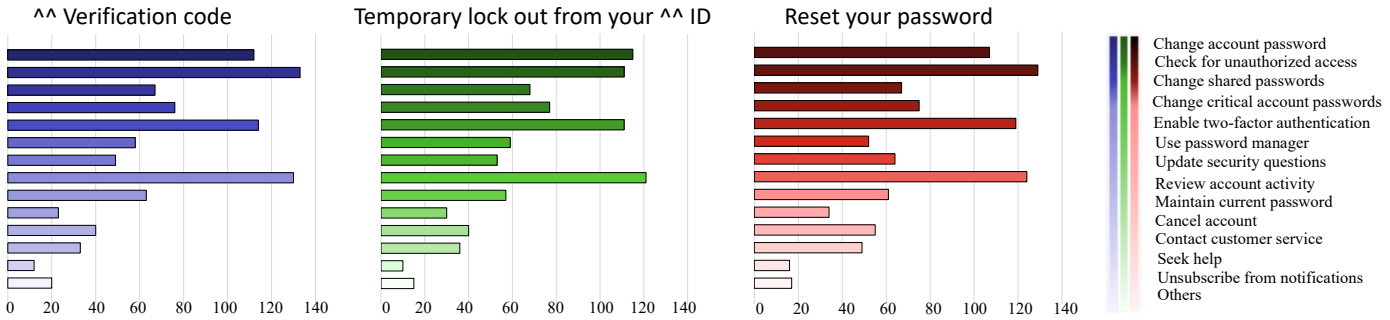


Fig. 5. The results of how users respond to the three types of RBA notifications (Q13). Note: We use ^^to represent the account name.

trigger a series of account changes (e.g., password changes or security settings updates). P022 indicates, *"I am concerned that changing my password might lead to a series of modifications to my account information, which I find not only troublesome but also insecure."* We compile the content of RBA notifications from various providers and ask participants to select their preferred course of action. Contrary to expectations, participants do not enhance the security of their linked accounts; Instead, they choose to sever these connections and either clear out, deactivate, or abandon some of their less critical accounts.

C. RQ3: Perceptions and Expectations

Q17 reveals a variety of factors that influence how participants respond to RBA notifications. Notably, 84% (216/258) participants state that the importance of the account significantly impacts their actions towards these RBA notifications. Furthermore, the content of risk warnings affects the behavior of 77% (199/258) participants, while the reasons for triggering the notifications influence 76% (195/258) participants. Changes in account status also play a critical role for 73% (189/258) participants. Additionally, 50% (128/258) participants are influenced by the sender's information and logo on the email, and the same number consider the validity of verification codes and links crucial in their response strategies.

Perceptions: satisfaction score. In the satisfaction score of RBA notifications by correct passwords, the highest satisfaction is observed with Namegreat (average score: 4.75), Samsung (average score: 4.5), and Constant Contact (average score: 4.4). 11/15 users appreciate detailed login information and a professional layout. "Professional layout" refers to a design that is clear, organized, and visually appealing, often adhering to industry standards or best practices. It typically includes elements like consistent formatting, appropriate use of colors and fonts, clear headings, and well-structured content (see Fig. 2). For incorrect passwords, LastPass (average score: 4.33), Unity3D (average score: 4.25), and GoG (average score: 3.86) are favored by the participants. Three participants prefer identity verification through a code rather than account linking. However, five participants indicate a desire to lock accounts to ensure security. One participant mentions, *"The website could lock the attacker's IP to prevent access to this account, rather than completely locking the account."* Regarding forgotten passwords, Zoom (average score: 4.33), ScienceDirect (average score: 4.25), and UI (average score: 4.11) lead to satisfaction (see Table IV).

However, six participants mistakenly believe that attackers have successfully logged in, causing them distress. One participant is concerned that someone might change their password, leading to a loss of control over their account, and wishes for official assistance to regain control. Four participants note that without a verification code, the password cannot be changed, and thus, the account remains secure. In the second RBA notification assessment, participants favor Google (average score: 4.7) for its risk warnings, LinkedIn (average score: 4.67) for its detailed information, and Adobe (average score: 3.1) for its lack of risk warnings (e.g., "If this wasn't you, please reset your password immediately!"). LastPass (average score: 4.55) receives high marks in the incorrect password category for its account locking feature, detailed unlock instructions, and clear explanation of the reasons behind the lock. For forgotten password notifications, UI's (average score: 4.3) clear and informative design is preferred, while Elsevier (average score: 3.2) is criticized for its use of *long URLs, which users perceive as resembling phishing links.*

The design of RBA notification content and the presentation of metadata significantly influence users' perception of a crisis. Our study delves into the components of RBA notifications and their impact on user responses, revealing that multiple factors play a critical role. Detailed account information within the email significantly influences the actions of 157 out of 258 participants, while 147 participants are affected by suspicions of unauthorized account access. The presentation of email metadata, such as sender and subject, also impacts user behavior. Furthermore, 121 participants are guided by

TABLE IV. SATISFACTION SCORES FOR RBA NOTIFICATIONS.*

Types	Rank	Website	Score I	Rank	Website	Score II
Correct password	16	Cloudflare	3.66	1	Google	**4.7**
	53	Adobe	3.14			
	128	Namecheap	4.75	14	LinkedIn	4.67
	645	Samsung	4.5			
	1054	Constantcontact	4.4	53	Adobe	3.1
	1075	Expedia	3.5			
	2170	GoG	4			
Incorrect password	144	Unity3D	4.25	2497	LastPass	**4.55**
	2098	Espncdn	3.38			
	2170	GoG	3.86	144	Unity3D	3.98
	2333	Instacart	3.8			
	2497	LastPass	4.33	2333	Instacart	3.3
	2763	Newegg	3.67			
Forget password	16	Cloudflare	3.2	191	Elsevier	3.2
	48	UI	4.11			
	53	Adobe	3.75	144	Unity3D	3.5
	63	Zoom	4.33			
	191	Sciencedirect	4.25	48	UI	**4.3**
	214	Cisco	3.6			

*The score is the average rating, with 5 being the highest score. A value shaded in light grey indicates the top three scores from the first evaluation. **Bold values** highlight the top scores from the second evaluation.

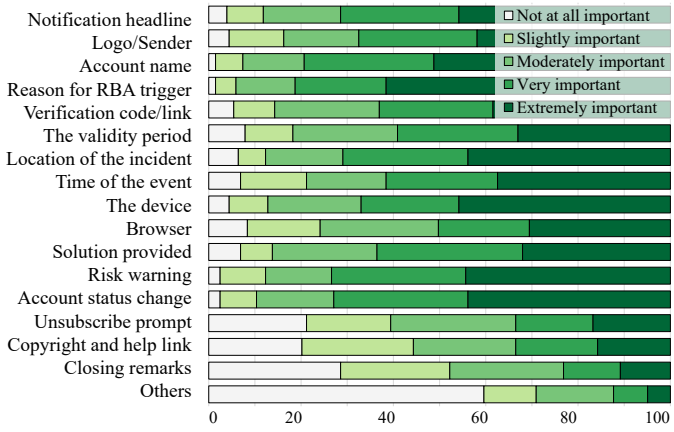


Fig. 6. The results concerning the impact and expectations of users regarding the content and design of RBA notifications (Q19).

the risk management advice provided in the emails, and 92 are influenced by the design of the email itself. Additionally, past experiences with similar notifications shape the responses of 83 participants, and experiences of actual account attacks following RBA notifications profoundly affect the reactions and behaviors of 95 participants (Q18). Further, our findings indicate a significant correlation between user gender and how the content of the email influences their handling of RBA notifications ($p<0.05$).

The authority of the sender and the integrity of RBA notification metadata are key factors in establishing user trust. In our interviews, participant P022 states, *"I do not respond to any unfamiliar emails unless I know they are sent by an authoritative institution."* When asked what makes her believe an email is from an authoritative source, she mentions, *"Initially, it is the design of the email that must look formal and professional."* Based on this insight, we deconstruct the RBA notifications and invite participants to assess the necessity of different components (see Fig. 6). The results of Q19 indicate that 80% (208/258) of participants consider the reason for triggering an RBA notification (79%, 165/208) and the account name (77%, 161/208) to be essential for users. Additionally, 58% of participants deem risk warnings (72%, 149/208), changes in account status (71%, 148/208), the notification's title (70%, 145/208), and the event's location (69%, 144/208) as very important for handling RBA notifications. Following these, 65% of participants find the sender and logo of the RBA notification (66%, 137/208) and the device triggering the RBA (65%, 136/208) necessary. Moreover, participants believe that guidance on resolving the issue (62%, 129/208), verification codes or links (62%, 128/208), the time of the event (60%, 125/208), and the validity period of verification codes (58%, 120/208) should be highlighted. Furthermore, 49% (102/208) of participants indicate that information about the browser version triggering the event is also necessary. 33.2% (69/208) of participants believe that notifications about unbinding and sender copyright marks are essential. 22.6% (47/208) of users mention the need for a closing statement in RBA notifications.

Expectation: RBA notification design. During our semi-structured interviews, participants describe their expectations for RBA notification content and rate them across three scenarios: notifications triggered by a correct password, an incorrect password, and a forgotten password. For each scenario, we randomly select three RBA notifications for evaluation. Participants then provide scores and explain their reasons.

More than one-third of the participants emphasize the importance of emails clearly establishing their identity as official notifications. For instance, participant P010 states, *"I do not trust unfamiliar emails unless they prove they are official by including the account name, password, verification code, the event's location and device, IP address, and a solution, along with a clear action plan within the RBA notification."* Participant P012 advocates for concision, *"RBA notifications should be designed clearly and concisely, informing me exactly what has happened without overly lengthy content, and key information should be prominently displayed."* We present two RBA notifications in Russian and Japanese. P012, P020, and P021 note that although they register on foreign websites, they prefer to receive notifications in their native languages.

Participant P026 comments on the appearance of the links in the notifications, observing, *"Long, stacked link addresses look informal and resemble phishing sites."* Participant P027 expresses confusion about how to handle some RBA notifications. Participant P029 highlights inconsistencies in messaging, saying, *"Some emails advise me to ignore the notification if it wasn't my activity, while others warn of account theft risks under similar circumstances. Whom should I trust? Should I ignore this risk notification? I hope the website provides a clear action plan and explains the reasons."*

Users want RBA to protect account security without disrupting their normal use. In the context of RBA notifications triggered by incorrect password attempts, one interviewee, P020, comments, *"The website locks the account after a certain number of wrong attempts, which I find disruptive to my normal usage. It would be more effective to lock the IP address causing the attempts, limiting its actions rather than hindering the usage of legitimate users like myself."* In dealing with RBA notifications, P027 remarks, *"The notification advises me to change my password and update my binding, which involves altering account information. This process feels both burdensome and unsafe to me."*

VI. Discussion

Our research findings show that users typically have high expectations for Risk-based Authentication (RBA) notifications triggered by unauthorized access. Over 90% of participants believe that RBA notifications play a vital role in account security by offering warnings and additional identity authentication. Despite this, the 46% of users often overlook these notifications due to their suspicion that the RBA notifications are phishing attempts or spam messages. Currently, the design and content of RBA notifications lack standardized guidelines, which may inadvertently lead users to disregard critical alerts. Additionally, our research indicates that RBA notifications lack risk level indicators, preventing users from effectively addressing the RBA notifications. Furthermore, 89% users prefer to read RBA notifications via email on their smartphones, while some layout designs are not compatible with mobile screens. Notably, most users hesitate to change their passwords when receiving RBA notifications, so offering diverse security measures based on risk can better protect accounts. Next, we offer several recommendations based on users' expectations to enhance the usability and security of RBA notifications.

A. Enhancement of RBA notification credibility and authority

Over 90% of participants consider RBA notifications important. However, we discover that 46% of participants perceive RBA notifications as phishing (Q10, see Sec. V-B), which contrasts sharply with the 1% in [28] who viewed login notifications as phishing. RBA notifications are mistaken for phishing emails for several reasons: in our interview, many users believe the additional authentication is not self-initiated, leading them to suspect phishing. Additionally, poorly formatted notifications can appear unprofessional or even garbled, further casting doubt on their legitimacy. About 29% of the participants indicate that they do not read these notifications in detail. Furthermore, we find that excessively long URLs and informal RBA notifications increase users' perceptions of RBA notifications as phishing emails (see Sec. V-C), which is a new finding that [11], [28], [29] have not observed.

Moxley [34] states that effective notifications should be clear, formal, and precise, incorporating legally recognized terms to boost their credibility. Furthermore, RBA notifications should be well-organized logically and appear professional and formal visually [6]. Therefore, to improve user response rates, it is crucial to ensure that these notifications uphold a professional visual and structural presentation. Delivering risks in a trustworthy manner enables users to respond effectively to RBA notifications and take timely actions to secure their accounts. To avoid phishing attacks [25], we recommend that users log in to the *official website* instead of clicking on directed links in notifications. RBA notifications regarding risks to users have prompted them to adopt security behaviors, which, to some extent, mitigates the risk of account theft through email [24].

B. Device-compatible RBA notifications

As indicated before, 86% of users prefer to receive RBA notifications via email, while 51% prefer SMS (Q15, see Sec. V-B). Our findings show that 89% of users prefer to receive RBA notification emails on their mobile phones, which is in line with research on the usability of RBA [52]. *However, some websites' RBA notifications are not suited for mobile screens*, lacking clear directional cues and proper line breaks (e.g., $cloudflare.com$). Based on these findings, we recommend that the design of RBA notifications should be optimized for both mobile screens and computer interfaces.

In our study, we find that 66% of respondents emphasize the importance of identifying the source and logo of the notification (Q19). Additionally, 51% of participants express a preference for receiving RBA notifications via SMS and text messages, which challenges the common belief that users prefer receiving RBA notifications only through email [29]. Besides, 65% of participants confirm that the RBA notifications they receive come from legitimate service providers (Q10). However, text messages received on mobile accounts tend to be brief [23], e.g., Apple's RBA notifications contain only a verification code without any accompanying explanation, which significantly differs from the more detailed email RBA notifications. However, when RBA notifications are sent via SMS, the sender's identity is often inconsistent, and the source is difficult to verify. Therefore, the design of RBA notifications delivered via text messages remains an unresolved issue, warranting further research and exploration.

C. Labeling the risk level of RBA notifications

Like other account security notifications [5], [28], [47], RBA notifications do not clearly differentiate risk levels. Our survey indicates that participants experience similar feelings (e.g., suspicion, nervousness, and anxiety) upon receiving three types of RBA notifications (Q4, see Sec. V-A). However, users who believe their accounts have been compromised are more likely to change their passwords or take other security measures, rather than ignore the notification (Q9, Q13, $p<0.01$). Prior research on warning design [11], [12], [28] has already noted the influence of contextual factors. Therefore, it is crucial to provide risk-related text descriptions (e.g., high, medium, or low risk in AWS's interface [29]) that differentiate notifications based on the level of account security threat.

In addition, the detailed reason for triggering RBA can also help users judge the level of risk. We confirm that most participants completely read login notifications [28]. However, RBA notifications triggered by correct passwords do not consistently include details, e.g., login time (25%), location (21%), and device (75%) in Sec. III. Much less do RBA notifications triggered by incorrect passwords or password resets contain these details (see Fig. 7 in Appendix A). We recommend that RBA notifications include more trigger details (e.g., time, location, and device) to help better identify the level of threat and understand why the RBA is triggered [29], [55].

D. User-friendly elements of RBA notifications

Designing a user-friendly and comprehensive RBA notification can significantly encourage users to focus on the security of their accounts [21]. In our study, participants have expectations and opinions about the content and design of RBA notifications (see Sec. V-C). Participants P023, P024, and P029 express a desire for RBA notifications to emphasize or highlight in red the warning texts or critical identifiers in emails that signal risks. Participants P023 and P025 seek notifications that provide clear, step-by-step instructions or categorically list precautions to take, concising the process for users to secure their accounts. Besides, for foreign account registrations, users prefer RBA notifications to be in their native language and easy to understand. Many participants advocate for concision (i.e., more concise text expression) and clarity in RBA notifications, as summarized by participant R231 with the phrase *"concision and clarity."*

At the same time, participant P022 raises a concern about the consequences of security measures, saying, *"Someone repeatedly trying wrong passwords resulted in my account being frozen, which affected my normal use. I suggest that the website freeze and prevent further operations from that IP or lock the device rather than preventing my normal use."* Our research suggests that applying these user-friendly principles could enhance the effectiveness of RBA systems in managing security risks while maintaining a positive user experience.

E. Comprehensive security measures in RBA notifications

It is reported that 22% of participants change their passwords after receiving unauthorized login notifications [28], while 43.3% of participants do so following RBA notifications (Q2). Additionally, some users mention that websites only request password changes; however, they abandon these changes if checking their accounts does not reveal any security

threats (Q2, see Sec. V-A). Besides, we find that 56% of users desire to enable 2FA to enhance account security (Q13, see Sec. V-B). This provides an alternative for users who prefer not to change their passwords for various reasons, thus expanding the options available to enhance account security. Therefore, it is more effective to provide users with comprehensive security measures (e.g., binding devices or setting security questions [19]) tailored to different risk levels, rather than making password changes the default response to all risks.

We test users' handling of RBA notifications through email messages, addressing issues overlooked in [11], [52]. We discover that 87% of users tend to read the complete RBA notification (Q12), while many participants express uncertainty about how to handle these RBA notifications. We confirm that some RBA systems only provide risk notifications without requiring secondary authentication [8]. Even if an attacker triggers the RBA, the account may not be adequately protected. Therefore, we recommend implementing secondary identity authentication for accounts where an RBA is triggered, ensuring stronger account security.

VII. Conclusion

We have conducted an online survey with 258 participants from the United States via the Prolific human data platform, and carried out offline RBA notification tests and interviewed an additional 15 participants, to explore *user reactions, perceptions, and expectations* regarding non-self-triggered RBA notifications of three types (i.e., correct password, incorrect password, forgotten password). Our RBA notification tests are conducted on 251 websites from the top 5K listed on Tranco. We have received 161 RBA email notifications from these 251 sites. Our findings reveal that RBA notifications are crucial for users. However, RBA notification design often lacks the necessary authority and credibility, which leads users to overlook or misunderstand them. This integration of empirical data with user sentiments and expectations compellingly illustrates the imperativeness to improve the design of RBA notifications. In summary, our new findings and insights provide a better understanding of user perceptions and reactions to current RBA notifications, and facilitate more informed design of future RBA notifications.

Acknowledgment

The authors are grateful to the shepherd and anonymous reviewers for their invaluable comments. Ding Wang is the corresponding author. This research was in part supported by the National Natural Science Foundation of China under Grants Nos. 62222208 and 62172240, and by the Fundamental Research Funds for the Central Universities, Nankai University (Grant No. 63243154). See the full version of this paper at https://bit.ly/3VsCsqe.

References

[1] *Why prolific? 2021*, Jul. 2021, https://bit.ly/4fYCdeG.

[2] M. Birks and J. Mills, *Grounded theory: A practical guide*. Sage, 2015.

[3] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Commun. ACM*, vol. 58, no. 7, pp. 78–87, 2015.

[4] C. Bravo-Lillo, L. F. Cranor, S. Komanduri, S. E. Schechter, and M. Sleeper, "Harder to ignore? revisiting pop-up fatigue and approaches to prevent it," in *Proc. SOUPS 2014*, pp. 105–111.

[5] B. Breve, G. Cimino, G. Desolda, V. Deufemia, and A. Elefante, "On the user perception of security risks of tap rules: A user study," in *Proc. SEUD 2023*, pp. 162–179.

[6] S. Dekker, *The safety anarchist: Relying on human expertise and innovation, reducing bureaucracy and compliance*. Routledge, 2017.

[7] F. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth, ""you still use the password after all" - exploring FIDO2 security keys in a small company," in *Proc. SOUPS 2020*, pp. 19–35.

[8] A. Gavazzi, R. Williams, E. Kirda, L. Lu, A. King, A. Davis, and T. Leek, "A study of multi-factor and risk-based authentication availability," in *Proc. USENIX SEC 2023*, pp. 2043–2060.

[9] M. Ghasemisharif, C. Kanich, and J. Polakis, "Towards automated auditing for account and session management flaws in single sign-on deployments," in *Proc. IEEE S&P 2022*, pp. 1774–1790.

[10] M. Ghasemisharif, A. Ramesh, S. Checkoway, C. Kanich, and J. Polakis, "O single sign-off, where art thou? An empirical analysis of single sign-on account hijacking and session management on the web," in *Proc. USENIX SEC 2018*, pp. 1475–1492.

[11] 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 *Proc. USENIX SEC 2021*, pp. 109–126.

[12] M. Golla, M. Wei, J. Hainline, L. Filipe, M. Dürmuth, E. M. Redmiles, and B. Ur, ""What was that site doing with my facebook password?": Designing password-reuse notifications," in *Proc. ACM CCS 2018*.

[13] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. M. Sadeh, and F. Schaub, ""it's a scavenger hunt": Usability of websites' opt-out and data deletion choices," in *Proc. ACM CHI 2020*, pp. 1–12.

[14] T. Huang, "Using sor framework to explore the driving factors of older adults smartphone use behavior," *HUM. SOC. SCI. COMMUN.*, vol. 10, no. 1, pp. 1–16, 2023.

[15] J. H. Huh, H. Kim, S. S. V. P. Rayala, R. B. Bobba, and K. Beznosov, "I'm too busy to reset my linkedin password: On the effectiveness of password reset emails," in *Proc. ACM CHI 2017*, pp. 387–391.

[16] A. Jankovič, T. Kolenik, and V. Pejović, "Can personalization persuade? study of notification adaptation in mobile behavior change intervention application," *Behav. Sci.*, vol. 12, no. 5, pp. 1–16, 2022.

[17] J. Jiang, D. Wang, G. Zhang, and Z. Chen, "Quantum-resistant password-based threshold single-sign-on authentication with updatable server private key," in *Proc. ESORICS*, 2022, pp. 295–316.

[18] F. Kreuter, S. Presser, and R. Tourangeau, "Social desirability bias in cati, ivr, and web surveys: The effects of mode and question sensitivity," *Public Opin. Q.*, vol. 72, no. 5, pp. 847–865, 2008.

[19] D. Landoll, *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press, 2021.

[20] L. Lassak, P. Markert, M. Golla, E. Stobert, and M. Dürmuth, "A comparative long-term study of fallback authentication schemes," in *Proc. CHI 2024*, pp. 1–19.

[21] L. Lassak, E. Pan, B. Ur, and M. Golla, "Why aren't we using passkeys? obstacles companies face deploying FIDO2 passwordless authentication," in *Proc.USENIX SEC 2024*, pp. 7231–7248.

[22] K. Lee, S. Sjöberg, and A. Narayanan, "Password policies of most top websites fail to follow best practices," in *Proc. SOUPS 2022*.

[23] J. Li, S. Zhang, and W. Ao, "Why is instant messaging not instant? understanding users' negative use behavior of instant messaging software," *Comput. Hum. Behav.*, vol. 142, pp. 655–670, 2023.

[24] Y. Li, H. Wang, and K. Sun, "Email as a master key: Analyzing account recovery in the wild," in *Proc. INFOCOM 2018*, pp. 1646–1654.

[25] X. Lin, P. Ilia, S. Solanki, and J. Polakis, "Phish in sheep's clothing: Exploring the authentication pitfalls of browser fingerprinting," in *Proc. USENIX SEC 2022*, pp. 1651–1668.

[26] Y. Liu, Y. Jia, Q. Tan, Z. Liu, and L. Xing, "How are your zombie accounts? understanding users' practices and expectations on mobile app account deletion," in *Proc. USENIX SEC 2022*, pp. 863–880.

[27] P. Markert, D. V. Bailey, M. Golla, M. Dürmuth, and A. J. Aviv, "On the security of smartphone unlock pins," *ACM Trans. Priv. Secur.*, vol. 24, no. 4, pp. 30:1–30:36.

[28] P. Markert, L. Lassak, M. Golla, and M. Dürmuth, "Understanding users' interaction with login notifications," in *Proc. CHI 2024*, pp. 1–17.

[29] 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 *Proc. SOUPS 2022*, pp. 483–501.

[30] K. Marky, K. Ragozin, G. Chernyshov, A. Matviienko, M. Schmitz, M. Mühlhäuser, C. Eghtebas, and K. Kunze, ""nah, it's just annoying!" a deep dive into user perceptions of two-factor authentication," *ACM Trans. Comput. Hum. Interact.*, vol. 29, no. 5, pp. 1–32, 2022.

[31] P. Mayer, Y. Zou, F. Schaub, and A. J. Aviv, ""now i'm a bit angry: " individuals' awareness, perception, and responses to data breaches that affected them," in *Proc. USENIX SEC 2021*, pp. 393–410.

[32] H. Mehraj, D. Jayadevappa, S. L. A. Haleem, R. Parveen, A. Madduri, M. R. Ayyagari, and D. Dhabliya, "Protection motivation theory using multi-factor authentication for providing security over social networking sites," *Pattern Recognit.*, vol. 152, pp. 218–224, 2021.

[33] S. M. Mohammad and P. D. Turney, "Crowdsourcing a word–emotion association lexicon," *IEEE Comput. Intell. Mag.*, vol. 29, no. 3, pp. 436–465, 2013.

[34] J. M. Moxley, *Credibility Authority – How to Be Credible Authoritative in Speech Writing*, Sep. 2023, https://writingcommons.org/section/information-literacy/authority/.

[35] S. Palan and C. Schitter, "Prolific. ac—a subject pool for online experiments," *J. Behav. Exp. Finance*, vol. 17, pp. 22–27, 2018.

[36] V. Petkauskas, *RockYou2024: 10 billion passwords leaked in the largest compilation of all time*, 2024, https://bit.ly/4g6LTUr.

[37] A.-M. Pietilä, S.-M. Nurmi, A. Halkoaho, and H. Kyngäs, "Qualitative research: Ethical considerations," *The Application of Content Analysis in Nursing Science Research*, pp. 49–69, 2020.

[38] V. L. Pochat, T. van Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen, "Tranco: A research-oriented top sites ranking hardened against manipulation," in *Proc. NDSS 2019*, pp. 1–15.

[39] G. Qin and J. Eisner, "Learning how to ask: Querying lms with mixtures of soft prompts," *arXiv preprint arXiv:2104.06599*, 2021.

[40] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," in *Proc. CHI 2018*, pp. 1–13.

[41] J. Saldaña, "The coding manual for qualitative researchers," *The coding manual for qualitative researchers*, pp. 1–440, 2021.

[42] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT Technol. J.*, vol. 19, no. 3, pp. 122–131, 2001.

[43] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," *NIST Special Publication*, vol. 800, no. 115, pp. 2–25, 2008.

[44] Stephan Wiefling, M. Dürmuth, and L. L. Iacono, "What's in score for website users: A data-driven long-term study on risk-based authentication characteristics," in *Proc. FC 2021*, pp. 361–381.

[45] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting accounts from credential stuffing with password breach alerting," in *Proc. USENIX SEC 2019*, pp. 1556–1571.

[46] R. Tourangeau and T. Yan, "Sensitive questions in surveys," *PSYCHOL BULL*, vol. 133, no. 5, pp. 859–883, 2007.

[47] C. Utz, M. Michels, M. Degeling, N. Marnau, and B. Stock, "Comparing large-scale privacy and security notifications," in *Proc. PETS 2023*, pp. 173–193.

[48] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in *Proc. ACM CCS 2016*, pp. 1242–1254.

[49] D. Wang, Y. Zou, Y.-A. Xiao, S. Ma, and X. Chen, "Pass2Edit: A Multi-Step Generative Model for Guessing Edited Passwords," in *Proc. USENIX SEC 2023*, pp. 983–1000.

[50] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Trans. Dependable Secure Comput.*, pp. 193–208, 2021.

[51] S. Wiefling, "Usability, security, and privacy of risk-based authentication," Ph.D. dissertation, Ruhr-Universität Bochum, 2023.

[52] S. Wiefling, M. Dürmuth, and L. L. Iacono, "More than just good passwords? A study on usability and security perceptions of risk-based authentication," in *Proc. ACSAC 2020*, pp. 203–218.

[53] S. Wiefling, L. L. Iacono, and M. Dürmuth, "Is this really you? an empirical study on risk-based authentication applied in the wild," in *Proc. IFIP SEC 2019*, pp. 134–148.

[54] S. Wiefling, P. R. Jørgensen, S. Thunem, and L. L. Iacono, "Pump up password security! evaluating and enhancing risk-based authentication on a real-world large-scale online service," *ACM Transactions on Privacy and Security*, vol. 26, no. 1, pp. 1–36, 2022.

[55] S. Wiefling, T. Patil, M. Dürmuth, and L. L. Iacono, "Evaluation of risk-based re-authentication methods," in *Pro. IFIP SEC 2020*.

[56] D. Wu, G. D. Moody, J. Zhang, and P. B. Lowry, "Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention," *INFO&MANAG*, vol. 57, no. 5, pp. 235–250, 2020.

[57] T. Wu, R. Zhang, W. Ma, S. Wen, X. Xia, C. Paris, S. Nepal, and Y. Xiang, "What risk? I don't understand. an empirical study on users' understanding of the terms used in security texts," in *Proc. ACM ASIACCS 2020*, pp. 248–262.

[58] K. Xiu and D. Wang, "PointerGuess: Targeted password guessing model using pointer mechanism," in *Proc. USENIX SEC 2024*, pp. 5555–5572.

[59] 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 *Proc. CHI 2019*, pp. 1–14.

[60] Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub, ""I've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach," in *Proc. SOUPS 2018*, pp. 197–216.

APPENDIX

A. Online study

Thank you for your interest in our survey. Your responses are invaluable to us. Please carefully read the following instructions:
(i)Take your time to read and answer the questions thoroughly.
(ii)Answer the questions truthfully rather than selecting what you think might be the right answer.
(iii)It is acceptable to indicate that you do not know an answer.

Q1. There are three Risk-based Authentication (RBA) notifications (see Fig. 7). You are receiving these notifications without any action on your part. Please describe what the RBA notifications are indicating. [Text explanation]

Fig. 7(a): [Text explanation]
Fig. 7(b): [Text explanation]
Fig. 7(c): [Text explanation]

Q2. Have you ever received verification codes or authentication information like the following for your online accounts when you did not initiate the operation yourself (see Fig. 7(a), Fig. 7(b) and Fig. 7(c))?
Fig. 7(a): ○Yes ○No ○Maybe ○Don't know
Fig. 7(b): ○Yes ○No ○Maybe ○Don't know
Fig. 7(c): ○Yes ○No ○Maybe ○Don't know

(If yes is selected) Please select from the following scenarios where your account was compromised. [Multiple choice]
☐ My account was attacked without receiving an RBA notification.
☐ I received an RBA notification but did not take any action, and as a result, my account was attacked.
☐ I received an RBA notification and reviewed it, but I did not change the password, which led to an attack on my account.
☐ I received an RBA notification, reviewed it, and updated my account password, but I still experienced an attack.
☐ I received an RBA notification, took no action, and my account remained secure.
☐ I received an RBA notification, changed the password, and my account remained secure.
☐ I received an RBA notification, checked the account status without changing the password, and my account was not compromised.
☐ Other_____
☐ Don't know

Q3. If you receive an RBA notification that you didn't trigger, do you think your account's security has been compromised?
Fig. 7(a): ○Strongly agree ○Agree ○Neither agree nor disagree ○Disagree ○Strongly disgree ○Don't know
Fig. 7(b): ○Strongly agree ○Agree ○Neither agree nor disagree ○Disagree ○Strongly disgree ○Don't know
Fig. 7(c): ○Strongly agree ○Agree ○Neither agree nor disagree ○Disagree

◯Strongly disgree ◯Don't know

Q4. Please select the feelings you experience when you receive an RBA notification that was not triggered by yourself: (Answer choice per item: ◯Very slightly or not at all ◯A little ◯Moderately ◯Quite a bit ◯Extremely)
Fig. 7(a): ○ Nervous ○ Anxious ○ Suspicious ○ Angry ○ Frustrated ○ Surprised ○ Calm ○ Happy ○ Satisfied ○ Excited ○ Indifferent ○ Restless ○ Other_____
Please provide an explanation for your intense emotions. [Text explanation]
Fig. 7(b): ○ Nervous ○ Anxious ○ Suspicious ○ Angry ○ Frustrated ○ Surprised ○ Calm ○ Happy ○ Satisfied ○ Excited ○ Indifferent ○ Restless ○ Other_____
Please provide an explanation for your intense emotions. [Text explanation]
Fig. 7(c): ○ Nervous ○ Anxious ○ Suspicious ○ Angry ○ Frustrated ○ Surprised ○ Calm ○ Happy ○ Satisfied ○ Excited ○ Indifferent ○ Restless ○ Other_____
Please provide an explanation for your intense emotions. [Text explanation]

Q5. Do you benefit from RBA notifications?
◯Never ◯Sometimes ◯About half the time ◯Most of the time
◯Always ◯Don't know

Q6. Do frequent RBA notifications cause you distress or negative emotions?
◯Never ◯Sometimes ◯About half the time ◯Most of the time
◯Always ◯Don't know

Q7. Do you think RBA notifications are important to you?
◯Extremely important ◯Very important ◯Moderately important
◯Slightly important ◯Not at all important ◯Don't know

Q8. Do you feel helpless and uncertain about what to do when you receive an RBA notification that was not triggered by you?
◯Definitely not ◯Probably not ◯Might or might not ◯Probably yes
◯Definitely yes ◯Don't know

Q9. What do you think are the reasons for receiving an RBA notification triggered by someone other than yourself? [Multiple choice]
☐ Unauthorized login attempts.
☐ Family/friends logging in due to shared account credentials.
☐ System or data processing errors.
☐ Malicious links sent by attackers.
☐ Other_____
☐ Don't know

Q10. Who do you think sends the RBA notifications that are triggered by someone other than yourself? [Multiple choice]
☐ Service provider
☐ Corporate IT department
☐ Third-party security service provider
☐ Scammers or phishing attackers
☐ Other_____
☐ Don't know

Q11. How soon do you typically check or respond to an RBA notification you did not trigger? (Focus on actual behavior rather than what you think is correct.) [Multiple choice]
Fig. 7(a): ☐ Immediately ☐ 3 Hours ☐ 24 Hours ☐ 3 Days ☐ A week ☐ Never ☐ Don't know
Fig. 7(b): ☐ Immediately ☐ 3 Hours ☐ 24 Hours ☐ 3 Days ☐ A week ☐ Never ☐ Don't know
Fig. 7(c): ☐ Immediately ☐ 3 Hours ☐ 24 Hours ☐ 3 Days ☐ A week ☐ Never ☐ Don't know

Q12. How do you realistically focus on the content when reading an RBA notification triggered by someone other than yourself? (Focus on actual behavior rather than what you think is correct.)
Fig. 7(a): ◯Ignore the RBA notification.
◯Read the source and subject, but not the body of the RBA notification.
◯Read the purpose and authentication information and ignore the rest.
◯Read the entire notification.
◯Others.
◯Don't know.
Fig. 7(b): ◯Ignore the RBA notification.
◯Read the source and subject, but not the body of the RBA notification.
◯Read the purpose and authentication information and ignore the rest.
◯Read the entire notification.
◯Others
◯Don't know.
Fig. 7(c): ◯Ignore the RBA notification.
◯Read the source and subject, but not the body of the RBA notification.
◯Read the purpose and authentication information and ignore the rest.
◯Read the entire notification.
◯Others
◯Don't know.

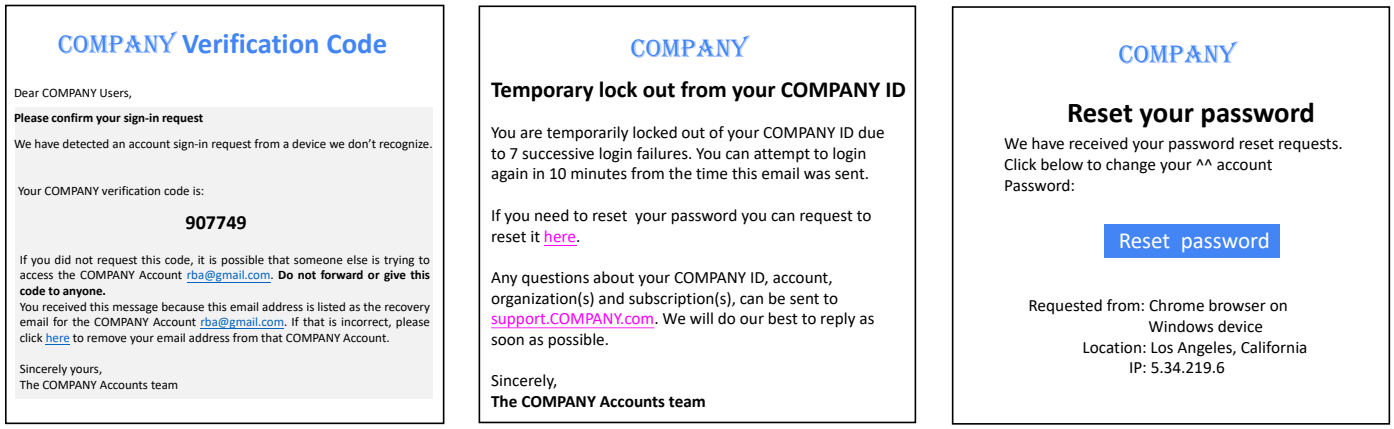
Q13. How do you actually handle an RBA notification that was not triggered by you? (Focus on your real actions rather than what you think is the correct approach) [Multiple choice]
Fig. 7(a): ☐ Change Account Password: Immediately change the password for the account that triggered the RBA notification.
☐ Check for Unauthorized Access: Log into the account to verify activity. If suspicious, change the password; if not, no action is needed.
☐ Change Shared Passwords: Update passwords of other accounts sharing the same password.
☐ Change Critical Account Passwords: Update passwords for critical accounts (like bank accounts) with the same password.
☐ Enable Two-Factor Authentication (2FA): Activate 2FA for added security.
☐ Use Password Manager: Use a password manager to secure credentials.
☐ Update Security Questions: Refresh security questions and answers.
☐ Review Account Activity: Check recent activities for anomalies.
☐ Maintain Current Password: Keep the password unchanged if deemed secure.
☐ Cancel Account: Consider account cancellation if necessary.
☐ Contact Customer Service: Reach out to official support for assistance.
☐ Seek Help: Share the situation to get help.
☐ Unsubscribe from Notifications: Opt out of receiving RBA notifications.
☐ Others.
Please explain why. [Text explanation]
Fig. 7(b): ☐ Change Account Password: Immediately change the password for the account that triggered the RBA notification.
☐ Check for Unauthorized Access: Log into the account to verify activity. If suspicious, change the password; if not, no action is needed.
☐ Change Shared Passwords: Update passwords of other accounts sharing the same password.
☐ Change Critical Account Passwords: Update passwords for critical accounts (like bank accounts) with the same password.
☐ Enable Two-Factor Authentication: Activate 2FA for added security.
☐ Use Password Manager: Use a password manager to secure credentials.
☐ Update Security Questions: Refresh security questions and answers.
☐ Review Account Activity: Check recent activities for anomalies.
☐ Maintain Current Password: Keep the password unchanged if deemed secure.
☐ Cancel Account: Consider account cancellation if necessary.
☐ Contact Customer Service: Reach out to official support for assistance.
☐ Seek Help: Share the situation to get help.
☐ Unsubscribe from Notifications: Opt out of receiving RBA notifications.
☐ Others.
Please explain why. [Text explanation]
Fig. 7(c): ☐ Change Account Password: Immediately change the password for the account that triggered the RBA notification.
☐ Check for Unauthorized Access: Log into the account to verify activity. If suspicious, change the password; if not, no action is needed.
☐ Change Shared Passwords: Update passwords of other accounts sharing the same password.
☐ Change Critical Account Passwords: Update passwords for critical accounts (like bank accounts) with the same password.
☐ Enable Two-Factor Authentication (2FA): Activate 2FA for added security.
☐ Use Password Manager: Use a password manager to secure credentials.
☐ Update Security Questions: Refresh security questions and answers.
☐ Review Account Activity: Check recent activities for anomalies.
☐ Maintain Current Password: Keep the password unchanged if deemed secure.
☐ Cancel Account: Consider account cancellation if necessary.
☐ Contact Customer Service: Reach out to official support for assistance.
☐ Seek Help: Share the situation to get help.
☐ Unsubscribe from Notifications: Opt out of receiving RBA notifications.
☐ Others.
Please explain why. [Text explanation]

Q14. On which devices do you typically view your RBA notifications? (5 indicates the most frequently used device.) (◯1 ◯2 ◯3 ◯4 ◯5 ◯ Don't know)
○ Smartphone ○ Tablet ○ Desktop computer ○ Laptop ○ Smartwatch
○ Don't know ○ Other_____

Q15. What channels would you prefer to receive RBA notifications? [Multiple choice]
☐ Email ☐ SMS ☐ Third-party app ☐ Other_____ ☐ Prefer not to say

Q16. Please assess the impact of the following factors on how you handle RBA notifications. (5 indicates the most relevance, ◯1 ◯2 ◯3 ◯4 ◯5 ◯ Don't know)
○ Different times of receiving the RBA notification.
Why? [Text explanation]
○ Different devices of receiving the RBA notification.
Why? [Text explanation]
○ Different locations of receiving the RBA notification.
Why? [Text explanation]

Q17. Which of the following factors would influence your response or level of concern regarding an RBA notification triggered by someone other than yourself? (Answer choice per item: No effect (1) – Major effect (5).)
○ The importance of the account
○ Logo/Sender
○ Reason for RBA trigger (e.g., authorized access from a new device, password change request, or too many failed attempts)
○ The validity period of the verification code or link (e.g., Please enter the verification code within five minutes.)
○ Risk warning (e.g., notification to change password due to unauthorized access detection)



(a) RBA notification with correct password. (b) RBA notification with incorrect passwords. (c) RBA notification with reset option.

Fig. 7. Real-world examples of the three types of RBA notification (e.g., correct password, incorrect password, and reset password). We use the name "company" as a substitute for "Google" to reduce user bias.

○ Account status change (e.g., re-authentication required or account locked)
○ Other_____

Q18. How much did the following factors influence your reaction? (Answer choice per item: No effect (1) – Major effect (5).)
○ Email metadata (e.g., sender, subject)
○ Email content (e.g., details of account information, wording)
○ Email design (e.g., structure, color, font size)
○ Guidance for users on handling suspicious RBA notifications triggered by unauthorized actions (e.g., "If this wasn't you, please ignore"; "If this wasn't you, please change your password").
○ I suspect unauthorized access to my account and have received an RBA notification for verification.
○ I have previously received similar emails and experienced substantial loss or harm to my account.
○ I have previously received similar emails that I initially believed were legitimate, but they turned out to be phishing attacks.
○ Other_____

Q19. Please rate the necessity of the following RBA notification components (that the RBA was not triggered by you) (◯1 ◯2 ◯3 ◯4 ◯5 ◯ Don't know) (5 indicates the most needed).
○ Notification headline
○ Logo/Sender
○ Account name
○ Reason for RBA trigger (e.g., authorized access from a new device)
○ Verification code/link
○ The validity period of the verification code or link
○ Location of the incident
○ Time of the event
○ The device from which the event was triggered
○ Browser where the event occurred
○ Solution provided (e.g., please change your password)
○ Risk warning (e.g., there is a suspicious login activity.)
○ Account status change (e.g., re-authentication required or account locked)
○ Unsubscribe prompt (allowing non-account holders to unlink)
○ Copyright notice and help link
○ Closing remarks
○ Other_____

Personal information

Q20. What is your gender?
◯Male ◯Female ◯Non-binary/third gender
◯Prefer not to say

Q21. What is your age?
◯18-25 ◯26-35 ◯36-45 ◯46-55
◯56-65 ◯66+ ◯Prefer not to say

Q22. What is the highest degree or level of school you have completed?
◯No schooling completed
◯High school graduate, or equivalent
◯Bachelor's degree, or equivalent
◯Master's degree, or equivalent
◯Doctorate degree, or equivalent
◯Other (please specify)
◯Prefer not to say

Q23. Do you have a major in one of the following fields?
◯Natural Sciences
◯Humanities
◯Social Sciences
◯Engineering and Technology
◯Business and Management
◯Health Sciences
◯Education
◯Other (please specify)
◯Prefer not to say

Q24. Please describe your level of familiarity with computer security.
◯Not familiar (I never surf the Internet)
◯Basic (I use the computer)
◯Familiar (I can perform normal tasks on a computer)
◯Developer/Professional
◯Prefer not to say

Q25. (Optional) If you have any questions or suggestions, please leave a message.

B. Guideline for the offline interview

1. In the past week, have you received any emails similar to the image described (related to RBA notifications)?
a) If yes, how do you deal with it?
b) If no, why don't you receive any?
c) Did you open the email? Why or why not?
d) If you opened it, when did you do so? Right after receiving it, an hour later, 24 hours later, or three days later? Why at that particular time?
[Review three emails on-site.]
2. What were your emotions and feelings upon receiving the three different RBA notifications, and why?
3. Please open the relevant RBA notification email. What information did you derive from the email?
4. Which information in an RBA notification triggers your sense of urgency? In what situations do you perceive that your account's security is compromised?
5. What difficulties did you face with the RBA notification? Will you read the entire RBA notification? Why or why not?
6. Do you think that receiving an RBA notification not triggered by yourself impacts your account's security? Why or why not? What steps do you think should be taken to address the risks mentioned in the RBA notification?
7. In real life, what do you think are the reasons for receiving an RBA notification that you did not trigger?
8. What content and design do you expect in an RBA notification? [Please provide some examples.] Which style do you prefer? Rank them and explain why (e.g., design, content, components, etc).
[Show nine RBA notifications.]
9. What are the benefits and drawbacks of receiving an RBA notification that you did not trigger? Please explain or share relevant experiences.
10. When you receive an RBA notification you didn't trigger, do you worry about the security of linked accounts, like those sharing the same password or dependent on each other? Why or why not? What actions do you take?