Users' Perceptions of Chrome Compromised Credential Notification

Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov,
University of British Columbia

https://www.usenix.org/conference/soups2022/presentation/huang

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Users' Perceptions of Chrome's Compromised Credential Notification

Yue Huang
University of British Columbia

Borke Obada-Obieh
University of British Columbia

Konstantin Beznosov
University of British Columbia

Abstract

This paper reports the challenges that users experienced and their concerns regarding the Chrome compromised credentials notification. We adopted a two-step approach to uncover the issues of the notification, including qualitatively analyzing users' online comments and conducting semi-structured interviews with participants who had received the notification. We found that users' issues with the notification are associated with five core aspects of the notification: the authenticity of the notification, data breach incidents, Google's knowledge of users' compromised credentials, multiple accounts being associated with one notification, and actions recommended by the notification. We also identified the detailed challenges and concerns users had regarding each aspect of the notification. Based on the results, we offer suggestions to improve the design of browser-based compromised credential notifications to support users in better protecting their online accounts.

1 Introduction

The widespread availability of usernames and passwords exposed by data breaches remains a big threat to users and organizations. According to the Verizon 2021 data breach investigations report [9], credentials are the primary means by which an attacker hacks into an organization, with 61% of breaches attributed to leveraged credentials. By using the breached credentials, an adversary can try to log into other systems based on the assumption that users often reuse their credentials across multiple systems [18, 23, 88]. Credential stuffing, as this is known, is dangerous to both users and organizations.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

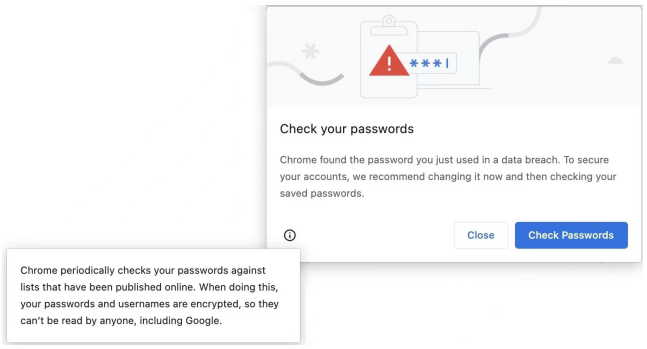

Figure 1: Chrome's Pop-up Compromised Credential Notification

For instance, in 2020, the credentials (i.e., username-password pairs) of over 530,000 Zoom teleconferencing accounts were found for sale on the dark web [108]. The credential information was not from any breach at Zoom itself; it was obtained through credential stuffing. This incident led many companies worldwide, including Google, SpaceX, and NASA [71], to ban the use of Zoom [108] and other video conferencing apps. If their accounts are hijacked, users can lose access to important information and documents and even suffer from fraudulent transactions, unauthorized fund transfers, other financial losses as well as impersonation [61].

In response, service providers and product developers started alerting users when their credentials appear in breaches. Compromised credential checking [118] has been adopted in browsers [94, 103], password managers (PMs) [101], browser extensions [20], and mobile devices (e.g., iPads [56] and smartphones [83]) to notify users when their passwords and/or usernames appear in the leaked data sets. For instance, Have I Been Pwned (HIBP) [59] is a website that allows users to check whether their personal data (e.g., phone number) has been compromised by data breaches. Browsers such as Firefox [107] and Microsoft Edge [103] are making use of HIBP to warn their users about leaked pass-

words. Google uses a similar approach to alert Chrome users if any username-password pairs saved in their Google account have been breached [47]. Specifically, whenever a user signs in to or registers on a site, a pop-up *notification* is triggered if the credentials used have been found in a data breach [43] (see Figure 1).

The notification about compromised credentials is different from warnings about an invalid TLS certificate, phishing, or other security issues. For instance, a phishing warning is often presented when a web page is considered suspicious [122]. In other words, no harm has been done yet (e.g., users have not been tricked into providing personal information) when the phishing warning pops up. In contrast, the notification of compromised credential alerts users that their credentials have already been leaked. The notification nudges users to take action to reduce the risk of account hijacking.

Prior studies focused on security *warnings* about phishing, malware, and invalid certificates. Researchers discovered that most people do not pay attention to the warnings [99], do not read the warning text [106] or do not fully understand it [12, 14], are unaware of the risks behind the warning [26], and simply fail to act on the warnings [40]. Design guidelines [10, 31, 53] and mechanisms (e.g., polymorphic warnings [16]) have been implemented to help users better understand the warnings [14] and respond to them [12, 40].

Users' perceptions about the browser-based compromised credential notification have received little attention. The most relevant work was conducted by Redmiles [95], who studied participants' responses to suspicious login incidents on their Facebook accounts. The results suggest that users often seek out additional information to understand the incident, that their threat models affect their understanding of the incident, and that their response behaviors are informed by their understanding of the incident. Other studies report that users' awareness of credentials compromises was so low that they might not take effective action (e.g., reset passwords) [12] or might not act until long after they receive a password breach email (i.e., a mean time of 26.3 days) [58]. However, no study has yet been conducted to specifically investigate users' perceptions of the browser-based compromised credential notification.

As compromised credential checking by web browsers is gaining popularity, there is a need to understand end users' perceptions. Differing from the notification of breached credentials of a certain account (e.g., Facebook accounts [95]), compromised credential notifications from browsers alert users concerning all credential information for an account that was potentially exposed in credential breaches. Millions of users have received such notifications [22], yet end users' perceptions, especially the issues and concerns they may have, have not been studied. An investigation of the challenges users are facing can inform the future design of such notifications to improve the user experience and help to better protect their accounts. Since Chrome has the greatest market share among web browsers [1], our study focused on the perceptions of Chrome users who had received a Chrome compromised credential notification (referred to in this paper as "3CN").

We conducted our investigation through analysis of online comments and interviews with participants. By analyzing users' online comments, we discovered various challenges they experienced and concerns they had regarding the 3CN. We later explored the reasoning behind the identified issues through semi-structured interviews with participants who had received at least one 3CN.

Our work makes the following contributions. First, to the best of our knowledge, our work is the first to investigate the challenges and concerns of users in relation to browser-based compromised credential notification. Second, we discovered that users' issues with the 3CN were associated with five core aspects of the notification. We also reported the detailed challenges and concerns users had regarding each core aspect of the notification. Last, we made design suggestions about better ways to communicate risks to users, to improve users' risk comprehension, to address users' concerns, and to motivate users to take action to protect their online accounts.

2 Background and Related Work

2.1 Google Password Checkup

Google's Password Checkup allows users to check the security of the passwords that they have saved in Chrome's password manager. This feature was originally released as a Chrome extension in 2019 [94] and was integrated into the browser in October 2019. As of February 2022, it is turned on by default in Chrome, but it can be turned off manually [47].

There are two ways for users to learn about their exposed passwords and usernames. In the first case, by turning on the Chrome setting "Warn you if your passwords are exposed in a data breach," users will get a pop-up notification on the website where they try to log in or register with exposed credentials (see Figure 1) [46]. The content of the 3CN has been updated several times with minor changes [54, 86] to convey the same takeaway message – the user's credentials have been found publicly online, and the user is advised to change the compromised passwords. From the moment the notification pops up, users have two options: click on "Close" to shut the notification or click on "Check Passwords" to be directed to `chrome://settings/passwords` to see the general information about their saved accounts. By clicking on "Check Passwords," users are directed to see all the detected issues with their saved credentials, including "Compromised passwords," "Weak passwords," and "Reused passwords," if there are any. For each account listed on the page, users can see the account's username, check the current password for the account, edit the saved credentials of the account, or remove the saved account (see Figure 2a). If users wish to change the password of an account, they are directed to the website to

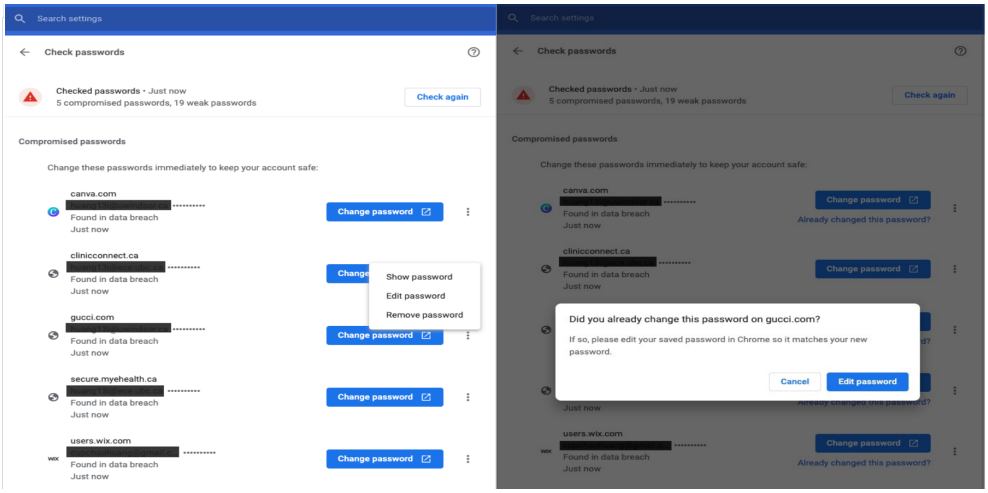

Figure 2: Screenshots of the researcher's Google account passwords displayed when they click "Check Passwords" on the 3CN warning. Users can show, edit, or remove passwords by clicking the three-dot menu (a) or can update their saved passwords in Chrome (b).

make the change there. After clicking on the "Change password" button (see Figure 2b), a note of "Already changed this password?" is shown under the button. Users are then directed to update their saved password to match their new password on Chrome. The second way to check password security is to manually go through several steps in the browser (i.e., Open Chrome → Settings → Passwords → Check Passwords) to get to the same page to learn about the issues that Chrome password manager has identified [47].

Chrome password manager never learns the plaintext of user credentials during password checking. By using multiple rounds of hashing, k-anonymity, and private set intersection with blinding [45, 111], Google can tell whether a user's credentials are compromised without knowing their unsafe username-password pair exposed by the data breach [46]. Specifically, Chrome first encrypts users' credentials and sends the encrypted credentials to Google servers to compare against an encrypted list of known leaked credentials. If the Google servers detect a match between the encrypted credentials, Chrome displays the 3CN that suggests the user change their password [45]. The detailed protocol of Google's Password Checkup is described in [111], and a simplified illustration of the protocol can be found in [45].

2.2 Risk Communication and Warnings

The main goal of risk communication is to inform individuals of risks so that they can make informed decisions [77]. Experts usually design the communication and deliver it to individuals. The communication can take the form of warnings, notices, status indicators, and polices [35]. It has been found that the mental models of technical experts and users are not always the same [73]. Therefore, one cannot assume that the experts recognize what users need to know [32]. Guidelines have been proposed to improve the design of risk communication [24, 81], such as dispelling misconceptions [13].

As one type of risk communication, security warnings have received considerable attention. Much work has been done to evaluate the various types of security warnings, including browser warnings in general [6, 10] and warnings about phishing [29, 90], malware [7], invalid certificates [5, 31], and PDF downloads [7]. For instance, Akhawe and Felt [6] conducted a field study to investigate people's perceptions about Google Chrome's and Mozilla Firefox's malware and phishing warnings. They found that the warnings were effective in practice and suggested communicating security information to users.

Many issues regarding the security warnings were identified. Studies have shown that most people do not pay attention to the computer warnings [99], often do not read the warning messages [16, 106], or do not fully understand the warning [12, 26] because of the technical words used [14, 36]. Users become habituated to security warnings [63, 66], and they end up not heeding them [40], even when the situation is hazardous or sensitive (e.g., online banking) [99].

Methods and guidelines have been proposed to motivate users to act on security warnings. For instance, varying the appearance of warnings (i.e., polymorphic warnings [16]) can help capture users' attention and convince them to take action to mitigate a hazard [31]. Showing the warnings less frequently has been shown to reduce the habituation effect [66, 121]. Attractors (e.g., icons, images, and colors) can be effective in attracting users' attention [15, 120]. Guidelines about how to design warnings also have been discussed [29, 31]. Suggested by Harbach et al. [53], several steps should be taken to reduce the text's difficulty as perceived by the user, such as keeping headlines simple, using

as few technical words as possible, and using short sentences.

2.3 Password Breaches

Researchers have explored users' responses after password breaches. Shay et al. [100] investigated users' perceptions about account hijacking. They found that users believed they share responsibility for keeping the accounts secure. Redmiles [95] explored how users respond to a suspicious login incident on their Facebook account. The results showed that participants may reach out for support to understand the incident. Participants' responses included on-platform behaviors (e.g., changing passwords) and off-platform behaviors (e.g., adjusting the security setting). Bhagavatula et al. [11] examined whether and how constructively users changed their passwords after a breach announcement and found that even though the participants were likely to be affected, that few users took action. Huh et al. [58] evaluated users' reactions upon receiving a LinkedIn password reset email and discovered that only 46% participants reset their passwords.

2.4 Password Reuse

People often reuse their passwords across accounts. One common strategy for users to cope with a large number of accounts is to reuse passwords across different accounts [23, 104]. People report that the more accounts they have, the more they reuse passwords across accounts [23, 85]. Researchers have also investigated how people reuse their passwords. Users' choice of passwords depends on whether they use the accounts frequently or perceive a greater need for account security. Some people reuse passwords that they have to enter frequently [116], and other people tend to reuse passwords on infrequently used accounts because those accounts were considered to have "less need for security" [104]. Furthermore, other studies [37, 85] suggested that people tend to reuse passwords more on low-importance accounts and avoid reusing passwords for high-importance accounts.

2.5 Password Managers

Password managers (PMs) can help users centrally store, organize, and auto-fill passwords for local applications and online services. There are three primary categories of password manager implementations: built into the browser (e.g., Firefox Monitor [107]), standalone password managers (e.g., 1Password [101] and LastPass [68]), and password management within operating systems (e.g., Keychain Access on Mac [119]).

Studies have been done to explore people's perceptions about PMs. Researchers have investigated the factors that influence people's intention to adopt PMs [62, 104, 105], users' PM use [78, 89, 102], and perceived issues with PMs [48, 64]. For instance, Karole et al. [64] conducted a comparative usability study of three PMs and found that users' comfort level with giving control to password managers influences their perceptions of the PMs.

To the best of our knowledge, our work is the first to study users' challenges with a browser-based compromised credential notification. We discovered five core aspects of the notification with which users had issues. We further identified the detailed challenges users experienced and concerns they had regarding each aspect. Our qualitative analysis of online comments and interviews allowed us to investigate not only *what* problems users faced with notifications, but also *why* these were problems. We believe these insights can improve notification design and better secure users' online accounts.

3 Method

We used a two-step approach to investigate the issues with 3CN. We first gathered and analyzed reviews, feedback, comments, and support requests posted on online platforms about 3CN. This approach allowed us to uncover a wide range of issues and concerns users had regarding the notification. Unless otherwise noted, we refer in this paper to all these types of collected data as "*comments*." To better understand users' reasoning for their concerns and challenges, we then conducted interviews with Chrome users who had received a 3CN. In this section, we describe our online comments collection, interview process, data analysis, and our method's limitations.

3.1 Data Collection

3.1.1 User Comments

We collected comments because they are considered promising and helpful data for studying users. Such comments contain a wealth of information about users' opinions, challenges, and experiences with systems and services [57, 60]. The abundance of online comments can be reliable and relevant indicators of the quality of the services and products from users' perspectives [75]. Analyzing user reviews has been frequently used by developers and researchers to understand and evaluate issues with many products, including mobile applications [70, 114], e-commerce services [74, 124], and websites [57, 117].

We gathered users' comments from various online platforms. The platforms included the Google Chrome Help Center [41], Reddit [3], news websites (e.g., The Verge [51]), IT support sites (e.g., WeLiveSecurity [34]), and Q & A websites (e.g., Quora [2]).[1] As our focus was on the issues and concerns users had regarding the 3CN, Chrome Help Center support requests [41] were the primary source for gathering users' comments. Specifically, we employed a keyword researching method [69] to search the Chrome Help Center

[1] See the list of online platforms at https://github.com/AUXResearcher/SOUPS102/blob/main/Online_sources.pdf.

using several keywords or phrases, such as "password notification," "compromised credentials," and "password pop-up alert." We also used the Google search engine to search the web for the same keywords, filtering the returned pages for those that were indeed about the 3CN and contained users' comments. We excluded pages without user comments (e.g., news websites [87]), pages about Chrome's phishing warning [42], and page about other subjects unrelated to the 3CN. We then manually checked the comments posted on each web page to ensure that they contained sufficient information regarding users' perceptions, concerns, or actions regarding the 3CN. We excluded comments that contained insufficient information (e.g., a comment on [55] that stated *"same issue"*). We stopped searching and collecting comments when data saturation was reached (§3.2). Users whose comments we included in the study are referred to as OC-users (online comment users).

Demographic Categories		# of Participants
Gender	Male	11
	Female	11
Age	19–29	6
	30–39	7
	40–49	4
	50–59	3
	60 or above	2
Educational level	High school	2
	Bachelor	9
	Community college	2
	Master	6
	Post-graduate	1
	University below bachelor	1
	Apprenticeship	1
Occupations	Student	2
	Retired	2
	Software developer	2
	Accountant	1
	An intervention worker	1
	Occupation therapist	1
	Theater technician	1
	Product developer	1
	Sport official	1
	Stay-at-home mom	1
	Business intelligence manager	1
	Dermatologist	1
	Business owner	1
	Landscaper	1
	Farmer	1
	Project manager	1
	IT specialist	1
	Unemployed	1
	Salesperson	1

Table 1: Summary of participants' demographics

3.1.2 Interviews

After gaining a sense of users' issues with the 3CN, we conducted semi-structured interviews with users who had received such a notification. Participants were recruited using Facebook advertisements. They were asked to fill out an eligibility survey.[2] To be eligible to participate in the study, they had to have received a 3CN within the two weeks before filling out the survey. This study was approved by UBC's research ethics board. Note that we did not recruit our interview participants from among OC-users.

The interviews served as a complementary approach to better explore users' reasons for their concerns, challenges, and actions (if any) regarding the notification. During each interview, we asked open-ended questions to facilitate in-depth discussion with the participants [27, 82]. We focused on exploring participants' reasoning about their concerns, challenges, and actions (if there were any) regarding the 3CN. For instance, during the interviews, we were able to explore participants' reasoning for not acting on the notification. Specifically, some OC-users did not change passwords for accounts they perceived as unimportant. We discovered through interviews that participants viewed accounts that do not have personal or financial information as unimportant (§4.6).

Our interviews focused on four topics.[3] First, we gained a basic understanding of how users interact with Chrome to manage their credentials. We asked such questions as, "For what kinds of accounts do you save your credentials using Chrome and why?" and "For which accounts do you reuse your passwords and why?" Second, we explored participants' experiences of receiving the 3CN by asking such questions as, "What is your impression of the 3CN?" Next, we explored users' understanding of 3CN, their concerns about it (if there were any), and their actions afterwards. We asked such questions as, "How do you think Chrome finds out about your breached credentials?" To better explore users' reasoning behind their concerns and actions, we asked follow-up questions. For instance, when a participant chose to change passwords for only some accounts, we explored their reasons behind such an action. Finally, to further explore users' unmet needs, we asked participants whether there was anything they would wanted to know regarding 3CN.

3.2 Data Analysis

We qualitatively analyzed users' comments. Similar to many prior studies (e.g., [19, 38]), we qualitatively analyzed the comments using thematic analysis. Thematic analysis is a widely used form of analysis within qualitative research that allows patterns (i.e., themes) within the data to be identified [8, 109]. Specifically, we copied each relevant comment into a spreadsheet with the username of the person who posted the comment (referred to as "OC-user"), the time the comment was posted, the content of the comment, and other information we found relevant to the study (e.g., the screenshot of the pop-up warning the user shared). We then analyzed the comments by generating codes mapped to relevant and important pieces of information in the comments. This allowed us to develop a codebook. Once all the comments were coded, we sorted

[2] See the screening survey at https://github.com/AUXResearcher/SOUPS102/blob/main/Screening_Survey.pdf.

[3] See the interview guide at https://github.com/AUXResearcher/SOUPS102/blob/main/Interview_Guide.pdf.

and grouped similar codes into themes. Then we reviewed and revised the themes to ensure that each one was accurately represented in the data. At this stage, we merged or broke down themes as necessary [109].

We also conducted a thematic analysis of the interview data. We started interview coding with the codebook developed from analyzing the comments. Following the same steps, we identified new codes and newly emerged themes. The combination of online comments and interviews allowed us to capture a more extensive picture of users' challenges and concerns, as well as their reasons behind them.

3.3 Limitations

Our study has several limitations. First, while we are confident that we reached data saturation during our analysis, we reviewed comments from a limited number of sources. There is also a chance that people used different usernames and went on different sites asking for help about the same issues. We might have missed web pages that were not returned by the search engine because of our choice of search keywords.

Second, because of the nature of interviews, our data are self-reported, which is always subjective [80] and may introduce selective memory bias [92]. Further, due to the nature of qualitative research, our study and our data are not amenable to generalizable quantification, such as the extent of the concerns in the target population. Our results point only to the existence of the identified concerns.

Last, with the end-goal of informing the future design of 3CN to help users better protect their online accounts, we focused on exploring the interview participants' considerations of the notification, instead of participants' individual differences (e.g., cultural background, educational background, or previous experience with data breaches). Future studies could be conducted to investigate whether and how people's individual differences correlate with their perceptions of the 3CN.

4 Results

4.1 Data Description

We collected 539 online comments from 81 sources. Each comment was posted using different usernames. Sources included 48 Google Chrome Help Center pages, 5 IT support sites, 3 Q & A websites, 4 news websites, and 20 Reddit posts. The earliest comment was posted on December 17, 2019, and the last on July 8, 2021. The longest comment contained 524 words, while there were 5 words in the shortest. We stopped the analysis when we reached thematic saturation after 493 comments [49, 57]. We coded 46 more comments to make sure no new codes were identified. Overall, we generated 139 codes and organized them into 10 themes.[4] As we focus on reporting the challenges users experienced and the concerns they had regarding the 3CN in this manuscript, we excluded the findings that were less relevant (e.g., users' strategies of creating credentials). We describe our reported five themes in Appendix B.

We recruited a diverse set of 22 interview participants from North America. The sample varied in age, occupation, and education level. Interview participants (referred to as "participants") were 20 to 74 years old (mean 40 and median 37), 11 of them identified as female (see the summary of participants' demographic information in Table 1). Interviews were conducted between August 2021 and January 2022. The interviews lasted an average of 26 minutes. Each participant was compensated with CAD 15. Data saturation was reached after 19 participants. We continued interviewing three participants and obtained no new codes [39]. We assigned 178 new codes in addition to those from the analysis of online comments and generated 11 new themes. In this manuscript, we reported 3 of the 11 new themes and related codes that are related to users' challenges with 3CN (see reported themes and codes in Appendix B). During the interview, some participants needed to review the UI to answer our questions. Upon their request, we showed them screenshots of the 3CN by the lead researcher sharing her screen.

In the rest of this section, we report the challenges and concerns identified regarding 3CN. We found that users' issues with 3CN are mainly associated with five major core aspects of the notification: the authenticity of the notification, data breach incidents, Google's knowledge of users' compromised credentials, multiple accounts being associated with one notification, and actions recommended by the notification. In the following, we explained how users' detailed challenges and concerns are associated with the identified aspects of the 3CN (see Table 2). The mapping between our findings and the identified themes is presented in Figure A.1.

4.2 Authenticity of the Notification

Believing the notification was a mistake. OC-users believed the notification was shown to them even though there were no security vulnerabilities. They therefore questioned the authenticity of the notification. To illustrate, OC-user128 commented: *"It [i]s wrong! ... I only get this on a website that only asks me for characters never the full password and chrome can [no]t store it."* OC-user341 reported the same issue: *"I'm getting this from one[-]time password entries. ... [I] think you guys need to reconsider the implementation."*

Misunderstanding that the cause of the notification was nothing related to compromised credentials. Some OC-users and participants believed the problems with their credentials were not about the credentials being compromised. Instead, they believe that the notification alerts them about having weak passwords in general. For instance, OC-user337 commented: *"The problem with this popup is weak passwords.*

[4] See the list of all identified themes at https://github.com/AUXResearcher/SOUPS102/blob/main/Themes.pdf.

Core Aspects of 3CN	Users' Perceived Challenges and Concerns
Authenticity of the notification	Believing the notification was a mistake
	Misunderstanding that the cause of the notification was nothing related to compromised credentials
Data breach incidents	Lack of information about the "data breach incidents"
	False assumption that the breach occurred on the website on which the notification appeared
	Misunderstanding about Google being breached
	Security concerns about Google
Google's knowledge of users' compromised credentials	Lack of explanation of how Chrome finds users' compromised credentials
	False assumption that Chrome learns about users' plaintext credentials
	Misunderstanding about Google checking users' non-saved credentials
	Privacy concerns about Google's management of users' data
	Concerns about losing control over own data
Multiple accounts being associated with one 3CN	Lack of an explanation of why more than one account was found insecure with one 3CN
	Notification appears on many websites
Actions recommended by 3CN	Lack of information about the severity of the risks
	Lack of justification of the recommended action
	Lack of motivation to take the recommended action
	Challenges in managing new passwords
	Lack of instructions for discontinued accounts

Table 2: The core aspects of 3CN and the detailed challenges OC-users and participants experienced and their concerns about each aspect. Contents in the gray background indicate the identified concerns, and contents in the blank background indicate the discovered challenges.

The end. It has nothing to do with breaches." Another example is OC-user69, who stated: *"If I had to guess [the reason for me getting the notification], Google is probably just pointing out that your password is too simple, and trying to light a fire under your ass to try to get you to change it."* There are OC-users who believed the reason for them getting the notification was that the website where the notification appears had security problems: *"[The issue] is [the] website not having their SSL certificates or the site itself has been detected for malware and phishing"*[OC-user155].

4.3 Data Breach Incidents

Lack of information about the "data breach incidents." OC users and participants were unable to find information about the data breach in which their credentials were leaked. The information was perceived as important for users to verify the incident's authenticity, understand the incident, and act on it. OC-users and participants wanted information such as when the breach occurred, where it happened, who was responsible for the incident, and what measures were taken by the responsible party as a response to the incident. To illustrate, OC-user88 stated: *"I find it very frustrating that no additional info[rmation] is provided in regard to the data breach. I [would] like to know more about the breach, and how my info was compromised and what logic was used to determine [that] I need to update passwords. This feels a bit non-transparent on google's part."* Another example is P4, who also wanted to know more about the data breach regarding where it happened: *"I would like to know more if the data breach happened on any of the trusted websites. Because they are always the targets. Then, I will definitely change my password."*

False assumption that the breach occurred on the website on which the notification appeared. Because the source of the breach was perceived as unclear, OC-users and participants started making assumptions that the website where they received the notification was breached. Although it was possible that the website issuing the notice was also breached, this was not always the case. Assuming the source of the data breach was the website was a misinterpretation. For instance, P6 stated: *"I assumed it is because that company's information [was] breached, like there was a data breach and maybe they were held at ransom for people's personal information and included their passwords."* P16, who also had such a misinterpretation, wanted an explanation from the company who owns the website: *"I want to know what the company did about [the breach incident]. When did they find out [that] they had a data breach? Why is Google telling me and why did not the company tell me [about the incident]?"*

This misinterpretation led participants to trust the website less and/or stop visiting the company's website. When explaining her perception of the website after getting the notification, P16 stated: *"I guess I trust them a little less. It makes me a little more careful about the data I put into different websites. Sometimes, I stopped going to the website altogether. Sometimes I unsubscribed from the newsletter."*

As a response, OC-users tried to contact the website to verify the source of the breach. For instance, OC-user123 described her actions: *"I contacted the websites that Google Chrome indicated had my passwords breached. They replied that my passwords and accounts had NOT been breached and warned me against this "third party" that was sending me misinformation perhaps to scam me."*

On the other hand, the organization's IT support technicians reported clients had asked about the notification they received on the website. They believed that misleading information in 3CN had caused unfounded concerns among their clients and harmed their business. To illustrate, OC-user138 commented: *"I have clients who are now deeply concerned about their security and they now somewhat distrust our work when they*

see a message [about] 'a data breach on-site'."

Misunderstandings about Google being breached. By interpreting the notification, some OC-users misunderstood that Google was breached. For instance, some OC-user235 stated: *"[G]oogle [has been] breach[ed] or it is an affiliate of theirs. ... Google has cookies everywhere for tracking and advertising purchases. [I]t is no wonder there are so many breaches when these companies require and share so much of our information while charging us to use many of their services."* This kind of misunderstanding has caused OC-users to stop using some features of Chrome: *"If chrome is going to tell me every few weeks [that I] need to change passwords then [I] will turn off the save passwords and just type them in myself from now on. ... [C]hrome is said to be so safe and now [I] see all my password saved on chrome have been compromised!!"*[OC-user144].

Security Concerns about Google. Because OC-users misunderstood that Google was breached, they expressed security concerns about Google. For instance, OC-user324 commented:*"This is a very convoluted feature. Makes me think Chrome has bad security and gets hacked regularly. ... [It] seems like a reoccurring problem, and changing the password will do nothing."* Another OC-user blamed Google for not keeping users' passwords safe and complained: *"How could Google keep saying it is safe to store passwords in chrome while they just had a data breach? how could they have a data breach of our data and not even spend the effort to publi[sh] it and explain who, when, where and WHY and what are the strict mitigation actions they put in place?????"*[OC-user47]

As a response to the perception that Google was breached, OC-users decided to stop saving credentials on Chrome or avoid using Chrome. To illustrate, OC-user531 remarked: *"Is Google Chrome security THAT frigging weak?? I no longer want to save passwords to my Chrome account."* OC-user269, on the other hand, decided to change to another browser because *"[on the other browser] I do not need to worry about "security breaches."*

4.4 Google's Knowledge of Users' Compromised Credentials

Lack of explanation of how Chrome finds users' compromised credentials. Users wanted more clarification about how Google knows their credentials were leaked. For instance, OC-user108 asked: *"Does this mean that [G]oogle are sending my username/password (even hashed) to a third site without notification?"* This perceived non-transparency reduced OC-users' trust in Google: *"Google is simple fear mongering, probably just to convert more users to Chrome. If [G]oogle truly cared or thought they were being helpful, they wouldn't go through great lengths to hide the details of their operation"* [OC-user41]. Participants believed that more knowledge of how Chrome learns about users' compromised credentials could help them build trust in Google and motivate them to take the proposed measures: *"[The information] will increase my knowledge. And if I know [Google] is taking good care of our data, maybe in the future, I would be more comfortable sharing information with them"* [P10].

False assumption that Chrome learns about users' plaintext credentials. Poorly informed users formed a hypothesis that Chrome checks users' plaintext credentials to facilitate the 3CN. For instance, OC-user427 stated: *"Is Google decrypting [users' credentials] to compare [them with] known list of compromised credentials? ... not certain I feel safe knowing that [G]oogle has a plain text version of my password to process even if it is for my better."*

Misunderstandings about Google checking users' non-saved credentials. Some OC-users and participants believed Google checked their credentials even if they were not saved in Google accounts. For instance, OC-user521 stated: *"If [G]oogle can find your password online; it means it is reading and processing your password before encrypting and storing. I think it is a terrible idea to save passwords on [G]oogle."*

Participants' past experiences with similar security incidents on Google played a role in this misunderstanding. During the interviews, we carefully explored how users developed such misconceptions. Previous work suggested that past experiences with similar incidents may reduce users' perception of the threat [95]. We, however, found that their past experiences contributed to participants' misunderstanding of 3CN. For instance, P10 explained that she had received a "suspicious sign-in prevented" email from Google. Through the email, she learned someone was trying to log in to her account from an unauthorized device. Based on this previous incident, she concluded that: *"Google keeps tracking of everything you are doing on your laptop or on your mobile. So, I think nothing is hidden from Google."*

Privacy concerns about Google's management of users' data. Believing Google tracks users' non-saved credentials, OC-users and participants raised corresponding privacy concerns. To illustrate, OC-user244 stated: *"Why is google tracking what I type for login credentials that I have not saved to Google? ... Getting the message about a breach might seem helpful, but considering how the warning came and what Google has to be doing to issue the warning, it is just really creepy."* Further, some participants wanted Google to be more transparent about how users' data was treated, such as *"who has access to [users' data] and how easily accessible is it for someone else?"*[P13] and *"if users' data are encrypted or if [users' data are] in the cloud or on a server"*[P16].

Participants adopted acceptance as the strategy to mitigate this privacy concern. To illustrate, P11 explained that taking a trade-off was the reason for not acting to stop Google from checking all his credentials: *"If something is being offered for free as a service, then you are the product."*

Further, several OC-users believed that Google facilitated scams by sharing users' data with other parties. To illustrate, OC-user486 commented: *"But, isn't it kind of fishy that*

Google would know that my old useless account was compromised in a data breach, but yet, no way to know which it is. In other words, Google yet again supports malicious scams through their services and records data of the [s]ite, email, and passwords you are creating in real-time." ... [G]oogle can now create a database of all email/pass[word] combos and the sites they are used on, for their users, to then "release" through planned data breaches to victimize more people."

Concerns about losing control over own data. Several OC-users disliked Google checking their credentials without asking for consent first. For example, OC-user112 remarked: *"Why on Earth does [Google] feel it [i]s appropriate to be doing this password/username background comparison without asking for explicit consent?"* In addition, OC-user453 felt this default feature took away users' ability to control their data: *"Almost all other security features are toggleable. It i[s] not an unreasonable request for this feature to be optional."* OC-user496 believed users should be given more control over their own data: *"My issue is that the user should have the ability to control Google's desire to enhance the user's security!!!"*

4.5 Multiple Accounts Being Associated with One 3CN

Lack of an explanation of why more than one account was found insecure with one notification. After receiving one notification, users were surprised to see that there were many accounts shown to be insecure. When the user's single username-password pair was leaked, all accounts that share the same credentials became insecure. Chrome's browser-based credential check service examines all the accounts users saved in their Google accounts. Since people often reuse their passwords [23, 104], when users receive a notification of a compromised username-password pair, they most likely will find a long list of accounts with the same breached credentials. But there is no explanation about the link between the identified accounts, so users tend to be confused and panicked when learning that many of their accounts were listed as insecure. As a result, some OC-users questioned the authenticity of the breach and resisted changing the passwords: *"1 day they are all fine and the next day 99 passwords are compromised. I still would like to know how. Because this is a lot of work to change all these passwords. ... No way someone hacked me on 90 sites"*[OC-user379].

Notifications appear on many websites. Another challenge is that OC-users reported the 3CN pop-up on many websites. The notification appears when users sign up/log in to an account with the breached credentials [43]. Suppose users reuse their breached credentials across accounts; whenever they try to sign in to the accounts, they receive a notification. However, without such knowledge, OC-users were confused with many notifications showing up on many websites: *"It pops up for EVERY webpage. I do [no]t want to live in password paranoia forever"*[OC-user46].

4.6 Actions Recommended by 3CN

Lack of information about the severity of the risks. 3CN was perceived as not communicating the severity of the risks to users. Such information was perceived as a contributor for users to take mitigation strategies. Specifically, OC users and participants wanted to know if it would be a significant risk if they decided not to change the breached passwords: *"I mean, how risky is it if I do not change my password?"*[P13] In addition, P18 wanted to know if there could be other security problems by not changing the compromised password: *"Is there a way to put some malware [in my device]? Will it be possible [that not changing the password] could compromise even the other sites?"* Further, the risk level was perceived as helpful for users to decide if it is worth making a lot of effort to change the passwords: *"Google is telling me [that] I have compromised passwords. How serious is this? ... I also really do not want to have to change my passwords if I do not need to. Because I have more than a hundred spread across many forums and sites"*[OC-user520].

Lack of justification of recommended actions. Participants wanted more clarification about why changing the password is the best practice and what risks would be avoided by doing this. Such information could influence their risk management behaviors. For instance, P6 stated: *"I would like to know if the best you can do is to just change [the password]. Or is it you just do the best you can and then, fingers crossed, hope for the best situation? ... I think it would be helpful to know what does [changing the password] actually mean for users."* Further, participants asked whether and how changing the password could mitigate the existing damage (i.e., breached credentials). P22 asked: *"If there has already been a data breach, what is the point of changing the passwords? I would like to know if [the breached credentials] are completely out of your control at this point or [if] changing the password can help with that."* P22 was also unclear about why changing the password was suggested and nothing else: *"... but they only tell you to change the password. That got me thinking maybe my username is Ok. But if not, why do not they ask us to change [the username] too?"*

Lack of motivation to take the recommended action. OC-users and participants argued that the notification alerted users about something (i.e., account hijacking) that may not happen. Therefore, they tend to delay or not take action until harm has occurred [125]: *"I read the message more and realized it was not saying my account had been compromised. It was just a warning, like there is a risk [that my account being compromised] may happen. So, I did not change my password"*[P7]. Several OC-users shared the same opinion: *"Randomly trying those compromised credentials in an account is like a 1 in a million shot, more actually, 1 in a billion probably"*[OC-user39].

Further, even if an adversary found the accounts with compromised credentials, the damage is perceived to be limited

because users have additional authentication methods set up. To illustrate, OC-user41 explained: *"[A]ny respectable website worth accessing (like a bank's website) is going to employ [usually multiple] additional traditional authentication methods - be it pin numbers, one-time passwords, 2-factor authentication, image recognition, geolocation, device recognition, etc. You can not simply bypass these and gain access with a simple username and password."*

Unimportant accounts were not worth the effort. Some OC-users and participants suggested that they change the passwords for "important accounts." Such accounts contained their personal information (e.g., pictures, medical record, social security number, and taxpayer ID number) or financial information (e.g., "PayPal account" [P14], "HSBC account" [P17], and "eBay account" [P18]). To illustrate, P11 explained his process of changing the passwords: *"I just went through the list [of insecure accounts] to see where could I have my credit card [information] saved. So, if it is like Home Depot, I probably bought something from [it]. It probably has my credit card. ... But if it is like a news site. I would just leave it there."* OC-user180 also decided not to change the passwords for accounts they did not consider important: *"They are not [the] websites I care about people getting my info. What are they going to do? Go on Carvana and buy a car for me?"*

They further justified their action by indicating that their passwords for the important accounts were different from those for non-important accounts (e.g., "Fandom account" [P3]). Therefore, even if the unimportant accounts were breached, it would not harm them. However, research shows that 33% of the time, it was possible to use a common password list and the user's password created in a "lower level" account to successfully guess their "higher-level" account passwords [52]. Therefore, if the passwords of non-important accounts are public, there is a risk that users' important accounts could be hijacked.

Challenges in managing new passwords. Participants struggled with creating new passwords. Through the interview, we found that participants were uncertain about whether the new passwords were "good enough" to resist being breached again. None of the participants recalled receiving any suggestions on Chrome in creating new passwords [44]. Similar to previous findings [50], our participants used the same strategies to create new passwords, such as making a slight change to their current password (e.g., adding "!" at the end of their current password). For instance, P18 explained his strategy of creating new passwords as using *"Same configurations. Not exactly the same. I just add different stuff. ... I am not sure if they are more secure. I hope so. ... I would like some kind of indicators saying that they are strong enough, like [the password] will not be breached again."* However, participants' new passwords are most likely vulnerable to credential tweaking attacks, where the attacker tries different variations of the leaked password [23, 115].

Lack of instructions for discontinued accounts. OC-users and participants wanted instructions about what to do when the accounts were not in use or when they no longer had access. For instance, P13 had some old accounts that she no longer used. She did not know the appropriate step regarding the breached credentials of such accounts: *"A lot of these [accounts] are like 10 years ago, I do not actually use them anymore. I do not think I have access to them anymore. Now, you are saying [the passwords] need to be changed. ... I am not sure what to do. What if I just delete the accounts? Will that get me in trouble?"*

5 Discussion

5.1 Novelty of Our Findings

We have contributed to the body knowledge in four ways.

First, to the best of our knowledge, ours is the first study to investigate users' perceptions of browser-based compromised credential notifications. Specifically, compared to a notification of breached credentials for a certain account (e.g., a Facebook account [95]), we captured the unique challenges users experienced in managing multiple accounts through a browser-based password manager. For instance, we discovered that OC-users and participants found it confusing that they received a 3CN on many websites, and that one 3CN might indicate that many accounts were in danger (§4.5).

Second, we contributed new findings on users' challenges in comprehending data breaches. Prior work regarding data breaches has focused on exploring people's familiarity with the data breaches [4, 110], their perception of the risks caused by the data breaches [65], and their behaviors after the data breaches [65, 125]. Our work highlighted the perceived critical information that contributed to users' comprehension of the data breach. We also discovered that the missing critical information played a part in users' misinterpretation of the source of the breach. Furthermore, users' misunderstanding of the data breach may result in them having unjustifiable concerns (§4.3). We therefore offer design recommendations aimed at improving the 3CN design to help users gain an accurate understanding of it (Recommendation 2 in §5.3).

Third, we not only corroborated previous findings indicating that few users act on the security warnings [40, 99], but also investigated their reasons for failing to take action and the challenges they experienced when they did act on a notification (§4.6). We provide suggestions for how notification instructions can be improved in several ways (§5.4).

Finally, we discovered the privacy and security concerns that OC-users and participants had regarding the notification (§4.3 and §4.4). Because of these concerns, they failed to mitigate the risk effectively. At the same time, the concerns resulted in some negative perceptions of Google. Recommendation 4 in §5.5 aims to address these concerns.

5.2 Layers of Information

Critical information about the credentials leaks was perceived as missing from the notification. Prior research on security warnings has offered many insights into the need to comprehensibly communicate various risks [10, 28], such as the consequences of not complying with a suggested action [10]. However, we discovered that the 3CN failed to communicate certain types of critical information to its users (§4.3 to §4.6). The missing information led OC-users and participants to be confused and make additional efforts to verify the authenticity of the risk and the need to take action to mitigate it.

Missing information is not easily accessible. For instance, an explanation of how Google learns about breaches in users' credentials is available [45], but this information is not linked to the process that users go through when responding to 3CN. In other words, users must search for such details proactively and may not find what they need.

Recommendation 1: Provide important information in a layered form. Prior work has suggested that the message in a security warning should specify the underlying risk clearly [10] but provide only the essential information to avoid overwhelming users [28,53]. However, previous work in other fields (e.g., group decision making [123]) has also shown that having more information improves people's decision making. *Therefore, there is a trade-off between the amount of information that should be included to enable users to understand the notification and the perceived effort required to read and process it.* As the information identified as missing was perceived to be essential, we suggest that a notification should include all such missing details listed in Table 2.

A layered approach has been proposed and evaluated as a way to present information about privacy and security to users, such as a privacy notification for IoT devices [21, 30]. The results of previous studies suggest that a layered approach allows users to obtain prompt, detailed, and accurate information about the privacy protection of an IoT device [21].

A layered approach can potentially provide the following benefits: First, it would enable the 3CN to convey a large amount of relevant information to its users without overwhelming them. The initial layer of the notification contains the most essential information [93]. Subsequent layers would each provide additional important information (such as the information we identified as missing in Table 2). The design for each layer would observe the well-known principles of risk communication [14, 36], such as using as few technical words as possible [53]. The pathway from one layer to the next should be made clear and straightforward [35]. Second, with all the relevant information linked directly through the layered approach, users could find the answers to all their questions without seeking help elsewhere. Another potential advantage of the layered approach is that it can benefit different types of users (e.g., the tech-savvy and the novice). Each user could decide how much information they want when learning about the notification.

However, the huge amount of information [53] may overwhelm (novice) users [28] and possibly push them away from responding to the notifications. Therefore, the usability and users' perceptions of such a layered approach will require further evaluation.

5.3 Correct and Adequate Understanding

We identified several challenges that users face when understanding 3CN. Knowledge enables both recognition and interpretation to occur [97]. Without knowledge, understanding is impossible [76, 79]. Therefore, we include our findings of the knowledge gaps in discussing users' perceptions of 3CN.

An example is the comprehension of the "data breach." Here, three types of challenges emerged: lack of information about the "data breach," false assumption of "data breach" due to being poorly informed, and having misunderstandings regarding the "data breach" (§4.3). Different approaches may be needed to solve each type of challenge. For the first type, more information can be provided to users to help them develop a better understanding of the notification (see our Recommendation 1 in §5.2).

The second challenge is that users' lack of knowledge results in misinterpretations. In other words, users were unclear about certain aspects of the 3CN. They started forming the wrong assumptions. Providing more information to users can potentially clear up some of these misinterpretations (Recommendation 1 in §5.2). However, when users have already formed their own hypotheses, a deeper explanation may be needed to correct a misinterpretation.

The third challenge is users developed misunderstandings of certain aspects of 3CN by interpreting the information they received (e.g., Google is breached §4.3). Getting additional information about the notification may not be enough to correct these users' misunderstandings. Once established, mental models (i.e., users' understanding of how something works) can be surprisingly hard to change, even when they are aware of contradictory evidence [113]. Instead of providing more information, explaining certain aspects of the notification may be necessary to dispel such misunderstandings.

Recommendation 2: Consider explaining certain aspects of the notification to dispel the misconceptions. Prior studies suggest that users may improve their understanding if a system makes its *reasoning transparent*, such as its purpose of accessing a particular type of users' information [67, 72]. Therefore, we suggest correcting users' misunderstandings by providing detailed explanations. For example, instead of saying that Google does not access users' plaintext passwords, C3N can focus on clarifying how Google learns that users' credentials are leaked without accessing their passwords. This explanation should be direct and easy to understand without too many technical terms and jargon [84, 91]. Assessing the effectiveness of such an approach requires future evaluation.

5.4 Action Recommendations

Instructions that merely suggest changing passwords were not perceived as helpful. As explained in Section 4.6, OC-users and participants experienced many challenges regarding taking the recommended action. These challenges resulted in some OC-users and participants being unsure about whether to take action, and if so, what that action should be.

Recommendation 3: Provide more details in the instructions. To better help users mitigate the risk of 3CN, we suggest that more explanations should be provided in the instructions to justify the necessity of changing the passwords. For example, we recommend explaining why it is necessary to change the breached password, but not the username, what risks can or cannot be mitigated by this action, and what risks the user may face if they do not change their passwords.

Additionally, more instructions could be provided on how to create new passwords. The focus can be on why a slight modification of an old password might not be effective in mitigating the data breach risks [23, 115]. Also, users can be assisted in understanding the quality of their new passwords (e.g., through a password strength meter [25, 98]). Other instructions [33] for creating unique passwords, such as not reusing passwords across accounts [33], could also be helpful for users. More research is needed to evaluate whether more detailed explanations in the instructions are more beneficial in persuading users to act effectively and protect their accounts.

Due to the similarities in the design of instructions provided by other browser-based PMs (e.g., Firefox Password Manager) and standalone PMs (e.g., LastPass and 1Password) and the design of 3CN, we believe we believe Recommendation 3 can also bring insights into these PMs' future designs. To illustrate, both Firefox and 1Password ask their users to change their passwords without providing more details [17, 107], such as the severity of the risks of not changing the passwords. There is a chance that their users find this instruction unhelpful as well. We suggest that these PMs also consider providing more information in the instructions to help their users better manage their credentials.

5.5 More Control and Data Transparency

Some users' security and privacy concerns were specifically related to Google. They criticized the company for having too much control over users' data, not being transparent about managing their data, and facilitating scams (§4.3 and §4.4). These concerns resulted in some of the OC-users refusing to use Chrome password manager or abandoning Chrome entirely. These concerns may be addressed by clarifying how Google detects breached credentials (see our Recommendation 2 in §5.3). In addition, providing more transparency about how users' data is protected might also help mitigate concerns and build trust in the company [95, 123].

Recommendation 4: Replace the one-or-nothing model by giving users more control over their data. Another step further would be to give users the ability to select and deselect accounts they want to receive notifications about breaches. Providing greater control to users might help address users' concerns and build their trust in the company [96, 112]. For instance, provided they are clear about the possible risks of certain behaviors (e.g., changing passwords for certain accounts, not changing passwords at all, or slightly changing passwords) (see Recommendation 3 in §5.4), users could be given a choice as to whether or not they wanted to be notified about breached credentials or not. Currently, users can either get notifications of all accounts with breached credentials or not get any notifications (by turning off the feature). This approach clearly does not work for all users. Our proposed approach could potentially motivate users to manage their credentials without being bombarded with notifications. However, the effectiveness of the proposed approach would need to be evaluated in future studies.

Similarly, we found that other PMs (e.g., Firefox Password Manager, LastPass, and 1Password) also check all users' saved credentials to alert them of compromised ones. Due to this similar all-or-nothing design, we suggest that these PMs also consider providing more control to users over deciding which accounts will receive a notification.

We want to clarify that we reviewed only the UI of other PMs and identified several aspects of the design similar to 3CN. As our users experienced challenges regarding these aspects, we believe our Recommendations 3 and 4 to improve the design of these aspects can also benefit other PMs. However, to what extent our recommendations will benefit the design of other PMs requires further research.

6 Conclusion

We report the challenges users experience and their concerns about the Chrome compromised credentials notification. Our findings suggest that developers consider improving the design of various aspects of the notification to support users in better protecting their online accounts.

Acknowledgments

This research has been supported by a gift from Scotiabank to UBC. We would like to thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who provided their feedback on the reported research. Our anonymous reviewers and shepherd provided important feedback and suggestions to improve the paper. Stylistic and copy editing by Eva van Emden helped to improve readability of this paper.

References

[1] Netmarketshare: Market share statistics for internet technologies. https://netmarketshare:com/browser-market-share:aspx. Accessed: 2022-01-18.

[2] What do you think of google chrome now warning you if your web passwords have been stolen? https://www.quora.com/What-do-you-think-of-Google-Chrome-now-warning-you-if-your-web-passwords-have-been-stolen, 2021. Accessed: 2022-05-24.

[3] Compromised passwords warning - what does this mean? https://www.reddit.com/r/chrome/comments/i7kcb5/compromised_passwords_warning_what_does_this_mean/, 2022. Accessed: 2022-01-31.

[4] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. *Consumer attitudes toward data breach notifications and loss of personal information*. Rand Corporation, 2016.

[5] Mustafa Emre Acer, Emily Stark, Adrienne Porter Felt, Sascha Fahl, Radhika Bhargava, Bhanu Dev, Matt Braithwaite, Ryan Sleevi, and Parisa Tabriz. Where the wild warnings are: Root causes of chrome https certificate errors. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1407–1420, 2017.

[6] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A Large-Scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., August 2013. USENIX Association.

[7] Hazim Almuhimedi, Adrienne Porter Felt, Robert W Reeder, and Sunny Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 113–128, 2014.

[8] Elaine Barnett-Page and James Thomas. Methods for the synthesis of qualitative research: a critical review. *BMC medical research methodology*, 9(1):1–11, 2009.

[9] Brian Barr. Everyone loves credentials: Highlights from the verizon 2021 data breach investigations report. https://spycloud.com/highlights-from-the-verizon-2021-data-breach-investigations-report/. Accessed: 2021-05-13.

[10] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. Warning design guidelines. *CMU-CyLab-13*, 2, 2013.

[11] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. (how) do people change their passwords after a breach? *arXiv preprint arXiv:2010.09853*, 2020.

[12] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. What breach? measuring online awareness of security incidents by studying real-world browsing behavior. In *European Symposium on Usable Security 2021*, pages 180–199, 2021.

[13] Ann Bostrom, Cynthia J Atman, Baruch Fischhoff, and M Granger Morgan. Evaluating risk communications: completing and correcting mental models of hazardous processes, part ii. *Risk analysis*, 14(5):789–798, 1994.

[14] Cristian Bravo-Lillo. *Improving computer security dialogs: an exploration of attention and habituation*. PhD thesis, Carnegie Mellon University, 2014.

[15] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–12, 2013.

[16] José Carlos Brustoloni and Ricardo Villamarín-Salomón. Improving security decisions with polymorphic and audited dialogs. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 76–85, 2007.

[17] Emily Chioconi. Received a data breach notification in 1password? take these 5 steps. https://blog.1password.com/what-to-do-when-you-get-a-data-breach-notification/. Accessed: 2022-05-27.

[18] Catalin Cimpanu. 2021 databreach investigation report. https://www.verizon.com/business/resources/reports/dbir/, 2021. Accessed: 2022-01-18.

[19] Carl J Clare. *Understanding the factors that influence the effectiveness of online customer reviews: a thematic analysis of receiver perspectives*. PhD thesis, Manchester Metropolitan University, 2012.

[20] Stephanie Condon. Okta offers free multi-factor authentication with new product, one app. https://www.zdnet.com/article/okta-offers-free-multi-factor-authentication-with-new-product-one-app/. Accessed: 2018-05-23.

[21] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 10:273, 2012.

[22] Ciaran Daly. Google Chrome warning as millions of users told to change their passwords, November, 02, 2021. https://www.dailystar.co.uk/tech/google-chrome-hacker-warning-millions-25355589.

[23] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *NDSS*, volume 14, pages 23–26, 2014.

[24] Sanchari Das, Jacob Abbott, Shakthidhar Gopavaram, Jim Blythe, and L Jean Camp. User-centered risk communication for safer browsing. In *International Conference on Financial Cryptography and Data Security*, pages 18–35. Springer, 2020.

[25] Xavier de Carné de Carnavalet and Mohammad Mannan. From very weak to very strong: Analyzing password-strength meters. In *Network and Distributed System Security Symposium (NDSS 2014)*. Internet Society, 2014.

[26] Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, pages 79–90, 2006.

[27] Alison Doyle. What Is a Semi-Structured Interview?, June 27, 2020. https://www.thebalancecareers.com/what-is-a-semi-structured-interview-2061632.

[28] Serge Egelman. *Trust me: Design patterns for constructing trustworthy trust indicators*. Carnegie Mellon University, 2009.

[29] Serge Egelman and Stuart Schechter. The importance of being earnest [in security warnings]. In *International Conference on Financial Cryptography and Data Security*, pages 52–59. Springer, 2013.

[30] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[31] Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving ssl warnings: Comprehension and adherence. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2893–2902, 2015.

[32] MM Fischhoff, G Baruch, A Bostrom, L Lave, and CJ Atman. Communicating risk to the public. *Environmental Science Technology*, 26(11), 1992.

[33] Dinei Florêncio, Cormac Herley, and Paul C Van Oorschot. Pushing on string: The'don't care'region of password strength. *Communications of the ACM*, 59(11):66–74, 2016.

[34] Tomas Flotyn. Chrome now warns you if your password has been stolen. https://www.forbes.com/sites/thomasbrewster/2019/12/10/google-chrome-will-now-warn-you-if-your-web-passwords-have-been-stolen, 2019. Accessed: 2022-01-26.

[35] Center for Long-Term Cybersecurity. Designing risk communications: A roadmap for digital platforms. https://cltc.berkeley.edu/2020/12/15/designing-risk-communications-a-roadmap-for-digital-platforms/, 2020. Accessed: 2022-01-18.

[36] Steven M Furnell, Adila Jusoh, and Dimitris Katsabas. The challenges of understanding and using security: A survey of end-users. *Computers & Security*, 25(1):27–35, 2006.

[37] Shirley Gaw and Edward W Felten. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, pages 44–55, 2006.

[38] Emma L Giles, Matthew Holmes, Elaine McColl, Falko F Sniehotta, and Jean M Adams. Acceptability of financial incentives for breastfeeding: thematic analysis of readers' comments to uk online news reports. *BMC pregnancy and childbirth*, 15(1):1–15, 2015.

[39] Barney G Glaser, Anselm L Strauss, and Elizabeth Strutzel. The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17(4):364, 1968.

[40] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "what was that site doing with my facebook password?" designing password-reuse notifications. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1549–1566, 2018.

[41] Google. Google Help Center. https://support.google.com/chrome/?#topic=9796470.

[42] Google. Manage warnings about unsafe sites. https://support.google.com/chrome/answer/99020?hl=en&co=GENIE.Platform%3DAndroid. Accessed: 2022-01-26.

[43] Google. Password manager. https://passwords.google.com/. Accessed: 2022-01-22.

[44] Google. Tired of memorizing p4ssw0rd$? the new chrome has your back. https://www.blog.google/products/chrome/chrome-password-manager/, 2018. Accessed: 2022-02-10.

[45] Google. Better password protections in chrome - how it works. https://security.googleblog.com/2019/12/better-password-protections-in-chrome.html, 2019. Accessed: 2022-02-08.

[46] Google. Protect your accounts from data breaches with password checkup. https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html, 2019. Accessed: 2019-02-06.

[47] Google. How chrome protects your passwords. https://support.google.com/chrome/answer/10311524#zippy=%2Chow-password-protection-works, 2022. Accessed: 2022-01-20.

[48] Joshua Gray, Virginia NL Franqueira, and Yijun Yu. Forensically-sound analysis of security risks of using local password managers. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, pages 114–121. IEEE, 2016.

[49] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field methods*, 18(1):59–82, 2006.

[50] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User behaviors and attitudes under password expiration policies. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 13–30, 2018.

[51] Rybe Hager. Google is making it easier to check if your passwords have been compromised in a data breach. https://www.theverge.com/2019/10/2/20892854/google-password-checkup-hack-detection-now-available, 2019. Accessed: 2022-01-26.

[52] SM Taiabul Haque, Matthew Wright, and Shannon Scielzo. A study of user password strategy for multiple accounts. In *Proceedings of the third ACM conference on Data and application security and privacy*, pages 173–176, 2013.

[53] Marian Harbach, Sascha Fahl, Polina Yakovleva, and Matthew Smith. Sorry, i don't get it: An analysis of warning message texts. In *International Conference on Financial Cryptography and Data Security*, pages 94–111. Springer, 2013.

[54] Google Account Help. Getting a compromised password warning, but no passwords are showing as compromised. huh? https://support.google.com/accounts/thread/89361664/getting-a-compromised-password-warning-but-no-passwords-are-showing-as-compromised-huh?hl=en, 2022. Accessed: 2022-01-20.

[55] Google Chrome Help. Compromised password warning. https://support.google.com/chrome/thread/73069988/compromised-password-warning?hl=en, 2020. Accessed: 2022-01-18.

[56] Maria Henriquez. Apple's new requirement puts additional focus on consumer and data privacy.

[57] Nicolas Huaman, Sabrina Amft, Marten Oltrogge, Yasemin Acar, and Sascha Fahl. They would do better if they worked together: The case of interaction problems between password managers and websites. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1367–1381. IEEE, 2021.

[58] Jun Ho Huh, Hyoungshick Kim, Swathi SVP Rayala, Rakesh B Bobba, and Konstantin Beznosov. I'm too busy to reset my linkedin password: On the effectiveness of password reset emails. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 387–391, 2017.

[59] Troy Hunt. Have i been pwned? https://haveibeenpwned.com/Passwords/. Accessed: 2022-01-19.

[60] Retail Insider. How much are online reviews actually worth? https://retail-insider.com/retail-insider/2020/04/how-much-are-online-reviews-actually-worth/, 2020. Accessed: 2022-01-26.

[61] Insurance Information Institute. Facts + statistics: Identity theft and cybercrime. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime, 2022. Accessed: 2022-01-24.

[62] Iulia Ion, Rob Reeder, and Sunny Consolvo. {"... No} one can hack my {Mind"}: Comparing expert and {Non-Expert} security practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[63] Jeffrey L Jenkins, Bonnie Brinton Anderson, Anthony Vance, C Brock Kirwan, and David Eargle. More harm than good? how messages that interrupt can make us vulnerable. *Information Systems Research*, 27(4):880–896, 2016.

[64] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology*, pages 233–251. Springer, 2010.

[65] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. Data breaches: user comprehension, expectations, and concerns with handling exposed data. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 217–234, 2018.

[66] Soyun Kim and Michael S Wogalter. Habituation, dishabituation, and recovery effects in visual warnings. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 53, pages 1612–1616. SAGE Publications Sage CA: Los Angeles, CA, 2009.

[67] Todd Kulesza, Simone Stumpf, Margaret Burnett, and Irwin Kwan. Tell me more? the effects of mental model soundness on personalizing an intelligent agent. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1–10, 2012.

[68] LastPass. Lastpass for chrome.

[69] Rachel Leist. How to Do Keyword Research for SEO: A Beginner's Guide, January 7, 2020. https://blog.hubspot.com/marketing/how-to-do-keyword-research-ht.

[70] Xiaozhou Li, Zheying Zhang, and Kostas Stefanidis. Mobile app evolution analysis based on user reviews. In *New Trends in Intelligent Software Methodologies, Tools and Techniques*, pages 773–786. IOS Press, 2018.

[71] Stacy Liberatore. More than 500,000 zoom user credentials have been stolen and sold on the dark web for less than a penny each. https://www.dailymail.co.uk/sciencetech/article-8218723/More-500-000-Zoom-user-credentials-sold-dark-web-PENNY-each.html, 2020. Accessed: 2020-04-14.

[72] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*, pages 501–510, 2012.

[73] Debin Liu, Farzaneh Asgharpour, and L Jean Camp. Risk communication in security using mental models. *Usable Security*, 7:1–12, 2008.

[74] Gang Liu, Shaoqing Fei, Zichun Yan, Chia-Huei Wu, and Sang-Bing Tsai. An empirical study on response to online customer reviews and e-commerce sales: from the mobile information system perspective. *Mobile Information Systems*, 2020, 2020.

[75] Zhiwei Liu and Sangwon Park. What makes a useful online review? implication for travel product websites. *Tourism management*, 47:140–151, 2015.

[76] Ephrat Livni. It's better to understand something than to know it. https://qz.com/1123896/its-better-to-understand-something-than-to-know-it/, 2017. Accessed: 2022-01-18.

[77] Ragnar E Löfstedt. Risk communication and management in the 21st century. *Available at SSRN 545724*, 2004.

[78] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 203–220, 2018.

[79] Emelda M. Difference between knowing and understanding. http://www.differencebetween.net/language/difference-between-knowing-and-understanding/, 2018. Accessed: 2022-01-18.

[80] Fiona MacKellar. Subjectivity in Qualitative Research. https://www.sfu.ca/educ867/htm/subjectivity.htm.

[81] Behnood Momenzadeh, Shakthidhar Gopavaram, Sanchari Das, and L Jean Camp. Bayesian evaluation of privacy-preserving risk communication for user android app preferences. *Information & Computer Security*, 2021.

[82] Gemma Morgan. Semi-structured, narrative, and in-depth interviewing, focus groups, action research, participant observation, 2016. https://www.healthknowledge.org.uk/public-health-textbook/research-methods/1d-qualitative-methods/section2-theoretical-methodological-issues-research.

[83] Shivali Best & Daniel Morrow. Android users can check to see if their password has been hacked by scammers. https://www.dailyrecord.co.uk/news/science-technology/android-users-can-check-see-22551580, 2020. Accessed: 2022-01-20.

[84] Emily Newman. Avoiding use of jargon with customers. https://corp.yonyx.com/customer-service/avoiding-use-of-jargon-with-customers/.

[85] Gilbert Notoatmodjo and Clark Thomborson. Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security-Volume 98*, pages 71–78. Citeseer, 2009.

[86] Joy Okumoko. "chrome password breach warning: How to check and fix asap. https://www.maketecheasier.com/fix-chrome-password-breach-warning/, 2021. Accessed: 2022-01-20.

[87] Joy Okumoko. Chrome Password Breach Warning: How to Check and Fix ASAP, August 24, 2021. https://www.maketecheasier.com/fix-chrome-password-breach-warning/.

[88] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[89] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 319–338, 2019.

[90] Justin Petelka, Yixin Zou, and Florian Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, pages 1–15, 2019.

[91] Anastasia Philopoulos. How cutting out jargon can help you achieve clear communication. https://www.shopify.ca/partners/blog/108716102-how-cutting-out-jargon-can-help-you-achieve-clear-communication.

[92] James H Price and Judy Murnan. Research limitations and the necessity of reporting them. *American Journal of Health Education*, 35(2):66, 2004.

[93] TechRadar Pro. The case for a privacy nutrition label. https://www.techradar.com/news/the-case-for-a-privacy-nutrition-label, 2020. Accessed: 2022-01-18.

[94] Jennifer Pullman, Kurt Thomas, and Elie Bursztein. Protect your accounts from data breaches with password checkup, 2019.

[95] Elissa M Redmiles. " should i worry?" a cross-cultural examination of account security incident response. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 920–934. IEEE, 2019.

[96] Harvard Business Review. With big data comes big responsibility, November, 2014. https://hbr.org/2014/11/with-big-data-comes-big-responsibility.

[97] Irvin Rock. Perception and knowledge. *Acta Psychologica*, 59(1):3–22, 1985.

[98] Tobias Seitz and Heinrich Hussmann. Pasdjo: quantifying password strength perceptions with an online game. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, pages 117–125, 2017.

[99] David Sharek, Cameron Swofford, and Michael Wogalter. Failure to recognize fake internet popup warning messages. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 52, pages 557–560. SAGE Publications Sage CA: Los Angeles, CA, 2008.

[100] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. " my religious aunt asked why i was trying to sell her viagra" experiences with account hijacking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2657–2666, 2014.

[101] Jeff Shiner. Finding compromised passwords with 1password. https://blog.1password.com/finding-pwned-passwords-with-1password/, 2022. Accessed: 2022-01-18.

[102] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manageruse cases and design paradigms. In *Annual Computer Security Applications Conference*, pages 528–540, 2021.

[103] Radames Cruz Moreno Sreekanth Kannepalli, Kim Laine. Password monitor: Safeguarding passwords in microsoft edge. https://www.microsoft.com/en-us/research/blog/password-monitor-safeguarding-passwords-in-microsoft-edge/, 2022. Accessed: 2022-01-18.

[104] Elizabeth Stobert and Robert Biddle. A password manager that doesn't remember passwords. In *Proceedings of the 2014 New Security Paradigms Workshop*, pages 39–52, 2014.

[105] Elizabeth Stobert and Robert Biddle. Expert password management. In *International Conference on Passwords*, pages 3–20. Springer, 2015.

[106] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying wolf: An empirical study of ssl warning effectiveness. In *USENIX security symposium*, pages 399–416. Montreal, Canada, 2009.

[107] Mozilla Support. Firefox password manager - alerts for breached websites. https://support.mozilla.org/en-US/kb/firefox-password-manager-alerts-breached-websites. Accessed: 2022-01-21.

[108] TeamPasword. What happened with the zoom credentials hack? https://www.teampassword.com/blog/what-happened-with-the-zoom-credentials-hack. Accessed: 2021-08-10.

[109] James Thomas and Angela Harden. Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC medical research methodology*, 8(1):1–10, 2008.

[110] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. Data breaches, phishing, or malware? understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 1421–1434, 2017.

[111] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, et al. Protecting accounts from credential stuffing with password breach alerting. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 1556–1571, 2019.

[112] Allison Schoop Timothy Morey, Theodore "Theo" Forbath. Customer data: Designing for transparency and trust, May, 2015. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[113] Joe Tullio, Anind K Dey, Jason Chalecki, and James Fogarty. How it works: a field study of non-technical users interacting with an intelligent system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 31–40, 2007.

[114] Christopher Vendome, Diana Solano, Santiago Liñán, and Mario Linares-Vásquez. Can everyone use my app? an empirical study on accessibility in android apps. In *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 41–52. IEEE, 2019.

[115] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. Targeted online password guessing: An underestimated threat. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1242–1254, 2016.

[116] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 175–188, Denver, CO, June 2016. USENIX Association.

[117] Brian Wentz, Dung Pham, Erin Feaser, Dylan Smith, James Smith, and Allison Wilson. Documenting the accessibility of 100 us bank and finance websites. *Universal Access in the Information Society*, 18(4):871–880, 2019.

[118] Wikipedia. Credential stuffing. https://en.wikipedia.org/wiki/Credential_stuffing. Accessed: 2022-01-22.

[119] Wikipedia. Keychain (software). https://en.wikipedia.org/wiki/Keychain_(software).

[120] Graham Wilson, Harry Maxwell, and Mike Just. Everything's cool: Extending security warnings with thermal feedback. In *Proceedings of the 2017 CHI conference extended abstracts on human factors in computing systems*, pages 2232–2239, 2017.

[121] Michael S Wogalter. Purposes and scope of warnings. *Handbook of warnings*, 864, 2006.

[122] Weining Yang, Aiping Xiong, Jing Chen, Robert W Proctor, and Ninghui Li. Use of phishing training to improve security warning compliance: evidence from a field experiment. In *Proceedings of the hot topics in science of security: symposium and bootcamp*, pages 52–61, 2017.

[123] Paul Zarnoth and Janet A Sniezek. The social influence of confidence in group decision making. *Journal of Experimental Social Psychology*, 33(4):345–366, 1997.

[124] Zhijie Zhao, Jiaying Wang, Huadong Sun, Yang Liu, Zhipeng Fan, and Fuhua Xuan. What factors influence online product sales? online reviews, review system curation, online promotional marketing and seller guarantees analysis. *IEEE Access*, 8:3920–3931, 2019.

[125] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. " i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 197–216, 2018.

Appendices

A How Are the Findings Associated with the Reported Themes?

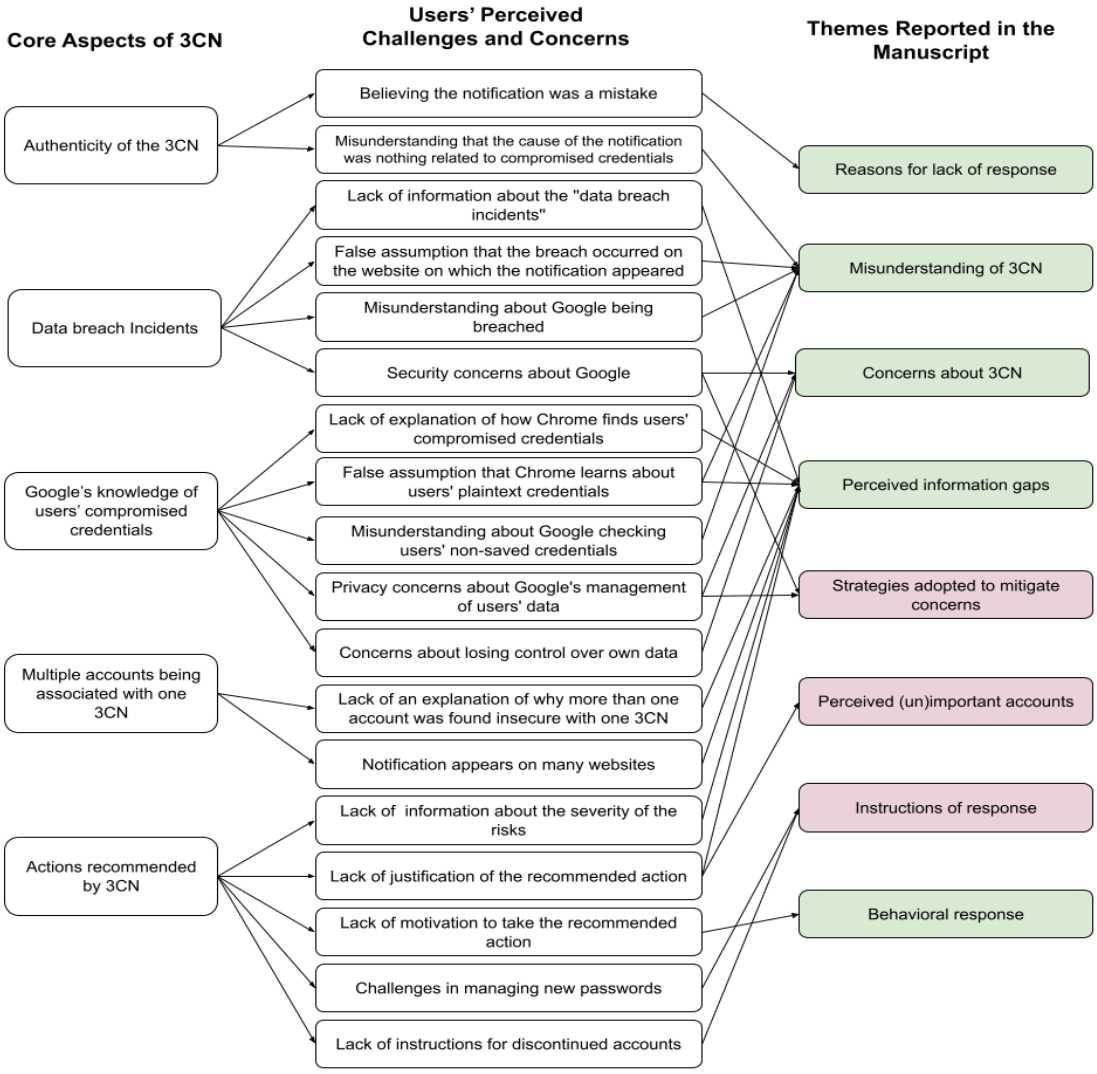

Figure A.1: A mapping between the core aspects of the app, the challenges and concerns OC-users and participants expressed, and the themes reported in this manuscript. The contents with a green background represent the themes that were identified by analyzing online comments, while the contents with a pink background indicate the themes were new themes identified through interviews.

B Themes and Related Codes Reported in the Manuscript

Themes	Codes	Number of online comments (N)	Number of participants (n)
Information Gaps	Risks of not changing passwords	4	2
	Severity of the risks	3	4
	Other security problems with the 3CN	3	1
	Whether changing the password is the best option?	2	3
	What other methods can take?	4	4
	When did the breach happen?	5	10
	Where did the breach happen?	25	8
	Who is responsible for the breach?	13	2
	Why did the company not notify users?	3	2
	What had been done as a response to the breach?	3	1
	Why there is no relevant news about the breach?	3	2
	Why do users receive so many 3CNs?	19	0
	Why does one 3CN represent so many insecure accounts?	14	0
	Why do users receive 3CN even after changing the passwords?	38	3
	How does Chrome know the about credentials being compromised?	30	15
	What information does Chrome check (credential or password)?	9	3
	What breached credentials does Chrome compare users' credentials with	8	6
	Does Chrome know users' plaintext passwords?	4	3
	Does Chrome check users' non-saved credentials?	7	5
	Why is changing the password suggested?	0	3
	How effective is changing the passwords to mitigate risks?	0	3
	Why is changing usernames not suggested?	0	2
	Can changing passwords mitigate existing damage?	0	2
Misunderstanding of the 3CN	The problem behind the 3CN is weak passwords	7	3
	Google's strategy to get people update passwords	6	2
	The website where the 3CN appears has security problems	9	2
	Google has been breached	16	0
	Chrome checks users' plaintext passwords	3	3
	Chrome checks non-saved credentials	3	3
Behavioral response	Click 3CN to learn more about it	6	4
	Disable the feature	4	2
	Lack of action	10	6
	Check other online sources to verify the data breach	8	3
	Email IT professional to learn more about the 3CN	5	2
	Ask friends/family about 3CN	4	4
	Search information about 3CN online	12	6
	Change all compromised passwords	3	2
	Change passwords for important accounts	8	6
	Delete stored credentials	13	3
	Ask help from Google live chat	1	0
	Change browser	7	0
	Contact the company where the 3CN appeared	6	0
	Run virus scan	2	0
	Intend to sue the company for not protecting data	1	0
	Changed some passwords then gave up due to too much effort	3	2
	Stop saving passwords on browser	3	4
	Decided to use other password managers	4	0
	Used Chrome suggested password as new passwords	2	1
	Stop visiting the websites where the 3CN appears	2	3
	Examined each account and decide whether to change the passwords	0	4
	Close the notification	0	5
Reasons for lack of response	3CN looks suspicious/not legitimate	20	2
	The message on 3CN is unclear/confusing	31	2
	Belief that no breach occurred	8	0
	Accounts are not important	8	6
	Perceived low chance of the account being taken	3	3
	Perceived low risk even if the account is hijacked	2	2
	Too much effort to change passwords for unimportant accounts	10	8
	Notification keeps appearing even after changing the passwords	38	3
	Unclear about how to deal with discontinued accounts	3	3
	3CN is alerting about something that has not happened	8	2
	3CN is exaggerating the risk	2	3
	Setting up additional protection methods	8	5
	Believing one should have the right to use any passwords they like	2	0
	Believing the passwords are complex enough	0	3
	Do not remember having such a compromised account	0	1
	The damage is already done	0	2
	Being too lazy to take action	0	2
Concerns	Google is breached and fails to protect users' data	23	0
	Google checks users' data without asking for permission first	8	2
	Google shares users' data with other parties	11	0
	Losing control over own data	12	0
	Ways to steal users' new passwords	6	1
Expected instructions of response	How to avoid being breached in the future	0	3
	How to create new passwords?	0	6
	Whether newly created passwords are secure enough	0	4
	Whether it is OK to use the same username	0	2
	How to deal with accounts that are no longer in use	0	2
	Whether certain accounts are riskier than others	0	1
	Whether more methods are needed to increase account security level	0	3
Perceived (un)important accounts	Accounts associated with financial information	0	9
	Accounts associated with personal information	0	9
Strategies to mitigate concerns	Accept the privacy-utility trade-off	0	3

Table B.1: Reported Themes and Codes. Themes and codes in pink are identified through interviews. We use "N" to indicate the number of online comments for each code and "n" to indicate the number of participants.