Users’ Perceptions of Chrome’s Compromised Credential Notification

Yue Huang, Borke Obada-Obieh, Konstantin Beznosov
Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
University of British Columbia
Leaked credentials remain a big threat
Alert users when their credentials appear in breaches

https://haveibeenpwned.com/
Chrome's compromised credential notification (3CN)

Check your passwords

Chrome found the password you just used in a data breach. To secure your accounts, we recommend changing it now and then checking your saved passwords.

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.
We studied users' challenges regarding Chrome's compromised credential notification.
Method
A two-step approach

Step 1: Users' reviews, feedback, comments, and support requests ("comments provided by OC-users")

How can I delete all compromised passwords at once, and why won't Google add a way to do this??

I have over 400 "compromised" passwords, but it expects me to go through and manually delete every password one by one.........
Online Platforms

“password notification,” “compromised credentials,” and “password pop-up alert.”

539 online comments from 81 sources
Method
A two-step approach

Step 1  Users' reviews, feedback, comments, and support requests ("comments provided by OC-users")

Step 2  Interviews with Chrome users who had received a 3CN
22 Interview participants

Gender

<table>
<thead>
<tr>
<th>Gender</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High school</td>
<td>8</td>
</tr>
<tr>
<td>Bachelor</td>
<td>4</td>
</tr>
<tr>
<td>Community college</td>
<td>2</td>
</tr>
<tr>
<td>Master</td>
<td>0</td>
</tr>
<tr>
<td>Post-graduate</td>
<td>0</td>
</tr>
<tr>
<td>University below bachelor</td>
<td>0</td>
</tr>
<tr>
<td>Apprenticeship</td>
<td>0</td>
</tr>
</tbody>
</table>

Education

<table>
<thead>
<tr>
<th>Education</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High school</td>
<td>8</td>
</tr>
<tr>
<td>Bachelor</td>
<td>4</td>
</tr>
<tr>
<td>Community college</td>
<td>2</td>
</tr>
<tr>
<td>Master</td>
<td>0</td>
</tr>
<tr>
<td>Post-graduate</td>
<td>0</td>
</tr>
<tr>
<td>University below bachelor</td>
<td>0</td>
</tr>
<tr>
<td>Apprenticeship</td>
<td>0</td>
</tr>
</tbody>
</table>

Age

<table>
<thead>
<tr>
<th>Age Group</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>19 - 29</td>
<td>6</td>
</tr>
<tr>
<td>30 - 39</td>
<td>8</td>
</tr>
<tr>
<td>40 - 49</td>
<td>4</td>
</tr>
<tr>
<td>50 - 59</td>
<td>2</td>
</tr>
<tr>
<td>60 or above</td>
<td>1</td>
</tr>
</tbody>
</table>

Occupation

<table>
<thead>
<tr>
<th>Occupation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountant</td>
<td>6</td>
</tr>
<tr>
<td>Product developer</td>
<td>8</td>
</tr>
<tr>
<td>Sport official</td>
<td>2</td>
</tr>
<tr>
<td>Stay-at-home mom</td>
<td>0</td>
</tr>
<tr>
<td>An intervention worker</td>
<td>4</td>
</tr>
<tr>
<td>Business intelligence manager</td>
<td>0</td>
</tr>
<tr>
<td>Landscaper</td>
<td>0</td>
</tr>
<tr>
<td>Farmer</td>
<td>0</td>
</tr>
<tr>
<td>Occupation therapist</td>
<td>0</td>
</tr>
<tr>
<td>Dermatologist</td>
<td>0</td>
</tr>
<tr>
<td>Project manager</td>
<td>0</td>
</tr>
<tr>
<td>Unemployed</td>
<td>0</td>
</tr>
<tr>
<td>Software developer</td>
<td>0</td>
</tr>
<tr>
<td>Theater technician</td>
<td>0</td>
</tr>
<tr>
<td>Business owner</td>
<td>0</td>
</tr>
<tr>
<td>IT specialist</td>
<td>0</td>
</tr>
<tr>
<td>Salesperson</td>
<td>0</td>
</tr>
</tbody>
</table>
Challenges associated with 5 core aspects

- Authenticity of the notification
- Data breach incidents
- Google’s knowledge of users’ compromised credentials
- Multiple accounts being associated with one 3CN
- Actions recommended by 3CN
Challenges associated with 5 core aspects

- Authenticity of the notification
- Data breach incidents
- Google’s knowledge of users’ compromised credentials
- Multiple accounts being associated with one 3CN
- Actions recommended by 3CN
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
Google’s knowledge of users’ compromised credentials

“Google is simply 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 their operation.” [OC-user41]
Google’s knowledge of users’ compromised credentials

False assumption that Chrome learns about users’ plaintext credentials
Google’s knowledge of users’ compromised credentials

Misunderstanding about Google checking users’ non-saved credentials
Google’s knowledge of users’ compromised credentials

"Why is google tracking what I type for login credentials that I have not saved to Google? ... Getting the message about 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."

[OC-user 244]
Google’s knowledge of users’ compromised credentials

Concerns about losing control over own data
Challenges associated with 5 core aspects

- Authenticity of the notification
- Data breach incidents
- Google's knowledge of users' compromised credentials
- Multiple accounts being associated with one 3CN
- Actions recommended by 3CN
Actions Recommended by 3CN

- Lack of information about the severity of the risks
- Lack of justification of recommended actions
- Lack of motivation to take the recommended action
- Challenges in managing new passwords
- Lack of instructions for discontinued accounts
Lack of information about the severity of the risks
"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." [P6]
“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]
Critical information about the credentials leaks was perceived as missing from the notification.
Takeaways

Critical information about the credentials leaks was perceived as missing from the notification.

Recommendation 1:

Provide important information in a layered form.
Takeaways

Challenges that users are facing when understanding 3CN
Takeaways

Challenges that users are facing when understanding 3CN

Recommendation 2:

Consider explaining certain aspects of the notification to dispel the misconceptions.
Instructions that merely suggest changing passwords were not perceived as helpful.
Takeaways

Instructions that merely suggest changing passwords were not perceived as helpful.

**Recommendation 3:**

Provide more details in the instructions.
Takeaways

Instructions that merely suggest changing passwords were not perceived as helpful.

Recommendation 3:
Provide more details in the instructions.
Takeaways

Perceived lack of control of own data
Perceived lack of control of own data

**Recommendation 4:**
Replace the one-or-nothing model by giving users more control over their data.
Summary

- Authenticity of the notification
- Data breach incidents
- Google's knowledge of users' compromised credentials
- Multiple accounts being associated with one 3CN
- Actions recommended by 3CN
Users’ Perceptions of Chrome’s Compromised Credential Notification

Yue Huang
University of British Columbia
huang13i@ece.ubc.ca

Borke Obada-Obieh
University of British Columbia
obadavoke@yahoo.com

Konstantin Beznosov
University of British Columbia
beznosov@ece.ubc.ca