Design Research Review

CSE 440 | Augustina Liu, Bill Phung, Celeste Cayetano, Ethan Cui

Summary of Key Findings and Takeaways

In our three semi-structured interviews, when asked about their account and password managing habits, all of our participants were aware of their own bad habits, despite knowing these practices might not be secure. We also noticed that our participants prefer to use physical forms, such as notebooks and sticky notes, to keep track of their passwords. Participants' approaches to managing their accounts seem to be correlated with their knowledge of computers: the more familiar they are with computers, the more secure their approaches are. Their trust in the internet seems to be influenced by their personal experience. If their accounts have been compromised before, their trust tends to be lower. When it comes to a potential new design that could help with online account security, all participants show a very clear desire for simplicity in the design. Overall, we think that there does not currently exist a simple enough way to track online account usage and security for seniors. Our findings have informed us potential directions of design, which are focusing on creating a simple, convenient, intuitive, and trustworthy design to help our customers manage their online accounts, considering different levels of comfort among different customers, and designing a product that motivates customers to use.

Design Research Participants

Participant 1: Semi-structured interview at a coffee shop in Tacoma. Participant is 60 years old, living in Lakewood. He does a variety of jobs, such as writing articles for local newspapers, driving Uber, and announcing for local sports teams. Though he tries to learn to be more comfortable with computers and relies on them for much of his work, he still often finds himself confused and frustrated with computers. He has a lot of accounts to keep track of, and used to keep different passwords for each but got tired of going through the process of recovering the password when he forgot, so now he just uses one. During the interview, he stated that he would rather have simplicity in his everyday life and deal with recovering his account if it ever came to that, rather than complicating everything just to be preventative.

Participant 2: Semi-structured interview at By George under the Odegaard Library at UW. Participant 2 is 77 years old living in the Seattle area. He studied Chinese at the University of California and used to work as a librarian in the Suzzallo Library and Odegaard Library at the University of Washington. He retired in June 2018. Now, he has started to enjoy his life. He is very familiar with computers because of his job and feels very comfortable using them. For managing online accounts, he writes his passwords in a diary. He uses different passwords with small variations and checks his bank account once a day to make sure there are no unexpected expenses. He uses software called Kasperski to protect the data and privacy on his computer.

Participant 3: Semi-structured interview at Starbucks. Participant 3 is a 64-year-old Seattle resident. He worked as a mechanic for most of his life and retired in 2008. He now spends most of his time enjoying life and spending time with his grandchildren. He interacted with the car shop data system intensively when he was working. For personal accounts, he only keeps the minimal ones, such as bank accounts and emails. He does not use any tools to manage his accounts and uses the same password for different accounts even though he is aware this might not be secure. He writes down his passwords as a backup but rarely needs it because of the minimal number of accounts he has. He hopes new design for tracking and managing online accounts can be simple.

Research Themes

Theme 1: *Participants are aware of their bad habits when managing different accounts.*
According to our interviews, participants have some sense that their means of tracking and managing online accounts are not secure enough, but they still choose to continue their habits out of convenience. Participant 1 mentioned that he just used the same password for everything and stated, “I know that’s bad”. Participant 2 wrote down all his passwords at the back of the diary book. Although someone told him that this was not a good habit, he still used this way to track his passwords. He explicitly mentioned that he didn’t care if someone steals his passwords. Participant 3 knew that he should check his bank account more frequently but he just checked it once in a while. This theme shows us that our design doesn’t necessarily need to be education-based since our participants know what they should be doing to protect their accounts already. Rather, we should focus on making those habits faster and convenient, so they will have more motivation to actually implement those habits.

Theme 2: *Participants have a different level of comfort when using the Internet.*
The trust over internet security is varied in these three participants. Participant 1 didn’t trust the Internet and he is not comfortable making online purchases because his account was being compromised before. Since participant 2 was a librarian at the University of Washington, he feels very comfortable about using the Internet. He labeled himself as an early adopter of the Internet. Participant 3 was comfortable using things he already knows but he is not willing to explore new things or use new software that he

is not familiar with. Hence, this inspires us to consider different levels of comfort within our target group when designing our product.

Theme 3: *Simplicity is the most important property if there is a new design.*
All participants kept track of their different passwords and account information using pen and paper. Participants also tend to use the same passwords for multiple accounts or use different passwords with small variations. These decisions are due to the fact that our participants favored simplicity and convenience over security. This is affirmed by the fact that many participants acknowledged the security risks of using the same password for multiple accounts and not updating passwords frequently, yet decided not to change their habits. Participants specifically pointed out that they don't like complicated things in the interview. Participants also tended to be uncomfortable with learning new technology. This theme tells us about an aspect of security (passwords) that participants are particularly lax in and that if a tool is not simple and intuitive then it will not be used. This inspires us to consider simple, convinient and intuitive solutions in our design.

Task Analysis Questions

1. **Who is going to use the design?**
   Our design is targeted towards older adults, specifically for those people who are approximately 55 and older. They are not technology-native and have different levels of education, although varying levels of comfort, with operating computers. Based on our research, it seems that our target customers take very limited measures to protect their online accounts.
2. **What tasks do they now perform?**
   Our participants are currently tracking their passwords either by writing them down on paper or by using the same password for everything and committing that password to memory. Some participants also track account activity for suspicious activities, but not all, with the most common being their bank account.
3. **What tasks are desired?**
   We would like our participants to be able to log passwords for different accounts, generate secure passwords, get notifications and steps to update passwords, track their account activities, be notified of suspicious behavior, and get steps to recover an account that has been compromised.

4. **How are the tasks learned?**
   Our participants generally learn their computer skills from their work, from friends and family, or experientially through having their accounts broken into. For the tasks that we want to introduce, we would aim to automate as much as possible so that only limited training is required. For instance, if we notify to update passwords, we should also have a guided process to do that, so that knowledge of how to do that is not assumed.
5. **Where are the tasks performed?**
   This can be performed anywhere where the participant has internet access. The participant would be able to receive critical notifications or access account information on their phone or through their computer, though responses to compromised accounts might be best performed through the comfort of their own home to better assess their situation.
6. **What is the relationship between the person and the data?**
   Part of the data is the accounts number and passwords used to access their different accounts. This data allows them to access the different services provided on different platforms including website, application, etc. Passwords are also a crucial layer of safety in regards to account security. Another data is information that could help companies to recognize customers' identity, such as security questions.
7. **What other tools does the person have?**
   Existing tools participants use are paper and pen to store their passwords. They also have access to the security measures in place by each individual company, for instance, one participant was notified of suspicious activity by his credit union, and they were able to give him steps to recover his account.
8. **How do people communicate with each other?**
   Our participants are fairly passive in account security communication. They often wait for account companies to reach out when there are suspicious activities on their accounts. And they mostly play the role of providers of their information when asked to do so. When participants' acquaintances have suffered from account compromisation, they also communicate about this process as well.
9. **How often are the tasks performed?**
   Most of the tasks that we aim to introduce are relatively infrequent, as too many password changes and notifications would be quite annoying to our participants who aim primarily for convenience and simplicity. Most of our tasks are only in the event that a company's data is breached, or there is some other reason for the participant to be concerned about the security of their accounts. The one exception would be using the passwords to log in, which is very frequent.

10. **What are the time constraints on the tasks?**
    Access to passwords should be fairly quick as a long process would be quite bothersome. There is also a time constraint on notifications on suspicious account security. Being notified quicker would allow a quicker response and that is crucial to limit damages a compromised account my cause.
11. **What happens when things go wrong?**
    When participants' accounts are compromised, it is most likely because they leaked their account credentials, either to spammers or malicious sites. We could potentially help avoid this situation by notifying participants when they go to a site that had a recent breach or could be malicious. If our security measures are not enough to avoid an account being compromised, we should have a list of steps that can be taken to recover the account.