

notE

A simple, non-invasive online account information
management notebook for Seniors

By

Augustina Liu

Bill Phung

Celeste Cayetano

Ethan Cui

Problem & Solution Overview

As technology and the digital world develop, people are becoming increasingly reliant on a number of online services, which all require separate accounts to keep track of. At the same time, with so much personal information attached to these accounts, including names, addresses, financial information, and even SSN in some cases, it becomes increasingly important for people to protect their online accounts. However, we noticed that seniors are one particular demographic who often seem to neglect the security of their online presence. Thus, we sought to design a tool to help seniors be more secure online. After further investigation, we discovered that the problem is not that seniors lack awareness of what it means to be secure online, but rather that they know what is secure and still choose insecure practices in favor of simplicity and convenience in their everyday lives. This is the main inspiration behind notE, a smart notebook where seniors can manage their accounts easily, in a comfortable and intuitive form. notE retains the look and feel of a normal notebook but has a few key differences that make it an optimal solution to the problem of online account security: it only shows account login information to recognized users, it gives notifications based on the status of its linked accounts, and provides assistance for account recovery.

Design Research Goals, Stakeholders, and Participants

For our design research, we decided to conduct semi-structured interviews. We felt that a semi-structured interview would be the most appropriate form of design research because online account security deals with a lot of potentially sensitive information and it would likely make our participants uncomfortable to ask to observe their practices directly. Our interviews were intended to help us learn about participants' awareness of online accounts security, numbers of frequently used online accounts, habits of tracking online accounts, and the frequency of updating passwords. Thus, in using these interview questions, we were able to better understand senior participants' habits and pain points when using online accounts without being overly intrusive.

Stakeholders and Participants

There are three participants in our semi-structured interviews.

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 many accounts to keep track of, and uses same passwords because he got tired of going through the process of recovering the password when he forgot. During the interview, he stated that he would rather have simplicity in his everyday life and deal with recovering his account.

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.

Some stakeholders we considered in our design are companies hosting those accounts who might have concerns exposing their account information to a third party tracking software and friends and family members of participants who would be affected by a compromised account (spam messages, viruses, etc).

Design Research Results and 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 was not comfortable making online purchases because his account had been 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 is 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 during the interviews. 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, convenient and intuitive solutions in our design.

Answers to Task Analysis Questions

1. Who is going to use the design?

Our design is targeted towards older adults, specifically those who are approximately 55 and older. They are not technology-native and have varying levels of education and comfort with operating computers. Based on our research, it seems that our target participants 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 usernames, passwords, and answers to security questions 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 their notebook. The participant would be able to receive critical notifications or access account information from the notebook. However, the location is most likely to be at home or in a working environment where the account information is being actively used, rather than in a context like a restaurant, for example.

6. What is the relationship between the person and the data?

Part of the data is the accounts' login credentials. 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 compromise, 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 may cause.

11. What happens when things go wrong?

If the notebook is lost or stolen, the information stored inside of it is still safe because it will only show its contents to recognized users, either by facial recognition or by fingerprint. If an account is compromised, a notification will display along with a guided process of steps that can be taken to recover the account.

Proposed Design Sketches - "3x4"

Design 1: Smart Glass

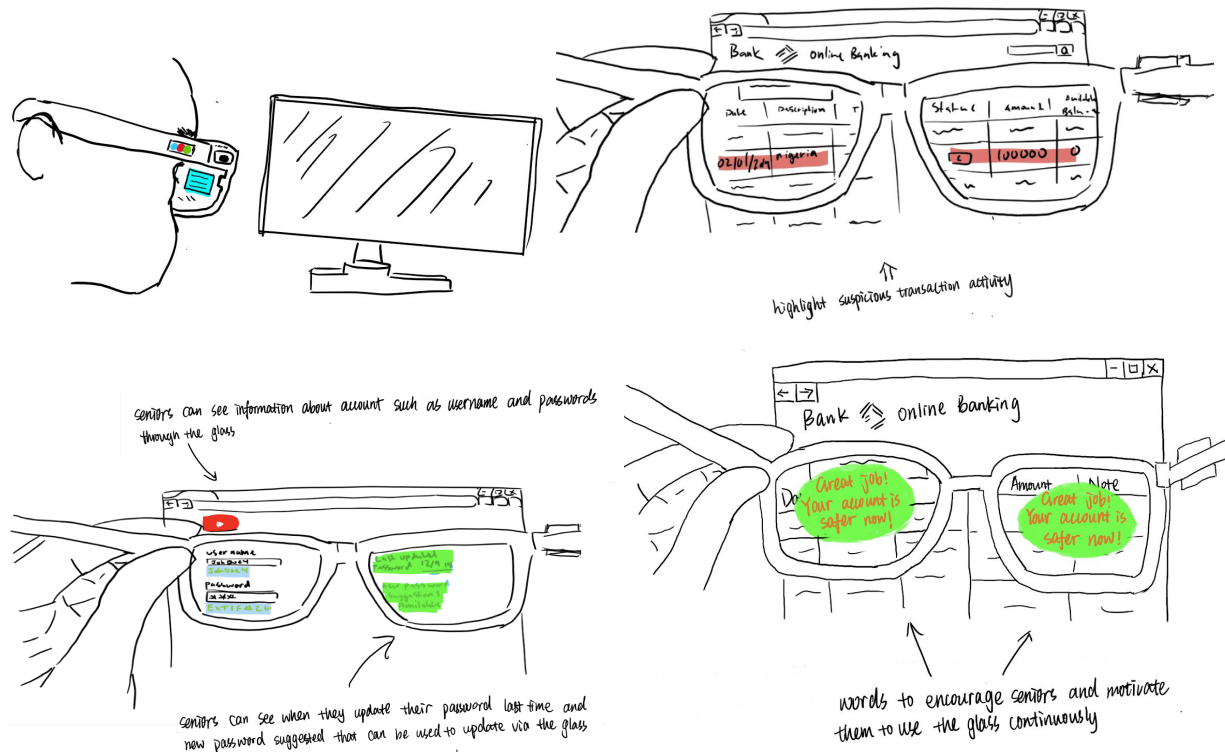


Figure 1: Smart Glasses

Figure 1 shows a pair of smart glass. The smart glasses design are wearable glasses that use augmented reality to display useful information when interacting with computers and other devices. It would display information such as stored usernames and passwords for websites. It would keep track of when passwords were last updated and display reminders to update them. It would assist in creating accounts and displaying password suggestions for updates. It would warn seniors if the website or the link is suspicious. Lastly it would display encouraging messages to help motivate safe internet usage.

Design 2: Smart Notebooks



Figure 2: Smart Notebook

Figure 2 shows a smart notebook. The smart notebook design is a type of Internet of Things where seniors can have a more secure way to write down account information including account numbers, passwords, and security questions etc., on their notebooks as what they usually do. The notebook will use the Optical Character Recognition to store the information seniors write down and store that information on the cloud. Then, that information is automatically stored on personal devices and can be used to login without manually typing in the login credentials. In order to assure that all personal information is safely stored even if the notebook is lost or stolen, the smart notebook uses facial recognition to display personal information to customers with authorizations. There is a small ink screen at the back to mimic the texture of the paper, which is used to display notifications to notify users about suspicious activity and new passwords generated for users to update their passwords.

Design 3: Online Account Security App

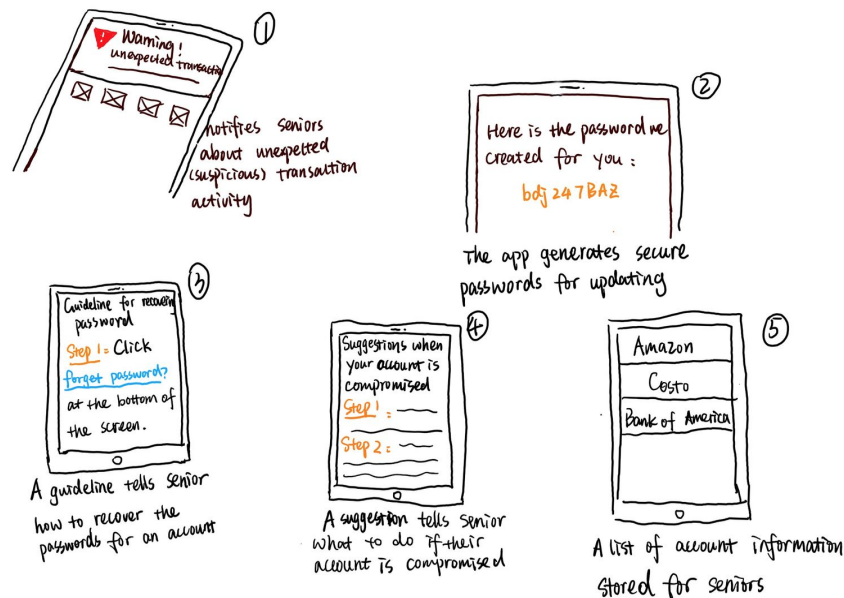


Figure 3: Online Account Security App

Figure 3 shows a mobile application. The online account security check app is a mobile phone application that helps seniors protect the security of their online accounts by keeping track of account information and recovering an account when things go wrong. The app will be designed to allow seniors to check their account information if they need, monitor suspicious activity on their online accounts, give notifications when companies have had a recent data breach or when accounts have potentially suspicious login, posting, or transactions, and find next steps to protect their accounts, such as updating passwords or disabling accounts.

Our Choice

We have chosen to pursue the Smart Notebook Design. Based on our research, we found that our participants strongly desire simplicity in their everyday lives compared to the desire of online security or protecting their accounts. So, to best support our target group, we chose a design that integrates secure habits into our participants' lives in a way based largely on the tasks that they are already doing. The notebook presents a unique opportunity and challenge to create something that looks simple and intuitive, but is a powerful tool under the surface, which is ultimately why we chose this design. Based on that, we selected these two tasks:

1. Storing, generating, and updating strong and secure passwords
2. Advice on what to do when an account is compromised

We interpreted that our participants' first priority is to have something that's not intrusive and requires their constant attention but a simpler and more secure way to manage their online accounts. In order to compensate for the lack of active tracking, they do desire more guidance in the case of account compromise such that they can minimize their loss and/or quickly recover their account ownership.

Written Scenarios - "1x2"

Scenario 1

Task 1: Storing, Generating, and Updating Passwords for Customers

John wants to create a Facebook account to better connect with his friend on Facebook. To better store his password, he decided to use notE, a smart notebook, to store his password. He uses facial recognition to unlock notE and find a blank page to record the company name, account number/email, password, security question, and special notes. Five days later, he wants to log in his facebook, but he forgets his passwords. So, he opens notE to find information and successfully log in on Facebook. Three months later, he gets a message to ask him to update his password for Facebook for better security concern. He follows the instruction on message and successfully gets the suggested passwords for the update.


Scenario 2

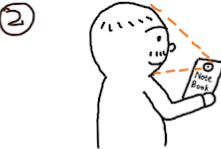
Task 2: Guiding Customers After Their Account Has Been Compromised


After seeing that the light on the notE in green now, John realizes that his Facebook account is compromised. Without knowing what to do, he directly opened his notE using facial recognition. He located the page of his Facebook account by clicking on the Facebook logo on the index page. He tapped on the "Help" button, notE notified Facebook about the incident with enough information to identify the customer. Then, Facebook contacts John to recover his account. After recovering account, John notices that the light on the notE turns into green and he knows his account is safe now.


Storyboards of the Selected Design


Storyboard for Scenario 1


①  John wants to create a Facebook account and he wants to store his password in his notebook.


②  John takes out the smart notebook and use facial recognition to open it

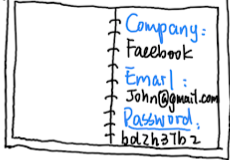
③  John writes down his account information in the smart notebook. All text in blue are templates in smart notebook. All account information now is stored in the smart notebook


④  5 days later John wants to login his Facebook but he forgets his password.

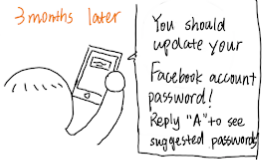
⑤  John remembers that he wrote the account information on his note book.


⑥  John opens the notebook but he forget where the page for Facebook is. He goes to the index which was auto-generated after he filled out the account information for those accounts.

⑦  After John presses the square of Facebook, the small tab pops out.

⑧  John uses the tab to flip to the page of Facebook and he finds out his password.

⑨  Finally, John successfully log in to the Facebook and start to browse friends' posts.

⑩  3 months later, John receives a message from the notebook to notify him update passwords for the Facebook. John can reply "A" to see the suggested new passwords. Since he needs to pass security check on his phone so there is no privacy issue here.

⑪  After updating passwords with suggested passwords, John feel secure about his account.

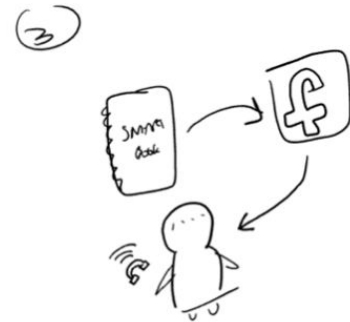
Storyboard for Scenario 2



The light on the notebook turns red so that John knows that his Facebook account is compromised.



John goes to the page of Facebook and taps on the square labelled "HELP" at the back page of the Facebook page.



Then, the notebook contacts Facebook to tell them that John needs help. Since John's information is stored in the notebook, the notebook tells Facebook John's contacts.



Facebook contacts John to guide him how to recover his account.



After recovering the account, the light turns green so that John knows that his Facebook account is safe now.