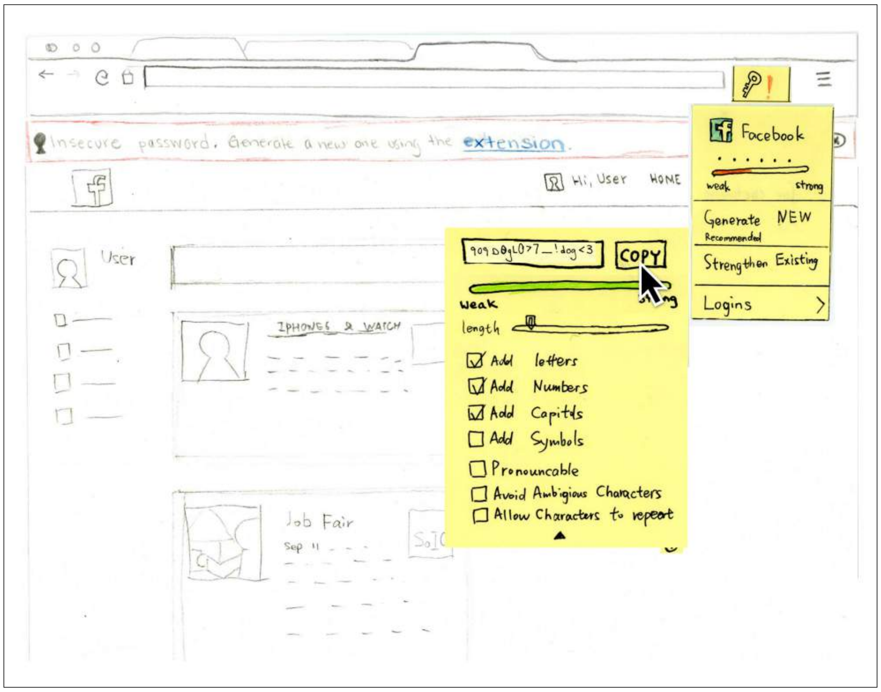
1Password Project



Team H

Shankar Balasubramanian

Michelle Gottschlich

Yangguang Li

Micah Nethery

Mentors

Julia Rickles, Jiaqi Li

Professor Marty Siegel

Interaction Design Practice

August 18th, 2014

TABLE OF CONTENTS

INTRODUCTION

THE PROBLEM

1Password is having trouble expanding their user base. As they understand it, users aren't using the generator feature and suspect, from research, that trust is the underlying issue. The generator creates extremely complex passwords--but why don't users believe they are secure? From our research, when users create passwords, they inflect it with personal details --where they're from, the year they're born, an object in the room--which fosters a memorable attachment to the password. From our point of view, the problem is three-fold. First, the present 1Password is too shined down for a new user base; it doesn't motivate users to use the generator or usher them along with directions and verifications. Second, the generator shuts users out of the process of creating a password, which is where our research shows the users develop trust. And last, the current product underestimates the crucial difference between strength and security. For us, strength is a technical measurement. What we want is security--the synthesis of strength and a human, restful sense of safety.

OUR DESIGN SOLUTION

GENERATE

The primary features of 1Password are its generator and vault. The generator is most important because it ensures that the passwords themselves are strong and secure. Duplicate passwords, for example, compromise the vault entirely. And yet, users don't look beyond the vault when using 1Password. Our solution motivates the user to rely on the generator more than anything else. We've added warning notifications for weak passwords, a simple and effective 'recommended' tag, and instructional prompts. Every feature of our design encourages the generate new feature--even the new 'Strengthen Existing Password' feature of the generator.

STRENGTHEN

Our strengthen existing password feature allows users to type in their own passwords and modify them using interactive strength bars. The current 1Password generator has the beginnings of this feature, but it seems markedly unrealized--when users type in their own passwords and adjust the strengthen bar, their password vanishes and a new, totally randomized password replaces it, bearing no vestiges of their original password. A staggering 60% people from our surveys don't trust randomized passwords. This design seeks a middle ground. Even though the vault stores each individual password, new users ignore the generator and store duplicate, weak passwords. We want new users to grow comfortable using the generator and strengthen what they have. This feature gives users back their sense of control and lets them have a say in the password generation process.

OUR MANTRA

"How do we get them to take their medicine?"
We strove for persuasive and reassuring design changes. We believe providing a creative approach to password generation encourages users to take their medicine, i.e. strengthen their passwords, leading to greater overall health of the 1Password software and security.

MOTIVATION FOR DESIGN

- Expand the user base
- Design for the novice
- Overcome new-user's timidity with the generator
- Retain expert-user appeal with hide options and hidden features

CONSTRAINTS

We cannot or do not attempt to:

- Alter the content or layout of the 1Password or any webpage
- Make changes to the 1Password native application. (However changes to the generator in general are reflected within the native app. At the end of this document we provide suggestions for native app alterations.)
- Provide a link that sends the user directly to a webpage's account settings.
- Measure the strength of the user's password before they give their explicit consent to save it into the 1Password vault. (We believe this could be felt as a breach of trust or "fishiness," especially for new users and our personas.)

OUR DESIGN SOLUTION

You'll get to know our personas Robert and Lisa in detail momentarily, but let's bring Robert in early to walk us through the design. In short, Robert is a new user of 1Password, he has high security concerns, but is non-tech savvy.

Robert has downloaded 1Password and the extension. Now let's have him Log-in to Facebook with his existing credentials.

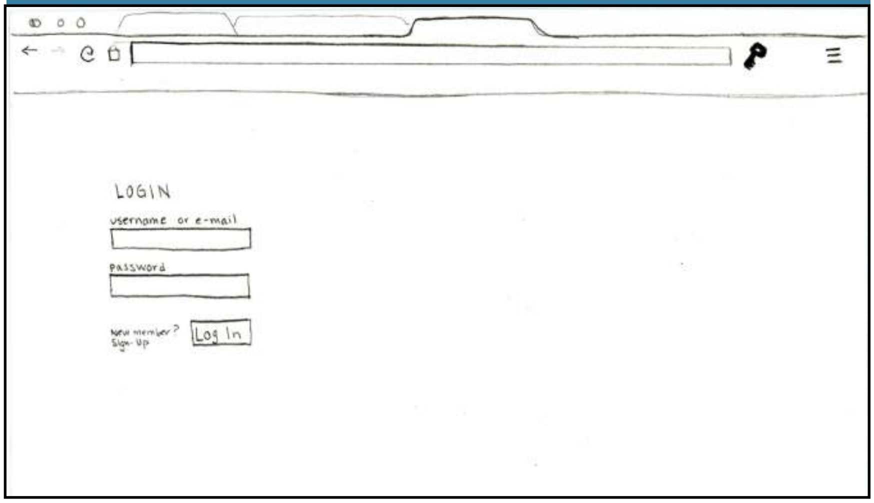


Figure 1.0 - Facebook.com log-in page.

Robert clicks Login and is prompted by 1Password to save his information. He clicks Save.

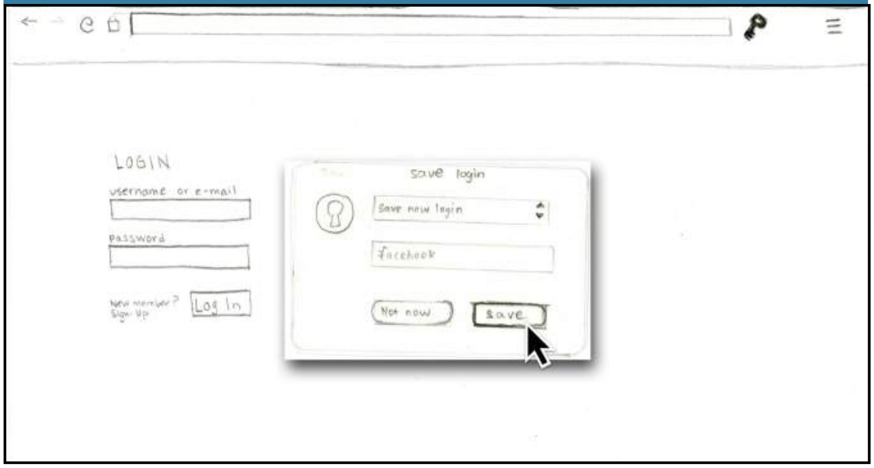


Figure 1.2 - The 1Password Save Login prompt box. Requests permission to save the login details into the vault.

Having stored his Login, Robert is given two warnings that his Facebook password has been analyzed and registers as weak.

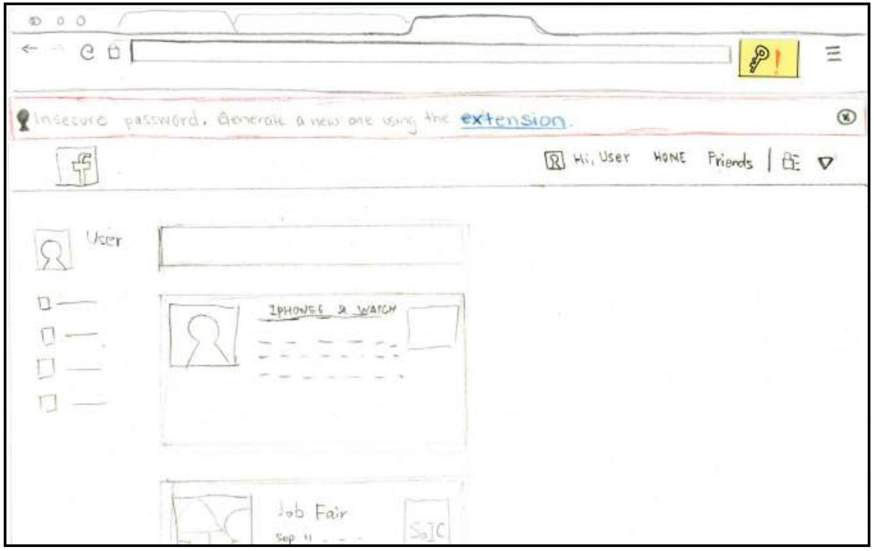


Figure 1.3 - The weak password notification bar appears at the top of the page and provides a link to the extension. A red exclamation mark appears next to the extension key.

THE 'GENERATE NEW' OPTION

Robert clicks the extension key, opening the generator. He can see his password (the secure masked dots), its strength, and his options.

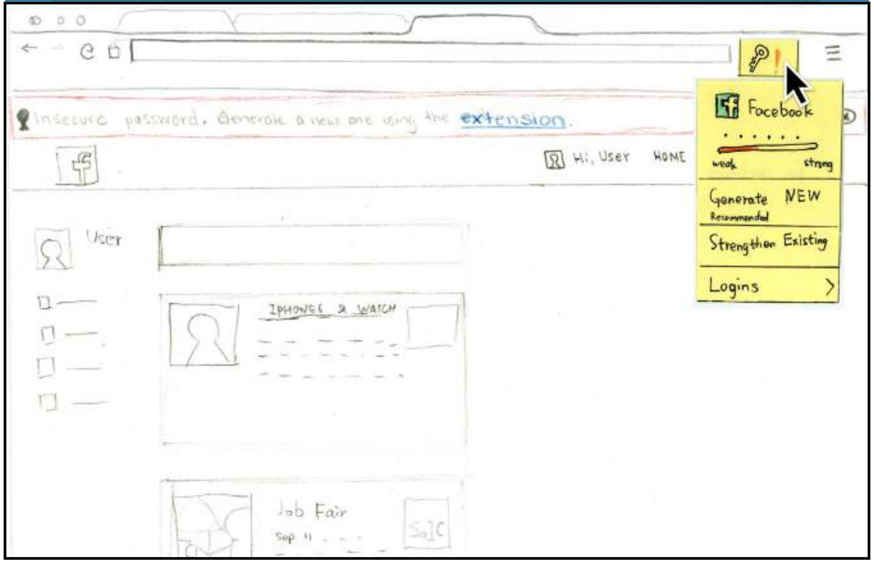


Figure 1.4 - Options: 'Generate New' feature, 'Strengthen Existing' password feature, and 'Logins.'

Here, let's go ahead and have Robert generate a new password and explore his customize options.

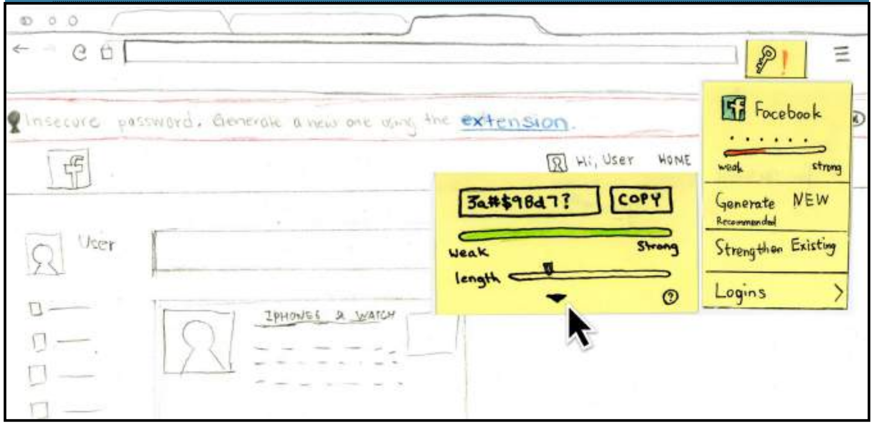


Figure 1.5 - The 'Generate New' feature. A new password is immediately generated in the type field. An arrow allows the user to open the additional interactive options.

Robert drags a slider forward, which customizes and strengthens his new password.

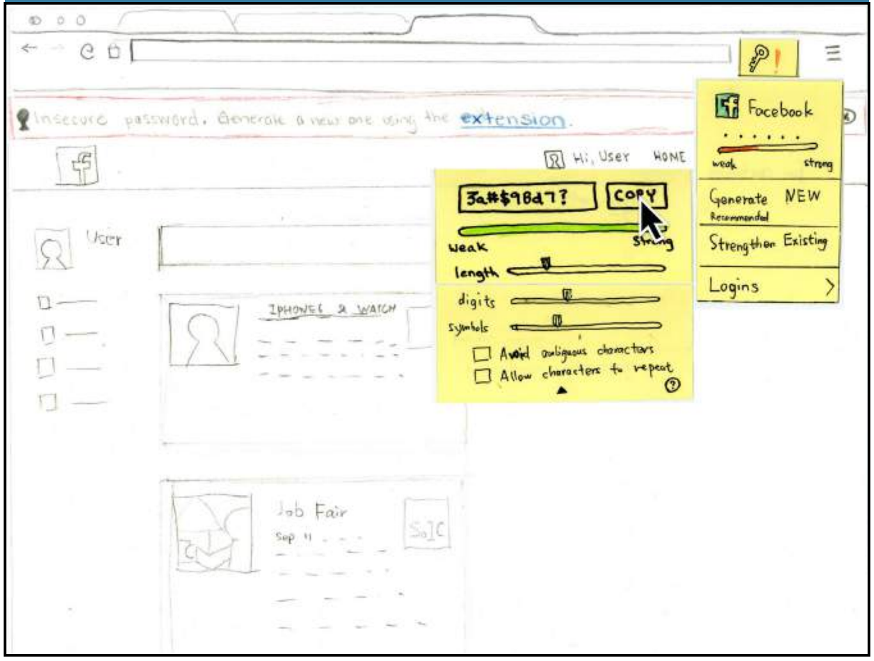
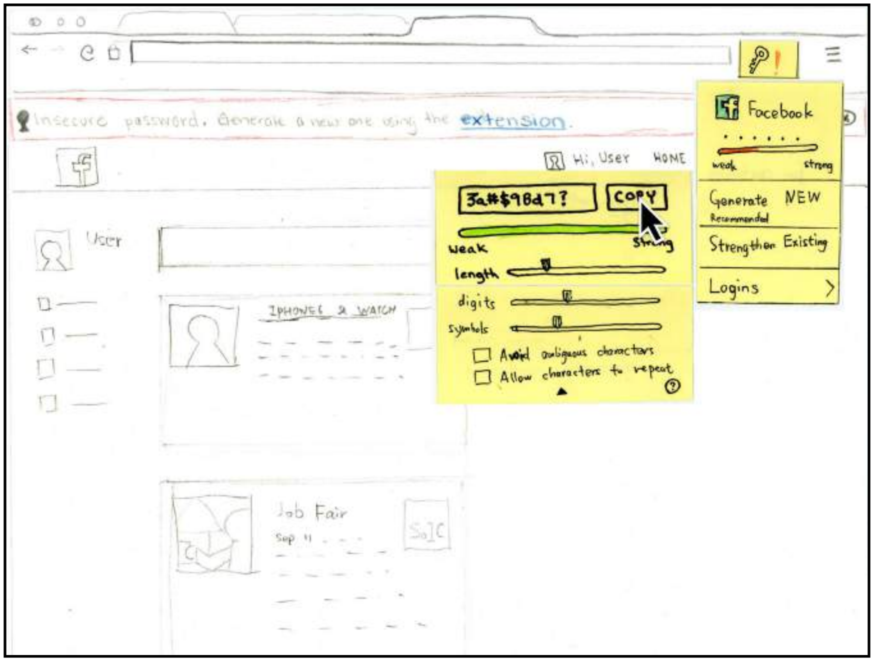


Figure 1.6 - The various customization options in the generator. (Note: Our design removes 1Password's 'Password Recipe' label for this feature in an effort to improve flow, increase perception of user control, and decrease ambiguity.)

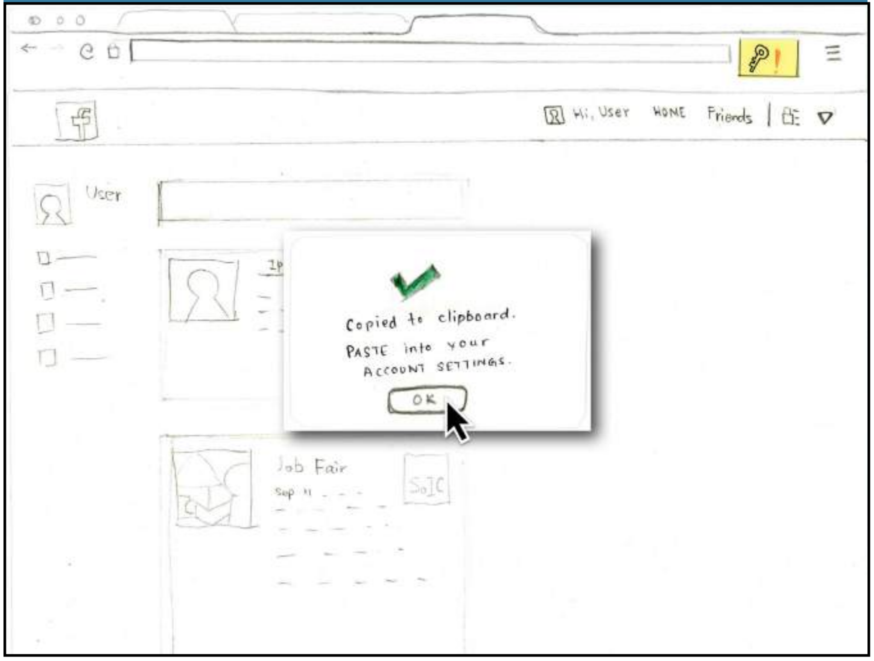
Robert has settled on his new password and clicks 'copy.'



Insecure password. Generate a new one using the extension.

Figure 1.7 - The generated password saves to their clipboard.

Robert receives verification for creating his new password and instructions to update it in the website account settings.



Copied to clipboard.
PASTE into your
ACCOUNT SETTINGS.

Figure 1.8 - The verification pop-up

Robert goes to his Facebook account settings. After he enters his existing password, pastes in his new password, and clicks update, he again receives a 1Password prompt. It asks him to 'Update' his Login information in the vault.

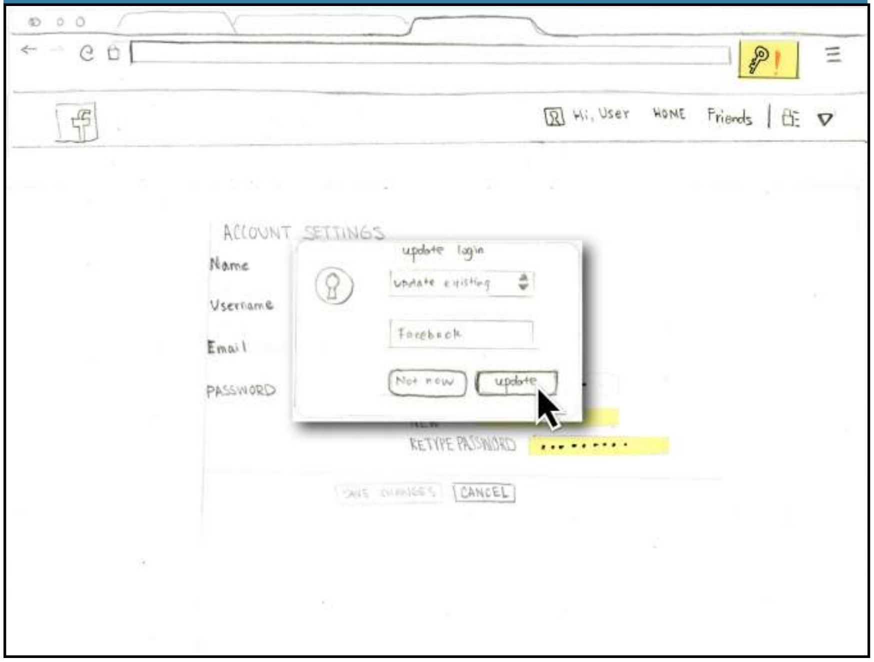


Figure 1.9 - The 1Password Update Login prompt laid over Facebook Settings >> Password page

Robert clicks 'Update' and receives a large green verification checkmark. He has finished the process.

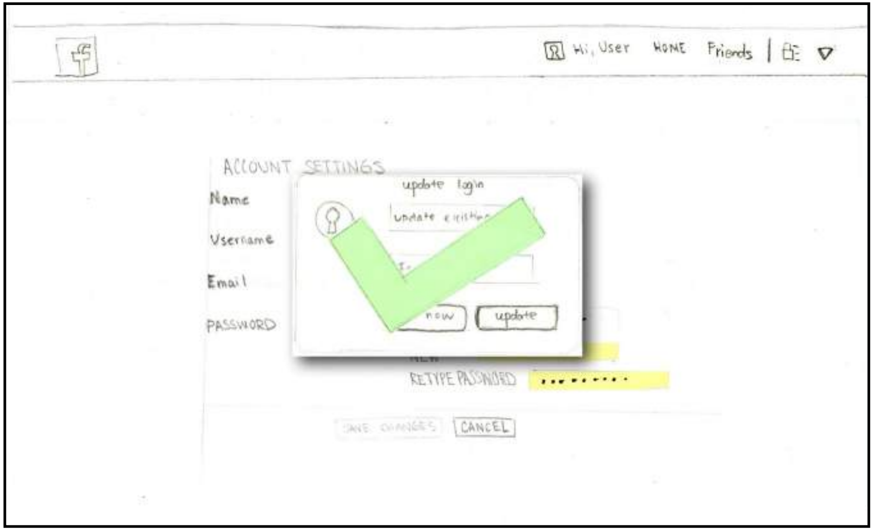


Figure 1.10 - The rewarding check mark. Fades away after a moment. The Update Login box disappears.

THE ‘STRENGTHEN EXISTING’ OPTION

The following steps show what happens when a user selects the ‘Strengthen Existing’ option in the generator. This feature gives the user more control over the customization of the password. It discourages the user from using duplicate passwords and allows them to create a password that is both secure and memorable.

Now, let’s say Robert is wary of a randomization (See research Fig. 1.5) and wants to use his existing password in some capacity. He passes over the recommended ‘Generate New’ option and clicks ‘Strengthen Existing.’

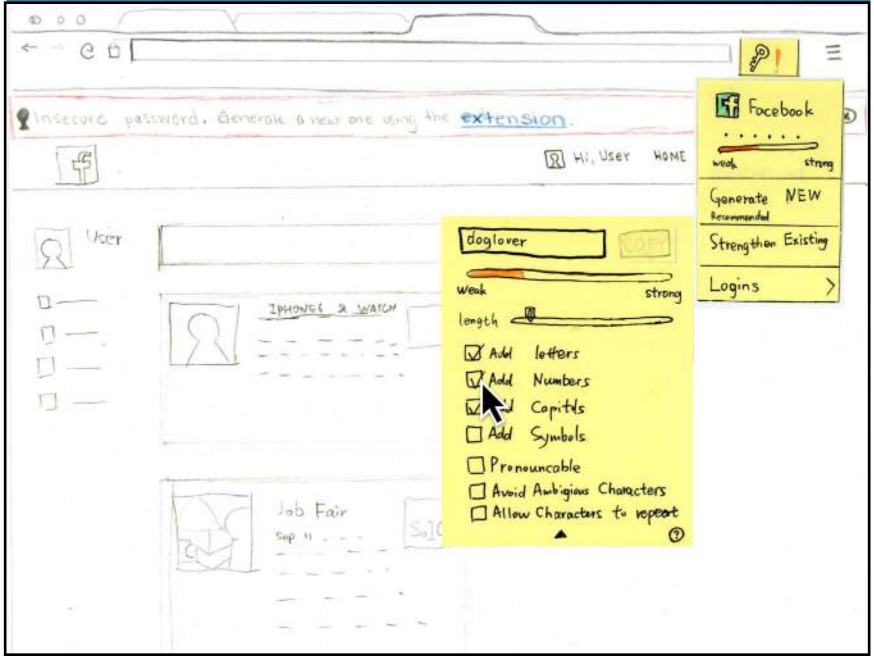


Figure 1.11 - The ‘Strengthen Existing’ option. There is a blank text field where the user types in a password, a strength bar that measures it, one interactive bar ‘length’ which begins customization, a down arrow to open more options).

Robert types in his password, reads the measure of its strength, and clicks the arrow to open the customize options.

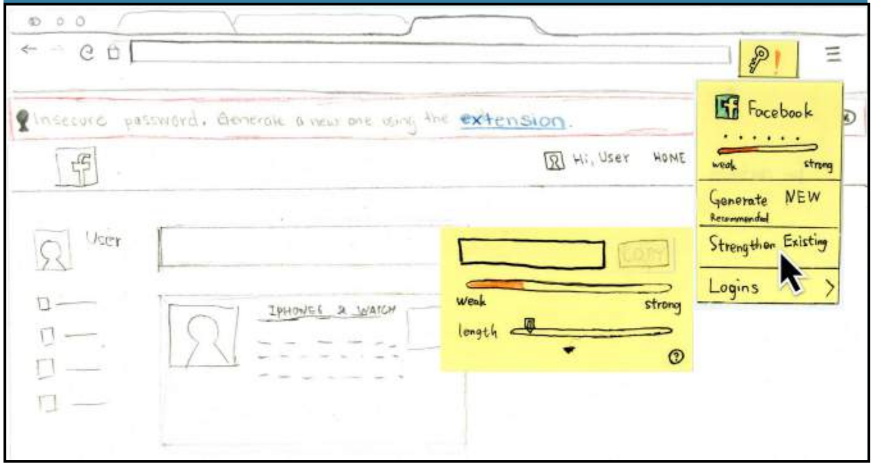


Figure 1.12 - The customizable options list. 'Add letters', 'numbers', and 'capitals' are checked by default. The user controls how much is added with the slider on the length bar, the complex software determines how the original password will be displayed with the chosen additions to length.

Robert copies his new "old' password and updates his account settings, ending the process.

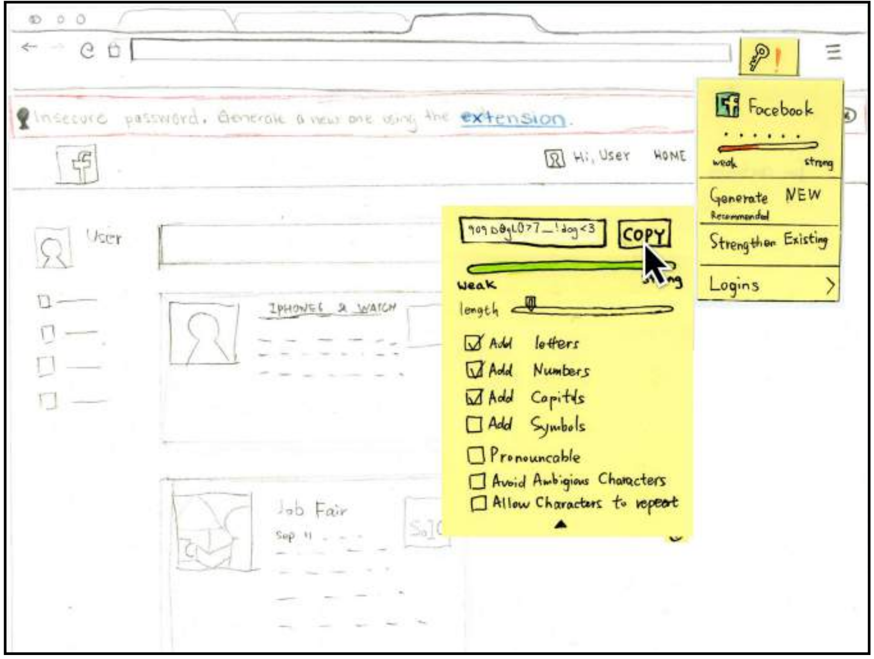


Figure 1.13 - Similar to the generator, the strengthen option has a copy feature which copies the current password to the user's clipboard.

THE PROCESS

Understanding The Problem -> Survey-> Personas-> Sketches->Usability Testing

UNDERSTANDING THE PROBLEM

Before started designing, we took two full days to understand the problem. We reflected on the following questions: “Do users really care about their passwords?”, “What issues does 1Password already create?”, “Why aren’t people using the generator?”

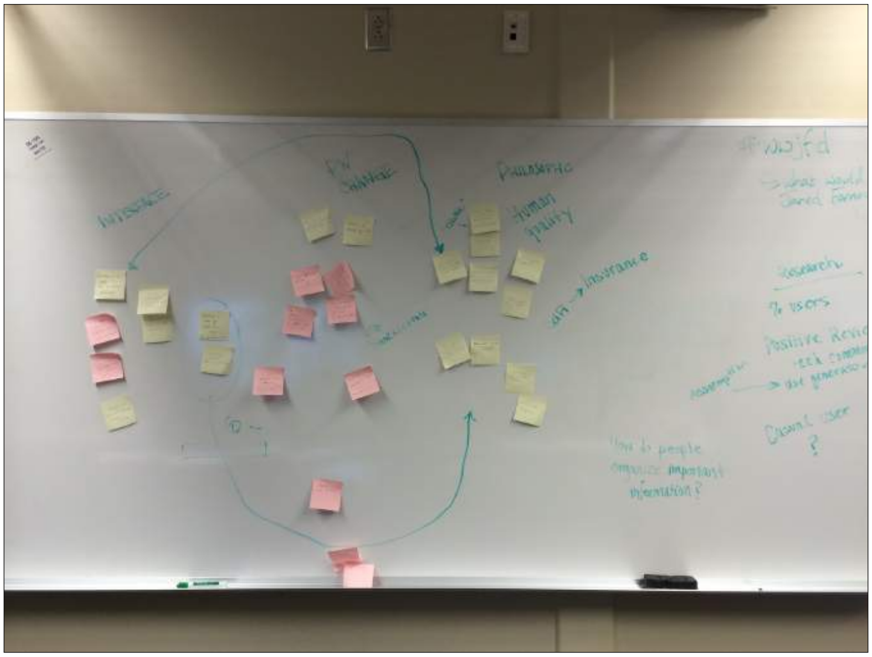


Figure 2.0 - Understanding the problem through categorizing sticky notes.

While we began to understand the problem by talking with each other, we realized that the only way to really get to the core of this problem was to ask people. So, we created a survey.

PASSWORD SURVEY

Our survey asked people wide questions and conceptual questions about passwords - the kind of passwords they use, their perception of a secure password, their expectations from a password manager, etc. Over 100 people participated. Below is a summary of the results:

Q: “What do you think is a secure password?”

The most common answer among our survey respondents was that a secure password was a mix of capital letters, symbols, numbers and personal information. A few examples of this were given: M@niF!y, H’buRg@1986 and 1ilove2great3danes45. While users acknowledge that secure passwords include these aspects, their passwords still tend to include personal details.

Q: “How did you come up with your password?”

The responses to this question were quite varied. Users will often find inspiration everywhere: a random object in their room, a favorite song lyric, an important date or a funny joke. These responses encouraged us to design for users who do not want to give up their old passwords. **Our design eases them towards more secure password creation.**

Q: “How often do you change your password?”

According to our survey, it is seldom that people actually change their password. Other results from the survey suggest an internal connection between users and their passwords, which may explain this unwillingness to change. **This strengthened our resolve to design a “middle ground” component of the generator.**

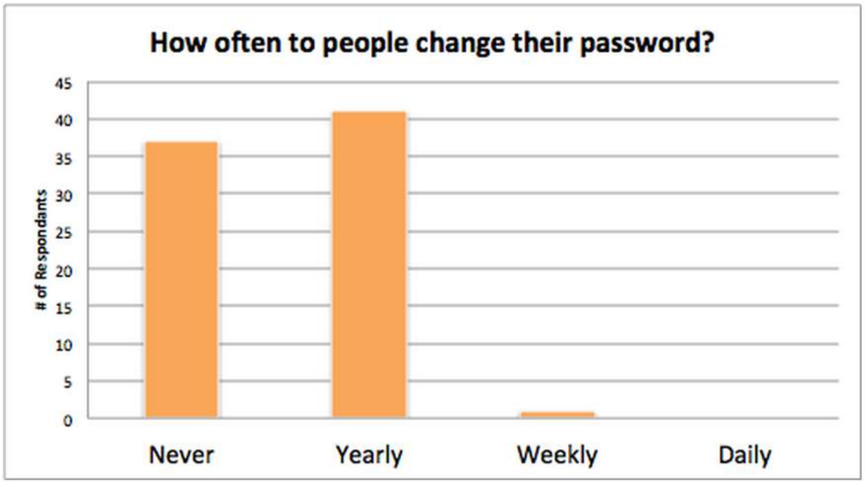


Figure 2.1 - Results from research survey.

Q: “Do you use the same password for multiple accounts?”

An alarming eighty-eight percent of our respondents reported that they use the same password for multiple accounts. This is the most defeating compromise for the 1Password vault as well as a major issue for secure web use generally. **On top of shepherding users to the generator, our design emphasizes and uses the password auditing feature more frequently.**

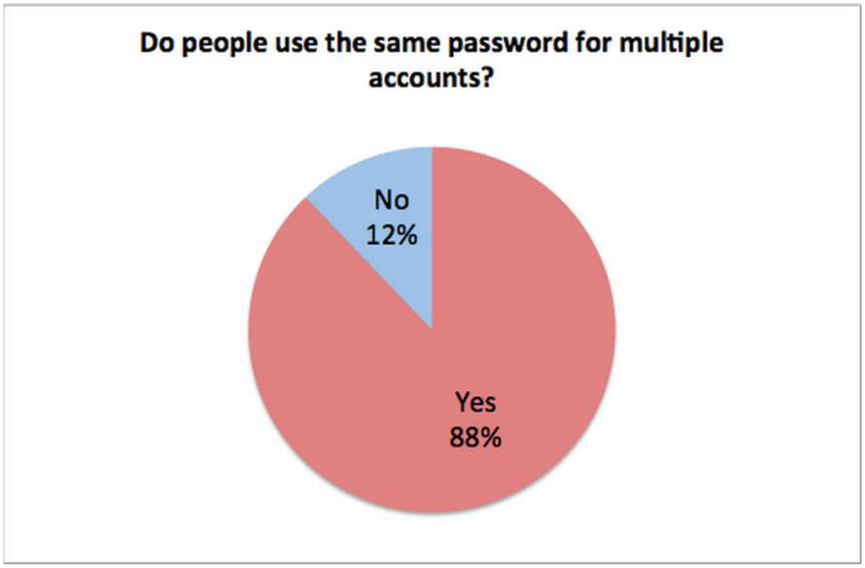


Figure 2.2 - Results from research survey.

Q: “Do you consider the strength bar when creating a password?”

Almost 3/4th of our respondents indicated that they consider the strength meter when creating their passwords. Our design has 1Password’s current strength bar appear more frequently and prominently. **However, nearly 30% of people is a large chunk. Tech- and security-savvy users can disable weak password notifications to streamline the generating process.**

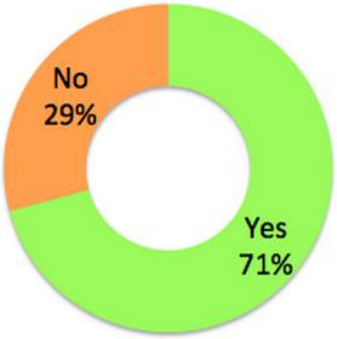


Figure 2.3 - Results from our research survey.

Q: “Would you feel more secure with a randomly generated password?”

The following graph may represent the most important information that we concluded from the survey. The large majority of users reported that randomly generated passwords do not feel more secure. One respondent specified that randomly generated passwords, “felt less familiar” while another described them as feeling “cold/mechanical”. This gestures toward a major root of the problem: a user’s trust wanes when given a password that is characteristically unfamiliar, robotic, and mechanical.

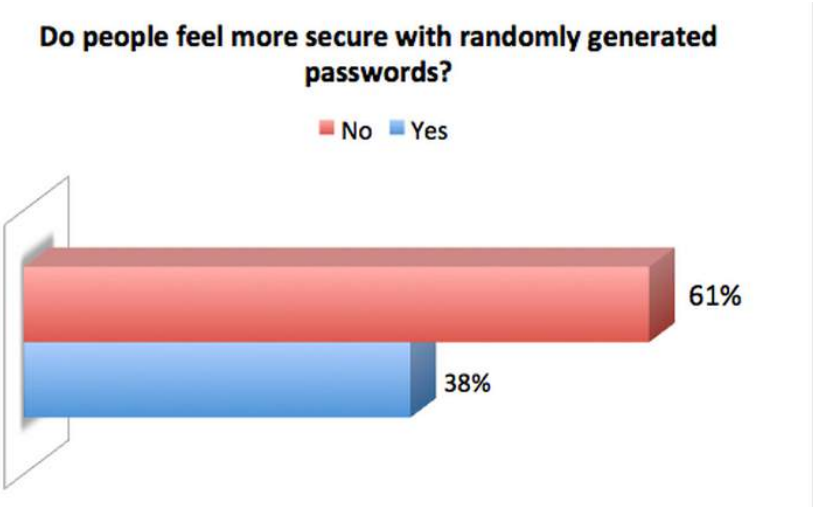


Figure 2.4 - Results from research survey.

Summary of Results

As the individual results indicated, people build trust into their passwords with personal and memory-sensitive details, including the active process of dreaming up the password. Our survey indicated that people are often unwilling to change their passwords for two main reasons: it takes too much time and they use the same password for multiple accounts. With these insights in our pockets, we created two personas and began to sketch.

PERSONAS

ROBERT

Low Tech Ability,
High Security Concern

Title: Retired Police Officer

Location: Rural, Private Area

User Type: Infrequent user, mostly stores important information into the 1Password vault.

Age: Mid 50's

Gender: Male

Characteristics

Robert is a very thorough individual and knows through experience that the devil is in the details. Having been in the police force for a greater part of his life, Robert has a very high concern for the security of his information.

Snapshot

He begins entering some of his information and passwords. He notices the security audit feature so he clicks it. It informs him that his passwords are strong but needs more strength to be more secure—it then recommends to him that he should use the generator feature to be more secure! He is a bit skeptical of the feature because he doesn't understand where these "generated" passwords are coming from. He decides to click the icon and scope it out a bit—but decides to leave it. After being confronted with all of the "what if's" of the program, he decides to himself that he can always come back later when he understands 1P better.

LISA

Tech Savvy,
Social Media Enthusiast

Title: Technology Manager
Location: Any City, USA.
User Type: Frequent user of 1Password and stores most of her social media accounts in the vault.
Age: Upper 20's
Gender: Female

Characteristics

Lisa is a very care-free individual who could be described as the life of the party. Even though she has a strenuous job, Lisa realizes in the evening with her friends who she is in constant communication with via social media.

Snapshot

In the morning, Lisa goes to the office and boots her computer. Before work, she checks her e-mail and spends at least 10 minutes on her social networks. Later in the day, she decides that she needs to create a new bank account and begins the registration process. During the process, Lisa is prompted by 1Password to generate a new password for her new account. Since 1Password doesn't have a very encouraging interface, she decides to come up with her own password and continue the registration.

PROGRESSION SKETCHES

With our persona's in mind, our team developed a series of preliminary sketches. Our sketches were considered individually and then combined into our initial prototype.

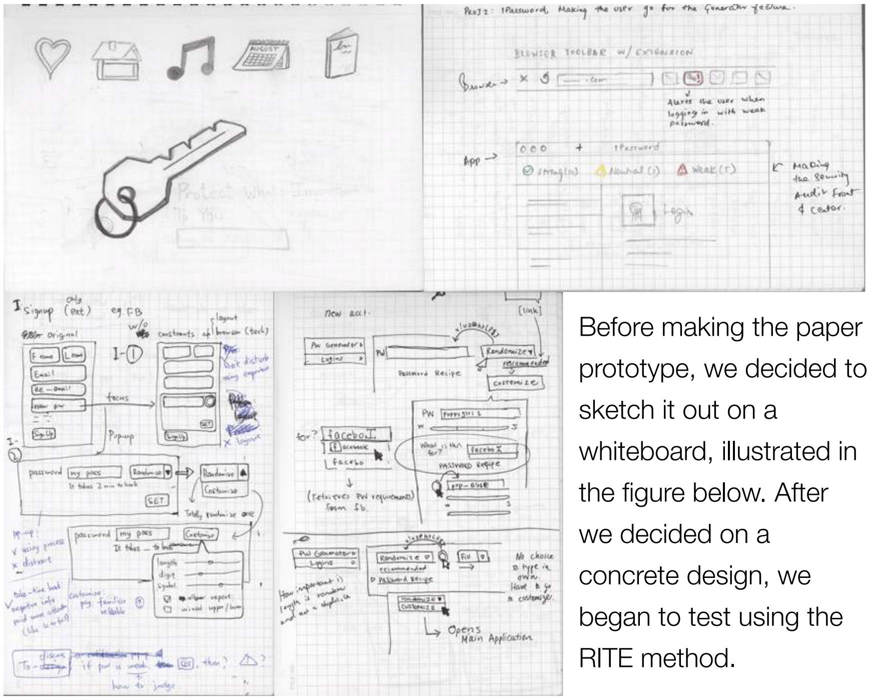

Protect What's Important To You
Browser Toolbar w/ Extension
Alerts the user when logging in with weak password.
App
1Password
Strong
Normal
Weak
Making the Security Audit Front & Center.
Login
Signup
Original
Popup
Randomize
Customize
SET
New acct
PW Generators
Logins
Password Recipe
facebook
Opens Main Application

Figure 2.5 - Preliminary Sketching

Before making the paper prototype, we decided to sketch it out on a whiteboard, illustrated in the figure below. After we decided on a concrete design, we began to test using the RITE method.

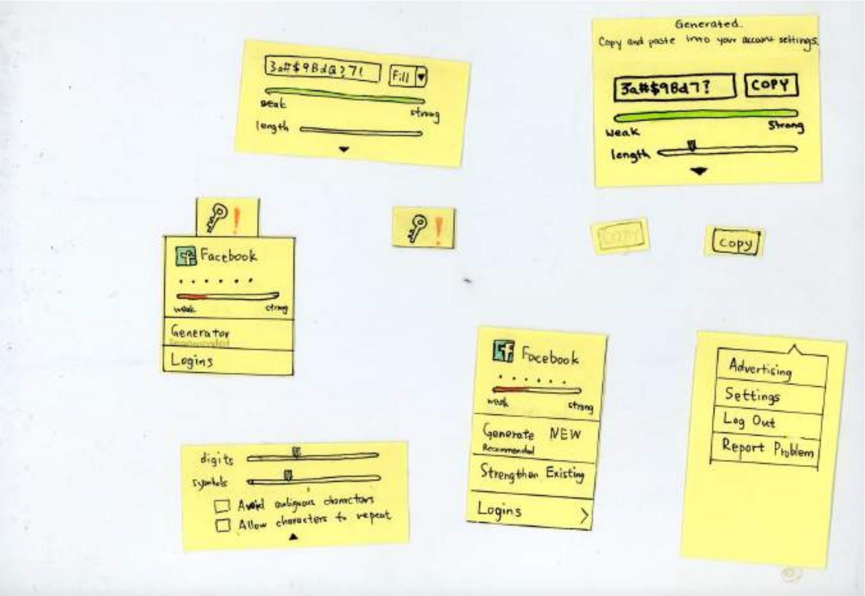


Figure 2.6 - Beginnings of prototype.

USABILITY TESTING - THE RITE METHOD

Introduction and Methodology

This is the usability test for our 1password redesign project. We used the RITE method to iterate our design and improve the prototype after every test. We iterated the testing-revising process 4 times.

Observing

We used both Think Aloud and Probe methods during the tests. The subjects were encouraged to talk through their process during the test, and we followed the test with a series of scripted questions and ended the test with one or two ad lib questions. We recorded by note-taking and image capture.

Testing Process

Before each test, we provided the subject with a prompt that introduces the main idea of 1password and some information of this test. During each test, the conductor one short set of directions: “Login, follow the 1password prompts” and, if we were testing the customize option, an additional step: “You want to use your existing password and make it more secure.” The other teammates took notes of the subjects’ behavior and words. After each test, we administered the follow-up questions.

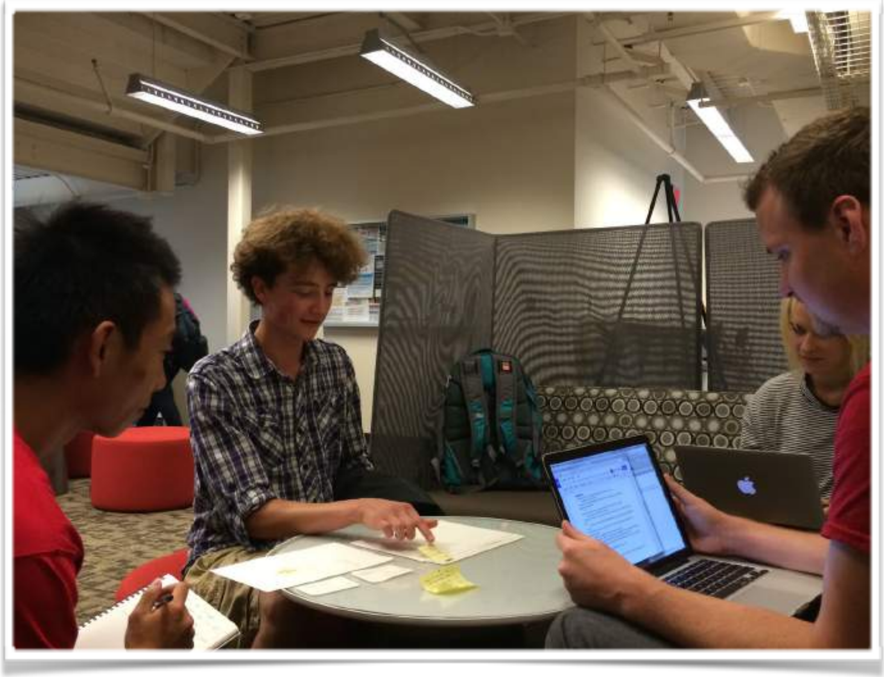


Figure 2.7 - First usability test in SoIC Study Booth

Test 1

Basic information

Test conductor: Micah
Test observers: Yangguang, Shankar, Michelle
Setting: Informatics West Entry

Goals

1.) To see if the user is compelled to generate a new password based on the prompts;
2.) To see is the user can use the generator error free.

Script

No.	Direction	User Behavior	Screen States
1	"Log into the website and follow the 1Password prompts"	Logs in with their own username and (weak) password	After the user clicks "Login", show pop-up to "Save new login"
2	(The "Save new login" pop-up)	Clicks "not now"	Show the content web page (**Test ends**)
3	(The "Save new login" pop-up)	Clicks "save"	Show notification bar and new extension icon. Show the content web page
4	(The notification bar)	Clicks the extension icon	Show the extension box
5	(The extension box)	Clicks the "Generator"	Show the "generator" box
6		Clicks the arrow in the bottom of the generator box	Show additional options

No.	Direction	User Behavior	Screen States
7		Clicks the “Fill”	If in the form web page, then fill the form. The generator box closed
8		Clicks the “Copy”	The generator box closed. (The new password copied to the clipboard)
9	(The notification bar)	Clicks the “Account settings” in the website	Show the account setting web page
10	(Account setting web page)	Fills in the form	Fill in the password
11	(Account setting web page)	Clicks “save”	Show the “Update” pop-up
12	(The “Update” pop-up)	Clicks “save”	Show the content web page (**Test ends**)

Results

No	1	2	3	4	5	6	7	8	9	10	11	12
Result	✓	N/A	✓	✓	✓	N/A	✓	✓	✓	✓	✓	✓

- The subject didn’t understand the prompt in the notification bar clearly at first.
- The subject used the “Fill” button in the generator box;
- *“The newly generated password didn’t have a confirmation that it went through”*
- The subject felt confused by the content page when logged in.

Revisions

1.) Edit the words in the notification bar;

2.) Set the copy as default in the generator;

Add confirmation after user copy the generated password;

3.) Refine the content web page to avoid misunderstanding.

Test 2

Basic Information

Test conductor: Shankar
Test observers: Yangguang, Micah, Michelle
Setting: Studio

Goals

1.) To see if the user is compelled to generate a new password based on the prompts;
2.) To see if the user can use the generator error free;
3.) To see if the user can successfully go through the flow with all the notifications and directions.

Script

No.	Direction	User Behavior	Screen States
1	"Log into the website and follow the 1Password prompts"	Logs in with their own username and (weak) password	After the user clicks "Login", show pop-up to "Save new login"
2	(The "Save new login" pop-up)	Clicks "not now"	Show the content web page (**Test ends**)
3	(The "Save new login" pop-up)	Clicks "save"	Show notification bar and new extension icon. Show the content web page
4	(The notification bar)	Clicks the extension icon	Show the extension box
5	(The extension box)	Clicks the "Generator"	Show the "generator" box
6		Clicks the arrow in the bottom of the generator box	Show additional options

No.	Direction	User Behavior	Screen States
7		Clicks the "Fill"	If in the form web page, then fill the form. The generator box closed
8		Clicks the "Copy"	The generator box closed. (The new password copied to the clipboard)
9	(The notification bar)	Clicks the "Account settings" in the website	Show the account setting web page
10	(Account setting web page)	Fills in the form	Fill in the password
11	(Account setting web page)	Clicks "save"	Show the "Update" pop-up
12	(The "Update" pop-up)	Clicks "save"	Show the content web page (**Test ends**)

Results

No	1	2	3	4	5	6	7	8	9	10	11	12
Result	✓	N/A	✓	✓	✓	N/A	N/A	✓	✓	✓	✓	✓

- *"I do like extra confirmation."*

Revisions

1.) If notification ignored, then periodically remind them.

2.) If generator is used successfully 5 times (5 successful PW updates) then user is considered "expert" and won't receive the notification bar of an insecure password, though the key will still be marked with an exclamation point.

3.) Once user hits "Save" on the 1Password Save new login popup, the box whites out and is replaced with a green check mark or green key-lock before disappearing.

Test 3

Basic information

Test conductor: Michelle

Test observers: Yangguang, Shankar, Micah

Setting: Informatics West Entry

Goals

1.) To see if the subject can use the customize generator successfully;

2.) To see how the subject will choose between the "Generate New" and "Strengthen Existing".

Script

No.	Direction	User Behavior	Screen States
1	You want to use your current facebook password but make it stronger. Log in to facebook and follow the 1Password prompts. Your existing password is "doglover".	Logs in with their own username and (weak) password	After the user clicks "Login", show pop-up to "Save new login"
2	(The "Save new login" pop-up)	Clicks "not now"	Show the content web page (**Test ends**)
3	(The "Save new login" pop-up)	Clicks "save"	Show notification bar and new extension icon. Show the content web page
4	(The notification bar)	Clicks the extension icon	Show the extension box
5	(The extension box)	Clicks the "Generator"	Show the "generator" box

No.	Direction	User Behavior	Screen States
6		Clicks the arrow in the bottom of the generator box	Show the "Customize existing" box
7		Clicks the arrow in the bottom of the generator box	Show additional options
8		Checks or unchecks the check boxes in the options	Change the password
9		Clicks the "Copy"	The generator box closed. (The new password copied to the clipboard)
		Clicks the "?" button	Show the help information
11	(The notification bar)	Clicks the "Account settings" in the website	Show the account setting web page
12	(Account setting web page)	Fills in the form	Fill in the password
13	(Account setting web page)	Clicks "save"	Show the "Update" pop-up
14	(The "Update" pop-up)	Clicks "update"	Show the content web page (**Test ends**)

Results

No	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Result	✓	N/A	✓	✓	✓	✓	N/A	N/A	✓	✓	✓	✓	✓	✓

- The subject chose to use the generator.
- The subject ignored the confirmation message.
- The subject got confused after copy the password.

Revisions

1.) Use pop-up to show the confirmation message

Test 4

Basic information

Test conductor: Yangguang
Test observers: Micah, Shankar, Michelle
Setting: Informatics West Entry

Goals

1.) To see if the subject can use the customize generator successfully;
2.) To see how the subject will choose between the “Generate New” and “Strengthen Existing”; To see if the subject can understand the confirmation message.

Script

No.	Direction	User Behavior	Screen States
1	You want to use your current facebook password but make it stronger. Log in to facebook and follow the 1Password prompts. Your existing password is “doglover”.	Logs in with their own username and (weak) password	After the user clicks “Login”, show pop-up to “Save new login”
2	(The “Save new login” pop-up)	Clicks “not now”	Show the content web page (**Test ends**)

No.	Direction	User Behavior	Screen States
3	(The “Save new login” pop-up)	Clicks “save”	Show notification bar and new extension icon. Show the content web page
4	(The notification bar)	Clicks the extension icon	Show the extension box
5	(The extension box)	Clicks the “Generator”	Show the “generator” box
6		Clicks the arrow in the bottom of the generator box	Show the “Customize existing” box
7		Clicks the arrow in the bottom of the generator box	Show additional options
8		Checks or unchecks the check boxes in the options	Change the password
9		Clicks the “Copy”	The generator box closed. (The new password copied to the clipboard)
		Clicks the “?” button	Show the help information
11	(The notification bar)	Clicks the “Account settings” in the website	Show the account setting web page
12	(Account setting web page)	Fills in the form	Fill in the password

No.	Direction	User Behavior	Screen States
13	(Account setting web page)	Clicks “save”	Show the “Update” pop-up
14	(The “Update” pop-up)	Clicks “update”	Show the content web page (**Test ends**)

Results

No	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Result	✓	N/A	✓	✓	✓	✓	N/A	N/A	✓	✓	✓	✓	✓	✓

- The subject didn’t read the confirmation and just clicked the button.
- The subject chose the “Strengthen Existing” by curiosity.

Revisions

1.) Add check mark in the confirmation pop-up;

2.) Don’t show the original password in the generator

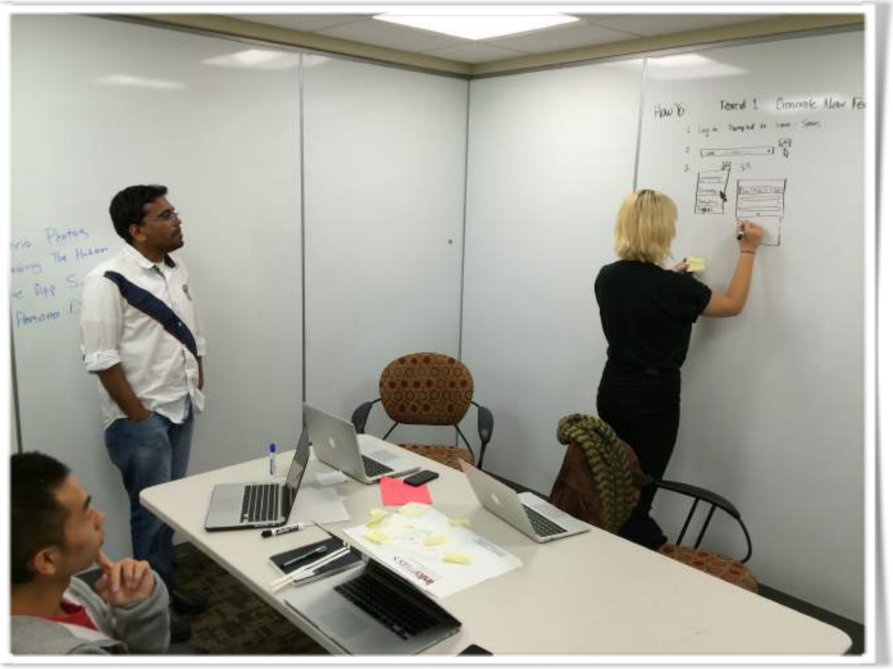


Figure 2.8 - Drawing out the final design on the whiteboard.

FINAL THOUGHT

We'd like to thank you for making it through our 1Password generator redesign rationale. It is our hope that our choice changes are both sweeping and subtle. We believe we've greatly increased the design's empathy for novice users, without disrupting 1Password's success at creating a product that integrates smoothly into a user's web flow.

Signed,
Shankur, Michelle, Yangguang, and Micah

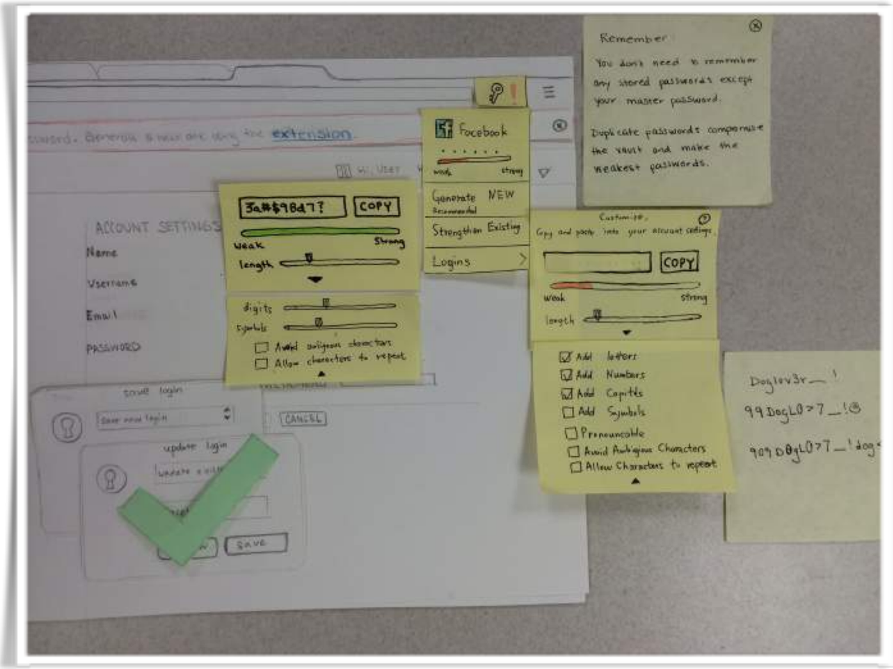


Figure 2.8 - Drawing out the final design on the whiteboard.

SUGGESTED CHANGES FOR THE NATIVE APPLICATION

While our design focused mostly on the extension, a major point of contact for the users, the native 1Password application is still very important. Used mainly as a vault, the native app comes with a slew of features and acts like a bank where you can look at all your accounts, cards, etc. People may only check this occasionally but it's still an important part of the whole 1Password system. 1Password offers a nifty feature called 'Security Audit' which audits all your accounts and provides a nice overview of the number of weak and strong passwords.

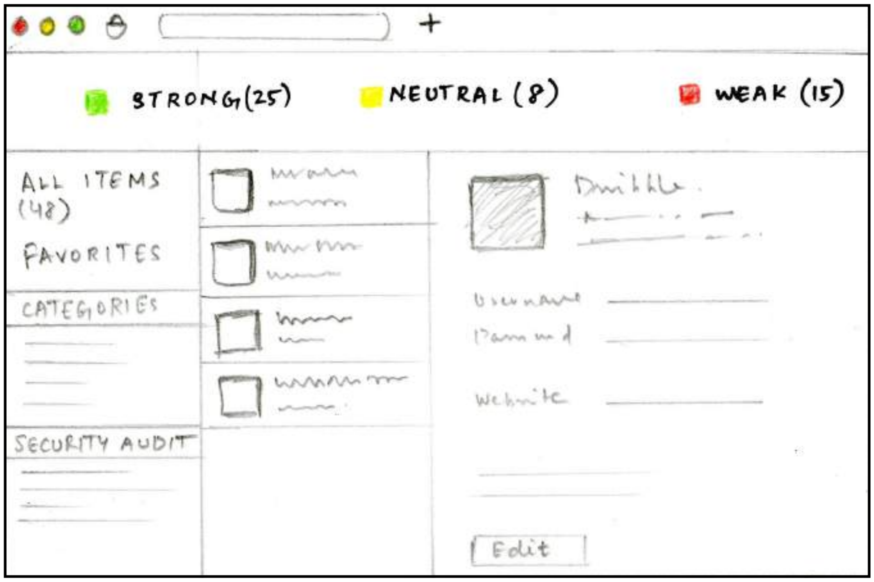


Figure 2.9 - Possible changes reflected in the native application.

We feel that this feature needs more visibility other than being in the sidebar. To do this, we propose a feature called 'Highlights' ; which is a bar right at the top in the native app. It shows the number of strong, neutral and weak passwords. The visual change might be small, but we believe that these numbers act like a badge and will push the user to bring down the 'Weak password' count to Zero. It's all about feeling good, and making all the passwords read strong feels great to the user.

Apart from the aforementioned change, the native app incorporates the same generator which is mentioned in our final design. Unlike the extension in the browser, the native app will be able to calculate the strength of your password as you type and allow you to use the generator on the fly. In the current 1Password design, the generator is not obvious and doesn't measure the strength of the user's password until after all the details are saved.

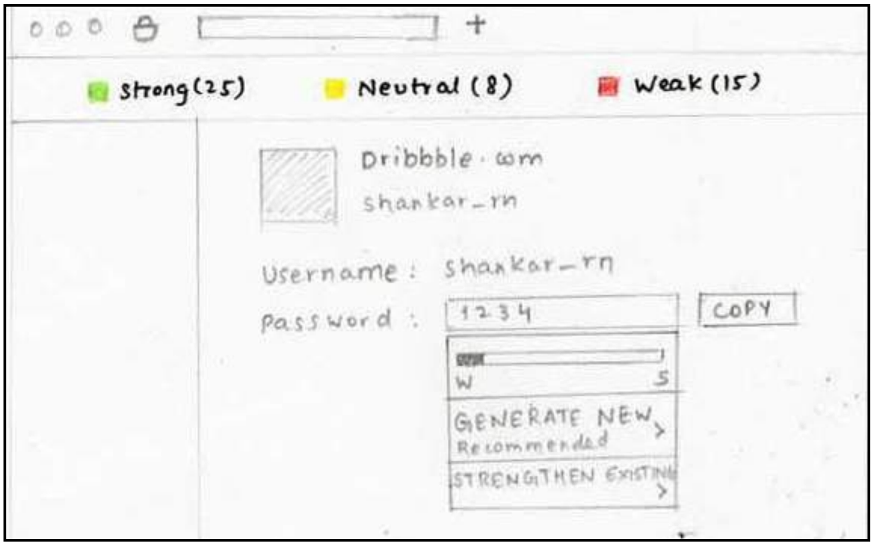


Figure 2.10 - Drawing out the final design on the whiteboard.

APPENDIX I - BIBLIOGRAPHY

PHOTO OF LISA

http://blogs-images.forbes.com/learnvest/files/2014/07/115039371.jpg

PHOTO OF ROBERT

http://assets.mrketplace.com/wp-content/uploads/2013/07/MarkWerts.jpg

1PASSWORD WEBSITE

https://agilebits.com/onepassword

PASSWORD SURVEY

https://docs.google.com/forms/d/1EpqHWM6ajWAK0TVolF_fkBj5Nq114wgAm4HFVOxFYzo/viewform

PASSWORD SURVEY RESPONSES

https://docs.google.com/spreadsheets/d/1EX0meykkb9ulPKMlf-L0mc7zyYlRWJKJ_JW08H_aV78/edit?usp=sharing

APPENDIX II - USABILITY TEST DOCUMENTATION

PROMPT FOR THE SUBJECT

You've been worried over the security of your online passwords and purchased 1Password as a solution. You've downloaded both the software and the extension. When you log-in to a website, your new software will prompt you to save your password into the vault. The vault is where all your passwords are securely stored, and any other sensitive information you may want. The main feature of 1Password is the password generator, which you can use to generate extremely strong passwords for all your web accounts, and which will be stored in the vault. You don't have to worry about remembering the passwords—all you have to remember is a single master password which lets you into the vault. Also, once you have passwords in the vault, 1Password works with your browser to auto fill login pages with the correct password. You've already set your Master Password and are currently logged into 1 Password.

For the purposes of this test, please make up usernames and passwords from scratch. It is not advised that you use your own password.

For this task you are using a common web browser and are about to sign into a low priority website, Facebook.

You are allowed and encouraged to think aloud. The conductor will not respond verbally, but will respond by progressing the test. The test will be followed by a set of questions.

AFTER TEST QUESTIONS

1.) What does this icon (key with exclamation point) indicate to you?

2.) Before the software indicated that your password was weak, did you believe your password as insecure?

3.) How did you feel when you were prompted that your password was weak?

4.) Was your impulse to come up with your own or use the program to generate a stronger

5.) What would, if anything, compel you more to change your password using the built in generator function?

6.) Was it annoying to have both the bar and the exclamation point warn you of your weak password?

7.) How do you come up with a password?