# 

# Results from the Pilot Study

## Introduction

In this phase, we conducted a pilot study with our peers during lab times. We asked 24 students from the class to participate in our questionnaire. Those interested in receiving participation marks were asked to sign their name when beginning the survey, and again after completing it. The participation sheets are included as part of this submission, along with the graphical response output as provided by Google Forms.

The questionnaire was divided into five distinct sections. The first section asked questions regarding the experiences participants have had with password managers. The second section walked users through our proposed browser extension using wireframe images, but did not ask any questions. The third section queried participants on their thoughts on master passwords and associated requirements. The fourth section asked questions comparing various user interface choices. We were especially interested in randomized password generation in this section. Finally, the fifth section allowed participants to share their thoughts and overall impression of the proposed manager.

Most of the questions asked of users were boolean or employed a Likert-type scale (1-3, negative, neutral, positive). Rarely, users could provide their own responses through a short-text form.

There are many different forms that password managers can take. As a result, we focused our efforts on browser-based password managers. We defined this to participants as:

*...a password manager that is accessed and employed through the user's web browser (e.g.: Google Chrome's built-in password manager). This differs from a password manager that must be launched separately from the browser (e.g.: KeePass).*

## Reflections

### Section 1

While we were pleased to see that a majority of respondents had used a password manager before, we were surprised that a large minority (6 ind., 25%) in a computer science class had never used one before. Of those that had used a password manager, only a single person had not used a browser-based password manager before.

When asked about a minimum criteria for password managers passwords, a large majority (18 ind., 75%) indicated that such restrictions should be put into place. Real-time feedback, where users are informed that their password is weak, was an even more popular idea (21 ind., 87.5%).

More polarizing, however, was the notion of random password generation by the password manager. The participants were split down the middle, with 12 users approving of the idea, while the other half disapproved or were unsure.

The final question of this section was a short-text response, with several pre-filled options, where users could indicate the reason for why they use password managers. As expected, the most popular reason was that users do not have to remember many passwords. Curiously, this response garnered 19 votes, when only 18 users had indicated their use of a password manager. We hope that our questionnaire has encouraged this user to try out a password manager. The other two major responses (“helps me generate secure passwords” and “it’s built into my browser”) each gained 6 votes.

### Section 3

The password scheme we chose in phase 1 (2words16) was reported as being cryptographically strong while also easily remembered. Participants seemed inclined to agree.

A majority of users reported that they understood the password requirements (15 ind., 62.5%) and deemed them reasonable (13 ind., 54.2%). More importantly, only a single participant did not understand the password requirements, and only two regarded them as unreasonable. We regard the neutral responses as successful, considering that the importance of a master password will necessarily require a convenience trade-off.

Finally, we showed a scenario in which the user has chosen a password that does not fit the requirements. While a slim majority (13 ind., 54.2%) of participants did understand why the password was rejected, we regard this as an area for improvement, as we would not want nearly half of our prospective users to reject the manager simply because they cannot choose a master password.

### Section 4

The first half of this section focused on encouraging users to use generated passwords. We showed two different images of suggested password generation. In the first scenario, the generation box was displayed to the side of the password input field. In the second scenario, the generation box was placed on top of the password input field. Participants were asked if they were likely to use a generated passwords, as well if they perceived that they could manually enter a password.

In the first scenario, only a third of respondents (8 ind., 33%) indicated that they were likely to use the generated password, while a quarter (6 ind, 25%) indicated they would not. Two thirds (16 ind., 66%) indicated that they were able to enter a manual password if they chose to do so.

The second scenario, on the other hand, increased the positive response for password generation over 10% (11 ind., 46%), and decreased negative response (4 ind., 17%). Neutral responses were relatively stable across both scenarios at 10 and 9 individuals, respectively. Critically, however, the second scenario achieved an equally positive response to the notion of manual password input, and a slight drop in users who did not feel they could enter a manual password.

In the second half of this section, we exhibited three possible methods with which users could update their saved passwords. After presenting the method, we then asked users if they would consider using it to update their saved password. The methods presented were a prompt for update after logging in with new credentials, a dialogue box that can be toggled from the password manager icon in the browser, and a dedicated password change webpage in the password manager.

As we expected, the pop-up prompt was the most popular (14 ind., 58%) with users. The other two methods were not far behind, however. The least popular option, the dedicated page, still received a plurality approval rating (12 ind., 50%).

After presenting all three methods, we asked users which they would be most likely to use. Paradoxically, the ordering preference was reversed in these responses. The webpage update option was chosen by 42% of participants. We wonder if this may be a consequence of using technology-minded individuals for our pilot study, who are used to more explicit interfaces.

### Section 5

In the concluding remarks section, we asked for general thoughts regarding how participants perceived the intended use and functionality of the manager, as well as whether they might use it themselves.

The vast majority of participants claimed they understood the manager (19 ind., 79%), and a sizable portion (14 ind., 58%) indicated that they would consider using the extension for their own browsing.

Participants also had the opportunity to provide short-text responses to highlight shortcomings of the manager, or any other thoughts that they desired to share with us. These questions garnered three non-trivial responses. One user expressed concern that it would be “difficult to understand” for “naive users”. We hope that this is an outlier, but obviously cannot say with any certainty given the small and biased sample. Other users highlighted that they may want to use the password manager on their phone, or store their credit card information. This is obviously out of scope for this project, but we are encouraged by the enthusiastic responses.

## Recommendations

Based on our pilot study, we have drafted the following recommendations for developers of password managers:

* Enforce a strong password scheme for master password, and consider doing so for individual passwords as well
  + Users understand that their master password is what protects their other passwords, and will therefore accept a more rigid scheme
  + Ensure that users understand the scheme by providing examples of appropriate passwords
* Encourage users to choose stronger passwords by assessing the strength of potential passwords
  + Providing this feedback in real-time may lead to more secure choices
  + This can be facilitated through the use of common password dictionaries
* Offer users randomly generated passwords on account creation pages
  + Placing the generation dialogue on top of the password field may strongly encourage adoption
* Allow for different password update mechanisms to account for different workflows
  + For example, a user may change all of their passwords on a regular basis, which means that a single webpage for updates is advantageous
  + Alternatively, users may only change passwords when necessary, so a prompt to update a changed password may be more appropriate