INVESTIGATING CRITERIA AND TECHNIQUES FOR INCREASED PASSWORD SECURITY AND MEMORABILITY FOR USERS

A Thesis

Presented to

The Faculty of the Department of Psychology

San José State University

by

Novia Wong

May 2017

The Designated Thesis Committee Approves the Thesis Titled

INVESTIGATING CRITERIA AND TECHNIQUES FOR INCREASED PASSWORD SECURITY AND MEMORABILITY FOR USERS

by

Novia Wong

APPROVED FOR THE DEPARTMENT OF PSYCHOLOGY

SAN JOSÉ STATE UNIVERSITY

May 2017

_____

Evan M. Palmer, Ph.D. Committee Chair

_____

David Schuster, Ph.D. Committee Member

_____

Valerie Carr, Ph.D. Committee Member

ABSTRACT

Today, passwords are a commonly used strategy for protecting online accounts. These accounts may include sensitive personal information such as financial statements in a bank account, or may include nearly no identifying information such as that in a gaming application on a phone. Yet, to increase the security of such accounts, users are often required to create passwords that comply with strict criteria (e.g., a minimum of one upper case, one lower case, one special character, one number, and a minimum character length). Using a self-reported questionnaire, Shay et al. (2010) found that when users were required to create passwords under such strict requirements, they often reused old passwords with little or no modifications. Users also reported to be more likely to forget passwords created under such restrictions because of the uncommon combinations used for "high security" passwords. With a memory recall test and a self-reported questionnaire, this study investigated the effect of three different password composition requirements on users' recall of the passwords they generated, their general attitudes, self-predicted memorability, and perceived security for the requirements. Results indicated that actual memorability was not affected by the choice of password composition requirement, but participants perceived each requirement differently. This study also explored other areas of interest, such as password composition strategies.

Investigating Criteria and Techniques for Increased Password Security and Memorability for Users

The Internet is essential for many aspects of peoples' daily lives, because a large amount of data is stored and accessed through this shared network. Some of the data is sensitive, such as confidential financial, health, and governmental information. On average, people have 27 accounts that are password protected (Ur et al., 2015). Although it is convenient to have the information available, keeping the data secure on the Internet is difficult. Researchers and engineers have developed various authentication methods to keep data on the Internet secured, such as passwords and biometric codes. Among these methods, the use of unique passwords matched to unique usernames is the most commonly used by companies and websites, because other methods are newer to users and not commonly implemented into electronic devices.

Challenges of Text-based Password Authentication

A strong password is important for ensuring data is secured by authentication, but password strength depends heavily on users. Hackers can use software to crack or "recover secret passwords stored in a computer system or transmitted over a network," (NIST, 2013). There are two types of password cracking that hackers use: targeted attacks and brute force attacks. Targeted attacks refer to hackers purposely choosing a user account and using identifying information to crack its password (Vu et al., 2007). Brute force attacks crack passwords through software implemented by hackers that checks each possible password by systematically cycling through all available

combinations of characters (Ur et al., 2015). Generally, a strong password is one that is difficult to crack for both targeted and brute force attacks.

To facilitate strong password generation, companies have implemented several strategies to aid the password creation process. The "complexity rule" is often used, which requires a password to be a minimum character length and contain both upper case and lower case letters, as well as numbers and special characters (Shay et al., 2010; Stanton & Greene, 2014). However, studies have found that simply adding such restrictions to password generation does not necessarily increase password strength (Vu et al., 2007; Ur et al., 2015). When users attempt to create passwords that follow the complexity rule, two major issues typically prevent them from creating strong passwords: memorability and misconceptions.

When creating passwords to meet the complexity rule, users tend to develop and follow strategies that make their passwords more memorable, thus reducing their cognitive load. Although they generally understand that identifying information should be omitted from passwords, they often include other forms of personal information, such as pets' names and family members' birthdates (Ur et al., 2015). While these strategies increase memorability, they make targeted attacks easier.

A factor contributing to the memorability issue is the inconsistency of password composition requirements across different accounts. Given the countless websites on the Internet, password policies range from having one character as a minimum requirement to restricting all aspects of a password, such as the type of special characters allowed (AlFayyadhm, Thorshiem, Josang, & Klevjer, 2012; Wheeler, 2012). When creating an

account, many sites also include password meters to facilitate the process. These meters indicate password strength as perceived by the companies and often are the major source of feedback of password strength for users (Ur et al., 2016). Dropbox found variability in password meters provided by different websites, suggesting that a password without numbers or special characters could be strong for one website while rejected by another (Wheeler, 2012). This inconsistency in password requirements poses a problem for password memorability, as users must match individual accounts with unique passwords that do not necessarily share the same password generation restrictions.

Users often have misconceptions of password security. They believe that a password that follows the complexity rule automatically increases the security of its associated account, overestimating the level of security that passwords with special characters can provide (Ur et al., 2016). Common strategies users employ include adding numbers and special characters after simple phrases found in the dictionary and substituting letters with special characters (Shay et al., 2010; Ur et al., 2015; Wash, Rader, Berman, & Wellmer, 2016). Passwords following a similar pattern are highly predictable for many password-cracking tools used for brute force attacks, such as l0phftcrack5 used in the study conducted by Vu et al. (2015). In this case, creating a password that satisfies the complexity rule could lead to cracking a password in a short period of time.

Memory and Passwords

In the current processes of password generation, there seems to be a tradeoff between memorability and the high level of security required by various websites. It is

important to first discuss what makes a concept memorable and easy to retrieve for people. Craik & Lockhart (1972) demonstrated that "deeper" information processing tends to be more memorable for individuals, which is accomplished through meaningful semantic and elaborative encoding. These information-processing techniques rely on prior knowledge that facilitates associations between concepts. In the case of password generation by users, this is often reflected through their strategy of incorporating names, meaningful dates, and other personal information into the passwords. By using information that they are already familiar with, users need not remember new information; they can simply reinforce an existing association in their semantic network to aid password retrieval for a specific account (Craik & Lockhard, 1972). Similarly, reusing passwords also increases memorability. Ebbinghaus (1913) well-known experiment on memory and nonsense syllables demonstrated the concept of repeated practice leading to more rapid retrieval. When users enter their passwords multiple times for different accounts, they are frequently retrieving the same string of characters, making that password easier to remember. Newell & Rosenbloom (1981) later related this concept to the "power law of learning," stating that although repeated learning could facilitate long term memory retention, there is an equilibrium after a certain amount of repetitions.

Interference often poses difficulties in day-to-day information encoding and retrieval. There are two types of interference: proactive and retroactive interference. Proactive interference is the tendency of previously learned information to block the retrieval of newly learned information (Anderson, 1981), which might occur when users

are asked to retrieve a new password but enter an old password instead. Retroactive interference is the tendency of newly learned information to block the retrieval of previously learned information (Anderson, 1981). In password retrieval, this would occur in instances such as users having a hard time remembering an old password for a seldom used account after updating to new versions of the password for more frequently used accounts. Both proactive and retroactive interference could cause users to forget the correct passwords during the retrieval process. When users forget their passwords and are given another attempt, they may use plausible retrieval to try to guess the correct password. Collins and Michalski (1989) defined plausible retrieval as an inference of typical patterns. Users entering a variation of a more frequently used password during the second attempt is an example of plausible retrieval. Also, users may rely on the heuristics and strategies they have developed over the years for password generation.

With complex requirements for password generation implemented on many websites, many users have developed standardized strategies to help with password retrieval. Besides using a standardized format for password generation, such as placing numbers and special characters in specific locations, users also manage their passwords using various methods. The level of memorability of passwords directly influences the ways users store their passwords (Choong, 2014). Some coping strategies include password reuse, password documentation on physical or digital storage, and password sharing, with password reuse being the most common (Shay et al., 2010). Several types of passwords are most commonly seen in password reuse, including passwords for

frequently used accounts and passwords users perceive to be strong, which often comply with the complexity rule (Wash et al., 2016).

Password Strength and Composition Requirements

As the National Institute of Standards and Technology (2017) recently proposed, a strong password should not be limited to the complex composition requirement many websites currently utilize. Instead, minimum length should be implemented along with increased characters for users to choose from, which could include increasingly popular emoji characters. However, despite NIST's suggestions, many websites continue to use standards they believe are secure. This is shown in the variance of password composition requirements across the Internet.

To understand what makes a strong password, one can consider the time password-cracking software takes to guess a password as a measurement. Using a brute force attack, hackers can try billions of combinations in a few seconds and find the correct password (Ur et al., 2016). Since this type of attack relies on combinations of characters, it is suggested that the longer a password is, the more time software would take to crack it. With this approach, the type of characters included in a password becomes less significant, and password length plays a larger role in password security. Ur et al. (2016) also highlighted that although users perceived passwords with numbers or special characters as high security passwords, those without such characters can be just as secure. For example, the researchers compared "astley123" with "asetleyabc" in both actual and perceived strength. They found that while the second password was a billion

times more difficult to crack than the second password, most users perceived both passwords having equally low security.

With the increased proposal of creating longer passwords, Stanton and Greene (2014) studied passwords of various character lengths with the complexity rule implemented. They found that longer passwords took more time to retrieve and were more prone to errors during the recall phase. Common errors included mistakes in capitalizing letters and using wrong character substitutions. However, the researchers did not test whether the same effect would be observed in longer passwords that did not follow the complexity rule. It is likely that the errors made in their study would be greatly reduced.

Purpose of the Study

Although past research has investigated relationships between various complex password composition requirements and memorability, there is a lack of research that looks at simple password composition requirements as suggested by NIST's latest proposal. In addition, despite increased outreach on how to create high security passwords, users continue to utilize strategies that favor memorability and weaken account security. This study aimed to explore the factors that past research speculated to influence password memorability. I manipulated password composition requirements on three different levels and looked at users' password management and storage strategies along with password memorability.

Hypotheses

Memory.

There are three hypotheses in relation to memorability of a password in this study.

Hypothesis 1. When the only composition requirement is a minimum length, shorter passwords will be better remembered than longer passwords.

Hypothesis 2. When the minimum length between two passwords is the same, passwords without special character requirements will be better remembered than passwords with the requirements.

Hypothesis 3. Long passwords without special character composition requirements will be better remembered than short passwords with such composition requirements.

Subjective opinions.

There are three hypotheses in relation to memorability and password strength in this study, looking solely at users' ratings on passwords generated from different password composition requirements.

Hypothesis 4. Passwords with special character requirements will be rated as more annoying to generate than passwords without those requirements.

Hypothesis 5. Passwords with special character requirements will be rated as more difficult to remember than passwords without those requirements.

Hypothesis 6. Passwords with special character requirements will be rated as more secure than passwords without those requirements.

Method

Participants

Undergraduate student participants from San Jose State University were recruited through the SONA system and completed the study in exchange for partial course credit. Of the 182 participants, 14 were excluded from the final analysis because they did not complete the memory recall test, or they missed two or all three of the catch questions in the self-reported questionnaire. The age of participants ranged from 18 to 32 years old, with an average of 19.4 years old, a 1.79 year standard deviation. Participants were from diverse racial and ethnic backgrounds; 58 participants were male, 109 were female, and one did not wish to answer.

Study Design

This study was a within-subject design conducted through Qualtrics and was divided into two parts: password generation and recall, and a self-reported survey. The independent variables I was interested in investigating were password composition requirements, particularly their length and special character requirements. There were three conditions in this study for password memorability. The first condition was a password composition requirement with the following criteria: (1) one upper case; (2) one lower case; (3) one special character; (4) one number, and; (5) at least 8 characters in length. The second condition was a password composition requirement with the following criteria: at least 8 characters in length. The third condition was a password composition requirement with the following criteria: at least 15 characters in length.

Participants received all three password requirement conditions in their survey. The answers from the password recall task were compared to the answers from the password self-generation task. The dependent variables of this study included memorability of passwords generated under each composition requirement and attitudes toward the requirements themselves. Other information related to users' password handling and composition strategies was also collected. All participants received a set of identical questionnaires asking for these strategies. These questions were answered through multiple choice and checkbox responses. No short answers were allowed.

Memory recall test.

There were two parts of a memory recall test in this study. The first part asked participants to self-generate three passwords. The participants were told to create new passwords for this study and not to document them anywhere throughout the study. However, they were not told other details, such as whether they could reuse the passwords created in condition one for condition two. They were also told to not include any identifying information in the passwords they generated. Then, participants were distracted by a self-reported survey for about five minutes. The second phase was the retrieval test. Participants were asked to recall the passwords they generated in the first phase, and were prompted with the password composition requirements. A password was considered memorable if the participants recalled all characters, including the order of the characters, correctly. Hypotheses 1, 2, and 3 were tested using this measure.

Self-reported survey.

The second part of the study involved a self-reported survey that aimed to collect subjective data, including regular Internet usage, attitudes toward password security and password composition requirements, and strategies for password handling and storage. Questions on strategies for password handling and storage were adapted from Shay et al. (2010), with an addition of the answer option "others" in one of the questions on password storage (see Appendix A for full questionnaire). Self-reported rating scales on attitudes toward password composition requirements were also adapted from Shay et al. (2010), with one additional statement added to the scale: "A password that follows the requirement above is easy for me to memorize." The same rating scale was used for three different password composition requirements, allowing the researchers to compare subjective ratings across all three conditions. Examples of statements on the self-reported rating scale include: "With the password requirement above, my account is more secured," "Creating a password that meets the requirement above is annoying," and "The requirement above is worth the effort of creating/remembering/using it because of its added protection." Hypotheses 4, 5, and 6 were tested using this measure.

Procedure

Participants were redirected to a Qualtrics Survey from SONA to complete the informed consent procedure. After the completion of the forms, participants were asked to create three different passwords according to the three different password composition requirements. They were told to not include identifying information or reuse current passwords, and were asked to memorize the passwords without documenting them

anywhere throughout the study. Participants then completed a series of questionnaires and self-reported rating scales on various topics related to passwords. These topics included password management, strategies to generate a password, and attitudes toward three different password composition requirements. Finally, participants were asked to recall the passwords generated at the beginning of the study and type them in textboxes provided on the survey. The study concluded with a debriefing paragraph.

Results

Password Memorability

A one-way within-subjects analysis of variance (ANOVA) was conducted to compare the effect of complexity of password composition requirements on password memorability when users self-generated their passwords. The three levels of complexity included a short and simple password, a short and complex password, and a long and simple password. The results did not reveal significant differences between the three conditions, $F(2, 166) = .248$, $p = .781$. This means that the levels of required password complexity had no significant influence on users' memory when recalling a password they had previously generated.

The means and standard deviations among the three conditions did not show significant differences, M = .815, SD = .030 for long and simple passwords, M = .804, SD = .031 for short and complex passwords, and M = .792, SD = .031for short and simple passwords.

Hypotheses 1, 2, and 3 were tested on password memorability across the three different conditions. Due to no difference between these conditions, none of the three

hypotheses were supported. Variances in composition requirements of minimum lengths and special character requirements did not make a password more memorable for users.

Password Attitudes

A one-way within-subjects ANOVA was conducted to evaluate users' attitudes of required password complexity. There were significant differences between the three levels of complexity, $F(2, 165) = 109.45$, $p = .001$. Post-hoc tests revealed a significant difference between scores for a short and simple password ($M = 2.38$, $SD = .081$) and a short and complex password ($M = 3.70$, $SD = .075$), and between scores for a short and simple password and a long and simple password ($M = 3.88$, $SD = .080$), such that a short and simple password was rated as significantly less annoying than either of the other two password types (Figure 1). No significant difference was found between a short and complex password and a long and simple password.

Hypothesis 4 was supported, in which passwords with special character requirements were rated as more annoying to generate than passwords without those requirements. However, this hypothesis was supported only when both passwords were the minimum length in the study.

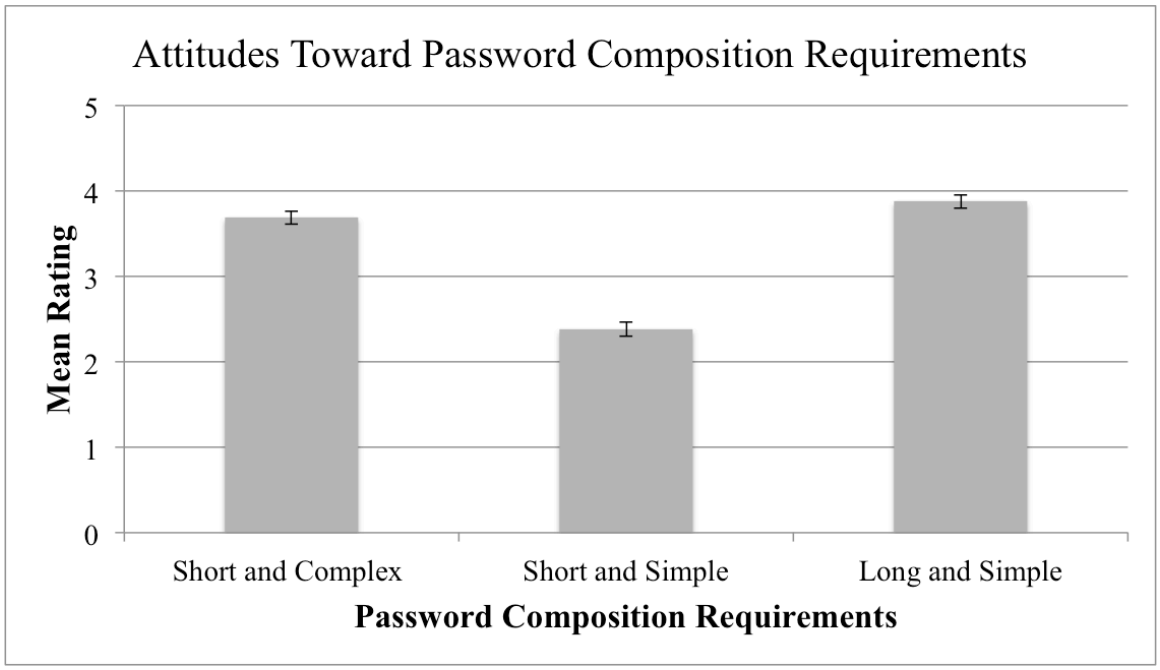

Figure 1. Mean scores and standard errors of password attitudes toward password composition requirements. Participants rated the statement of "Creating a password that meets the requirement above is annoying" on a scale of 1 to 5, with 1 being strongly disagree and 5 being strongly agree. Participants rated a long and simple password as the most annoying to create. Error bars indicate standard errors of the means.

Perceived Memorability

A one-way within-subjects ANOVA was conducted to compare the effect of required password complexity on users' attitudes on memorability toward generating a password that satisfies a requirement. There were significant differences between the three different levels of complexity, $F(2, 165) = 75.60$, $p = .001$. Post-hoc tests revealed a significant difference between scores for a short and simple password ($M = 3.83$, $SD = .077$) and a short and complex password ($M = 2.88$, $SD = .081$), between scores for a short and simple password and a long and simple password ($M = 2.65$, $SD = .085$), and

between scores for a short and complex password and a long and simple password, such that short and simple passwords were rated as being significantly more memorable than the other two password types (Figure 2).

Hypothesis 5 was supported, in which passwords with special character requirements were rated as more difficult to remember than passwords without those requirements. This hypothesis was supported regardless of the differences in requirements for minimum lengths.

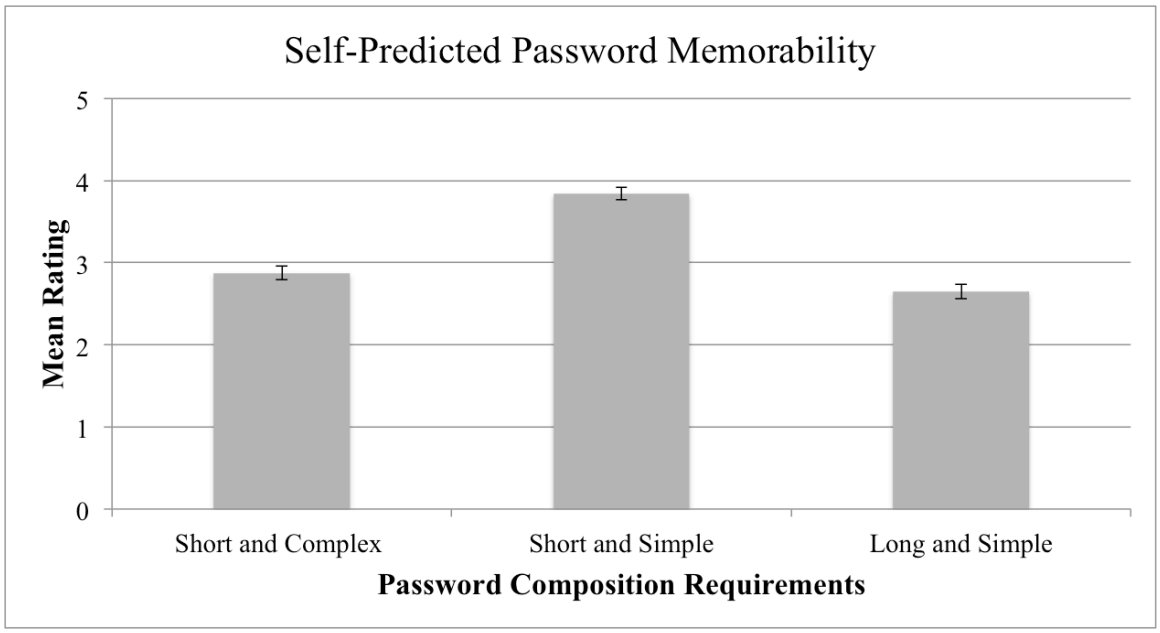

Figure 2. Mean scores and standard errors of participants' self-predicted memorability of passwords generated under different password composition requirements. Participants rated the statement of "A password that follows the requirement above is easy for me to memorize." Participants rated a short and simple password as the easiest to memorize. Error bars indicate standard errors of the means.

Perceived Account Security

A one-way within-subjects ANOVA was conducted to compare the effect of required password complexity on users' attitudes on account security. There were significant differences between the three levels of complexity, $F(2, 165) = 95.41$, $p = .001$. Post-hoc tests revealed a significant difference between scores for a short and simple password ($M = 2.81$, $SD = .083$) and a short and complex password ($M = 4.13$, $SD = .062$), between scores for a short and simple password and a long and simple password ($M = 3.67$, $SD = .078$), and between scores for a short and complex password and a long and simple password, such that short and simple passwords were rated as being significantly less secure than the other two password types (Figure 3).

Hypothesis 6 was supported in which passwords with special character requirements were rated as more secure than passwords without those requirements. This hypothesis was supported regardless of the differences in requirements for minimum lengths.

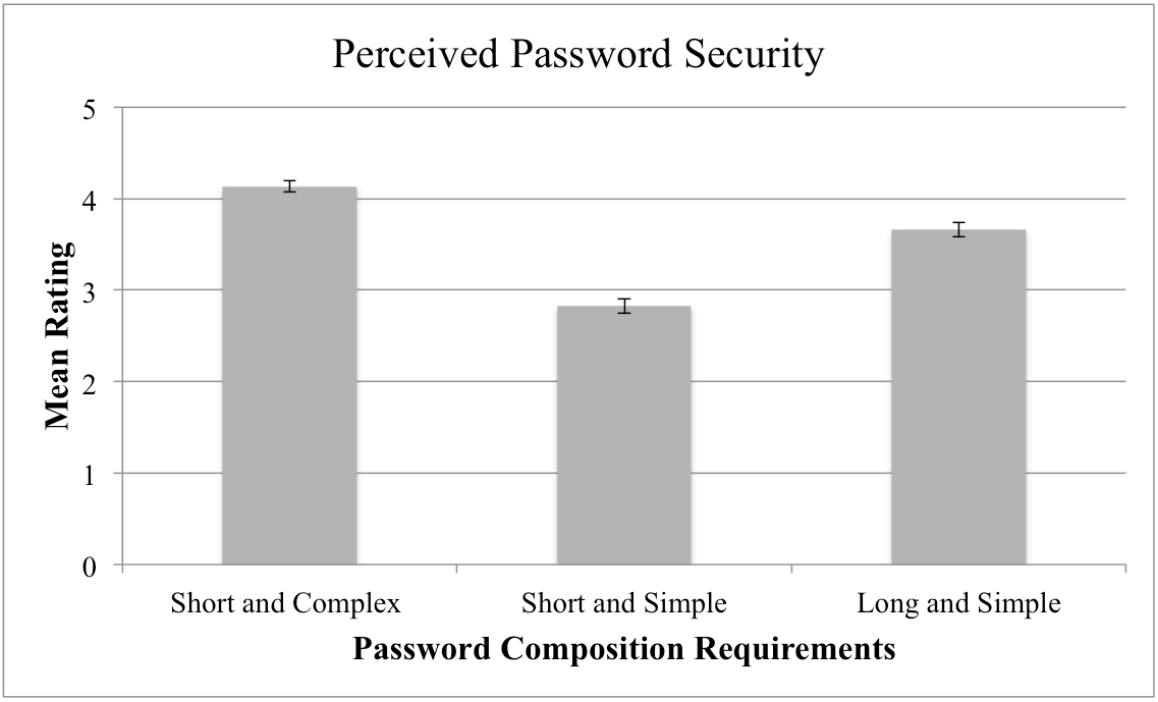

Figure 3. Mean scores and standard errors of participants' perceived security of accounts associated with different password composition requirements. Participants rated the statement of "With the password requirement above, my account is more secured." Participants rated a short and simple password as the least secure. Error bars indicate standard errors of the means.

Other Data on Password Generation and Composition

Password reuse and modification.

A frequency analysis was conducted to collect percentages of self-report answers on password generation strategies (Figure 4). One hundred and fifty-one of 168 participants (89.9%) reported that they had a set of passwords they reuse in different places. One hundred and thirty-two of 168 participants (78.6%) reported that they had a

password that they use for different accounts with slight modifications for each account. One response was missing for the question on password modification.

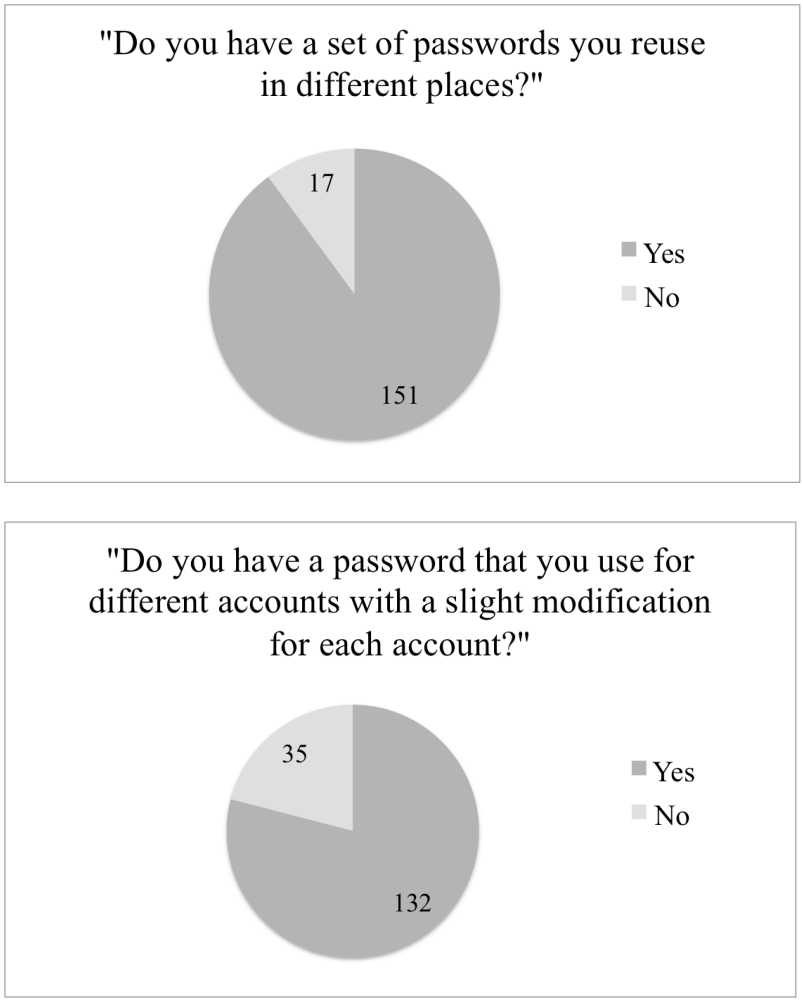

Figure 4. Participants' responses on password reuse and modification behaviors. Participants were given two choices when asked if they had a set of passwords they reused or modified for different accounts. The darker shade of color indicates "yes" as a response, and the lighter color represents the remaining responses for "no." The numbers on the graph represent the total responses for that option.

When asked more specifically about password generation strategies, participants were given the options of "reuse an old password from another account," "modify an old password from another account," "modify an old password from the same account," "create an entirely new password," and "other." Seventy-three of 168 participants (43.5%) chose the first option, sixty-six (39.3%) chose the second option, ten (6%) chose the third option, eighteen (10.7%) chose the fourth option, and there was one participant who responded with "other" (Figure 5).

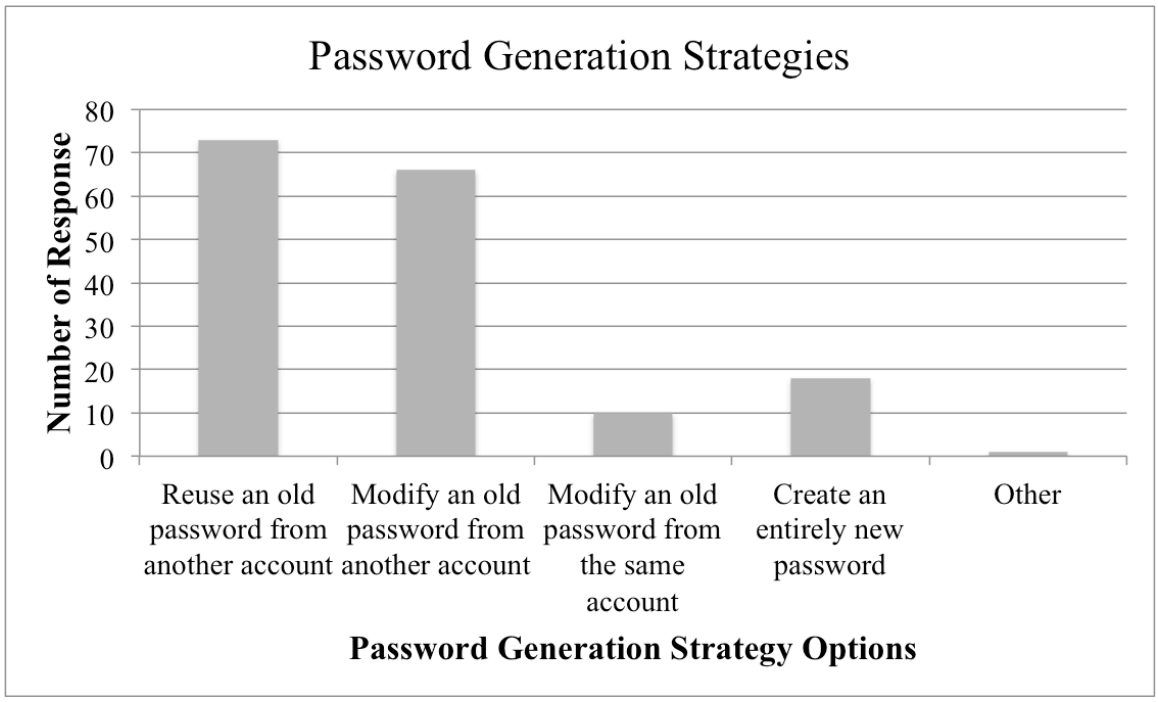

Figure 5. Frequency of password generation strategies. The y-axis indicates the total number of responses for each answer option when participants were asked if they had a set of passwords they modified for different accounts. Participants self-reported the answers shown in this graph.

Password composition strategies.

When asked about specific strategies for password composition, which included the use of letters, numbers, and special characters, participants were given 11 different options (see Figure 6 for detailed description of all 11 options). The option chosen the most was creating a password "based on a name of someone or something", with 114 of 168 participants (67.8%) choosing this option. The next most popular option was creating a password "based on a word or name with number or symbols added to the beginning or end", with 87 participants (51.8%) selecting this option. A complete graph of all responses compared to the findings of Shay et al. (2010) can be found in Figure 6.

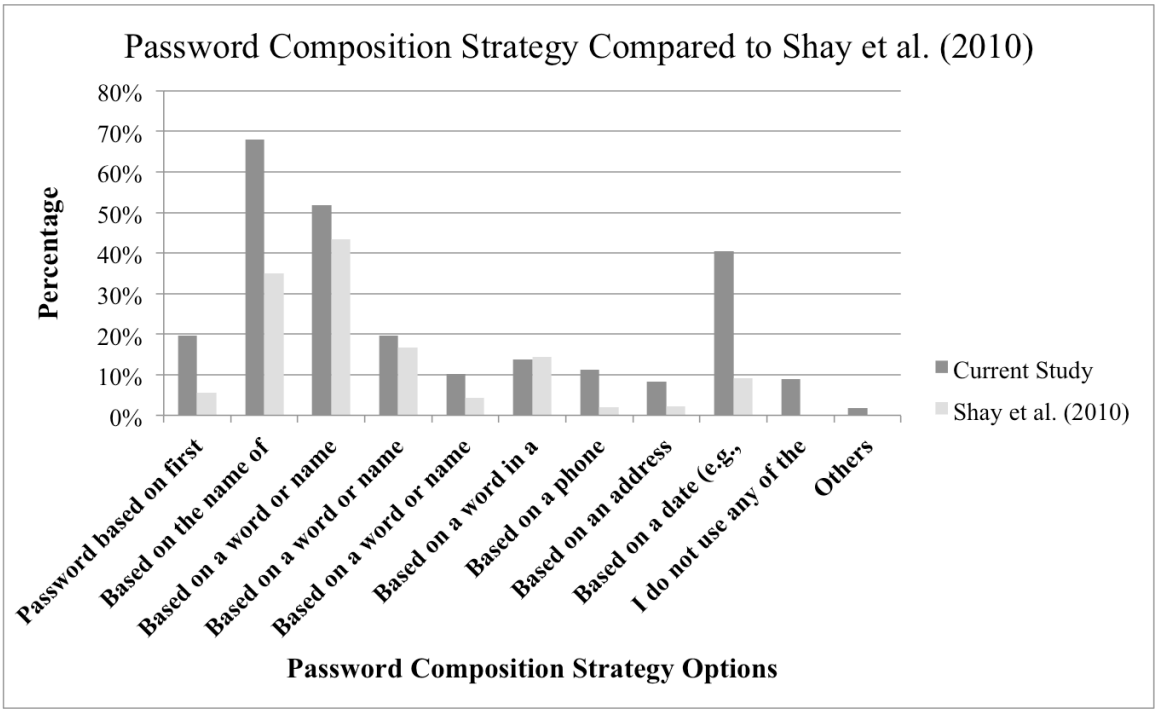

Figure 6. Participants' responses on password composition strategy compared to Shay et al. (2010). The darker shade of color represents the results from the current study, and the lighter shade of color represents the results from Shay et al. (2010). For full question with all 11 options, refer to Appendix A.

Discussion

The goal of this study was to investigate the effects of different password composition requirements on users' password memorability, users' general attitudes on simple and complex composition requirements, perceived memorability, and perceived security. I was also interested in exploring strategies users employ in everyday life when creating passwords. Memory recall test and self-reported questionnaire were used in this study.

Overview of the Findings

Memorability.

Statistical test results showed that none of the hypotheses on password memorability were supported by the research findings. Therefore, this study was unable to support prior research that suggested a password without complex composition requirements is more memorable than a password with complex composition. The memory recall test showed that the levels of required password complexity do not affect users' memory of passwords. When looking at the means, the test revealed that users could remember passwords they generate by themselves relatively well regardless of the variances of composition requirements. However, no further conclusion can be made regarding the memorability of passwords in relation to password composition requirements.

Subjective opinions.

In contrast to password memorability, statistical test results showed that all hypotheses on users' subjective opinions were supported by the research findings. Similar to Shay et al (2010), participants found that a complex password composition requirement was annoying. Participants rated a long and simple password as the most annoying to create, a short and complex password as second most annoying, and a short and simple password as the least annoying.

Shay et al (2010) found that participants typically rated a short and complex password as difficult to recall at later. This study found similar results, but participants generally perceived a long and simple password as more difficult to remember than a

short and complex one. Participants rated a short and simple password as the easiest to remember.

When looking at participants' perceived account security associated with each of the password composition requirements, participants believed that a short and complex password was the strongest and most secure, followed by a long and simple password. In general, participants disagreed that their accounts would be secure with a short and simple password.

Password reuse and modification.

A majority of participants reported the tendency to reuse passwords with slight modifications, and I had more participants reporting reusing and modifying passwords than Shay et al. (2010), but the results were mostly consistent with their findings of widespread password reuse (81%) and password modification (59.8%).

Password composition strategies.

Over half of the participants reported using names or dictionary words as a basis for creating a new password, supporting findings by Ur et al. (2015), who suggested users rely on familiar information to create memorable passwords. Participants also reported attaching numbers and symbols only in the beginning or the end of the phrase when creating new passwords. This finding was consistent with previous research on users' strategies for complying with complex password composition requirements (Shay et al, 2010)

Implications of the Findings

Although the study did not detect any differences in password memorability between the three conditions, comparing the perceived memorability and the results from the memorability test allowed us to make an interesting observation. Participants had equally good memory for passwords that were generated under all three conditions, but when they were asked to rate password memorability, there were significant differences in their subjective opinions. They perceived that a long password would be the most difficult to remember for future recall. Yet, the memory recall test showed that a long password was just as memorable as a short and simple password, which participants rated as easy to remember.

Given that password complexity requirements did not influence actual password memorability, other possible factors may be contributing to users' behaviors in password handling and users' tendency to forget passwords. These factors may include the number of passwords users must retain in their memory and how frequently they retrieve the passwords. However, if memorability is not a critical factor that determines which composition requirement is better for users, then password strength should be the major considering factor when companies determine which password composition requirement to implement in the future. As NIST (2017) suggested, a long password with or without complex symbols can be more secure and difficult for software to crack than many passwords users create nowadays. Therefore, companies should implement a password composition requirement that is simple (i.e., not requiring numbers and special characters) and requires only a minimum length that is reasonably long.

The finding that participants perceived a short and complex password as more secure than the long and simple password indicates that users have misconceptions about strong passwords. Many of them believed that a password with numbers and special characters automatically increases the security of the account associated with the password. Although they generally acknowledged that a longer password was better than a shorter password, they did not perceive it being more secure than a shorter one with numbers and special characters. Their misconceptions of strong passwords were also shown in their self-report questionnaires, in which many of them utilized the predictable strategy of adding numbers and symbols to the beginning or end of their passwords. These predictable strategies can increase the chance of having a password guessed by software or a hacker. The questionnaire also revealed that many users did not practice safe password generating and handling behaviors. They showed perceived memorability as more important than what truly makes a high security password. Although it is understandable that users put memorability as the top priority for future account access, this study showed evidence that more education and clarification is needed to ensure users understand what constitutes a strong password. Users should be encouraged to refer to examples of high security passwords and to password management software that negates the need to remember individual passwords.

Looking at the raw data of the passwords generated by users, the study showed that users continued to apply the same strategies of a complex composition rule to situations without such requirements. For example, 178 of the 336 passwords generated under simple password requirements contained numbers or special characters. This

indicates that users likely already have templates they typically follow when generating passwords. Even though users express some amount of concern for Internet security, they often do not take the time to ensure they have strong passwords to protect their sensitive data from hackers. They rely on heuristics to create memorable passwords and have password reuse behaviors. Perhaps it is time to consider other options that can help reduce users' cognitive load, such as the use of a password manager.

Limitations

There were several limitations to this study. First, the significant findings of this study relied solely on self-reported data. This could have contributed to the statistical differences found in this study instead of true differences. Also, the memory recall test had a delay of 5 to 15 minutes, at most. Baddley and Hitch (1974) suggested the theory of working memory, in which people can manipulate short-term memory and retain it through constant rehearsal. This concept could be a contributor to the high recall accuracy shown in this study. It would be more ideal for studies such as this one to have a longer delay. However, due to anonymity of participants, this study could not contain a long delay, where the study would be performed in multiple parts. In addition, the delay did not truly simulate a real-life scenario. An improved study design would involve asking participants to create multiple additional passwords between the password generation phase and the recall phase.

The greatest limitation to this study was the study environment. The entire study was conducted online using Qualtrics, including the memory recall test. This means that the researcher was unable to monitor participants' behaviors during the password

generation phase, leaving the participants to potentially document the passwords elsewhere. As suggested by the research on password handling strategies (Shay et al., 2010; Choong, 2014), it was possible that participants recorded the data on paper or stored them on their computers before performing the recall test. If this were the case, the non-significant differences but high mean values in the statistical analysis could be a false negative.

Finally, it is common to see websites with complex composition requirements for password generation. Participants might have already developed strategies and habits to create and remember short and complex passwords. Compared to long and simple passwords, participants might have been more familiar with creating passwords that satisfied the complex rules, which led them to perceive that the new composition requirement would be more annoying, difficult to remember, and less secure than the more typically seen requirement.

Future Research

To further explore how companies can facilitate the security of sensitive data, future research should focus on more than just password composition requirements. Other factors should be taken into consideration, including the number of passwords users have to retain and retrieve when generating a new password or recalling an old one. Two future steps for this study are to increase the delay between generation and free recall and to have participants complete the study in person. Another factor to add to future study design would be to increase the number of passwords participants remember throughout the study, thereby creating a scenario that better simulates real life situations.

Password managers may be a solution for the future of text-based authentication. Instead of remembering many different passwords, users store all passwords in a secure location that is encrypted and protected with a master password, or another form of authentication. This method can reduce the cognitive load in users greatly, but it also increases the time consumed for maintenance in password handling. However, this method is not as commonly used as purely relying on memorization for password storage.

Although password memorability was not affected by password composition requirements, participants perceived them differently. Also, it was revealed that users remembered passwords better than the research previously suggested, as shown in the high accuracy in the recall task across all participants in all three conditions. The research findings were unable to explain why users have the tendency to forget passwords, but other factors could be involved. While the technological industry constantly tries to find innovative and more secure ways to protect sensitive data on the Internet, more research needs to focus on facilitating password composition and management in all users.

References

AlFayyadh, B., Thorshiem, P., Josang, A., & Klevjer, H. (2012). Improving usability of password management with standardized password policies. *Proceedings of the Seventh Conference on Network and Information Systems Security.* Cabourg, France.

Anderson, J. (1981). Interference: the relationship between response latency and response accuracy. *Journal of Experimental Psychology: Human Learning and Memory, 7*, 311-325.

Baddeley, A. D., & Hitch, G. (1974). Working memory. *Recent Advances in Learning and Motivation, 8*, 47–90. New York, NY.

Choong, Y. (2014). A Cognitive-Behavioral Framework of User Password Management Lifecycle. *Lecture Notes in Computer Science Human Aspects of Information Security, Privacy, and Trust*, 127-137.

Collins, A. & Michalski, R. (1989). The logic of plausible reasoning: A core theory. *Cognitive Science, 13*, 1-49.

Craik, F. I. M., & Lockhart, R. S. (1972). Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal Behavior, 11,* 671-684.

Ebbinghaus, H. (1913). *Memory: a contribution to experimental psychology*. New York, NY: Columbia University.

Grassy, P. A., Garcia, M. E., & Fenton, J. L. National of Institute of Standards and Technology. (2017). *Draft NIST Special Publication 800-63-3 Digital Identity Guidelines.*

Kissel, R. National of Institute of Standards and Technology. (2013) *Glossary of Key Information Security Terms*. Gaithersburg, MD.

Newell, A., & Rosenbloom, P. S. (1981). Mechanisms of skill acquisition and the law of practice. In J.R. Anderson (Ed.), *Cognitive Skills and Their Acquisition* (pp. 1-55). Hillsdale, NJ: Erlbaum.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., & Cranor, L. F. (2010). Encountering stronger password requirements. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*.

Stanton, B. C., & Greene, K. K. (2014). Character strings, memory and passwords: What a recall study can tell us. *Lecture Notes in Computer Science Human Aspects of Information Security, Privacy, and Trust,* 195-206.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N., Cranor, L. F. (2015). "I added '!' at the end to make it secure": Observing password creation in the lab. *Proceedings from Symposium on Usable Privacy and Security 2015*. Ottawa, Canada.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality? *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. San Jose, CA.

Vu, K. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B., Cook, J. & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(2007), 744-757.

Wash, R., Rader, E., Berman, R. & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. *Proceedings from Symposium on Usable Privacy and Security 2016*. Denver, CO.

Wheeler, D. (2012, April 10). Zxcvbn: realistic password strength estimation [Web log post]. Retrieved from https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation/

Appendix A

Create a password based on the following criteria for a new account. Try your best to memorize this password for the remaining of this survey and do not document this password anywhere, including writing it down or typing it elsewhere.

Remember that this password should **NOT** contain any part of your current passwords, identifying information, and you should **NOT** reuse this password in the future.

Your password must contain at least:
One upper case letter
One lower case letter
One special character
One number
Must be at least 8 characters in length

_____

Create a password based on the following criteria for a new account. Try your best to memorize this password for the remaining of this survey and do not document this password anywhere, including writing it down or typing it elsewhere.

Remember that this password should **NOT** contain any part of your current passwords, identifying information, and you should **NOT** reuse this password in the future.

Your password must contain at least:
Must be at least 8 characters in length

_____

Create a password based on the following criteria for a new account. Try your best to memorize this password for the remaining of this survey and do not document this password anywhere, including writing it down or typing it elsewhere.

Remember that this password should **NOT** contain any part of your current passwords, identifying information, and you should **NOT** reuse this password in the future.

Your password must contain at least:
Must be at least 15 characters in length

_____

Demographic Questions:

1. How old are you?
   _____

2. What is your gender?
   a. Male
   b. Female
   c. Other: _____
   d. I prefer not to answer.

3. On average, how often do you use the Internet on a daily basis?

Never	Seldom	Sometimes	Often	Always
1	2	3	4	5

4. How concerned are you on Internet or online account security? (This includes bank, school, online gamin, and social media accounts.)

Not at all	Slightly	Somewhat	Very	Extremely
1	2	3	4	5

The following questions will be about your current passwords. Read the following questions carefully before selecting or entering your answers.

5. On average, how often do you use the "remember me" option when you log in to an account?

Never	Seldom	Sometimes	Often	Always
1	2	3	4	5

6. Do you use password manager?
    a. Yes
    b. No
    c. I do not know what a password manager is.

7. Select all that apply. What do you do to store a newly created password?
    a. Write it down
    b. Type it up in another document
    c. Share it with someone else
    d. Use a password manager
    e. Other: _____
    f. I do not physically store my passwords (i.e., I memorize it)

8. For passwords that are not required to be changed regularly, how often do you change your passwords?
    a. Daily
    b. Weekly
    c. Monthly
    d. Every Three Months
    e. Every Six Months
    f. Yearly
    g. Never

9. Do you have a set of passwords you reuse in different places?
    a. Yes
    b. No

10. Do you have a password that you use for different accounts with a slight modification for each account?
    a. Yes
    b. No

11. In a given month, on average, how many times do you forget your password when you are asked to log in to an account?
    a. 0

b. 1-2
c. 3-4
d. More than 5

12. What do you usually do when you are asked to create a password?
    a. Reuse an old password from another account
    b. Modify old password from anther account
    c. Modify old password from the same account
    d. Create an entirely new password
    e. Other: _____

13. Select all that apply. What strategy do you usually use when you are asked to create a password?
    a. Password based on first letter of each word in a phrase
    b. Based on the name of someone or something
    c. Based on a word or name with number OR symbols added to the beginning or end
    d. Based on a word or name with numbers AND symbols substituting for some of the letters (e.g., "@" instead of "a")
    e. Based on a word or name with letters missing
    f. Based on a word in a language other than English
    g. Based on a phone number
    h. Based on an address
    i. Based on a date (e.g., birthday, anniversary, graduation date)
    j. I do not use any of the strategies listed above
    k. Others: _____

Please give a rating for the extent to which you agree or disagree with the following statements, based on these password requirements:

Your password must contain at least:
One upper case letter
One lower case letter
One special character
One number
Must be at least 8 characters in length

1. With the password requirement above, my account is more secure.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

2. Creating a password that meets the requirement above is annoying.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

3. Creating a password that meets the requirement above is difficult.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

4. Creating a password that meets the requirement above is fun.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

5. The requirement above is worth the effort of creating/remembering/using it because of its added protection.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

6. A password that follows the requirement above is easy for me to memorize.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

Please give a rating for the extent to which you agree or disagree with the following statements, based on these password requirements:

Must be at least 8 characters in length

1. With the password requirement above, my account is more secured.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

2. Creating a password that meets the requirement above is annoying.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

3. Creating a password that meets the requirement above is difficult.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

4. Creating a password that meets the requirement above is fun.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

5. The requirement above is worth the effort of creating/remembering/using it because of its added protection.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

6. A password that follows the requirement above is easy for me to memorize.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

Please give a rating for the extent to which you agree or disagree with the following statements, based on these password requirements:

Must be at least 15 characters in length

1. With the password requirement above, my account is more secured.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

2. Creating a password that meets the requirement above is annoying.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

3. Creating a password that meets the requirement above is difficult.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

4. Creating a password that meets the requirement above is fun.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

5. The requirement above is worth the effort of creating/remembering/using it because of its added protection.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

6. A password that follows the requirement above is easy for me to memorize.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

Please recall the passwords you created at the beginning of this survey.

Your password must contain at least:
One upper case letter
One lower case letter
One special character
One number
Must be at least 8 characters in length

_____

Must be at least 8 characters in length

_____

Must be at least 15 characters in length

_____

Thank you for your time.