*Neuroergonomics and Cognitive Engineering,* Vol. 102, 2023, 203–213
https://doi.org/10.54941/ahfe1003020

# Remembering Passwords: The Role of Instructions

**Kim-Phuong L. Vu, Ha M. Nguyen, and Uyen Bui**

California State University Long Beach, Long Beach, CA 90840, USA

## ABSTRACT

Most users follow predictable patterns and create weak passwords because they are unaware how to generate strong, secure passwords (Ur et al., 2015). Yet, more secure, system-generated passwords tend to be more difficult to remember (Vu et al., 2003). The current study examined whether system-generated passwords could be made more memorable through use of different types of instructions that help the users associate text and/or images to the passwords or password components. Over 100 participants were asked to memorize three system-generated passwords for three fake accounts: bank, email and social media, either in a lab-based setting with a moderator or completely online. Participants were given no instructions, text-based instructions, image-based instructions, or a combination of both text and image-based instructions to help them understand and memorize each password. Participants were then asked to recall their password after no delay or a short delay. We found that users were able to remember complex system-generated passwords when provided with detailed text-based or image-based instructions to help the users map the password components to a structure. Our findings did not clearly show which instructional technique was better. Future studies should explore additional instructional techniques for password generation and memorization.

**Keywords:** Password memorability, System-generated passwords, Mnemonic techniques, Role of instructions

## INTRODUCTION

The username-password combination method remains the most widely used authentication method for online accounts, even though passwords are known to be less secure than biometrics, smart cards, and two-step verification, because of the method's simplicity and cost-effectiveness (Taneski et al., 2019; Wiedenbeck et al., 2005). Yet, reliance on text-based passwords can lead to issues surrounding the memorability of such passwords, as memorable passwords tend to be easy to guess or crack and more secure passwords tend to be more difficult to remember (Vu et al., 2003). Most self-generated passwords follow common trends and patterns, where special characters and numbers are placed at the end of a common word. Although companies have attempted to create crack-resistant passwords with password generators, the random letters and numbers are not meaningful to users, making the passwords difficult to remember. When users have difficulty remembering passwords, they may engage in risky password storage behaviors, such as writing them down or leaving written passwords on sticky notes next to their monitors (Adams & Sasse, 1999; Florencio & Herley, 2007).

The balance between memorability and security of passwords is known as the "password problem" (Wiedenbeck et al., 2005). The problem can be seen in user-generated passwords and system-generated passwords, as more memorable passwords tend to be less secure, while more secure passwords tend to be less memorable. Ideally, generated passwords should be both memorable and secure. Thus, if secure, system-generated passwords were organized more meaningfully, it may increase the memorability of those passwords. Training users on how to make system-generated passwords more memorable can result in their use of secure passwords without risky behaviors, such as writing down the passwords or reusing the same password for multiple accounts.

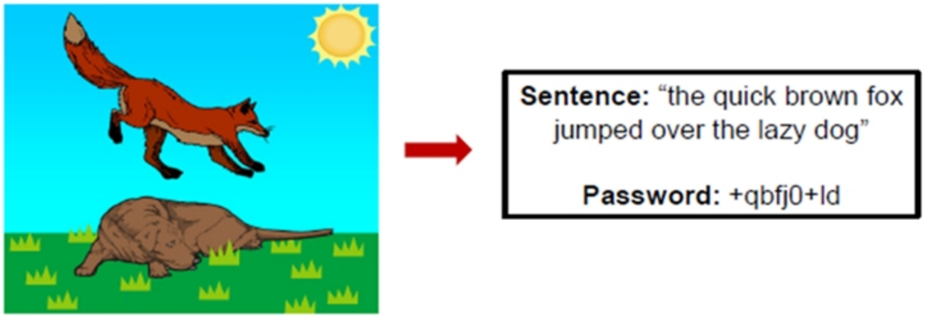
## Mnemonics and Password Techniques

Mnemonic devices are a common memory technique used to improve memory of information by organizing the to-be-remembered information in a meaningful structure (Bellezza, 1996). Mnemonic instructions have been used for password creation, with the first-letter mnemonic and whole-word passphrase (Carlson et al., 1981; Vu et al., 2007; Yan et al., 2004) being two common methods. The first-letter mnemonic is used when the user generates a sentence and takes the first letter of each word that then becomes the password, while the whole-word passphrases replace words or parts of words with special characters or numbers that are phonetically similar (Keith et al., 2007; Vu et al., 2007, see Table 1). Nelson and Vu (2010) additionally found that when text-based mnemonic techniques were paired with an image, users were able to generate more memorable passwords, which can be attributed to a picture superiority effect (Paivio et al., 1968). A combination of these techniques can also be used (see Figure 1 for an example).

Past research has also found that instructions and the examples given to participants when generating the mnemonic-based passwords can influence the memorability of the passwords. Yang et al. (2016) evaluated the effectiveness of six different variants of mnemonic strategies: (1) generic passphrase with a concrete example, (2) passphrase that emphasized personalization with a concrete example, (3) passphrase that emphasized personalization without a concrete example, (4) passphrase that emphasized personalization with several concrete examples, (5) passphrase that emphasized on personalization with several concrete and generic examples, and (6) passphrase with several personalized and concrete examples. Yang et al. found that using

**Table 1.** Examples of how the first-letter and whole-word passphrase for transforming the phrase "the quick brown fox jumped over the lazy dog" into a password.

| **Phrase: "the quick brown fox jumped over the lazy dog"** | |
|---|---|
| First-letter Mnemonic | tqbfjotld |
| Whole-word Passphrase | +heQBFjump0vr+lzyd0g |



**Sentence:** "the quick brown fox jumped over the lazy dog"

**Password:** +qbfj0+ld

**Figure 1:** Example of how an image can be paired with the first-letter mnemonic and passphrase technique for transforming the phrase "the quick brown fox jumped over the lazy dog" into the password, *+qbfj0+ld*.

generic examples resulted in weak passwords. However, the use of instructions that included both personalization emphasis and high-quality examples resulted in users generating more secure passwords. Thus, the instructions given to users are important to consider, and in the present study, we examined whether instructions could have an impact on the memorability of system-generated passwords.

## Current Study

Prior studies examined the role of instructions on the memorability and security of user-generated passwords (e.g., Nelson & Vu; 2010; Yang et al., 2016). Yet, another approach for use of secure passwords is to examine whether instructions can be used to help improve the memorability of system-generated passwords. We used two strategies for improving memory of the system-generated passwords: mnemonics and images. Four types of instructional conditions were examined:

1. **No Instructions:** Participants were not given any specific instructions to memorize their assigned passwords.
2. **Text-based Instructions:** Participants were given a combination of the first-letter and whole-word mnemonic instructions to memorize their assigned passwords.
3. **Image-based Instructions:** Participants were given instructions on how to relate the password to an image to memorize their assigned passwords.
4. **Combination of Text- and Image-based Instructions**: Participants were given both the text-based and image-based instructions to memorize their assigned passwords.

All system-generated passwords in the study met recommended proactive password checking restrictions: being at least eight characters, including one uppercase letter, one lowercase letter, one digit, and one special character. For the conditions with text-based instructions, image-based instructions, or both, participants were provided with detailed descriptions of the mnemonic technique. These descriptions were designed to help ensure that users were processing the password more deeply and relating parts of the password or image to the mnemonic structure provided. In addition, participants were given concrete examples and encouraged to use personalization. To increase ecological validity, we had users memorize passwords for three different accounts, testing them immediately after learning all of them and after a short, interrupted delay. We also examined whether there were any differences in whether the study was administered asynchronously online or in person with a moderator.

## METHOD

### Participants

A total of 108 participants (female = 80; male = 27, non-binary = 1) aged 18 to 27 years ($M = 18.92$, $SD = 1.57$) were recruited from Introductory Psychology courses at California State University, Long Beach to participate in the study, either fully online (n = 60) or in person (n = 48).

### Materials

The PsyToolKits program was used to administer the entire study. The platform was used to provide the instructions and tasks to the participant and record responses and response times (in milliseconds).

### Design

The study employed a 2 (Text Instructions: yes or no) x 2 (Image Instructions: yes or no) x 2 (Mode of Instruction: online or in-person) x 2 (Delay interval: no or short) mixed design. The factorial, between-subjects manipulation of the two variables, Text Instructions and Image Instructions, resulted in four conditions of no instructions, text-based instructions, image-based instructions, and both text- and image-based instructions. Delay Interval was manipulated within-subjects. Although we had three account types, we averaged the dependent measures across the accounts. The dependent measures included memorization time (in seconds), password recall time for accurate attempts (in seconds), the number of attempts to recall the passwords (up to three attempts), and the number of passwords forgotten (i.e., the participant was unable to enter the correct password within three attempts).

### Procedure

Study procedures were conducted in accordance with an approved protocol from our university's Institutional Review Board (IRB). Participants completed the study in a single session lasting 30–60 minutes. For the online mode, participants launched the web study by clicking on its URL and were presented with an electronic consent form. To consent to participate in the study, participants were asked to read the form and click on the "I agree" checkbox. Then, participants were tasked with memorizing unique system-generated passwords for fictional accounts (labelled bank, email, or social media).

Participants were told to take as much time as they needed to memorize each password based on the instructions for their specific condition. For example, in the text-based instructions condition, participants were given the following instructions:

> *Memorize the following password for the bank account: M@8egg$4B*
> *M@8egg$4B → "Matt ate eggs for breakfast"*

*At first glance, some passwords may look like random strings of letters and numbers. However, these passwords are actually organized meaningfully into mnemonic words or phrases. Additionally, personal meaning can be incorporated into the password. When examined more closely, the password "M@8egg$4B" can be remembered as the phrase "Matt ate eggs for breakfast." Since the two are phonetically similar, "Matt" can be transformed into "M@" which also incorporates the "@" special character. "Ate" and "8" are also phonetically similar and allows a person to incorporate a number into their password, making it more secure. The dollar sign "$" at the end of "egg$" looks similar to the letter "s" which makes "egg$" and "eggs" phonetically similar and incorporates a special character into the password. "4" and "for" are phonetically similar and incorporates a number, and "B" represents "breakfast" but utilizes a capital B to incorporate an uppercase letter.*

*A person typically eats breakfast, and eggs are a common breakfast food. This information can be easily made personally relevant by thinking of your family member or friend named "Matt" who ate eggs for breakfast this morning.*

Participants were also asked not to write the password down anywhere. After participants indicated that they have memorized the password for the first account, the procedure repeated for the remaining two accounts.

Then, participants were asked immediately to recall the passwords that they just memorized (i.e., no delay interval). Participants were informed that an account name would appear on the screen and they would have up to three attempts to correctly enter each password for that account. Following the no delay recall task, participants completed a filler task, consisting of simple math problems for 10 minutes. Subsequently, participants were asked to recall the passwords again in a randomized order. Finally, participants were asked to complete a post-experiment survey consisting of demographic questions and other survey items.

The in-person mode followed the same procedures as the online mode, but a researcher was present, and instructions were read aloud to the participant. Additionally, participants were allowed to ask the researcher for any clarifications regarding the purpose of the study, procedures, and instructions on how to navigate the experiment.

## RESULTS & DISCUSSION

### Memorization Time

The mean memorization times across the three accounts were averaged and submitted to a 2 (Text Instructions: yes or no) x 2 (Image Instructions: yes or no) x 2 (Mode of Instruction: online or in-person) ANOVA. Only the 3-way interaction was significant, $F(1,100) = 5.10$, $p = .026$, see Figure 2.

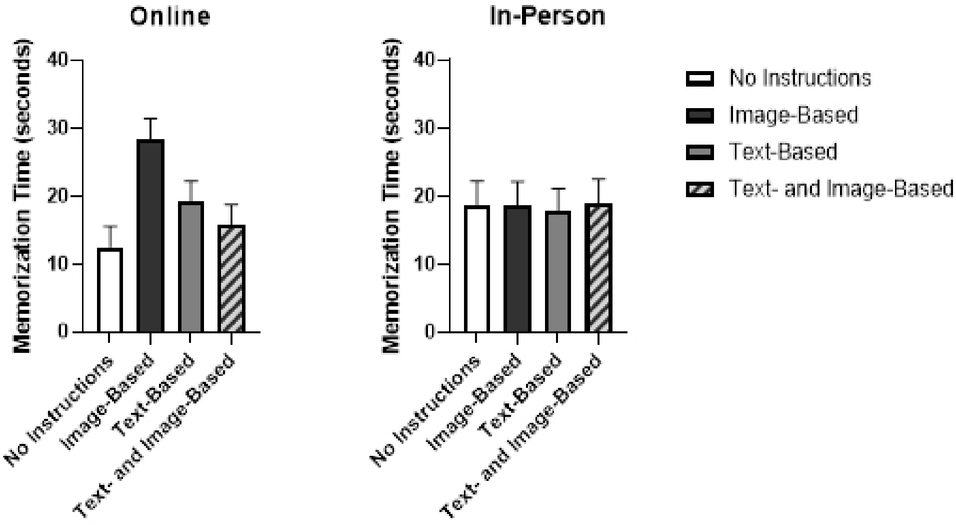


**Figure 2**: Mean memorization time (in seconds) for the four instructional conditions when the study was conducted online (left) or in-person (right).

Tests of simple effects showed that the Text Instructions x Image Instructions interaction was significant for the online mode, $F(1,56) = 6.14$, $p = 0.02$, where participants spent the most time memorizing passwords with image-based instructions ($M = 28.41$ s), intermediate amounts of time with text-based instructions ($M = 19.15$ s) and both text and image-based instructions ($M = 15.74$ s), and the least amount of time with no instructions ($M = 12.52$ s). There was no significant difference in memorization times between the four conditions for the in-person mode.

It is not surprising that the memorization time was shortest for the no instructions group when the study was conducted online because the instructions were short (e.g., "*Memorize the following password for the bank account: M@8egg$4B*". The participants did not have to read the detailed description on how to use the mnemonic or to personalize the information. Perhaps the participants in the no instructions group of the in-person mode spent a longer time to memorize the password because a moderator was present. For the in-person mode, the memorization time was similar for all conditions and was an intermediate value similar to the text-based and image- and text-based instructions for the online mode. Participants in the online mode spent much more time memorizing the password in the image-based instructions without the explanatory text. This longer time in the online mode likely reflects participants' trying to figure out how the image related to the password on their own. Whereas those participants receiving image-based instructions in the in-person mode could ask the experimenter for clarifications.

### Recall Time for Remembered Passwords

For the 88 participants who were able to recall all three passwords, mean recall time was submitted to a 2 (Text Instructions: yes or no) x 2 (Image

Instructions: yes or no) x 2 (Delay Interval: no or short) x 2 (Mode of Instruction: online or in-person) mixed ANOVA. There was a significant main effect of Delay, $F(1,80) = 4.47, p = .038$, where recall was faster after a short delay ($M$ = 16.8 s) than with no delay ($M$ = 20.0 s). The Delay x Mode of Instruction interaction was also significant, $F(1,80) = 7.96, p = .006$, see Figure 3. For the online mode, the difference between delay conditions was not significant, but for the in-person mode, participants were 7.42 s faster after a short delay than with no delay. For the in-person mode, the longer recall times at the short delay could be due to more effort required to recall the password with the moderator present in the room. However, once the participant was able to successfully recall the password, their memory for it was strengthened, decreasing the recall time at the short delay. This finding is consistent with that of Vu et al. (2007), who found that recall times were shorter at a week delay when the participant had to perform the same recall task shortly after generating their passwords. No other effects were significant.

## Number of Attempts and Forgetting

The average number of attempts participants took to enter each password across all three accounts was submitted to a 2 (Text Instructions: yes or no) x 2 (Image Instructions: yes or no) x 2 (Delay interval: no or short) x 2 (Mode of Instruction: online or in-person) mixed ANOVA. The main effect of Mode of Instruction was significant, $F(1,100) = 5.12$, $p = .026$, with participants taking more attempts to recall their password when the mode was in-person ($M$ = 2.09 attempts) than online ($M$ = 1.81 attempts). Mode of Instruction also had a significant 2-way interaction with Text-based Instructions, $F(1,100) = 6.20$, $p = .007$, see Figure 4. When the study was administered online, participants made fewer attempts if they were given text-based instructions compared to no text-based instructions. However, when the study was administered in person, there was no significant difference. Finally, there was a significant 3-way interaction of Mode of Instruction with Delay and Image Instructions, $F(1,100) = 6.00$, $p = .016$, see Figure 5. Follow-up analyses

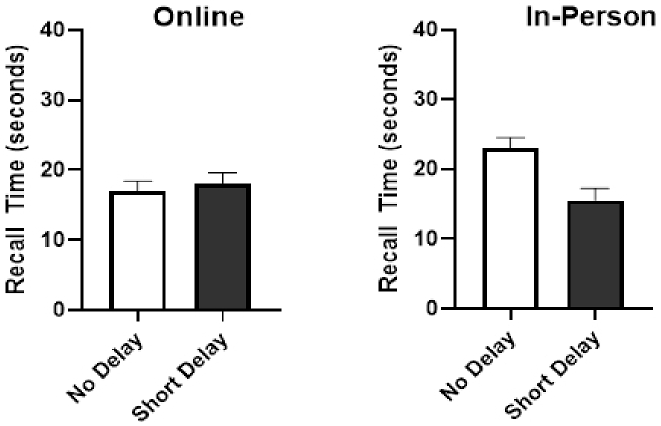


**Figure 3:** Mean accurate recall time (in seconds) after no delay and a 10-minute delay when the study was conducted online (left) or in-person (right).

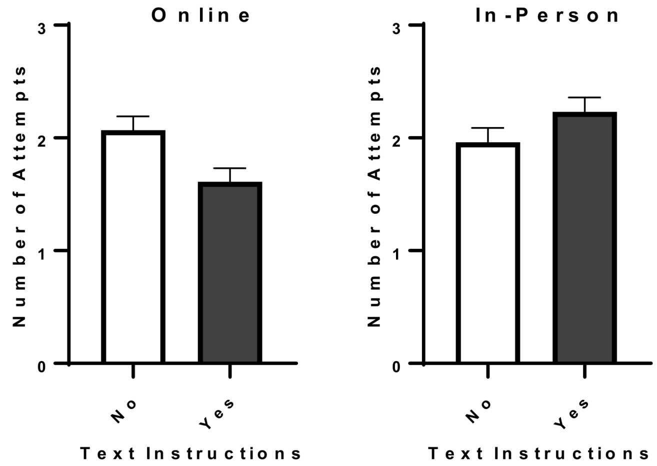


**Figure 4:** Average recall attempts when participants were given text instructions or no text instructions when the study was conducted online (left) or in-person (right).

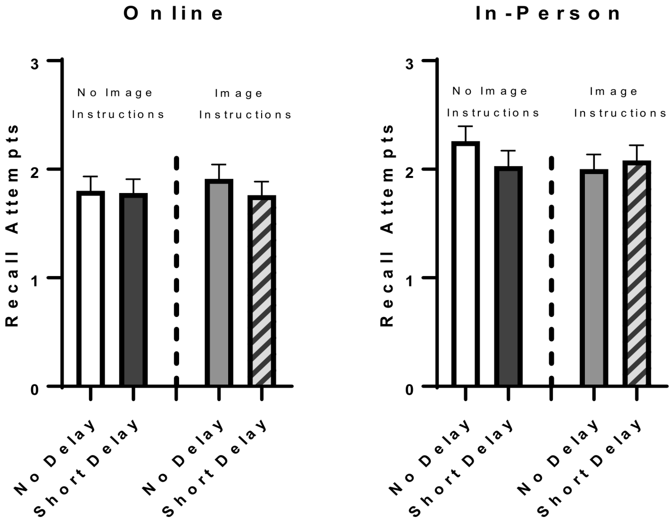


**Figure 5:** Average recall attempts as a function of Image Instructions (no or yes), Delay (no or short) and Mode of Instruction: online (left) or in-person (right).

showed that the Delay x Image Instructions interaction was not significant when the Mode of Instruction was online, $F(1,58) = 1.43, p = .23$, but was significant when it was in-person, $F(1,46) = 4.24, p = .045$. For the in-person mode, participants made more attempts at no delay than at the short delay when no image-based instructions were provided, $p = .03$, but made similar number of attempts regardless of delay when image-based instructions were provided. Requiring more attempts to recall the password for the in-person mode in specific conditions is consistent with notion that more effort was exerted by participants to recall the passwords when the study was conducted in that mode.

The number of passwords forgotten was submitted to a 2 (Text Instructions: yes or no) x 2 (Image Instructions: yes or no) x 2 (Delay interval: no or short) x 2 (Mode of Instruction: online or in-person) mixed ANOVA. The average number of passwords forgotten was 1, and this analysis yielded no significant main effects or interactions.

## LIMITATIONS

One critique of online studies is that researchers are not able to control what participants are doing during the study, which can affect the reliability and validity of the data. For example, although participants were asked not to write the passwords down, we could not verify that they did not do so in the online administration. However, because the results were not at optimal performance (i.e., perfect recall of passwords) and the image-based instructions without text-based instructions led to longer memorization times (suggesting that participants were exerting more effort), we have no reason to believe that the participants were not performing the task as instructed. Campus closures resulting from the COVID-19 pandemic made online work the norm. Students may have become used to performing academic activities, including research participation, online. In fact, we found it was difficult to recruit participants for in-person participation once we repopulated from the COVID-19 campus closure. The participation rate for the in-person mode was essentially null until the last two weeks of the semester when students faced time pressure to complete their research requirements. These factors may have led to the different effects of online versus in-person mode found in our study. We note that many studies conducted prior to the pandemic have found that online and in-person administration of studies result in equivalent findings (see e.g., Meyerson & Tryon, 2003).

## CONCLUSION

Although user-generated passwords are more memorable than system-generated passwords, they are less secure and typically follow trends that can be easy to guess (Kuo et al., 2006). Since system-generated passwords can provide more security, exploring ways on how to train users to create and memorize system-generated passwords should be explored. The current study showed that users are able remember complex system-generated passwords when provided with detailed text-based or image-based instructions to help map the password components to a structure. Our findings did not indicate whether one type of instructions, text or image, was better than the other. We also found differences in multiple performance metrics when the study was administered online versus in person. This finding indicates that contextual factors need to be taken into account when training participants.

## ACKNOWLEDGMENT

The authors would like to acknowledge all of the student assistants in the Center for Usability in Design and Accessibility who helped with data collection.

## REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Bellezza, F. (1996). Mnemonic methods to enhance storage and retrieval. In E. L. Bjork & R. A. Bjork (Eds.), *Memory: Handbook of perception and cognition* (pp. 345–380). San Diego, CA: Academic Press.doi:10.1016/B978-012102570-0/50012-4

Carlson, L., Zimmer, J. W., & Glover, J. A. (1981). First-letter mnemonics: DAM (don't aid memory). *Journal of General Psychology*, *104*, 287. Retrieved from http://search.proquest.com/docview/1290501822?accountid11164

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *In Proceedings of the 16th international conference on World Wide Web* (pp. 657–666).

Keith, M., Shao, B., Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies*, *65*(1), 17–28. https://doi.org/10.1016/j.ijhcs.2006.08.005.

Kuo, C., Romanosky, S., & Cranor, L. F. (2006). Human selection of mnemonic phrase-based passwords. *In Proceedings of the second symposium on Usable privacy and security* (pp.67–78).

Meyerson, P., & Tryon, W. W. (2003). Validating Internet research: Atest of the psychometric equivalence of Internet and in-person samples. *Behavior Research Methods, Instruments, & Computers*, *35*, 614–620.

Nelson, D. L., & Vu, K.-P. L. (2009). Effects of a mnemonic technique on subsequent recall of assigned and self-generated passwords. In M. J. Smith & G. Salvendy (Eds.), *Human interface and the management of information. Designing information environments* (vol. 5617, pp. 693–701). Springer Berlin Heidelberg.https://doi.org/10.1007/978-3-642- 02556-3_78

Nelson, D. L., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, *26*(4), 705–715. https://doi.org/10.1016/j.chb.2010.01.007

Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words? *Psychonomic Science*, *11*(4), 137-138. https://doi.org/10.3758/bf03331011

Taneski, V., Hericko, M., & Brumen, B. (2019). Systematic overview of password security problems. *Acta Polytechnica Hungarica*, *16*(3), 143–165. https://doi.org/10.12700/aph.16.3.2019.3.8

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. *In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 123–140).

Vu, K.-P. L., Bhargav, A., & Proctor, R. W. (2003). Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *47*(11), 1331–1335. https://doi.org/10.1177/154193120304701103

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), 744–757. https://doi.org/10.1016/j.ijhcs.2007.03.007

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Pass Points: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1-2), 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy Magazine*, *2*(5), 25–31. https://doi.org/10.1109/msp.2004.81

Yang, W., Li, N., Chowdhury, O., Xiong, A., & Proctor, R. W. (2016). An empirical study of mnemonic sentence-based password generations trategies. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2978346