**Title.**

Does image-based mnemonic training improve memorability of system-generated passwords?

**Background and need or significance of the research.**

Textual passwords in the username-password combination are the most used authentication method due to their simplicity and cost-effectiveness (Taneski, Hericko, & Brumen, 2019). Although alternative authentication methods (e.g. biometrics, two-step verification) can be more secure, it is unlikely they will replace textual passwords since they are more expensive, require users to carry a physical device to access the system, and are generally difficult to implement on a large scale. However, passwords in general are prone to “the password problem”—memorable passwords are not very secure, while secure passwords are not very memorable (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). As a solution to insecure user-generated passwords, companies may issue secure system-generated passwords to users (Vu, Bhargav, & Proctor, 2003). However, secure system-generated passwords tend to be strings of random letters and numbers that are meaningless and therefore not very memorable. Additionally, due to the generation effect which states that people are more likely to remember words generated themselves versus words that are merely presented to them (Slamecka & Graf, 1978), it is no surprise that user-generated passwords have been shown to be recalled at a higher rate (27.2%) than system-generated random passwords (12.7%; Zviran & Haga, 1993). Essentially, system-generated passwords need to be made more meaningful and memorable to be a viable alternative to user-generated passwords. Investigating the benefits of existing mnemonic password techniques (Vu et al., 2007) along with the self-reference (Rogers, Kuiper, & Kirker, 1977) and picture superiority (Shepard, 1967) effects on system-generated passwords could be a starting point to creating memorable system-generated passwords, as they have been shown to improve memorability of user-generated passwords.

 Past studies have shown that text-based and image-based mnemonic techniques have helped users create secure and memorable passwords. Mnemonics allow users to organize information in a meaningful manner (Yates, 1966), which then improves memory and later recall of that information (Bower, 1970; Roediger, 1980). Generating passwords using mnemonic techniques allows users to think about and process their password more deeply at the semantic level (Craik & Tulving, 1975) by relating their password or parts of their password to existing knowledge. This deeper processing allows sufficient attention to be placed on the password during encoding, which will prevent absent-mindedness during password retrieval (Shacter, 1999). When using text-based mnemonic techniques, the user first creates a sentence that could have some personal meaning and can form a password by using the whole-word technique, where entire words or parts of words in the sentence are replaced by special characters or digits that are phonetically similar (e.g. “Later I ate tofu” → L8teEye8+tofu; Vu et al., 2007). With the image-based technique, the user has a picture accompanying their sentence or can create a sentence based on a picture and then uses a text-based mnemonic technique to transform the sentence into a password (Nelson & Vu, 2010). Generating a password using the image-based mnemonic technique has led to higher memorability of the password than using the text-based mnemonic technique most likely due to the picture superiority effect which states images are recalled more accurately than words or sentences (Shepard, 1967). However, there have not been many studies examining the benefits of mnemonic techniques on memorability of system-generated passwords.

 When using mnemonic techniques to generate passwords, it is important that adequate instructions and examples are given to users. In particular, users generate the most secure passwords when they are given clear instructions to select a personally relevant sentence that other people are unlikely to choose (e.g. “I went to London four and a half years ago”) accompanied by personalized examples of passwords were created from sentences (Yang, Li, Chowdhury, Xiong, & Proctor, 2016). When transforming their sentence into a password, participants were instructed to replace entire words in the sentence with either a letter, number, or special character and were informed that the most common technique was to use the first letter of each word. With these instructions, the sentence “I went to London four and a half years ago” can become the password “iwtl4&ahya.” If participants were given general instructions and examples, they were told to select a memorable sentence (e.g. “Four score and seven years ago our fathers brought forth on this continent”) and given the same instructions to replace words in the sentence. Although participants generated less secure passwords with general instructions than with personalized instructions, memorability of the generated passwords was not significantly different. This result is surprising as personalized sentences and examples should provide recall benefits due to the self-reference effect, which states that people best remember information relevant to themselves (Rogers et al., 1977). Perhaps memorability differences could be further investigated with the use of the image-based mnemonic technique, as there could be memorability benefits from both the self-reference effect and picture superiority effect (Shepard, 1967)

Researchers have also investigated the usability performance of system-generated passphrases (i.e. passwords consisting of a sequence of words) compared to system-generated passwords that are assigned to users (Shay et al., 2012). One prediction was that pairing system-generated passphrases with instructions to visualize the words in the passphrase in an imaginary scene would increase memorability. However, results revealed that system-generated passwords and passphrases performed similarly in terms of forgetting, user difficulty and annoyance, and recording rate (i.e. most participants wrote down their passwords or passphrases). Additionally, including instructions did not significantly improve memorability of passphrases. Based on these findings, researchers suggested that different instructions should have been given to the participants. Perhaps the instructions could have been further improved by instructing the users to relate the system-generated passphrases to themselves to benefit from the self-reference effect (Rogers et al., 1977) and including an image to benefit from the picture superiority effect (Shepard, 1967). As mnemonic techniques appear to use the passphrase approach (i.e. a password is created from a sentence or sequence of words), it may be beneficial to include these types of instructions when teaching users how to utilize the mnemonic techniques.

 Training users with adequate instructions on how to memorize secure system-generated passwords that were created using a mnemonic technique could improve memorability for the system-generated passwords. In the past, user-generated passwords that were created using a text-based mnemonic technique were more memorable than user-assigned secure passwords where users were trained on how the text-based mnemonic technique was used to generate the passwords (Nelson & Vu, 2009), likely due to the generation effect (Slamecka & Graf, 1978). However, prior studies have not yet examined how memorability would be impacted if participants were instead given more extensive training on the image-based mnemonic technique to memorize system-generated passwords that were created using a text-based mnemonic technique. Training will include information on how the system-generated password was created to be personally relevant and then instructing participants to relate the password to themselves, which will increase meaningfulness of the password. Memorability of the passwords will then increase due to both the self-reference (Rogers et al., 1977) and picture superiority effects (Shepard, 1967). With memorable system-generated passwords, there could be less burden on users to create secure and memorable passwords for several accounts.

Bower, G. H. (1970). Imagery as a relational organizer in associative learning. Journal of Verbal

Learning and Verbal Behavior, 9(5), 529-533. [https://doi.org/10.1016/s0022-5371(70)80096-2](https://doi.org/10.1016/s0022-5371%2870%2980096-2)

Craik, F. I., & Tulving, E. (1975). Depth of processing and the retention of words in episodic

memory. *Journal of Experimental Psychology: General*, *104*(3), 268-294. [https://doi.org/10.1037/0096-3445.104.3.268](%20https%3A//doi.org/10.1037/0096-3445.104.3.268)

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., & 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>

Roediger, H. L. (1980). The effectiveness of four mnemonics in ordering recall. *Journal of*

*Experimental Psychology: Human Learning & Memory*, *6*(5), 558-567.<https://doi.org/10.1037/0278-7393.6.5.558>

Rogers, T. B., Kuiper, N. A., & Kirker, W. S. (1977). Self-reference and the encoding of

personal information. *Journal of Personality and Social Psychology*, *35*(9), 677-688. [https://doi.org/10.1037/0022-3514.35.9.677](%20https%3A//doi.org/10.1037/0022-3514.35.9.677)

Schacter, D. L. (1999). The seven sins of memory: Insights from psychology and cognitive

neuroscience. *American Psychologist*, *54*(3), 182–203. <https://doi.org/10.1037/0003-066X.54.3.182>

Shay, R., Kelley, P. G., Komanduri, S., Mazurek, M. L., Ur, B., Vidas, T., Bauer, L., Christin,

N., & Cranor, L. F. (2012). Correct horse battery staple: Exploring the usability of system-assigned passphrases. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12. https://doi.org/10.1145/2335356.2335366

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of*

*Verbal Learning and Verbal Behavior*, *6*(1), 156-163. [https://doi.org/10.1016/s0022-5371(67)80067-7](%20https%3A//doi.org/10.1016/s0022-5371%2867%2980067-7)

Slamecka, N. J., & Graf, P. (1978). The generation effect: Delineation of a phenomenon.

*Journal of Experimental Psychology: Human Learning & Memory*, *4*(6), 592-604 [https://doi.org/10.1037/0278-7393.4.6.592](%20https%3A//doi.org/10.1037/0278-7393.4.6.592)

Taneski, V., Hericko, M., & Brumen, B. (2019). Systematic overview of password security

problems. Acta Polytechnica Hungarica, 16(3). <https://doi.org/10.12700/aph.16.3.2019.3.8>

Vu, K.-P. L., Bhargav, A., & Proctor, R. W. (2003). Imposing password restrictions for

multiple accounts: Impact on generation and recall of passwords. *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., Cook, J., & Eugene 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). PassPoints:

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>

Yang, W., Li, N., Chowdhury, O., Xiong, A., & Proctor, R. W. (2016). An empirical study of

mnemonic sentence-based password generation strategies. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*.<https://doi.org/10.1145/2976749.2978346>

Yates, F. A. (2013). *Art of memory*. Routledge & Kegan Paul.

Zviran, M., & Haga, W. J. (1993). A comparison of password techniques for multilevel

authentication mechanisms. The Computer Journal, 36(3), 227-237. <https://doi.org/10.1093/comjnl/36.3.227>

**Description of the research/Research design.**

We hypothesize that participants will have better memory for passwords generated or memorized after extensive training is provided on the image-based mnemonic technique in comparison to passwords generated or memorized after training on the text-based mnemonic technique due to the additional benefits of the picture superiority effect (Shepard, 1967). The independent variables at the construct level are mnemonic technique: text-based or image-based, password type: system-generated or user-generated, and memory duration: short or long. The operation for mnemonic technique is having participants trained on either the text-based whole-word or image-based mnemonic technique, which will be used to later memorize or generate personally relevant passwords. The operation for password type is having participants either memorize assigned system-generated passwords or having users generate their own passwords after being trained on how to use a mnemonic technique to either memorize or generate personally relevant passwords. The operation for memory duration is having participants hold the generated passwords in memory until shortly after the last password is generated or memorized and for 20 minutes after password generation or memorization before having to re-enter their passwords. The dependent variable at the construct level is memory for passwords. The operation for memory for passwords is counting how many passwords participants correctly wrote down within ten attempts. Four conditions will be created to test this hypothesis, where participants will be asked to either generate passwords or will be assigned system-generated passwords to memorize for five fictional accounts. In both the user-generated and system-generated password conditions, half of the participants will be trained on the text-based mnemonic technique and the other half will be trained on the image-based mnemonic technique. For all conditions, participants will also be trained on how to relate passwords to themselves. The system-generated passwords will be created using the text-based whole-word mnemonic technique.

**Anticipated outcomes and goals of the activity**.

It was previously hypothesized that memory will be higher for passwords generated or memorized after being extensively trained on the image-based mnemonic technique. Participants who generated passwords using the image-based mnemonic technique will recall significantly more passwords than participants who generated passwords using the text-based mnemonic technique as seen in a past study (Nelson & Vu, 2010) and the difference will be equally large both immediately after generation and 20 minutes after generation, as seen in Figure 1. For assigned system-generated passwords, it is predicted that the number of recalled passwords immediately after memorization will be significantly higher for participants who were trained on the image-based mnemonic technique. The number of passwords recalled 20 minutes after memorization is predicted to still be significantly higher for participants trained on the image-based mnemonic technique, though the difference will not be as large as immediately after memorization, as seen in Figure 2. The reason for this decreased gap is because the picture superiority (Shepard, 1967) and self-reference effects (Rogers et al., 1977) may not be as strong 20 minutes later as the participants ultimately did not go through the process of creating the passwords themselves and therefore may not have adequately related parts of the password to existing or personal knowledge, leading to shallower encoding of the password during memorization and overall poorer recall at later times. In other words, participants who had to memorize system-generated passwords will not have the additional benefits of the generation effect (Slamecka & Graf, 1978).

*Number of User-Generated Passwords Recalled Immediately and After a 20-Minute Delay*

Figure 1.The number of user-generated passwords recalled is shown upon immediate recall and after a 20-minute delay for participants trained on the text-based or image-based mnemonic technique. A password is considered “recalled” if the participant was able to correctly write down the password within ten attempts.

*Number of System-Generated Passwords Recalled Immediately and After a 20-Minute Delay*

Figure 2.The number of system-generated passwords recalled is shown upon immediate recall and after a 20-minute delay for participants trained on the text-based or image-based mnemonic technique. A password is considered “recalled” if the participant was able to correctly write down the password within ten attempts.

**Value of research.**

Past literature on password memorability generally focuses on mnemonic techniques (Vu et al., 2007; Nelson & Vu, 2010) as well as the generation (Slamecka & Graf, 1978), self-reference (Rogers et al., 1977), and picture superiority (Shepard, 1967) effects with regards to user-generated passwords. However, these areas have not been as deeply explored with system-generated passwords. For instance, although the image-based mnemonic technique has been shown to generate more secure and memorable passwords in comparison to the text-based mnemonic technique for user-generated passwords (Nelson & Vu, 2010), training on the image-based mnemonic technique has not yet been studied with assigned system-generated passwords created using a text-based mnemonic technique. Additionally, studies that focus on training the user to help generate or memorize passwords have not found anything definitive regarding improved memorability and suggest that instructions could be further improved (Yang et al., 2016; Shay et al., 2012).

The results of this study will show whether or not providing extensive training on the image-based mnemonic technique (i.e. informing participants on how the image-based mnemonic technique was used to generate the password and how to make the password personally relevant) will improve memory for assigned system-generated passwords generated through a text-based mnemonic over extensive training participants on the text-based mnemonic technique. The predicted results of this study show that there are memorability benefits to training participants on how to personalize system-generated passwords and incorporating images with mnemonic techniques. Unfortunately, these benefits are predicted to begin fading after 20 minutes due to the lack of the generation effect. However, as there is at least some benefit from the image-based mnemonic training, further research could focus on the types of images used, improving the written instructions, or perhaps even investigating the benefits of user-generated pictures to accompany passwords. Essentially, the effects from training need to be further strengthened to last over a longer period of time to ensure long-term memorability of system-generated passwords. With more memorable system-generated passwords, the burden on users to create multiple secure passwords for several websites could be reduced and discourage users from insecure password behaviors, such as reusing one password for multiple accounts.

Rubric:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **4** | **3** | **2** | **1** | **Points** |
| **Quality of Information** | Information clearly relates to the main topic and follows requirements of assignment.**10-12 Points** | Information relates to the main topic and generally follows the assignment.**7-9 Points** | Parts of paper don’t follow the main topic or the assignment. **5-8 Points** | Information has little or nothing to do with the main topic or does not follow assignment.**0-4 Points** |  |
| **Accuracy of Information** | No inaccuracies noted. **10-12 Points** | Few inaccuracies noted.**7-9 Points**  | Some inaccuracies noted **5-8 Points** | Many inaccuracies noted**0-4 Points**  |  |
| **Organization and Readability**  | Information is very organized easily readable. **10-12 Points** | Information is organized and readable. **7-9 Points** | Organization of information not totally clear or readability is less than good.**5-8 Points** | The information appears to be disorganized or readability is bad.**0-4 Points** |  |
| **Sources** | Adequate number of primary sources used.**7-8 Points** | Number or quality of sources falls short of adequate.**5-6 Points** | Number or quality of sources clearly inadequate.**3-4 Points**  | Few if any sources actually used.**0-2 Points** |  |
| **APA Style** | Perfect APA formatting**7-8 Points** | Mostly follows APA formatting.**5-6 Points** | Some elements of APA style present.**3-4 Points** | Doesn’t seem to follow APA format at all.**0-2 Points** |  |
| **Mechanics** | No grammatical, spelling or punctuation errors.**7-8 Points**  | Almost no grammatical, spelling or punctuation errors.**5-6 Points**  | A few grammatical spelling, or punctuation errors.**3-4 Points**  | Many grammatical, spelling, or punctuation errors.**0-2 Points** |  |