# Password Rehearsal Memory Games

Michael Lutaaya
Carleton University
michael.lutaaya@carleton.ca

Sonia Chiasson
Carleton University
chiasson@scs.carleton.ca

## 1. INTRODUCTION

As increasingly personal and sensitive information gets stored electronically, there is a growing need for secure mechanisms to protect access to this information. Today, the most common user-facing technique is text passwords. Unfortunately, analysis of user behaviour suggests that most people engage in poor security practices with respect to their passwords. For instance, it is estimated that the average password is reused between approximately six websites [1]. Additionally, research has shown that the task of creating passwords that are both secure and memorable is challenging for users [2]. In spite of these findings, Bonneau and Schechter found that with enough practice "most users can memorize strong cryptographic secrets" [3].

One approach that could be used in support of password memorization is the use of puzzle games, such as those originally proposed in Nintendo's *Brain Age* [4], to develop an individual's ability to retain information and perform other cognitive tasks. Brain Age exercises the brain through short activities, such as solving twenty simple math equations in as little time as possible. Other researchers suggest that Brain Age successfully persuades users to perform tasks otherwise seen as dull and that its persuasive strategies may be applied to user authentication [5]. These conclusions led to the development of *Password Rehearsal Memory Games*—puzzle games created to assist users with password memorization and encourage the use of strong passwords. A user study conducted by Ling [6] on Password Rehearsal Memory Games had promising results suggesting that users may see a benefit by using these types of games when memorizing passwords but that additional research would be needed. To further explore this hypothesis, we developed and conducted a pilot study of another Password Rehearsal Memory Game known as *Password Scramble* that improved on flaws identified by Ling.

## 2. PASSWORD SCRAMBLE

The objective of Password Scramble is to correctly unscramble your password in each round with as few errors as possible. Password Scramble was influenced by *Word Scramble*, a game from Brain Age. In Word Scramble, the player must unscramble the letters shown on-screen to spell a word. With Password Scramble, the player is given one minute to memorize an eight-character password. Once the minute has passed, the individual characters of the password are scrambled and the player must unscramble their password to advance. If the player is having difficulty, they may start over or, once per game, they may use a hint that randomly inserts one character in its correct position. After successfully placing all characters, the player advances to the next round. In each new round, the last visible character of the password is hidden by a wildcard for the rest of the game. The user must type in this hidden character from memory after placing all other characters (see Figure 1). By the time they reach the last round, all of the characters are hidden and the user must type in the entire password from memory.

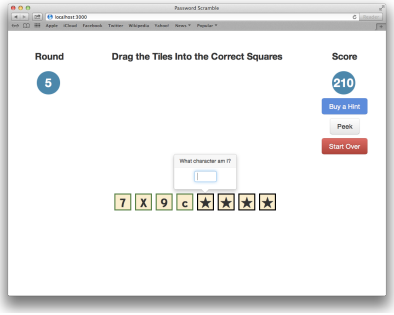


Figure 1: The Password Scramble game during the wildcard stage

## 3. EVALUATION METHODOLOGY

The goal of the study was to evaluate whether Password Scramble was more effective at assisting users with password memorization than a control condition where users were simply given a random password to memorize (*Text-Only* system). In the Password Scramble condition, participants interacted with our prototype game, while in the Text-Only condition, participants were required to correctly enter their assigned password three consecutive times to show that the password had been committed to memory. Twenty-one participants were recruited through posters placed throughout Carleton University's campus.

The one-week between-subjects lab study consisted of three stages on Day 1 (background, testing, feedback) and an online follow-up one week later.

**Background:** Participants completed a demographic questionnaire and a questionnaire asking about their password management strategies. The information gathered in this stage helped us develop an understanding of how participants handle having many passwords.

**Testing:** Participants were introduced to a "demo version" of their assigned password tool to ensure they understood how the tool worked and what tasks they would be performing with it. Then, the participant was tasked with using the real version to memorize one password. The participants were told that they will be asked to recall the password in one week and that they may use the tool for a maximum of ten minutes. They could stop using the tool if they felt they had sufficiently memorized the password. In order to ensure each of the assigned passwords were of similar complexity, participants were assigned one of five pre-generated random passwords. These passwords were eight characters in length and had exactly two digits, five letters (at least one uppercase and one lowercase), and one of the following characters: !@#$%^&*_+-=.

**Feedback:** After using one of the password tools, participants provided feedback on ways the tool could be improved and explained whether or not they would use the tool in their normal lives. They completed a questionnaire that had both Likert-scale questions and open-ended questions.

**Follow Up:** Seven days later, participants received an email requesting they complete an online questionnaire. The questionnaire asked participants to recall the password as best they can and asked for details regarding their experience with memorizing the password (e.g., if they used any additional techniques to memorize).

# 4. RESULTS

Our main measure of success was whether participants remembered their assigned password in the one-week follow up. The Levenshtein distance between their entry during the follow up stage and their original password was measured. The Levenshtein distance counts the fewest number of single-character operations

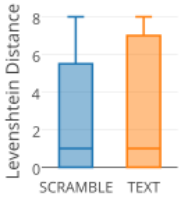


Figure 2: Levenshtein distances between participants' entries during the follow up stage and their original passwords.

(insertions, deletions or substitutions) required to transform one string into another. Figure 2 shows the Levenshtein distances for Password Scramble and the Text-Only system. The mean Levenshtein distance for a user of Password Scramble was 2.82 operations compared to an average of 3.30 operations for a user of the Text-Only system. Although lower for Password Scramble, a *t*-test, using an alpha value of 0.05, showed that the results were not statistically significant.

Figure 3 displays responses provided for the Likert-scale questions analyzed using two-tailed Mann-Whitney U tests. The responses ranged from 1 (strongly disagree) to 10 (strongly agree). The mean responses were higher for Password Scramble, suggesting that it was easier to use, had higher engagement, was more useful, and increased memorability. However, the differences between the Password Scramble and the Text-Only conditions were not statistically significant. Our results further show that users did find that remembering their passwords was significantly easier after using Password Scramble ($p < 0.05$, $U = 26$, $z = 2.007$).

When surveyed, most users of both the Password Scramble game and the Text-Only system expressed a willingness to use the systems to memorize new passwords. A number of users of Password Scramble said they would use the game for passwords that were "difficult" or randomly generated. Common suggestions for improving the game included adding a time limit to assemble the password to make the game more challenging, using sound effects to indicate correct and incorrect attempts, and changing the position of the stars to be random rather than sequential. Suggestions to improve the Text-Only system included increasing the number of repetitions during memorization, providing phrases that map to the password's characters, and having the user recall the password after a short break.

# 5. DISCUSSION AND CONCLUSION

In this paper, we have introduced Password Scramble—a Password Rehearsal Memory Game that encourages memorization by unscrambling an assigned password several times with

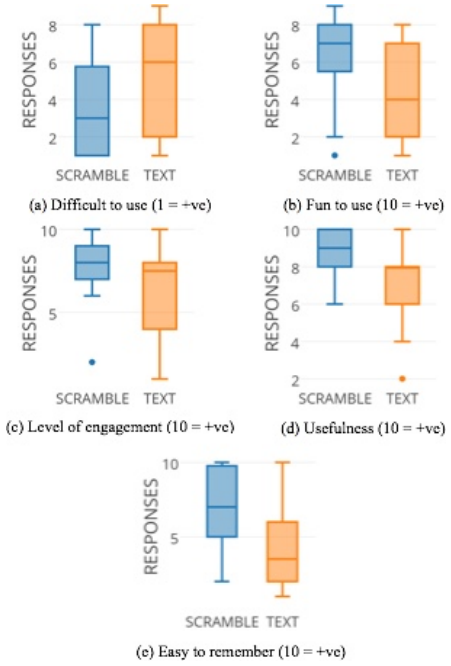


Figure 3: Likert-scale responses from the questionnaires

increasing difficulty. Although results suggest that Password Scramble was more effective as a memory aid than the Text-Only system that was devised as a control, our small sample size meant that results were not statistically significant. Our preliminary results align with the findings of Bonneau and Schechter who stated that most users can memorize passwords when using tools that support learning over time. While some users explained that they would not use Password Scramble in situations where they create their own password, its ability to support the memorization of random passwords is promising. Limitations of this work include the small sample size and the fact that users had to memorize only one password for one week. More research would be necessary to determine whether the game is an effective tool for memorizing multiple passwords and whether incorporating more concepts found in traditional games, such as achievements, has an impact on memorization.

# 6. REFERENCES

[1] D. Florencio and C. Herley. A large-scale study of web password habits. In *ACM WWW* 2007.

[2] A. Adams and M. A. Sasse. Users are not the enemy. In *Communications of the ACM* 42(12), 1999.

[3] J. Bonneau and S. Schechter. Towards reliable storage of 56-bit secrets in human memory. In *USENIX Security*, 2014.

[4] R. Kawashima. *Brain Age: Train Your Brain in Minutes a Day!*. Nintendo of America, Inc., 2006.

[5] A. Forget, S. Chiasson, and R. Biddle. Lessons from Brain Age on persuasion for computer security. In ACM *CHI Extended Abstracts,* 2009.

[6] C. Ling. Password Rehearsal Memory Games. Computer Science Honours Thesis, Carleton University, April 2013.