The Influence of Password Restrictions and Mnemonics on the Memory for Passwords of Older Adults

Kim-Phuong L. Vu and Martina M. Hills

Department of Psychology,
California State University Long Beach,
1250 N Bellflower Blvd, Long Beach CA 90840
Kim.Vu@csulb.edu,
martinirox99@gmail.com

Abstract. Accessing Internet accounts can provide convenient services to users, regardless of age. However, these online services typically require that users enter a username and password. Forgetting one's password, then, often results in the inconvenience of having to reset your password. Although there has been research on the memorability of passwords, this research often focuses on younger adults. Little research has taken older adults into consideration when designing password requirements. Older adults show cognitive decline in memory, which can make the task of remembering passwords especially difficult. However, older adults experience less difficulty in memory for familiar pictures, making the use of pictures an ideal candidate for cuing passwords. Participants in this study were asked to generate passwords for five different fictitious online accounts using a text-based or image-based mnemonic technique. Older adults were less likely to forget passwords that were generated using image-based mnemonic technique compared to the text-based one, implying that pictures can be used as cues for password recall for older adults.

1 Introduction

The advantage of relying on online services is quite clear in that it allows users to access web-based services at almost any time and from any place where there is an internet connection. However, accessing online accounts requires that users enter a username and password [1, 2]. With the increased use of the internet, the number of passwords per user has grown [3], making it a difficult task to remember unique passwords for each account. The use of unique passwords is preferred because recycled passwords can result in unauthorized access to multiple accounts of a particular user if one account is compromised. Techniques for helping users to remember secure passwords are needed because even with the fast growth of alternative authentication tools such as tokens, smart cards, and biometric devices, the username-password technique has continued to be the main choice for security systems because of its ease of implementation [4].

Companies that use internet services have the option of providing users with a secure password to use. However, these passwords tend to be random strings of

S. Yamamoto (Ed.): HIMI/HCII 2013, Part I, LNCS 8016, pp. 660–668, 2013.

characters that are difficult for users to remember. As a result, users tend to write these types of passwords down, decreasing their effectiveness in terms of security. Companies can also add password requirements to improve the security of user-generated passwords. These password restrictions often require the use of both uppercase and lowercase letters, digits and/or special characters, and a minimum password length [5]. Although the addition of these restrictions can also cause difficulty in password memorability for many users [2], these generated passwords tend to be more memorable than computer-generated ones. The forgetting of passwords is likely to be more pronounced among older adults due to the decline in memory that is associated with the normal aging process [6].

This issue of increasing older adults' ability to remember passwords needs to be examined promptly due to the rapidly increasing age of the American population [7]. According to a report from The United States Census Bureau entitled, "Expectation of Life and Expected Deaths by Race, Sex, and Age: 2006," the average life span of adults has increased by eight years from 1970 to 2010. This means that adults are living longer than they were 40 years ago. The number of older adults using the internet has also increased over the years. In 1996, only 2% of older adults age 65 and older used the internet, but this percentage increased to 22% by 2004 [8] and 53% of by 2012 [9]. Due to the escalating number of tasks that can be completed online, the number of accounts and passwords that need to be remembered can put a toll on older adults' memory capabilities. Thus, it is vital to consider the population of older adult users when it comes to password recall.

A couple of studies have shown that memorability of passwords can be improved with the use of mnemonic techniques [2, 10]. Mnemonic strategies encourage deeper processing of information by relating new knowledge with knowledge already established in memory [11]. One of the most effective password generation mnemonic techniques is the image-based one [2]. The image-based mnemonic allows users to generate their own passwords using well-known pictures instead of generating complex words or letter/character combinations to abide by required website guidelines. However, the effectiveness of the image-based mnemonic technique has been examined only with a sample of younger adults.

Teaching older adults how to create passwords that are both secure and easier to remember is crucial for their ability to take advantage of the services provided by the online world. Images can be stored in memory and retrieved more easily than words [12], a phenomenon known as the "picture superiority effect." This is so, even with the deterioration of cognitive processing [12]. Thus, the image-based mnemonic method has the potential to be employed by both older and younger adults.

The goal of the present study was to determine whether teaching older adults how to create passwords using image-based mnemonics can lead to better memory for those passwords. Teaching older adults how to memorize strong passwords through use of the image-based mnemonic technique will not only help them secure their accounts, but may also reduce the expense associated with resetting lost passwords.

2 Current Study

This study examines the effectiveness of two different password generation methods for older adults (i.e., age 55 and over) and younger adults (age 18 to 30). All participants in each group were responsible for creating their own passwords for each of five different fictitious online accounts. Participants were then tested on their ability to recall the passwords at a 10-min and 1-wk delay interval. Cracking software was used to analyze the strength of each password, and differences in password length and complexity were examined for each age group by password generation technique.

2.1 Method

Participants. Thirty-seven older adult participants and 40 younger adult participants were recruited from California State University Long Beach (CSULB) and its surrounding communities. Older adult participants ranged from 55-86 years old (M = 71.06, SD = 8.78; 25 female and 9 male). Younger adult participants ranged from 18-25 years old (M =19.3, SD = 1.57; 34 female and 6 male).

Older adults were paid $15 to participate in the entire experiment, which consisted of two sessions lasting less than 1 hour each. The younger adults were recruited from the university's Introductory Psychology Participant pool, and the students received experimental credits for participating in the study. At the time participants signed up, they were informed that they were taking part in a study examining password generation and memorability. All participants were asked to bring to the first session of the experiment five different personal pictures that they knew well and could put into five different categories. For the older adult group, 18 participants were randomly assigned to the image-based mnemonic group and 19 to the text-based mnemonic group. For the younger adult group, 20 participants were randomly assigned to the image-based mnemonic group and 20 to the text-based mnemonic group.

Design, Apparatus, and Procedure. The methods and procedures were closely modeled after Nelson and Vu [2]. A 2 (Password generation technique: image-based mnemonic or text-based mnemonic) by 2 (Recall delay: 5-min or 1-wk delay) by 2 (Age: Older adults or Younger adults) mixed design was used. Password generation technique and age were the between-subjects variables and recall delay was the within-subject variable.

A Java program was used to present the experiment on a laptop computer with a 14" screen. Participants were presented instructions on what type of generation technique they were employing. The program also checked that each password met the set criteria for each generation technique. It also recorded the generated password and the amount of time it took the participant to recall their passwords at both the 10-min interval and the 1-wk interval.

All participants were tested individually in a quiet, well-lit room. The experiment consisted of two sessions, held one week a part. The first session consisted of two parts, and the second session only consisted of one part. At the beginning of the first session, participants were introduced to the experiment, asked to sign a consent form

and provided the five personal pictures to the experimenter. The pictures were added to a multimedia storage device and kept for the duration of the experiment. In the first session, participants generated five different passwords that satisfied a set of password restrictions for five different fictitious accounts. The password restrictions included: being generated from a sentence that made sense; being at least eight characters; use of a capital letter; use of a special character (e.g. @, #, $, or %); use of a digit; being generated from a sentence that had the special character and digit embedded in the way that it makes sense relative to the context of the sentence; being unique for each account. The five different accounts consisted of: E-mail, bank, computer, social networking, and bookstore.

Even though all participants provided the five personal pictures to the experimenter, only those randomly assigned to the image-based mnemonic group used their pictures in the experiment. The image-based mnemonic group was taught how to use this technique by giving participants examples of two different pictures used to create two different passwords. One example used a picture of a skateboard with the phrase "I like to skateboard" written underneath the image (see *Figure 1)*. The participant was given 10 s to look at the image and the statement. The participant was informed as to the relationship the picture might have with personal knowledge and how to incorporate that knowledge into a password. For example, the person likes to skateboard so "I like to skateboard" could be used as a basis for the password.

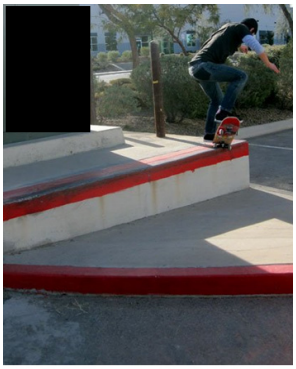

Fig. 1. Example picture shown to participants in the image-based mnemonic group

As part of their training, the experimenter explained how pieces of information gathered from the picture could become more complex and meaningful to the participant. The experimenter pointed out that the skateboard was red and reminded her of learning her first trick on the red curb at school. The experimenter then demonstrated how the red color could be translated into the password by replacing "I" with "Eye" and capitalizing it because the red curb really caught her eye when she first learned to skate. The word "to" could be changed to number "2" and "skateboard" could be changed to "sk8board" by transforming part of the sound associated with the word to the number "8." The experimenter also pointed out that the letter "s" could be

substituted for "$" to denote the money she spent buying her skateboard. The final transformation of the combination of letters to create the complex password of "EyeLike2$k8board." A second example was also provided to the participants.

For the text-based mnemonic technique group, participants were instructed to generate passwords based on self-generated phrases using the same examples employed in the image-based mnemonic technique but without the added benefit of the personal pictures.

After generating a password for each account, participants were tested for their recall of the passwords after a 5-min delay, and again after a 1-wk delay. For the recall session, participants were asked to recall each of the five passwords they created. The participants were instructed to enter the correct password for each account name that was prompted. The fictitious account names were displayed on the computer screen in a random order for four times each. The number of passwords forgotten at each interval was recorded as a measure of password memorability.

3 Results

3.1 Generation Time and Number of Attempts

The amount of time (in seconds) taken by a participant to generate a password that satisfied the password restrictions for each of the five fictitious accounts was recorded and averaged across the five accounts to determine a mean password generation time for each participant. A 2 (Password generation technique: image-based mnemonic or text-based mnemonic) by 2 (Age: Older adults or Younger adults) mixed analysis of variance (ANOVA) was run on mean generation time as a function of password generation technique and age group. There was a significant effect of age, $F(1,73) = 13.48$, $p < .001$ (see Figure 2). Older adults took over 1-min longer to generate an acceptable password than did younger adults. No other effects were significant for generation time.

The number of attempts needed by a participant to generate an acceptable password was also recorded and then averaged across the five accounts. The same two-way ANOVA was conducted as for mean generation time on the mean number of attempts. However, this analysis did not yield any significant effects.

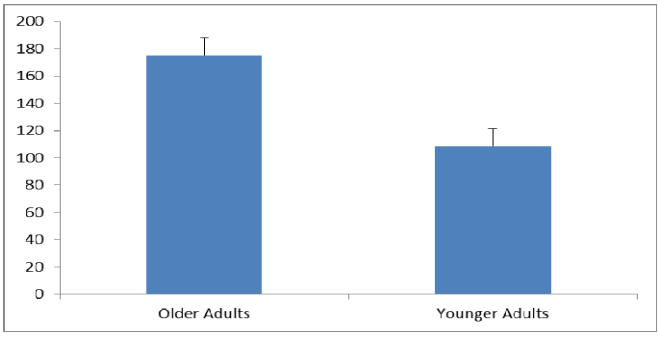

Fig. 2. Mean Password Generation Time (in Seconds) for Older and Younger Adults

3.2 Memorability of Passwords

The mean number of passwords forgotten by each participant was analyzed using a 2 (Password generation technique: image-based mnemonic or text-based mnemonic) by 2 (Recall delay: 10-min or 1-wk delay) by 2 (Age: Older adults or Younger adults) ANOVA. There was a significant main effect of delay on forgetting, $F(1, 73) = 12.08$, $p < .01$. Participants forgot more passwords ($M = 1.94$) after the 1-wk delay when compared to the 10-min delay ($M = 1.44$). There was also a main effect of age on forgetting, $F(1, 73) = 13.40$, $p < .01$, where older adults forgot ($M = 2.24$) more passwords than younger adults ($M = 1.14$).

Recall delay also interacted with age, $F(1, 73) = 8.68$, $p = .004$. Older adults showed a larger increase in the number of passwords forgotten from the 10-min to 1-wk delay compared to younger adults (.91 vs. 0.18 increase, respectively). This two-way interaction was qualified by a significant three-way interaction between age, recall delay, and password generation technique, $F(1, 73) = 4.25$, $p = .04$ (see Figure 3).

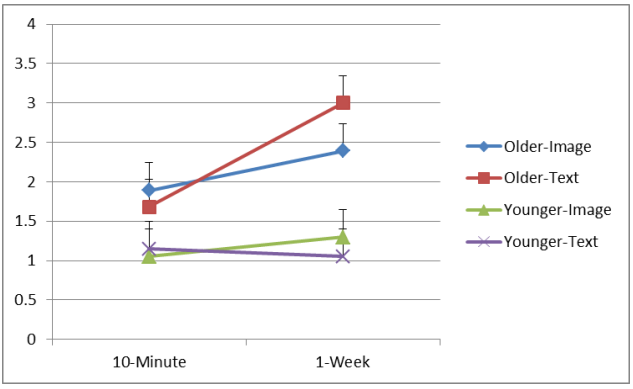

Fig. 3. Mean Number of Passwords Forgotten for Older and Younger Adults at the 10-Minute and 1-Week Interval

To determine the nature of these differences, simple effects analyses of participants' forgetting were conducted separately in the image-based mnemonic and text-based mnemonic conditions. In the image-based mnemonic condition, there was no statistically significant interaction between age and delay, $F < 1.0$. In the text-based mnemonic condition, though, a significant age × recall delay interaction was obtained, $F(1, 37) = 10.05$, $p = .003$. To characterize these differences, a comparison of the number of text-generated passwords forgotten by younger and older adults at each recall delay was performed. With a 10-min recall delay, there was no difference in older and younger adults' short term forgetting, $F(1, 38) = 1.16$, $p = .29$. However, with a 1-wk delay older adults forgot significantly more text-based mnemonic passwords ($M = 3.00$) than did younger adults ($M = 1.05$), $F(1, 38) = 15.77$, $p < .001$.

3.3 Password Security

The security of the generated passwords was assessed by the ability of the Cain and Abel software to crack the passwords. Each password was encrypted and turned into a HASH file. The document was then submitted to the Cain and Abel Cracking software in an attempt to recover the password. All passwords generated in this study were submitted to the cracking software for a 12-hour period. The software was not successful in cracking any of the passwords submitted. Thus, the passwords generated in both the image based and text-based groups were somewhat secure.

4 Discussion

Since accessing online services is important for all age groups, using mnemonic techniques to generate secure passwords can be very useful. The present study showed that older adults can generate passwords that are more resistant to being forgotten by using the image-based mnemonic technique compared to the text-based mnemonic technique. Although, older adults took longer to generate an acceptable password, they did not differ from younger adults in terms of the number of attempts needed to do so. The longer generation time is expected due to decreased processing speed and slower rates of information activation [13, 14] experienced by older adults. Thus, the present study supports the notion that the image-based mnemonic technique could be used by older adults to generate passwords that are more resistant to forgetting than those generated by a text-based mnemonic technique.

Consistent with the notion that passwords generated with both the text-based and image-based techniques are secure [2], Cain and Abel, a powerful password cracking system, was not able to crack any of the passwords submitted from both the image-based and text-based groups for a 12 hour period. Since none of the passwords were successfully cracked, a viability test of Cain and Abel cracking software was performed. Eight variations of the password "password" (password; Password; password1; Password1; p@ssword; P@ssword; p@ssword1; P@ssword1) were submitted to the Cain and Abel cracking software to test the cracking rate for each word. All variations were cracked by the software, indicating that the software is viable cracking tool. It is likely that the software needed more time for the brute-force attack to be successful in cracking passwords generated with the mnemonic techniques used in the present study.

5 Limitations of the Study and Recommendations for Future Research

The study was limited by a couple factors. The first factor was that the Java program used in this study was the same one we have previously used in our lab to study passwords generated by younger adults. Many of the older adult users, though, were confused by how the program functioned given its text-based interface. Using a more graphic interface may have facilitated the older adult's performance. The second

limitation of the study was in regards to the use of the images for generating passwords. With limited directions to participants to bring in five significantly different images for five categories, some users reported not being able to make a good connection between the picture and account name. Many of the participants stated that they would have chosen different pictures for the study if they understood the significance of linking the pictures to the different accounts beforehand. Finally, participants also reported that there was some additional interference associated with having to generate five passwords for different accounts at the same time. Generally speaking, online account users are only responsible for generating one username and one password for an account at a time. The requirement to generate five unique passwords that met all the requirements at once may have been overwhelming to participants, especially the older ones. Despite these limitations, though, the older adults in this study still showed a benefit for generating passwords using the image-based mnemonic technique.

Future research should focus on helping users make better connections with the images and the different accounts. Improving such connections would enable users to have a better understanding of the password technique as well as be able to process the pictures along with the account name at a deeper level.

References

1. Renaud, K., Ramsay, J.: Now what was that password again? A more flexible way of identifying and authenticating our seniors. Behaviour and Information Technology 26, 309–322 (2007)
2. Nelson, D., Vu, K.P.L.: Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. Computers in Human Behavior, 1–11 (2010)
3. Renaud, K., De Angeli, A.: My password is here! An investigation into visuo-spatial authentication mechanisms. Interacting with Computers 16, 1017–1041 (2004)
4. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Applied Cognitive Psychology 18, 641–651 (2004)
5. Gehringer, E.F.: Choosing passwords: Security and human factors. Department of Electrical and Computer Engineering, Department of Computer Science, North Carolina State University, pp. 369–373 (2002)
6. Luo, L., Craik, F.I.M.: Age differences in recollection: specificity effects at retrieval. Journal of Memory and Language 60, 421–436 (2009)
7. Wagner, N.L., Hassanein, K., Head, M.M.: Computer use by older adults: A multidisciplinary review. Computers in Human Behavior 26, 870–882 (2010)
8. Gatto, S.L., Tak, S.H.: Computer, internet, and e-mail use among older adults: Benefits and barriers. Educational Gerontology 34, 800–811 (2008)
9. Zickuhr, K., Madden, M.: Older adults and internet use: For the first time, half of adults ages 65 and older are online. Pew Research Center's Internet & American Life Project Report (2012),
`http://pewinternet.org/Reports/2012/Older-adults-and-internet-use.aspx`

10. Vu, K.P.L., Proctor, R.W., Bhargav-Spanzel, A., Tai, B.-L., Cook, J., Schultz, E.E.: Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies 65, 744–757 (2007)
11. Roediger, H.L.: The effectiveness of four mnemonics in ordering recall. Journal of Experimental Psychology: Human Learning and Memory 6, 558–567 (1980)
12. Renaud, K., De Angeli, A.: Visual passwords: Cure-all or snake-oil? Communications of the ACM 52, 135–140 (2009)
13. Bailey, H., Dunlosky, J., Hertzog, C.: Does differential strategy use account for age-related deficits in working-memory performance? Psychology and Aging 24, 82–92 (2009)
14. Hertzog, C., Dixon, R.A., Hultsch, D.F., MacDonald, W.S.: Latent change models of adult cognition: Are changes in processing speed and working memory associated with changes in episodic memory? Psychology and Aging 18, 755–769 (2003)