Frequently Using Passwords Increases Their Memorability – A False Assumption or Reality?

Emergent Research Forum Paper

Naomi Woods
University of Jyväskylä
naomi.woods@jyu.fi

Abstract

Password memorability is a significant problem that is getting worse as the numbers grow. As a direct result of memory limitations, adopted insecure password practices have substantial consequences as organizations lose millions to security breaches and helpdesk costs. IS research has examined memory theories to increase the memorability of passwords. However, in our research we have discovered some anomalous findings. It is commonly known that more frequently and recently recalled information is more easily remembered (assumed for password recall also); our previously collected objective data revealed no effect on password recall. This study will strive to confirm whether or not password memorability is affected by the frequency of password use and the time between use. If this study confirms our previous results, then this suggests that future IS research should look to other factors to increase password memorability and security, than just directly applying memory theories to the password problem.

Keywords

Password security, memory theory, frequency of use, memorability, information security.

Introduction

Password authentication is currently the most commonly used mechanism for securing organizational and personal data (Das et al. 2014; Grawemeyer and Johnson 2011; Ur et al. 2016; Zhang et al. 2009). There are several issues pertaining to password security, but the main problem stems from the sheer number of accounts, and therefore passwords, a user has to remember (Duggan et al. 2012; Gaw and Felten 2006; Zhang et al. 2009). Nowadays, many users can have in excess of 10, 15, sometimes 20 passwords, and while attempting to meet security policies, they are often required to change them regularly (Marquardson 2012). Users are struggling (Shay et al. 2010). What's more is that when users forget their passwords, there can be consequences in terms of time (e.g., when employees are unable to work due to limited access, and through contacting helpdesks), inconvenience (e.g., when users are unable to access their accounts), and money (e.g., money lost from lack of productivity, lack of access to accounts, and helpdesk costs) (Brown et al. 2004; Ives et al. 2004; Mujeye and Levy 2013). Many companies lose tens of thousands of dollars on employees forgetting their passwords and consequently calling helpdesks to reset their passwords (Brown et al. 2004, Saastamoinen 2014). All these consequences lead many users to develop a fear of forgetting (Inglesant and Sasse 2010), and therefore adopt insecure password behaviors as coping strategies for their memories' limitations (Grawemeyer and Johnson 2011). Insecure password behaviors can include password reuse, writing passwords down, and choosing weak passwords (Adams and Sasse 1999; Inglesant and Sasse 2010; Zhang et al. 2009). And through these insecure behaviors, users are undermining the whole password mechanism, as this means of securing data can be manipulated to gain unlawful access to secure accounts (Adams and Sasse 1999; Ives et al. 2004). Therefore, IS researchers should continue to find ways in which to increase the security and memorability of passwords.

Previous research, theory, and current motivations

IS research has examined password security and password memorability, looking at password behavior, and to different aspects of memory (e.g. Adams and Sasse 1999; Nelson and Vu 2010; Zhang et al. 2009). The human memory is complex, and one of the most prominent memory models that IS researchers refer to is the Stages of Memory theory, suggesting three storage systems involved with the encoding/learning, storing of information, and the retrieval process (Atkinson and Shiffrin 1968). There are many different factors that can affect the memory process or cause it to fail (Anderson 2009); if we do not, for example give enough attention to the learning process, information is not encoded properly, or it can sometimes not even move from the short-term memory (STM) to the long-term memory (LTM) (Nilsson 1987). Likewise, if we do not put enough effort into retrieving information from our LTM, it may not be retrieved, or even forgotten. One theory of forgetting is trace decay which suggests that we just forget information just through the passage of time (Anderson 2009), and recalling this information regularly prevents it from decaying (Ebbinghaus 1885). Therefore, if information is more frequently and recently recalled, it is more easily remembered (Anderson and Schooler 1991).
Throughout IS literature, several researchers have assumed that the more that a password is used or more frequently it is used, the better it is remembered (e.g. Adams and Sasse 1999; Brostoff and Sasse 2000; Duggan et al. 2012; Inglesant and Sasse 2010; etc.). This would make sense based on memory theory; however, is this really the case? Or does it? How many times has muscle memory stopped users from recalling a frequently used password because of a different keyboard layout? So, has this actually been empirically studied? Zviran and Haga (1999) found a relationship between password frequency of use and password memorability. Even so, firstly, this was based on participants reporting on one password, not multiple passwords as required today. Secondly, the participants were reporting their perceived memorability and password usage, their data was subjective, and possibly not representing the "true" picture, only what they expected. In contrast to Zviran and Haga, while running further analysis on data we collected for a previous study (Woods 2016), we found that our results showed something different.

In our previous study (Woods 2016), we employed a longitudinal design to collect password recall data over 12 weeks. This design allowed us to manipulate the password recall frequency and the time between recall tasks. Although this was not the focus of the study, the idea of this manipulation was to see whether there was an effect of the frequency of password use (or the number of times in which the passwords were recalled), and the time between the frequency of password use on password recall and password interference. Ten passwords were created for 10 accounts, and were recalled for each account between 3-6 times over the 12 weeks, with a variety of time between recall tasks. The frequency of password recall did not have a significant effect on password recall, i.e. password correct recall did not increase as the frequency of recall increased. Further analysis was performed examining the difference between different accounts with different frequency recall rates, and accounts with different amounts of time between password recall. There were a couple of significant differences between accounts, but these were not supported by other accounts. Furthermore, the effect of time between password recall, where passwords had been recalled in succession leading to the final recall task in week 12, compared with accounts where there had been weeks between recall and weeks between the final recall, were analyzed and no difference in password memorability was found.
Although our previous research findings contravenes previous IS research, for the current study we will propose two experimental hypotheses grounded in memory theory; however the objectives of this research would be supported by these hypotheses being rejected:

H1: an increase in the frequency of password use will have a positive effect on password memorability.
H2: the less time between password use will have a positive effect on password memorability

Based on our previous findings, these results suggest that the frequency of password recall and/or the time between recalling passwords does not have an effect of password memorability. We believe this warrants further investigation as if there are no differences in password memorability with respect to how frequently the password is used or the time between password recall; this could mean many things. Firstly, there could be other factors involved that could be affecting password memorability. These factors could be produced by the user, for instance, their perception of security, or their memory, or their motivation towards the password process. However, it could also be a result of the fact that passwords are

not created and recalled in any other circumstance in life, as a structure (combination of upper and lower case letters, numbers, and special characters); nor with the importance that they carry (protecting our information), passwords are not recalled anywhere, and memory studies test different elements of memory based on words, pictures, numbers, etc., not passwords (Woods 2016). It is important to confirm these findings as then future password research could then focus on not directly applying memory theories to increase password memorability, but to investigate other factors in more detail that can affect password memorability, and reconsider developing theories specifically to increasing password memorability (Woods 2016).

Experimental Design and Procedure

To study the effects of frequency of password use, and the time between use of passwords on password memorability, a longitudinal experimental design will be employed. The data will be collected from participants that will consist of staff and students from a Finnish university (N = 100). Age of the participants will be equally distributed through groups of different age ranges, and will be monitored for an effect, as age is known to have an effect on memory (Baddeley 2009b).

All participants will take part in the same procedure throughout the study. A website where participants are asked to sign in, create and recall passwords will monitor and log all password data produced by the participants. The participants will be sent emails to ask them to recall passwords for specific accounts. Initially, participants will be asked to create six passwords for six fictitious accounts. Six has been chosen as any more could have a significant effect on the participants' cognitive load, and therefore could reduce password memorability (Baddeley 1992). When the passwords are created, to check that they have been learnt properly, the participants will be asked to immediately recall their passwords in the password verification stage. This will be three times to reinforce the memory. Then they will be asked to recall them one more time following a questionnaire, to confirm that the passwords have entered the long-term memory (Baddeley 2009a).

After the initial creation of the passwords, the participants will be asked on several occasions within the three weeks to recall their passwords (shown in Table 1.) Each account will vary in the amount of times it is recalled and the time between the recall. This design was chosen to control for the frequency and distribution of password recall across the available weeks of the experiment. Two independent variables that will be examined are: frequency of use and time between use. They will be operationalized by two accounts representing low and high times between use, i.e. consecutive days of recall compared with several days between recall, or in other words, massed recall vs distributed recall (Nelson 1977), for each increment of frequency of use (i.e. passwords recalled 3, 5, or 7 times). There will also be a final recall of all passwords on the final day of the study, to see if there would be an effect of either or both independent variables of frequency of use and/or time between use on password recall overall; but also to see if there would be an effect on password recall from the passwords that had been intensively recalled in the first week.

Frequency of use (number of times passwords recalled)	**Week**	**1**							**2**							**3**				
	Day	**M**	**T**	**W**	**T**	**F**	**S**	**S**	**M**	**T**	**W**	**T**	**F**	**S**	**S**	**M**	**T**	**W**	**T**	**F**
	Password																			
3	**1**	1	1	1																1
3	**2**	2				2						2								2
5	**3**	3	3	3	3	3														3
5	**4**	4							4				4					4		4
7	**5**	5	5	5	5	5			5	5										5
7	**6**	6			6				6		6		6			6		6		6

Table 1: Password study schedule

Various methods would be employed to analyze the data and the differences between frequencies of use and the times between use on password memorability, and to see further if there is an interaction. A repeated measure design would look at the differences between recall on day 1 and the final recall. An ANOVA would be employed to examine the differences between the different frequencies of password use (3, 5, 7). An independent *t*-test will look at the difference of times between use, massed recall vs. distributed recall. Then further ANOVAs will examine the interactions between frequency of use and time between use.

Conclusion

Users struggle to remember multiple passwords, which is resulting in a fear of forgetting, which ultimately leading to the adoption of insecure password practices, such as password reuse and choosing weak passwords (Adams and Sasse 1999; Campbell et al. 2006; Inglesant and Sasse 2010; Zhang et al. 2009). This has serious consequences for the individual user and for organizations; for instance, millions of dollars are being lost or spent on, for instance, security breaches and password resetting through IT helpdesks (Brown et al. 2004; Ives et al. 2004). This is still an important issue, as alternatives to passwords are still not common practice (Bang et al. 2012; Vu et al. 2007), and therefore is it imperative to encourage users to employ secure password behaviors, and help increase the memorability of passwords.

IS research assumes, based on memory theory, that if passwords are recalled more frequently and more recently, then they will have higher memorability. However, based on our previous research (Woods 2016), our results suggest that not to be the case. Therefore, we propose conducting another longitudinal study with password frequency of use and time between password use as the focus. Although, based on our previous results, we are not expecting to see an effect of either variable; if either or both do show to have an effect on password memorability, these results will provide more enriched data to support factors that will have been empirically tested to increase password memorability, and support ways in which this can be successfully achieved. This could be applied to, for instance, PIN memorability, two-factor authentication techniques, or even to password managers, to increase memorability of complex unique passwords. On the other hand, if there is no effect of either frequency of use nor time between use on password recall, then this also has important implications where it will suggest that future research should be focusing on other factors to increase password memorability, e.g. user motivation, and that applying memory theories directly to the password problem may not be enough.

Acknowledgements

I would like to thank Prof. Mikko Siponen, Dr. Nan Zhang, and Dr. Markus Salo for their encouraging feedback and guidance during the writing of this paper.

REFERENCES

Adams, A., and Sasse, M. 1999. "Users are not the enemy," *Communications of the ACM* (42:12), December, pp.41–46.

Anderson, M. 2009. "Incidental Forgetting," in *Memory*, A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, Hove & New York, NY: Psychology Press, pp.191-216.

Anderson, J.R., and Schooler, L.J. 1991. "Reflections of environment in memory," *Psychological Science* (2:6), November, pp. 396–408.

Atkinson, R. C., and Shiffrin, R. M. 1968. "Human memory: A proposed system and its control processes," *Psychology of Learning and Motivation* (2), pp. 89-195.

Baddeley, A. D. 1992. "Working memory," *Science* (255), January, pp. 556–559.

Baddeley, A. D. 2009[a]. "What is Memory?" in *Memory*, A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, Hove & New York, NY: Psychology Press, pp.1-18.

Baddeley, A. D. 2009[b]. "Memory and Aging," in *Memory*, A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, Hove & New York, NY: Psychology Press, pp.293-316.

Bang, Y., Lee, D., Bae, Y., and Ahn, J. 2012. "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure," *International Journal of Information Management* (32), February, pp. 409– 418.

Brown, A. S., Bracken, E., Zoccoli, S., and Douglas, K. 2004. "Generating and remembering passwords," *Applied Cognitive Psychology* (18:6), June, pp. 641–651.

Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. 2014. "The Tangled Web of Password Reuse," in NDSS (14), February, pp. 23-26.

Duggan, G. B., Johnson, H., and Grawemeyer, B. 2012. "Rational Security: Modelling everyday password use," *International Journal of Human-Computer Studies* (70), March, pp. 415–431.

Ebbinghaus, H. 1885. Uber das Gediiehtnis. Leipzig: Duncker and Humblot. Translated edition: *Memory*. (1964). New York: Dover.

Gaw, S. and Felten, E. 2006. "Password management strategies for online accounts," in the *Proceedings of the Second Symposium on Usable privacy and security. ACM Press,* New York.

Grawemeyer, B., and Johnson, H. 2011. "Using and managing multiple passwords: A week to a view," *Interacting with Computers* (23), April, pp. 256-267.

Ives, B., Walsh, K. & Schneider, H. 2004. "The domino effect of password reuse," *Communications of the ACM,* (47:4), April, pp. 75–78.

Inglesant, P., and Sasse, M. A. 2010. "The true cost of unusable password policies: password use in the wild," in the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 383-392). ACM*.

Marquardson, J. 2012. "Password Policy Effects on Entropy and Recall: Research in Progress," *in Proceedings of the 8th Americas Conference on Information Systems,* August, Seattle, Washington.

Mujeye, S., and Levy, Y. 2013. "Complex passwords: How far is too far? The role of cognitive load on employee productivity," *Online Journal of Applied Knowledge Management* (1:1), pp.122-132.

Nelson, T. O. 1977. "Repetition and depth of processing," *Journal of Verbal Learning and Verbal Behavior* (16:2), pp. 151-171.

Nelson, D., and Vu, K. L. 2010. "Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords," *Computers in Human Behavior* (26:4), February, pp. 705–715.

Nilsson, L.-G. 1987. "Motivated memory: Dissociation between performance data and subjective reports," *Psychological Research* (49), August, pp. 183-188.

Saastamoinen, A. 2014. "Lomalla unohtuneet salasanat tulevat työnantajille kalliiksi – jopa satojen tuhansien kustannukset". Retrieved September 24, 2015, from http://yle.fi/ylex/uutiset/lomalla_unohtuneet_salasanat_tulevat_tyonantajille_kalliiksi_jopa_satojen_tuhansien_kustannukset/3-7580109.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. 2010. "Encountering stronger password requirements: User attitudes and behaviors," *in the Symposium on Usable Privacy and Security, SOUPS' 10*, Redmond, WA, USA.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., and Cranor, L. F. 2016. "Do Users' Perceptions of Password Security Match Reality?," *in the Proceedings of the CHI Conference on Human Factors in Computing Systems*, ACM, pp. 3748-3760.

Woods, N. 2016. "Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory" PhD thesis, University of Jyväskylä, Finland.

Zhang, J., Luo, X., Akkaladevi, S., and Ziegelmayer, J. 2009. "Improving multiple password recall: An empirical study," *European Journal of Information Systems* (18:2), February, pp.165–176.

Zviran, M., and Haga, W. J. 1999. "Password security: an empirical study," *Journal of Management Information Systems* (15:4), March, pp.161-185.