The Light Side of Passwords: Turning Motivation from the Extrinsic to the Intrinsic
Research in Progress

Naomi Woods[1]
Faculty of Information Technology, University of Jyväskylä,
Jyväskylä, Finland

ABSTRACT

There are many good and bad aspects to password authentication. They are mostly without cost, securing many accounts and systems, and allowing users access from anywhere in the world. However, passwords can elicit dark side phenomena, including security technostress; with many users feeling negatively towards them, as they struggle to cope with the sheer numbers required in their everyday lives. Much research has attempted to understand users' interactions with passwords, examining the trade-off between security, memorability, user convenience, and suggesting techniques to manage them better. However, users continue to struggle. Many studies have shown that users are more concerned with goals other than security, such as convenience and memorability. Therefore, we need to offer another reason that will entice users to engage with the password process more securely. In this study, we suggest that engaging with the password process (creating, learning and recalling passwords) well, is similar to memory training. Therefore, we propose that the "light side" of passwords – the positive reason for properly creating and learning strong passwords, and recalling them successfully, will improve users' memories for passwords and memory functioning in general. Consequently, changing their motivation from an extrinsic goal to an intrinsic goal – improved memory functioning.

Keywords: passwords; authentication; memory; motivation; mnemonics; memory training

[1] Corresponding author: naomi.woods@jyu.fi +358 408054417

INTRODUCTION

Password numbers are consistently growing (Das et al. 2014; Grawemeyer and Johnson, 2011; Zhang et al. 2009). This is not necessarily due to their popularity, but is due to the number of accounts that users accumulate, and the issues pertaining to password alternatives (e.g., biometrics and password managers), such as trust, habit and usability (Alkaldi et al. 2019; Renaud and De Angeli 2004; Stobert and Biddle 2014).

The problem with passwords is that there are too many accounts nowadays; and trying to create, learn and recall unique, strong passwords that meet password policy requirements to secure each account, is incredibly demanding (Nelson and Vu 2010; Tam et al. 2010). Therefore, many users will adopt insecure password behaviors such as, creating weak passwords, reusing passwords, storing passwords in an insecure manner, and sharing passwords (Adams and Sasse 1999; Marquardson 2012; Zhang et al. 2009). These behaviors have numerous consequences in terms of loss of money and time, security breaches, reduced productivity, and increased inconvenience (Mujeye and Levy 2013; Renaud and De Angeli 2004; Vu et al. 2007). Overall, these consequences give passwords a negative reputation, and many users feel frustrated and suffer with security technostress (a dark side phenomenon) as a result (Ament and Haag 2016; Herley and Oorschot 2012). Moreover, these negative feelings affects users' motivations to put effort into interacting with passwords securely and the memorability of them (Nelson and Vu 2010; Zhang et al. 2009).

Information Systems (IS) research has examined password security from two different perspectives. The first considers password security behavior and policy compliance in terms of all other IS security behaviors and compliance, and identify ways in which to increase security. Researchers apply behavioral theories such as deterrence theory, protection motivation theory, and self-determination theory, examining intrinsic and extrinsic motivation towards security

compliance and to explain why users adopt insecure behaviors (Herath and Rao 2009; Johnston et al. 2015; Padayachee 2012; Siponen et al. 2014; Vance et al. 2013; Workman et al. 2008). Although, there has been some valuable findings, these theories do not take into account the user's memory. The second perspective examines password security behavior and the interaction and effect of the user's memory on the behavior. Many studies have investigated different aspects of the human memory; the effects of password policies; and explore memory techniques and technologies to improve memorability and security (Adams and Sasse 1999; Campbell et al. 2011; Chiasson et al. 2009; Das et al. 2014; Nelson and Vu 2010; Stobert and Biddle 2014; Woods and Siponen 2019; Yang et al. 2016; Zhang et al. 2009). There have also been suggestions to make the process "more fun" with a game-style experience (e.g., Brumen 2019; McLennana et al 2017); although, still with the goal of increasing security. Security should be the goal, and is the ultimate goal; but this may not be the goal of many users. Research has consistently shown how "users are the weakest link in security" (Sasse et al. 2001), and value convenience and other goals over security (Grawemeyer and Johnson 2011; Tam et al. 2010; Zhang et al. 2009). Research could approach this from another angle and look at the positive things that users would appreciate. Several studies have shown that practicing and training people's memories will enhance their capabilities (e.g., Baniqued et al. 2014; Strobach and Huestegge 2017). The password process has many similarities in the tasks undertaken in memory training. Therefore, this study proposes the "light side" of passwords, that through engaging in the password process thoroughly and properly (through using memory techniques to create and learn strong unique passwords, and recall them successfully), this could increase users' memory capabilities for remembering passwords and their memory in general. This will increase users' intrinsic motivation, giving users a valuable reason to interact with password authentication, and increase security.

MEMORY THEORIES AND THE PASSWORD CONTEXT

Understanding how the human memory functions and processes information is an important area of investigation within cognitive science, psychology, and more recently, information systems. IS researchers apply theories such as the Modal Model – a multi-store model of memory by Atkinson and Shiffrin (1968), to understand the characteristics of the memory, how information is processed, and how passwords are processed.

Motivation to learn and recall information can have an effect on the success of the process (Woods and Siponen 2019), so too as with learning and recalling passwords. From the self-determination theory (Ryan and Deci 2000), motivation can be divided into two different types: intrinsic motivation (internal) and extrinsic motivation (external). Intrinsic motivation is the internal drive to pursue new experiences, to gain knowledge, and learn new things to further one's own cognitive and social development. It is a result of an interest or enjoyment in the task, existing internally, not due to external pressures, for example, learning a computer package to gain better skills for a job. Extrinsic motivation is the drive to pursue activities due to external goals, for example, rewards such as money, or sanctions when misbehaving (Ryan and Deci 2000). Motivation and intention to learn and recall is important for focusing attention (Nilsson 1987). If there is a lack of interest or negative attitude towards the information, attention will be diverted, and therefore, learning and recalling is less likely to occur (Anderson 2009).

Improving memory: techniques

There are countless mnemonic techniques and strategies that improve people's memories, including visual imagery techniques such as, method of loci, and the pegword system. Verbal mnemonics are another type of mnemonic technique that can equally improve people's memory (Eysenck 2009). They include word mnemonics, when the first letters of each word to be learnt are used to form another word, for example, "HOMES" (Huron, Ontario, Michigan, Erie, and

Superior – the Great Lakes). Story mnemonics on the other hand is another verbal mnemonic technique that helps people learn a sequence of unrelated words in a specific order by linking the words together through the context of a story (Bower and Clark 1969).

Most people use memory techniques and strategies in their everyday lives, including writing a shopping list and notes (Dixon et al. 1988; Eysenck 2009). However, external techniques like this become a security issue when using them to remember passwords, for example, writing passwords down (Woods and Siponen 2018). Therefore, internal memory techniques and strategies such as, mnemonics are suggested by many researchers to help learn and retain passwords, and also create strong passwords (e.g., Nelson and Vu 2010; Vu et al. 2007; Yang et al. 2016).

UTILIZING THE PASSWORD PROCESS TO INCREASE INTRINSIC MOTIVATION

Many people's intrinsic motivation have led them to seek ways to improve their brain: metal agility, memory and intelligence; by the means of brain training and brain games (Makin 2016; Simons et al. 2016). Much research has suggested that cognitive improvements, including enhancements in memory performance, can be achieved through training; however, the notion that intelligence can be increased just through sheer gaming is hotly contested (Strobach and Huestegge 2017). Many studies have shown inconsistent findings which has been suggested due to issues in the measurement and interpretation of outcomes, and issues with control groups (Makin 2016). However, the upshot of most studies are that even with these conflicting results, any improvements that occur are for similar tasks that are related to those used in the training (near-transfer); but it still remains unclear if improvements occur in other memory tasks (Makin 2016; Strobach and Huestegge 2017).

Even with these inconsistent results, many people still engage with memory games for self-improvement purposes (Owen et al. 2010). However, there is a process that involves

practicing memory tasks that most people have to engage with every day, and in most cases many times a day: the password process. Security motivations seem to not be enough to motivate users to engage with password authentication in a proper manner. Therefore, we suggest that we should promote what is "good" about passwords to entice users through the potential improvement to their memory functioning. It is unclear if this cognitive improvement will be extended to other (more general) memory tasks; however, even if users' memories are not significantly improved, will believing they will be improved motivate them enough to engage with password practices more securely and thoroughly? We therefore, propose these hypotheses in Table 1.

Table 1: Proposed hypotheses

Hypothesis number	Hypothesis description
H1	Learning and practicing memory techniques will have a positive effect on memory functioning in similar tasks.
H2	Learning and practicing memory techniques will positively improve memory functioning in general tasks.
H3	Learning and practicing memory techniques will have a positive effect on successfully recalling passwords.
H4a	Learning and practicing memory techniques will have a positive effect on how fast passwords are created.
H4b	Learning and practicing memory techniques will have a positive effect on how easily passwords are created.
H4c	Learning and practicing memory techniques will have a positive effect on the level of convenience when creating passwords.
H5	Learning and recalling passwords using learnt memory techniques will have a positive effect on users' memory performance.
H6	Being informed that learning and recalling passwords is a successful brain training exercise will have a positive effect on memory performance.
H7	Being informed that learning and recalling passwords is a successful brain training exercise will have a positive effect on successful password recall.

PROPOSED EXPERIMENTAL DESIGN AND PROCEDURE

To study the effects of learning and practicing memory techniques on users' memory and password performance, two longitudinal studies are proposed (summarized in Table 2).

Table 2: Details of proposed studies – groups, design, and procedure

Study 1	**Group content**	**Pre-test**	**Intervention**	**Post-test**
Control Group	Minimum 30 participants Matched on age	Memory performance test	Game (e.g., Angry Birds – not a memory game)	Memory performance test
Experimental Group 1	Minimum 30 participants Matched on age	Memory performance test	Word mnemonic training	Memory performance test
Experimental Group 2	Minimum 30 participants Matched on age	Memory performance test	Story mnemonic training	Memory performance test
Study 2	**Group content**	**Pre-test**	**Intervention**	**Post-test**
Control Group	Same as Study 1 Matched on age	N/A – continuation from Study 1	Password Process (creating, learning, recalling passwords)	Memory performance test
Experimental Group A	Half of Exp Grp 1 + half of Exp Grp 2 Matched on age	N/A – continuation from Study 1	Password Process (creating, learning, recalling passwords)	Memory performance test
Experimental Group B	Half of Exp Grp 1 + half of Exp Grp 2 Matched on age	N/A – continuation from Study 1	Password Process (creating, learning, recalling passwords) + informed the process will improve memory functioning	Memory performance test

Measures

Pre- and post-tests will measure memory performance through standardized memory tests (e.g., Auditory-Verbal Learning Test (AVLT) (Rey, 1964), and Wechsler Memory Scale – Revised (WMS-R) (Wechsler, 1987)), to gauge the effect of the interventions. In Study 1, experimental group 1 will be given word mnemonics instructions, and experimental group 2 will be given story mnemonics instructions. Both experimental groups will be given a list of 10 words, and asked to create 10 responses based on the memory technique of their group. For example, list word: "home"; response example: "T'snplh:WoO" (word mnemonic of "**T**here**'s n**o **p**lace **l**ike **h**ome" from the **W**izard **o**f **O**z); or "Catpianosleepwork" (story mnemonic; participants could choose the word group and the story that links them all together). Both groups

will be asked to learn, and then recall them several times over the period of a week. The control group will be provided with a game to play, that will not be similar in task (e.g., Angry Birds – not a memory test). Questionnaires will ask participants to report on their experiences. The post-intervention test will finalize Study 1. Study 2 will involve all groups creating, learning and recalling passwords for five fake accounts on a purpose-built website, using a similar experimental design in studies from Woods and Siponen in 2018 and 2019. Both experimental groups will apply their mnemonic techniques. However, experimental group B will be informed that engaging with the password process is a form of brain training and will ultimately improve their memory. The website will monitor all login attempts and times, including successful attempts, and login failures. Questionnaires will be provided for participants to report their experiences with creating learning and recalling passwords, and their motivation towards the process. All groups will be given one final post-intervention memory test, and a questionnaire to report their experiences and their awareness and belief that engaging with the password process is a form of memory training (as a manipulation check).

EXPECTED RESULTS

Various between- and within-subject ANOVAs will be employed to test the seven hypotheses, examining the effects of memory training on the password process and on memory performance. Based on previous research suggesting that brain training can improve memory in 1-transfer (similar) tasks (Strobach and Huestegge 2017), we expect the results to show an improvement in memory performance, and all aspects of the password process (creating, learning and recalling passwords). However, with learning from previous research issues in methodology, we will also examine the effect of whether believing the password process will have an effect on memory performance, and whether this belief will motivate (intrinsically) users to engage more thoroughly with the password process. Therefore, even though we expect to improve

participants' memories through engaging with the password process as a memory training practice, if there is no or very little improvement, we do expect that believing that it will, will have an effect on participants' motivations.

IMPLICATIONS AND CONCLUSION

This study strives to find reason to successfully motivate users to assign more effort to the password process and engage more thoroughly, as security goals do not seem to be enough for many (Grawemeyer and Johnson 2011; Tam et al. 2010; Zhang, et al. 2009). The expected results would suggest that engaging with the password process in a more thorough way, by putting in the effort to use a memory technique to create and learn strong unique passwords, and recall them successfully could act as memory training, ultimately increasing users' memories. The results could have important implications, highlighting the "light side" of passwords – a positive reason to increase users' intrinsic motivation, not just extrinsic motivation with security as the goal. Through increasing password memorability, and through the creation of stronger passwords, this will have important security implications as it could potentially lead to a decrease of other insecure password behaviors, less security breaches, and less money lost and spent on security breaches.

REFERENCES

Adams, A., and Sasse, M. A.1999. "Users are not the enemy," *Communications of the ACM* (42:12), pp. 41–46 (doi: 10.1145/322796.322806)

Alkaldi, N., Renaud, K., and Mackenzie, L. 2018. "Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs," In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, HICSS, Hawaii, (doi: 10.24251/HICSS.2019.582).

Ament, C., and Haag, S. 2016. "How Information Security Requirements Stress Employees," *Thirty-Seventh International Conference on Information Systems*, Dublin 2016.

Anderson, M. 2009. "Retrieval," in *Memory* (1st. ed.), A. Baddeley, M. W. Eysenck and M. C. Anderson. (eds.), Hove & New York, NY: Psychology Press, pp. 163 – 190.

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.

Baniqued, P. L., Kranz, M. B., Voss, M. W., Lee, H., Cosman, J. D., Severson, J., and Kramer, A. F. 2014. "Cognitive training with casual video games: points to consider," *Frontiers in psychology*, (4), pp. 1010.

Bower, G. H., and Clark, M. 1969. "Narrative stories as mediators for serial learning," *Psychonomic Science,* (14), pp. 181 – 182.

Brumen, B. 2019. "Security analysis of Game Changer Password System," *International Journal of Human-Computer Studies*, (126), pp. 44-52, (doi: doi.org/10.1016/j.ijhcs.2019.01.004)

Campbell, J., Ma, W., and Kleeman, D. 2011. "Impact of restrictive composition policy on user password choices," *Behaviour and Information Technology* (30: 3), pp. 379–388, (doi: 10.1080/0144929X.2010.492876)

Chiasson, S., van Oorschot, P.C., and Biddle, R. 2006. "A Usability Study and Critique of Two Password Managers," in *Proceedings of the 15th USENIX Security Symposium '06*, pp.1-16.

Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. 2014. "The Tangled Web of Password Reuse," in Proceeding of NDSS'14, San Diego, CA, pp. 23-26.

Dixon, R. A., Hultsch, D. F., and Hertzog, C. 1988. "The metamemory in adulthood (MIA) questionnaire," *Psychopharmacology Bulletin,* (24), pp. 671–688.

Eysenck, M. W. 2009. "Improving your memory," in *Memory* (1st. ed.), A. Baddeley, M. W. Eysenck and M. C. Anderson. (eds.), Hove & New York, NY: Psychology Press, pp. 357 – 380.

Grawemeyer, B., and Johnson, H. 2011. "Using and managing multiple passwords: A week to a view," *Interacting with Computers* (23), pp. 256-267, (doi: 10.1016/j.intcom.2011.03.007).

Herath, T., Rao, H.R. 2009. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Herley, C., and Van Oorschot, P. 2011. "A research agenda acknowledging the persistence of passwords," *IEEE Security & Privacy*, (10:1), pp. 28-36.

Johnston, A.C., Warkentin, M., Siponen, M. 2015. "An Enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric," *MIS Quarterly* (39:1) pp. 113–134.

Makin, S. 2016. "Memory games," *Nature*, (531:7592), pp.S10.

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

McLennan, C. T., Manning, P., and Tuft, S. E. 2017. "An evaluation of the Game Changer Password System: A new approach to password security," *International Journal of Human-Computer Studies*, (100), pp. 1-17.

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, 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), pp. 705–715, (doi: https://doi.org/10.1016/j.chb.2010.01.007).

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

Owen, A. M., Hampshire, A., Grahn, J. A., Stenton, R., Dajani, S., Burns, A. S., Howard, R. J., and Ballard, C. G. 2010. "Putting brain training to the test," *Nature*, (465: 7299), pp. 775.

Padayachee, K. 2012. "Taxonomy of compliant information security behavior," *Computers & Security* (31:5), pp. 673-680.

Renaud, K.., and De Angeli, A. 2004. "My password is here! An investigation into visuo-spatial authentication mechanisms," *Interacting with Computers* (16: 6), pp. 1017–1041, (doi: https://doi.org/10.1016/j.intcom.2004.06.012).

Ryan, R.M., Deci, E.L. 2000. "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being," *American Psychologist,* (55:1), pp. 68–78.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security," *BT Technological Journal* (19:3), pp. 122-131, (doi: 10.1023/A:1011902718709).

Simons, D. J., Boot, W. R., Charness, N., Gathercole, S. E., Chabris, C. F., Hambrick, D. Z., and Stine-Morrow, E. A. (2016). "Do Brain training programs work?" *Psychological Science in the Public Interest,* (17:3), pp. 103–186.

Siponen, M., Mahmood, M.A., Pahnila, S. 2014. "Employees' adherence to information security policies: An exploratory field study," *Information & management* (51:2) pp. 217-224.

Stobert, E., and Biddle, R. 2014. "A Password Manager that Doesn't Remember Passwords," in *Proceedings of the 2014 New Security Paradigms Workshop,* NSPW '14, New York, NY: ACM, pp. 39-52, (doi: 10.1145/2683467.2683471).

Strobach, T., and Huestegge, L. 2017. "Evaluating the effectiveness of commercial brain game training with working-memory tasks," *Journal of Cognitive Enhancement*, (1:4), pp. 539-558.

Tam, L., Glassman, M., and Vandenwauver, M. 2010. "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology* (29:3), pp. 233–244.

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

Woods, N., and Siponen, M. 2018. "Too many passwords? How understanding our memory can increase password memorability," *International Journal of Human-Computer Studies* (111), pp.36-48, (doi: https://doi.org/10.1016/j.ijhcs.2017.11.002).

Woods, N., and Siponen, M. 2019. "Improving password memorability, while not inconveniencing the user," *International Journal of Human-Computer Studies,* (128), pp. 61-71.

Workman, M., Bommer, W.H., Straub, D. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24) pp. 2799–2816.

Yang, W., Li, N., Chowdhury, O., Xiong, A., and Proctor. R.W. 2016. "An empirical study of mnemonic sentence-based password generation strategies," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16,, New York, NY: ACM, pp. 1216 – 1229, (doi: 10.1145/2976749.2978346).

Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J., 2009. "Improving multiple password recall: An empirical study," European Journal of Information Systems (18: 2), pp.165–176, (doi: 10.1057/ejis.2009.9).