Improving Password Memorability, While Not Inconveniencing the User

Naomi Woods , Mikko Siponen

PII: S1071-5819(19)30010-2
DOI: https://doi.org/10.1016/j.ijhcs.2019.02.003
Reference: YIJHC 2289

To appear in: *International Journal of Human-Computer Studies*

Received date: 15 December 2017
Revised date: 31 January 2019
Accepted date: 6 February 2019

Please cite this article as: Naomi Woods , Mikko Siponen , Improving Password Memorability, While Not Inconveniencing the User, *International Journal of Human-Computer Studies* (2019), doi: https://doi.org/10.1016/j.ijhcs.2019.02.003

Highlights

- Increasing the number of password verification times by twice or three times, can significantly increase password memorability.
- Increasing the number of password verification times by twice or three times does not increase user inconvenience.
- The trade-off between password memorability and user convenience is not proportionately affected.

IMPROVING PASSWORD MEMORABILITY, WHILE NOT INCONVENIENCING THE USER

Naomi Woods and Mikko Siponen

University of Jyväskylä

Faculty of Information Technology

Agora, Mattilanniemi 2

40100 Jyväskylä

Finland

naomi.woods@jyu.fi

mikko.t.siponen@jyu.fi

Corresponding author: Naomi Woods

naomi.woods@jyu.fi

tel. +358 40 805 4417

Abstract

Passwords are the most frequently used authentication mechanism. However, due to increased password numbers, there has been an increase in insecure password behaviors (e.g., password reuse). Therefore, new and innovative ways are needed to increase password memorability and security. Typically, users are asked to input their passwords once in order to access the system, and twice to verify the password, when they create a new account. But what if users were asked to input their passwords three or four times when they create new accounts? In this study, three groups of participants were asked to verify their passwords once (control group), twice, and three times (two experimental groups). Psychological literature suggests that applying repetition in learning to the password process has significant effects on password memorability. However, previous password research has found a trade-off between password security and memorability, and more recently, user convenience. Our results suggest that verifying passwords three times can increase password memorability from 42% (verifying passwords just once as with current practices) to 70%. Even by increasing the verification to just two times can increase password memorability by 17%. However, we found that through increasing the number of verifications did not equate to a decrease in user convenience. What this means is that small changes to the password verification stage can have significant results on password memorability while not necessarily inconveniencing the user. The implications of these results could ultimately have a positive effect on password security, and the consequences of forgetting passwords.

Keywords: Password security; password memorability; repetition; password verification; user convenience; password security behavior

1. Introduction

Passwords are one of the most frustrating, inconvenient, yet essential part of users' daily lives (Hoonakker et al., 2009; Zhang et al., 2009). Over the past few years, the number of passwords has risen with users accumulating more and more accounts and services (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009). Despite that users are more aware of password security issues; as a result of difficulties in remembering multiple passwords, users often employ risky password behaviors as coping strategies to aid password memorability (Biddle et al., 2012; Campbell et al., 2006; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011; Notoatmodjo and Thomborson, 2009; Zhang et al., 2009). These insecure password behaviors include, password reuse, writing passwords down, sharing passwords, choosing weak passwords, and not changing passwords regularly (Adams and Sasse, 1999; Campbell et al., 2006; Guo, 2013; Zhang et al., 2009). As a consequence of adopting these insecure password behaviors, organizations spend thousands (in costs) each year on resetting passwords when they are forgotten, and through the losses due to security breaches (Brown et al., 2004; Hayashi et al., 2012; Inglesant and Sasse, 2010; Ives et al., 2004; Saastamoinen, 2014; Tari et al., 2006; Vu et al., 2007). Users forgetting their passwords and adopting insecure password behaviors bring into question the ultimate security of passwords and the future of the mechanism (Grawemeyer and Johnson, 2011).

Although passwords are an unpleasant necessity, users cannot (currently) live without them as they secure personal and organizations' finances, communications and information (Bang et al., 2012; Vu et al., 2007). There are alternatives such as password managers and biometrics. However, several studies have found that even though password manager software has been around since the 1990's, their use has been reported to be limited. Das et al. (2014) found that out of 224 participants, 61% memorize their passwords, where only 6% use password managers; and Alkaldi et al. (2019) found that during a study using persuasive

messages in favor of password managers that 70% of users did not download the software. Low acceptance of password managers has been reported due to issues such as users believing that they are vulnerable to attacks, preferring to trust their own memory (Gaw and Felton, 2006), and that they are not adequately usable for most users (Chiasson et al., 2006). Biometrics also have the disadvantages, and have not become mainstream due to money (i.e., the cost of the new technology, and changing systems), convenience (users having to learn a new technology), and habit – users like familiarity, and place trust in it (Florêncio and Herley, 2007). Despite the issues with passwords, they are the most popular authentication mechanism (Grawemeyer and Johnson, 2011; Zhang et al., 2009). Therefore, researchers have spent many years attempting to find ways in which to increase their memorability, while not consequently affecting their security, or increasing the inconvenience of the process – which is proving to be an arduous (and perhaps, impossible), but critical task (Grawemeyer and Johnson, 2011).

This study focuses on password verification – a part of the password creation stage – where the user is asked, after creating his or her password, to re-enter it. Although previous password research has considered repetition/rehearsal as a means of increasing memorability, and have incorporated additional verification into their study design (Bonneau and Schechter, 2014; Vu et al., 2007; Wiedenbeck et al., 2005; Woods and Siponen, 2018; Zhang et al., 2009); no previous research has examined the practicalities of learning passwords through the repetition of verification, while considering the impact on user convenience. Based on psychological literature, we suggest that increasing the number of times a user is required to verify their password could have a positive effect on the memorability of that password. Furthermore, small changes to the password verification process could be implemented with any authentication system, which could have significant results on password memorability. However, increasing the number of password verification times would increase the amount of

time given to the password process of creating, learning, and recalling passwords, which would surely increase user inconvenience (Jenkins et al., 2014; Renaud and De Angeli, 2004; Zhang and McDowell, 2009). Therefore, in this study, we examine the balance between memory and convenience, to see whether the small increase in the number of verification times significantly affects password memorability, and user convenience.

We test our hypotheses using an experimental design, involving participants creating and recalling passwords on a web-based system. We examine the effects of three experimental conditions (verifying passwords x1, x2, x3) on password recall and user convenience in verifying passwords at the creation stage. Our findings suggest that increasing the number of times a password is verified, has a positive effect on password memorability, while not having a considerable effect on the users' convenience. In the next section, we discuss previous research in password security, memorability, and user convenience. Then we examine memory theories, and more specifically, theories of learning and retention, and develop our hypotheses. In the following sections, we discuss the research methodology, including the experimental design, and then present our findings. Finally, we discuss our findings and their implications.

2. Previous password research

Users are required to find the time to create and learn passwords, while trying to comply with password policies (Inglesant and Sasse, 2010; Marquardson, 2012). They are then required to remember their passwords out of a multitude of often similar passwords, and match them to the right account (Grawemeyer and Johnson, 2011; Nelson and Vu, 2010). And users must do all of this while contending with their everyday tasks, be it work, shopping, banking, or communication (Grawemeyer and Johnson, 2011; Hoonakker et al., 2009). Previous research has examined these issues from the perspective of the password

problem as a memory problem (Adams and Sasse, 1999; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011; Nelson and Vu, 2010; Wiedenbeck et al., 2005; Woods and Siponen, 2018; Vu et al., 2007); and from the perspective of the password problem being a security behavior issue as like any other security behavior (Crossler et al., 2013; Jenkins et al., 2014; Johnston et al., 2015; Pahnila et al., 2007; Vance et al., 2013; Workman et al., 2008). Through the first stream of research, studies have shown that there is a trade-off not only between memorability and security (Vu et al., 2007; Zhang et al., 2009), but also between password security and convenience (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009).

2.1. The password problem: a trade-off between password security, password memorability, and user convenience

The authentication mechanism should be secure, memorable, usable, and convenient, that is, not too time-consuming (Renaud and De Angeli, 2004). Previous research suggests that there is a trade-off between password security and password memorability (Vu et al., 2007; Zhang et al., 2009). Strong versus weak passwords, and meaningful passwords are preferred over random passwords (Marquardson, 2012; Nelson and Vu, 2010; Sasse et al., 2001; Wiedenbeck et al., 2005). For example, users will choose names or dictionary words as passwords because users perceive them to be memorable. However, such passwords are easily cracked (Nelson and Vu, 2010; Wiedenbeck et al., 2005); with security being compromised for more memorable passwords. However, just because a password is random (and potentially stronger) does not mean that it is not meaningful to the user (Sasse et al., 2001). Nonetheless, users are more concerned with remembering their passwords than with securing information (Grawemeyer and Johnson, 2011). Therefore, more often than not, weak passwords are created, and passwords are reused and written down as a coping strategy for cognitive offloading (Grawemeyer and Johnson, 2011; Zhang et al., 2009).

Researchers are beginning to find that convenience is also an important contributing factor that influences password security and memorability (Bang et al., 2012; Hoonakker et al., 2009; Jenkins et al., 2014; Tam et al., 2010; Thing and Ying, 2009). Inconvenience caused to the user within the password context refers to the inconvenience experienced when time and mental effort are spent on the password process (creating, learning, and recalling passwords) (Jenkins et al., 2014; Renaud and De Angeli, 2004; Zhang and McDowell, 2009). An example of this would be when a user has to change a password and takes the time to create a new one that meets the service's password policy requirements. Previous research suggests that the inconvenience experienced by the user while engaging in the password process can lead to the adoption of insecure password behaviors, such as writing passwords down, creating weak passwords, and reusing passwords, due to passwords being too hard to remember and/or the password process being too inconvenient (Marquardson, 2012; Nelson and Vu, 2010; Sasse et al., 2001; Tam et al., 2010; Wiedenbeck et al., 2005).

A study by Tam et al. (2010) reported users saying that "If I have to, I can remember my password even if it is complex, but I'd rather not put the mental effort into it. I'd rather write it down and tape it to my computer because it is more convenient . . . one less thing to be bothered with" (p. 237). Issues with password memorability and forgetting passwords can be an expensive security issue, as well as lead to user inconvenience (Al-Ameen et al., 2015). Users are motivated by, and prioritize minimizing inconvenience over increasing security, and adapt their behavior accordingly (Duggan et al., 2012; Notoatmodjo and Thomborson, 2009; Tam et al., 2010; Weir et al., 2009). Moreover, password policy requirements increase the effort users expend on the password process (Inglesant and Sasse, 2010). Therefore, the inconvenience experienced by the user can result in insecure password practices (Tam et al., 2010). Examples of these insecure behaviors include users frequently creating passwords that are easy to remember, as they are considered more convenient, and therefore, aid memory

limitations (Campbell et al., 2011; Zhang and McDowell, 2009). Changing passwords is also considered inconvenient, and therefore, users will not change their passwords regularly (Bang et al., 2012; Furnell, 2013; Gaw and Felten, 2006; Zhang and McDowell, 2009). Another insecure password behavior is password sharing. Users sometimes share passwords, not necessarily because they are incapable of remembering their passwords, but because this practice is convenient, even though they are aware of the security implications (Cheroen et al., 2008).

"When users perceive inconvenience and have to pay a price of time and effort, they are usually reluctant to adopt the recommended action" (Zhang and McDowell, 2009, pp. 191). Therefore, more research is needed to examine the trade-off between convenience, memorability, and security (Hoonakker et al., 2009; Weir et al., 2009), when considering ways in which to increase these factors concurrently.

3. Theoretical background

One of the major issues with the password mechanism is the number of passwords users require in their everyday lives (Chiasson et al., 2009; Zhang et al., 2009). With an increase in the number of accounts, the number of passwords has just exploded over the past few years (Sharma and Sefchek, 2007). However, this escalation has resulted in a snowballing of insecure passwords behaviors, as a result of users' memories being unable to cope with the sheer number of passwords to learn and remember (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). Therefore, understanding how the users' memory functions is imperative when attempting to solve these issues. Thus, several researchers have studied memory theories to attempt to make passwords more memorable and easier for our brains to process while learning and remembering

(Nelson and Vu, 2010; Sasse et al., 2001; Woods and Siponen, 2018; Vu et al., 2007; Zhang et al., 2009).

3.1. Memory theories

When looking to memory theories to help with issues of password memorability, researchers have examined long-term memory (LTM) for storage and retrieval, in terms of remembering and recalling multiple passwords (Adams and Sasse, 1999; Nelson and Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007; Zhang et al. 2009). Many researchers have made reference to Atkinson and Shiffrin's (1968) Stages of Memory Theory. This prominent theory suggests that the human memory is composed of three memory stores, the sensory memory, short-term memory (STM), and long-term memory (LTM). The sensory memory is thought to be an interface between perception and memory. The STM, or working memory (updated by Baddeley and Hitch (1974)) stores information for a brief period of time, while the information is being processed. The LTM stores information indefinitely after it has been processed, ready for retrieval. When this theory is applied to the password process, the password would be observed and attended to by the sensory memory, it would be learned and rehearsed in STM/working memory, and stored (long-term) in LTM, ready for it to be retrieved.

In addition, studies have examined STM or working memory regarding learning passwords and factors that affect it, such as cognitive load (Jenkins et al., 2014; Marquardson, 2012), depth of processing (Nelson and Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007), and STM capacity limitations (Bang et al., 2012; Proctor et al., 2002; Zhang et al., 2009). The working memory (STM) model was proposed by Baddeley and Hitch (1974) which consists of several components that manipulate information before it is transferred to LTM, or is just forgotten. This processing and manipulation of information is what is

considered as learning. However, the STM has a limited capacity (Baddeley, 2009b). This was first shown by Miller (1956) in his study on the "magical number seven" in information processing. Miller argued that without error, the number of items that could be recalled was usually 7 ± 2. This limitation is an important factor in password memorability, as security policies encourage users to create longer and longer passwords to increase security (Campbell et al., 2011; Marquardson, 2012). However, users can get around this limitation through ordering information into "chunks", for example, USA is one chunk of three larger items: "United States of America"; this recoding of information allows more to be encoded and learned (Baddeley, 2009b). Mnemonic passwords and passphrases work on the same principle, additionally increasing the meaning of the password and therefore, the depth of processing (Nelson and Vu, 2010; Vu et al., 2007).

Depth of processing approach proposed by Craik and Lockhart (1972) suggests that information is processed on several levels. Therefore, with more meaning, information will have many levels. For example, the word "apple" is processed visually as the image, as the word, in terms of it being a fruit, in specific terms as perhaps a person's favorite fruit. This information is processed more deeply, and thus, would be retained better. Several studies have shown that the more levels of processing and deeper levels of meaning would show better retention (Baddeley, 2009d; Craik and Lockhart, 1972; Craik and Tulving, 1975). In terms of passwords, Nelson and Vu (2010) suggested that to add meaning to a password while keeping it secure could be achieved through mnemonic techniques, which would increase memorability.

Cognitive load theory refers to the amount of "mental energy" or effort required to process information (Feinberg and Murphy, 2000). As the amount of information increases, so does the cognitive load on our mental resources. When the amount of information and instruction exceed the capacity and limitations of our mental resources (as the working

memory has a limited capacity in processing information), it can become overloaded (a heavy cognitive load), and therefore, learning decreases (Baddeley, 1992; Miller, 1956). Cognitive load can affect password learning and recall (Jenkins et al., 2014; Marquardson, 2012). Learning passwords requires users to concentrate and use their mental energy to attend to the password. However, there can be distractions, such as attempting to meet password policies, people speaking, work tasks, or personal goals that add to the cognitive load, as this information is processed concurrently (Adams and Sasse, 1999; Jenkins et al., 2014; Notoatmodjo and Thomborson, 2009; Zhang and McDowell, 2009). The level of mental effort expended to learn a password also affects how well it is stored and eventually retrieved from LTM (Nelson and Vu, 2010). Nelson and Vu (2010) found that users do not put enough effort, with no in-depth consideration, into creating their passwords, and this would negatively affect their password recall.

Having discussed these factors that affect learning, and learning passwords, we now look to how information is transferred from STM to LTM in terms of repetition/rehearsal, and how repetition can be incorporated into the password process to encourage this transfer.

3.2. Repetition/rehearsal, learning, and transferring information to LTM

"The process of rehearsal is repeating information over and over" (Goldstein, 2011, pp. 173). Studying learning by scientific experimentation can be traced back to Ebbinghaus in the mid-1880s (Baddeley, 2009a; Ranganath et al., 2012). Ebbinghaus discovered that repetition facilitates learning (Nelson, 1977): "as the number of repetitions increases, the series are engraved more and more deeply and indelibly" (Ebbinghaus, 1885, pp. 53). Repetition in learning is an important part of general memory theories. Atkinson and Shiffrin (1968) emphasized in their Stages of Memory Theory, the role of repetition in improving memorability. There is a relationship between rehearsal and storage in LTM (Jacoby and

Bartz, 1972; Rundus and Atkinson, 1970). Through repetition or rehearsal, information is kept or maintained for longer in STM and subsequently transferred to LTM (Atkinson and Shiffrin, 1968; Jacoby and Bartz, 1972; Nelson, 1977; Rundus and Atkinson, 1970).

However, over the years of psychological research, the understanding that rehearsal alone, as means of transferring information from STM to LTM has been brought into question (Nelson, 1977). Jacoby and Bartz (1972) proposed that continuous rehearsal alone does not increase LTM storage. They suggested that rehearsal may just ensure that information is held in STM; the transfer of information from STM to LTM may be considered as a different process (Jacoby and Bartz, 1972). Furthermore, Craik and Lockhart (1972) with their depth of processing approach also argued that repetition does not affect memorability if the depth of processing is constant. They suggest that only rehearsal which leads to increased depth of processing will have an effect on memory performance (Craik and Lockhart, 1972).

In response to the criticism of repetition and rehearsal, Nelson (1977) discovered in contrast to Craik and Lockhart's findings that recall increased with the number of repetitions. Nelson examined distributed repetition and massed repetition, and found that repetitions, even when massed, have an effect on recall. Nelson concluded that the proposition that same-depth repetition does not facilitate memory recall was not supported, and that the number of rote repetitions is actually correlated to memory recall.

Throughout the years, repetition and rehearsal were thought by many theorists to be all that is needed to learn. A more contemporary view suggests learning can be increased through linking new information to what is already known — this is referred to as elaborate processing (Baddeley, 2009d). When considering specifically learning through repetition, there are two types of rehearsal: maintenance rehearsal and elaborative rehearsal (Goldstein, 2011). Maintenance rehearsal, through the repeating of, say a telephone number, will keep

the information within STM for immediate use, for instance, until you make a call. Elaborative rehearsal is what is used to transfer information from STM to LTM as it incorporates thinking about the meaning of the information and relating it to what is already known (Goldstein, 2011). Furthermore, if the recall of information is expected later after a delay, more retrieval cues will be formed while rehearsing (Jacoby and Bartz, 1972). In addition, Nilsson (1987) found that motivation and intention to learn are important for the focus of attention. Recent studies suggest that repetition without motivation from the learner to organize the information may not necessarily result in learning (Baddeley, 2009d).

3.3. Repetition as password verification

"We are often asked to produce a password under hurried circumstances […] with no opportunity for rehearsal" (Brown et al., 2004, pp. 650). Several studies have noted that repetition and rehearsal have an effect on password memorability (Bonneau and Schehter, 2014; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009), and can also be beneficial when creating passwords (Helkala and Svendsen, 2011). Zhang et al. (2009) suggested that rehearsal is a successful method for learning passwords, as it keeps them in STM longer, and therefore, they would have a higher chance of entering LTM. A study by Wiedenbeck et al. (2005) suggested that passwords are learned only through rote, repetition learning. This would affect password security, as through the lack of meaningful content in random passwords, users would create weak passwords that contain more meaning (Wiedenbeck et al. 2005). Therefore, Wiedenbeck et al. (2005) proposed that due to the meaningful content in graphical passwords, the meaning would aid learning through repetition or rehearsal. On the other hand, Bonneau and Schechter (2014) studied spaced repetition in password learning, where participants entered additional security codes that increased over time. The authors found that gradually increasing the size of the security code, adding a little at a time, allowed

94% of the participants to successfully learn the security codes. Furthermore, research by Vu et al. (2007) found that when they used repetition by adding a verification stage during password creation (one extra time to re-enter) in their study design, participants felt that the login repetitions helped them remember their passwords. The results suggested that logging in several times after generating a password increased password memorability as the repetitions incorporated a delay between creation and initial recall. However, the authors found that re-entering the password as verification at the generation stage had an effect, but not a significant effect, on password memorability. This finding supports the results found by Nelson (1977) when he examined distributed and massed repetition. Distributed over time, repetition has a stronger effect on learning, as found in the study by Bonneau and Schechter (2014). Nevertheless, Nelson (1977) still found that massed repetition also had an effect on memorability. Consequently, in the real-world setting, asking users to re-enter their passwords several times after a delay in creating them would not be practical or convenient. Thus, massed repetition in terms of verification at the password creation stage would be more beneficial.

These studies have noted the importance of repetition in password learning; however, only Bonneau and Schechter (2014) examined repetition as the main focus of their study. Vu et al. (2007) added a re-entry stage to their study design when participants created their passwords, while investigating proactive password checking techniques. Zhang et al. (2009), while investigating interference techniques, encouraged participants to rehearse their passwords, but used no method such as verification to enforce this. It was left to the participants to mentally rehearse the password to retain it better. These studies also entailed creating a number of passwords at one time; this action would have an effect on the participants' cognitive load. Jacob and Bartz (1972) argue that repetition does not necessarily lead to improved memorization but acknowledged that when individuals learn shorter lists of

words, they would be held in STM longer than longer lists of words, and thus, have a higher probability of entering LTM. Therefore, learning many passwords at once would affect password recall. Moreover, this situation would not occur in the real world as multiple passwords are rarely created at the same time. Furthermore, Bonneau and Schechter (2014) examined spaced repetition, but required their participants to learn only one password, again not representing the real-world situation. When Wiedenbeck et al. (2005) used repetition in learning passwords, it was used as an argument for the use of graphical passwords. However, the authors used repetition at the creation stage to increase memorability, through asking participants to re-enter their passwords successfully ten times. Nevertheless, incorporating repetition into learning passwords is acknowledged as having an effect on password memorability (Bonneau and Schechter, 2014; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009). However, all these studies did not consider the practical application of using verification for learning through repetition, while considering the effect of repetition on convenience, and the levels of convenience on password memorability and security.

4. The Current study

In this study, we examine the effects of repetition on password recall. When users create passwords, they are asked to re-enter their passwords for verification, as a part of the password creation stage (Vu et al., 2007). Through increasing the number of times a user is required to verify their password, can we utilize this stage in the password creation process to increase the memorability of passwords? However, would increasing the number of times a password is verified decrease user convenience? Users cannot be expected in the real world to enter their passwords five, ten, or fifteen times when creating them. Therefore, we examine the balance between password memorability and user convenience, to see whether a small increase in the number of verification times can have a significant effect on password

memorability, with the prospect of increasing password security. Thus, we propose the following hypotheses:

H1: Increasing the number of password verification times would have a positive effect on password recall.

H2: Increasing the number of password verification times would have a negative effect on user convenience.

5. Research methodology

To test the hypotheses, we employed a longitudinal experimental design, collecting objective data in terms of password recall (over 1500 passwords) and subjective data in the form of questionnaire responses measuring user convenience.

5.1. Participants

One hundred five participants were recruited from a Finnish university; they included staff, faculty, and students. All participants had work experience and were experienced computer users. Out of the 105 participants initially recruited, 15 participants did not complete the experiment (dropping out after recruitment). Therefore, 90 participants completed the entire study. Study credits or movies tickets were offered to the participants as an incentive for taking part and for completing the study. The 90 participants were allocated into three groups: control group (verification x1 (N=30)), and two experimental groups: (verification x2 (N=30), and verification x3 (N=30)). Due to the effect of age on memory, all participants were matched on age across all three groups (Baddeley, 2009c).

5.2. Measures

A website was created to collect all data for the study. The website allowed participants to create and recall passwords, and answer questionnaires that measured the participants'

experience. However, for the purposes of this study, only the user convenience construct related to password verification was examined. The website also contained information about the study, the schedule details, and guidelines for participants to create passwords. The website would ask the participants when they were creating their passwords to verify their passwords once, twice, or three times, depending on the group to which the users were allocated.

5.2.1. Objective data

The objective password recall data was collected via the website regardless whether the participants entered their passwords correctly or incorrectly. Over five weeks, the participants created five passwords for five fictitious accounts, and recalled the passwords several times. The account types were of varying importance and sensitivity: online banking, email, social networking, online shopping, and online gaming. Five accounts and passwords were chosen as there are a number of studies that have also used this number (Nelson and Vu, 2010; Vu et al., 2007; Zhang et al., 2009); based on the suggestion that users can successfully remember that number of unique passwords (Adams and Sasse, 1999). A longitudinal design was employed to prevent cognitive overloading, as the increased cognitive load would affect the learning and recalling process (Baddeley, 1992). This type of design was also employed to make the study as realistic as possible, as it is rare that users are asked to create and recall several passwords all at one time.

Seven password creation rules imposed a minimum length, complexity, and variety (reported in Table 1). These password composition policy rules were chosen for two reasons. First, the rules added more realism to the study in terms of context, as these rules are common on the most popular and top websites on the internet (Mayer et al., 2017; Zhang et al., 2009). Second, the rules added more realism in terms of the types of password users have to memorize in their everyday lives. Having no rules with minimum requirements would

allow participants to create passwords, such as "A" or "1," that would not really represent a realistic test of password memorability. The password creation rules were based on NIST SP 800-63 (Burr et al., 2006). Although these rules have been recently updated (Grassi et al., 2017), they are still imposed on many popular websites (Mayer et al., 2017) and used in several password memorability studies (e.g., Vu et al., 2007; Zhang et al., 2009). The system criteria were the requirements that enforced the password creation rules on the website used in this study (see Table 1).

Table 1. Password rules and system criteria for creating passwords

Each password must:
1. contain at least eight characters. 2. contain at least one number (0–9). 3. contain at least one lowercase letter (a–z). 4. contain at least one uppercase letter (A–Z). 5. contain at least one special character (e.g., !, %, &). 6. contain no words or names (e.g., J78skyl8?). 7. be unique = different from every other password created, preferably different in meaning too (e.g., J78skyl8? and ilo>TV1!).
System criteria: passwords must contain:
• more than eight characters consisting of the English alphabet A–Z, a–z. • at least one uppercase and one lowercase letter. • at least one number 0–9. • at least one special character !,"#¤. etc. • no words or names. • all passwords to have less than 3 of the same characters in the same sequence. The system should not allow passwords to have more than 4 characters in sequence in common with each other, regardless if they are uppercase or lowercase.

5.2.2. Subjective data

The participants were required to answer questionnaires provided on the website, at the recruitment stage, after creating their passwords, after recalling their passwords, and one final questionnaire at the end of study. All these questionnaires gathered data on the participants' experience with creating and recalling passwords within the experiment, and in the participants' everyday lives. For the purposes of this study's objectives, the user convenience data was collected from the questionnaires completed by the participants after they had

created their passwords, immediately after verifying them. The questions that referred only to measuring user convenience of verifying passwords after creation were included in the final analysis (see Table 2). These questions were adapted to be more specific for password verification, from questions used by Shay et al. (2010) and Workman et al. (2008) in their studies on password and security behavior. A pilot study was conducted in which the reliability of the questionnaire items was calculated. When reliability was analyzed in both the pilot and the current study (for each of the three weeks of password creation, and the overall scores), the user convenience construct showed to have a good level of reliability (Cronbach alpha score of 0.70 and above).

Table 2. Questionnaire items to measure user convenience of password verification – taken from questionnaires at the password creation stage

Construct	Items
User convenience (Cronbach alpha: >0.70) "Password verification refers to when you are asked to re-enter your password after creating it."	Verifying my passwords after creating them was annoying: Strongly agree; Agree; Neutral; Disagree; Strongly disagree Verifying my passwords after creating them was demanding: Strongly agree; Agree; Neutral; Disagree; Strongly disagree Verifying my passwords after creating them was time-consuming: Strongly agree; Agree; Neutral; Disagree; Strongly disagree The inconvenience from verifying my passwords after creating them was: 1=Very high . . . 7=Very low 1st password: 1 2 3 4 5 6 7 2nd password: 1 2 3 4 5 6 7

Further to the questionnaire items answered, during and after the study, several participants emailed and visited the experimenters to give feedback and discuss their experience with the study informally. The information gathered in these discussions enriched the understanding of the reported user convenience.

5.3. Procedure

Ethical approval was sought and approved by the university's ethics committee, before recruitment began for the study. The participants were recruited through replying to an advertisement sent out across the entire university. They were given information about the study and what to expect; this included information about receiving emails with instructions, when they would be taking part, how to create the passwords (including verifying them), how to recall the passwords, and information about completing the questionnaires. This information was also provided on the website throughout the study. Participants who agreed to take part gave their formal consent. However, they were also informed at the beginning of the study that they had the right to withdraw at any point. Further information regarding withdrawal was supplied on the website during the recruitment stage and throughout the study.

All participants completed the same tasks throughout the study. However, the group to which the participants were allocated determined the number of times the participants verified their passwords.

The participants were emailed each time they were required to complete a task. They would login to the website and would create or recall their passwords, followed by completing a questionnaire about their experience. When the participants created their passwords, if the passwords did not meet the rules/criteria, an error message would appear saying which rule was not met. Once the passwords met the password rules, the participants were asked to verify the passwords (how many times the participants did this depended on the group), shown in Figure 1. However, if the passwords were verified incorrectly, then the password would be reset. The participants were asked to learn their newly generated passwords and were told not to write them down. After the passwords were created for each session, the participants were provided with a questionnaire, with questions specific to their

experience of creating passwords. At the recall stage, the participants were given three attempts to recall their passwords. If the participants failed, the following message would appear: “You have had three attempts, you will not be able to make any further attempts at this time. You may however, be asked to enter this password again later in the study.” The participants were provided with this message as their login failure could have been a result of a temporary lapse in memory, and if they thought that they would not need to use the password again, this could have affected the password’s retention for future recall. After recalling the passwords for each session, the participants were then given another questionnaire, with questions specific to their experience of recalling passwords. In the final recall session, the participants were asked to recall all their passwords, and were given the recalling password questionnaire and a final questionnaire to report on their experience with recalling their passwords and their experience with the study.

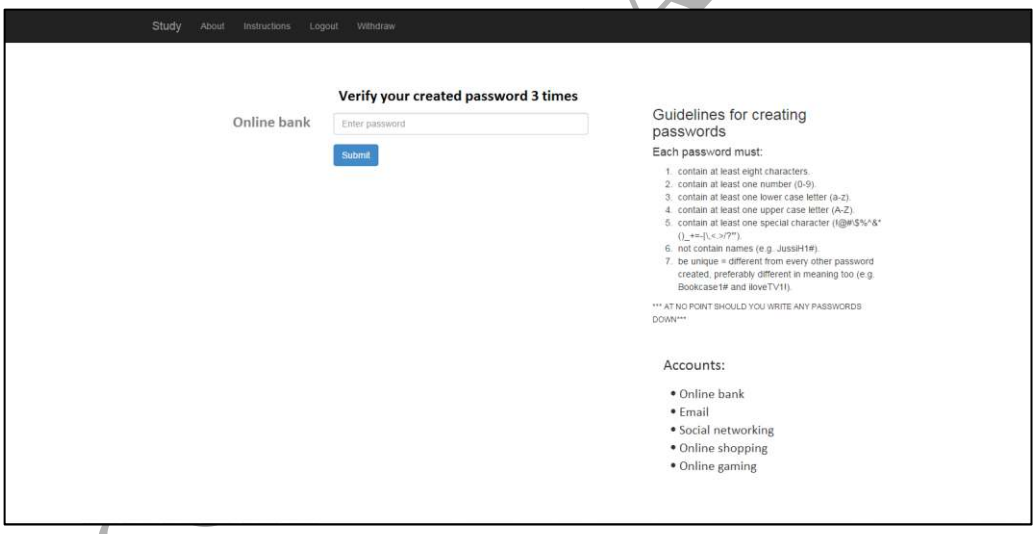

Fig 1. The password creation page

The schedule for creating and recalling passwords within the week was chosen for regularity, and for that enough time had passed between creating and recalling passwords for recall to represent long-term recall. At the beginning of week 1, one password was created; in weeks 2 and 3, two passwords were created each week. At the end of week 1, one password

was recalled; in weeks 2, 3, and 4, two passwords were recalled; and in week 5, all five passwords were recalled (creation and recall schedule is illustrated in Table 3). Participants had a set amount of time to create and recall their passwords. To create the passwords, the participants were given three days, and for recalling passwords, the participants were given four days (recall was longer as it covered the weekend). The participants were informed via email when they had to complete the task, and on the last day of each task period, an email was sent to those who had not completed the task to remind them to do so.

Over 2000 passwords were input into the website, and more than 800 questionnaires were completed over the five weeks.

Table 3. Password (study) schedule

Week	Creating passwords (number)	Remembering passwords (number)	Account types
1 beginning	1		Online Banking
1 end		1	Online Banking
2 beginning	2		Email/Social Networking
2 end		2	Online Banking/Email
3 beginning	2		Online Shopping/Online Gaming
3 end		2	Online Shopping/Online Gaming
4 beginning			
4 end		2	Social Networking/Online Shopping
5 beginning			
5 end		5	All

6. Results

Of the 105 participants who originally signed up for the study, data was analyzed from 90 participants who completed the entire study. A large amount of objective and subjective data was collected, including over 2000 passwords, and questionnaire responses measuring user convenience. To test the hypotheses, analysis of variance (ANOVA) tests were employed to show differences between the groups, and independent *t*-tests were used to confirm the results in more detail.

6.1. Password recall

Correct password recall was categorized by the total number of passwords correctly recalled over the five weeks, as well as the number of passwords correctly recalled on the first attempt each time they were recalled. A between-subjects ANOVA was employed to examine the effect of the password verification group on total correct password recall. There was a significant effect of the password verification group on total correct password recall ($F_{(2,90)} = 11.600$, $p < 0.001$); thus, supporting H1. Another between-subjects ANOVA showed there was also a significant effect of password verification on the correct first attempt password recall ($F_{(2,77)} = 10.807$, $p < 0.001$), further supporting H1. Total correct password recall and correct first attempt password recall were highest in the three-times verification group, followed by the two-times group, and then the control (one-times) group (represented in Figure 3). These success rates (total correct password recall and correct first attempt) are shown in Table 4 and represented in Figure 2. The descriptive and inferential results are summarized in Table 5 and Table 6.

Table 4. Success rates of correct password recall

	Verification group		
	Control group - verification x1 (*N*=30)	Experimental group - verification x2 (*N*=30)	Experimental group - verification x3 (*N*=30)
Total correct password recall	42%	59%	70%
Correct first attempt password recall	31%	44%	58%

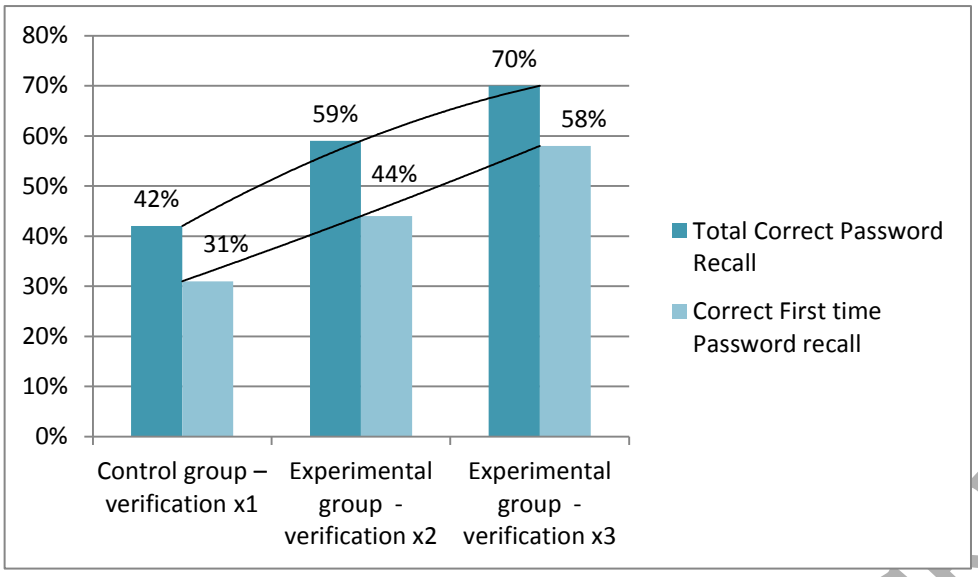

Fig 2. Success rates of correct password recall

6.2. User convenience

User convenience was measured through questionnaire responses in relation to the perceived inconvenience experienced by the user when having to verify their passwords at the creation stage. A between-subjects ANOVA was employed to examine the difference between groups, and the effect of password verification on user convenience. There was no significant effect of the password verification group on user convenience ($F_{(2,120)} = 2.512$, $p = 0.087$), not supporting H2. To support the results of H2, a post-hoc power analysis was performed using R STUDIO (version 3.4.3 (2017-11-30)) and showed a good level of statistical power (0.88). With further analysis, an independent *t*-test was performed, which showed no significant difference between the control group (with only one-times verification), and the three-times verification password group ($t = 1.021$, df = 58, $p = 0.156$). When the descriptive statistics were examined, the results revealed that user convenience (when all three groups were compared) was highest in the two-times verification password group, followed by the control group. The lowest was the three-times verification password group (shown in Figure 4). Therefore, additional *t*-tests were performed. They revealed that there was a significant difference between the two-times password verification group, and the

three-times password verification group (t = 2.404, df = 58, p = 0.01), showing that user convenience was lower in the three-times group. However, a t-test also revealed that there was no significant difference in user convenience between the one-times group and the two-times group (t = –1.154, df = 58, p = 0.127), and user convenience was actually higher in the two-times password verification group than in the one-times group. The descriptive and inferential results are summarized in Table 5 and Table 6.

Table 5. Descriptive results

	Verification group		
Mean (std. dev.)	Control group - verification x1 (*N*=30)	Experimental group - verification x2 (*N*=30)	Experimental group - verification x3 (*N*=30)
Total correct password recall	5.00 (2.92)	7.10 (2.77)	8.43 (2.65)
Correct first attempt password recall	3.77 (2.73)	5.30 (2.72)	6.97 (2.55)
User convenience	35.43 (7.77)	37.50 (5.99)	33.50 (6.87)

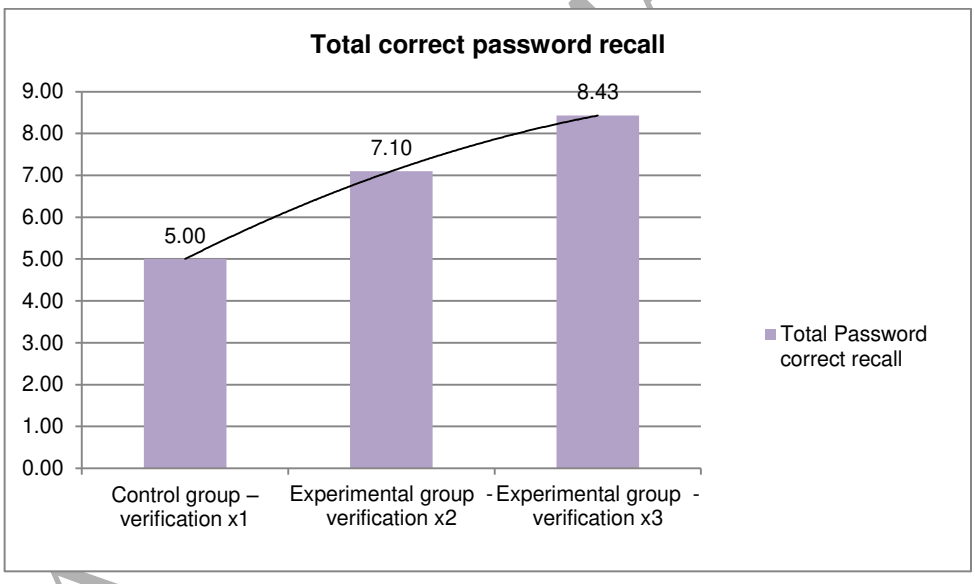

Fig 3. The mean score of total correct password recall

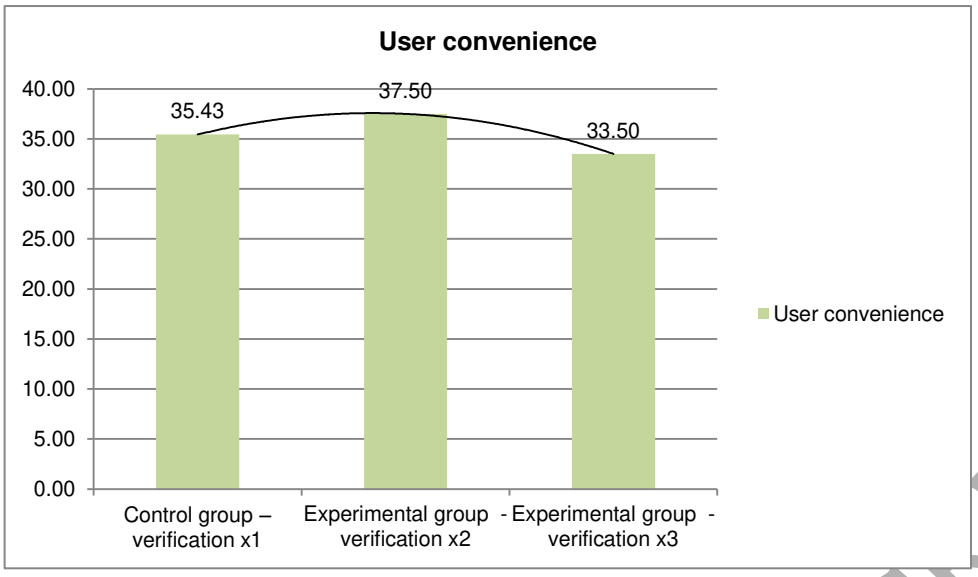

Fig 4. The mean score of user convenience

Table 6. Inferential results

Dependent variable	Hypothesis	Supported/Sig. (Eta squared)
Correct password recall	H1: Increasing the number of password verification times would have a positive effect on password recall	Supported - total correct $p < 0.001$ (0.21) Supported – correct first time $p < 0.001$ (0.20)
User convenience	H2: Increasing the number of password verification times would have a negative effect on user convenience.	Not supported $p = 0.087$ (0.06)

7. Discussion

Password security is an important issue that needs to be addressed, in terms of making passwords more secure and more memorable, while not increasing user inconvenience. Therefore, the focus of this study was to investigate whether increasing the number of password verifications would have an effect on password memorability, and user convenience.

7.1. Verification and password memorability

The results have important implications as they suggest that increased numbers of password verification can increase password memorability. Verifying passwords three times

increases password memorability by 28% when compared with current practices (verifying passwords just once), from 42% correct password recall to 70%. Even increasing the verification to only two times increased password memorability by 17%, from 42% correct password recall to 59%. The increases in success rate are similar for both total correct password recall and for the correct first attempt at password recall. These results are significant, especially for the amount of change or difference between the three conditions, i.e., one or two extra verification times. These findings provide evidence that to increase password memorability does not require substantial changes in practices or devices; small changes can be effective.

7.2. Verification and user convenience

The results of the study suggest that small increases in password verification do not have a notable effect on the levels of inconvenience experienced by the user. Although previous research suggested that the more time users spend on the password process of creating, learning, and recalling passwords, the higher their inconvenience (Renaud and De Angeli, 2004; Zhang and McDowell, 2009); we found that this was not necessarily the case. We found not only that user convenience levels were similar across all three groups (51–58%) but also that the number of times of verification did not equate to a decrease in user convenience. The lowest level of user convenience was experienced by the three-times password verification group, with one-times group being only 3% higher. The two-times password verification group had the highest user convenience levels, 7% higher than the three-times group, and 4% higher than the one-times group. Although there was no significant difference across the three groups, the convenience result for the second group was unexpected. In discussions with participants, several reported that they felt that through repeating the verification stage, it was "helping" their memory; whereas the participants in

the third group reported the same, they were more negative about the benefits as the procedure was time-consuming. For example, the findings suggest that user convenience is not affected by time spent on the password process, as previous research suggested (Renaud and De Angeli, 2004; Zhang and McDowell, 2009), or changes in practices, i.e., increasing the number of verifications.

7.3. Trade-off between password memorability and user convenience

Previous research on security vs. memorability (Vu et al., 2007; Zhang et al., 2009) and security vs. convenience suggests that one will decrease as the other increases (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009). Our findings provide new insights into this issue. First, our findings suggest that if one factor (e.g., memoribility) increases, the other does not automatically decrease. Second, significant changes in one factor may or may not have significant effects on the other factors involved. Therefore, password memorability can be increased, while user convenience is relatively unaffected.

Overall, our findings suggest that password memorability can be increased, while not significantly affecting the users' convenience. The findings also highlight that although the relationship between password memorability and user convenience can be complex, the relationship is not necessarily as rigid as thought by previous research.

7.4. Study limitations

7.4.1. Ecological validity

The study was conducted online to incorporate a reasonable level of realism into the design, because monitoring participants' real passwords would have been a security issue and could have affected their responses. While the study was designed in such a way to eliminate as many confounding variables as possible, conducting an online study can have drawbacks.

7.4.2.1. Writing passwords down

Due to the study being conducted online, the participants had the opportunity to write their passwords down. However, throughout the experiment, participants were instructed not to write their passwords down, and were given warnings about security breaches if they broke the rules. Furthermore, in the final questionnaire, the participants were asked, "During this study, did you use any memory aids, techniques or coping strategies to help remember your passwords?" and were given the options of "Yes/No, if yes…. wrote it down, saved it electronically, used a memory technique to remember, or other…." Many participants said they had used memory techniques, such as mnemonics; however, none of the participants reported writing down their passwords or saving them electronically.

7.4.2.2. Fictitious accounts

Participants created passwords for five fictitious accounts during the study. Fictitious accounts were chosen because monitoring password recall could have been a security issue if they had been real accounts and passwords. The five accounts included online banking, email, social networking, online shopping, and online gaming and were chosen because of their range of importance and data sensitivity. However, it has to be acknowledged that on one hand, testing password memorability may have resulted in participants trying harder to learn and recall passwords as they knew they would be tested. On the other hand, by contrast, the participants may have placed less importance into learning and recalling their passwords for the study as the accounts were not the participants' real accounts. Although, according to Fahl et al. (2013), while examining password study ecological validity, found that many participants use their real or very similar passwords from their real life in password studies. This behavior could have potentially increased the passwords' value to the participants. Nevertheless, to attempt to counter this issue, previous password studies have asked their participants to role-play (Gaw and Felton, 2006; Forget et al., 2008; Shay et al., 2010).

Within this study, a similar approach was adopted providing this statement before the study began, “We would appreciate it if you not only learn your passwords to the best of your ability, but consider them as protecting “real” accounts, as we will monitor your interaction with the system.”

7.4.3. Population sample

The participants consisted of university staff and students. However, the participants were from a variety of education and demographic backgrounds, we acknowledge the potential bias that using university staff and students brings, such as being more aware of memory techniques. However, we attempted to counter this problem by recruiting our participants from a variety of staff from various positions and faculties within the university and a variety of students from different program levels and faculties.

7.4.4. The construct of user convenience

Several studies have examined user convenience in the password context (Bang et al., 2012; Jenkins et al., 2014; Renaud and De Angeli, 2004; Tam et al., 2010; Weir et al., 2009) and have found that user convenience is a key factor affecting password security (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009). However, user convenience has still not been fully defined by, or examined in terms of a theoretical basis. Therefore, in future research, user convenience should be examined in more depth and in terms of a psychological theory and be properly defined as a concept. Moreover, user convenience also needs to be operationalized, possibly from the motivation perspective for consistent measurement.

7.5. Future research

Several studies have investigated human memory to understand the password problem, and attempt to solve it. However, as with the adoption of biometrics, cost and familiarity is

reported to be more favored over a mechanism that could possibly solve these issues (Florêncio and Herley, 2007; Keith et al., 2009).

In this study, we looked to make small changes in the existing password process. Our results are very promising. We found that increased verification increases password memorability but does not affect user convenience proportionately. Therefore, future research should examine the interaction between security, memorability, and convenience in more depth, to gain a better understanding of the relationships between all these significant factors that influence each other and the password process. Future studies should also look to measuring increased numbers of verification attempts (such as five or even ten times), on memorability and user convenience, to consider the practical implications of further increasing password memorability. Other future studies could also consider the effects of different password policies and different creation processes on the trade-off between password memorability and user convenience.

8. Conclusion

Users are increasingly finding it difficult to recall their passwords as the number of accounts continue to rise (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). As users push their memory capabilities, many adopt insecure password behaviors as they see the behaviors as coping strategies that help them remember their passwords, regardless of the potential security risks to their accounts and their employers' accounts (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009). This disregard for security comes at a cost to both organizations and the users themselves, as insecure password behaviors can lead to unauthorized access to accounts, forgetting passwords, and inconvenience in terms of resetting and restricted authorized access (Brown et al., 2004; Hayashi et al., 2012; Inglesant and Sasse, 2010; Tari et al., 2006; Vu et al.,

2007). Previous research suggests that there is a trade-off between password security, memorability, and convenience, which insinuates that increasing password memorability would decrease the other two. This study examined whether increasing the number of password verification times could increase password memorability, and whether this would decrease user convenience. The study and its results have important implications for password security practice. First, simple adjustments to the password process via increasing the number of verifications can make passwords more memorable while not concurrently increasing user inconvenience. Second, this change could reduce the chance of forgetting passwords, and the financial consequences that can then occur. Finally, increasing the number of verifications could also reduce insecure password behaviors and the security issues pertaining to these behaviors.

Acknowledgments

We would like to thank the Associate Editors and the anonymous reviewers for their insightful comments. The authors would also like to thank the participants for taking part in the long study. This research was supported by the University of Jyväskylä.

References

Adams, A., Sasse, M., 1999. Users are not the enemy. Communications of the ACM, 42 (12), 41–46.

Al-Ameen, M. N., Wright, M., Scielzo, S. 2015. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In Proceedings of the Enhanced Security with Passwords & CAPTCHAs, CHI '15, Seoul, Republic of Korea, 2315-2324.

Alkaldi, N., Renaud, K., 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.

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

Baddeley, A.D., 1992. Working memory. Science, 255, 556–559.

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

Baddeley, A.D., 2009[b]. Short-term Memory, in: Baddeley, A.D., Eysenck, M.W., Anderson, M.C., Memory. Psychology Press, Hove & New York, NY, pp.19-40.

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

Baddeley, A.D., 2009[d]. Learning, in: Baddeley, A.D., Eysenck, M.W., Anderson, M.C., Memory. Psychology Press, Hove & New York, NY, pp. 69-92.

Baddeley, A.D., Hitch, G.J. 1974. Working memory, in: Bower, G.A. (Ed.), Recent Advances in Learning and Motivation (8). Academic Press, New York, pp. 47-89.

Bang, Y., Lee, D., Bae, Y., 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, 409– 418.

Biddle, R., Chiasson, S., Van Orschot, P.C., 2012. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44 (4), 19:11-19:41.

Bonneau, J., Schechter, S. 2014. Towards reliable storage of 56-bit secrets in human memory. In USENIX Security Symposium, 607-623.

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

Burr, W.E., Dodson, D.F., Polk, W.T. 2006 Electronic Authentication Guideline. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1 0 2.pdf (accessed: 28.5.2018).

Campbell, J., Kleeman, D., Ma, W., 2006. Password Composition Policy: Does Enforcement Lead to Better Password Choices?. In Proceedings of the 17th Australasian Conference on Information Systems Password Composition Policy, Adelaide, Australia.

Campbell, J., Ma, W., Kleeman, D., 2011. Impact of restrictive composition policy on user password choices. Behaviour and Information Technology, 30, (3), 379–388.

Cheroen, D., Raman, M., Olfman, L. 2008. Improving End User Behaviour in Password Utilization: An Action Research Initiative. Systemic Practice and Action Research, 21(1), 55-72.

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

Chiasson, S., Forget, A., Stobert, E., Van Orschot, P.C., Biddle, R., 2009. Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. In Proceedings of the 16th ACM conference on Computer and communications security, CCS '09, Chicago, Illinois, 500-511.

Craik, F., Lockhart, R. 1972. Levels of processing. A framework for memory research. Journal of Verbal Learning and Verbal Behaviour, 11, 671-684.

Craik, F., Tulving, E. 1975. Depth of processing and the retention of words in episodic memory. Journal of Experimental Psychology: General, 104, 268-294.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., Baskerville, R. 2013. Future directions for behavioral information security research. Computers & Security, 3(2), 90-101.

Duggan, G.B., Johnson, H., Grawemeyer, B., 2012. Rational Security: Modelling everyday password use. International Journal of Human-Computer Studies, 70, 415–431.

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

Fahl, S., Harbach, M., Acar, Y., Smith, M. 2013. On the ecological validity of a password study. In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS), ACM, 13.

Forget, A., Chiasson, S., Van Oorschot, P. C., Biddle, R. 2008. Improving text passwords through persuasion. In Proceedings of the 4th symposium on Usable privacy and security (SOUPS), ACM, 1-12

Feinberg, S., Murphy, M. 2000. Applying cognitive load theory to the design of web-based instruction. In Proceedings of the IEEE professional communication society international professional communication conference and Proceedings of the 18th annual ACM international conference on Computer documentation: technology & teamwork, IEEE Educational Activities Department, 353-360.

Florêncio, D., Herley, C. 2007. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web, ACM, 657-666.

Furnell, S. 2013. Getting past passwords. Computer Fraud & Security, (4), 8-13.

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

Goldstein, B. 2011. Cognitive Psychology: Connecting Mind, Research, and Every-day Experience--with coglab manual. (3rd ed.). Belmont, CA: Wadsworth.

Grassi, P.A., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Choong, Y.Y., Greene, K., Theofanos, M.F. 2017. Digital identity guidelines: Authentication and lifecycle management. National Institute of Standards and Technology, Special Publication (NIST SP)-800-63B.

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

Guo, K.H., 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32, 242-251.

Hayashi, E., Pendleton, B.A., Ozenc, F.K., Hong, J.I., 2012. WebTicket: Account Management Using Printable Tokens. In Proceeding of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2012, Austin, Texas, 997-1006.

Helkala, K., Svendsen, N. K. 2011. The security and memorability of passwords generated by using an association element and a personal factor. In Proceedings of the Nordic Conference on Secure IT Systems, Springer Berlin Heidelberg, 114-130

Hoonakker, P., Bornoe, N., Carayon, P. 2009. Password authentication from a human factors perspective: Results of a survey among end-users. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, Vol. 53, No. 6, 459-463.

Inglesant, P., Sasse, M.A., 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2010), Atlanta, Georgia, 383-392.

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

Jacoby, L. L., Bartz, W. H., 1972. Rehearsal and transfer to LTM. Journal of Verbal Learning and Verbal Behavior, 11(5), 561-565.

Jenkins, J.L., Grimes, M., Proudfoot, J., Lowry, P.B., 2014. Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time warnings. Information Technology for Development, 20 (2), 196-213.

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) 113-134.

Keith, M., Shao, B., Steinbart, P. 2009. A Behavioral Analysis of Passphrase Design and Effectiveness. Journal of the Association for Information Systems, 10(2), 63-89.

Marquardson, J. 2012. Password Policy Effects on Entropy and Recall: Research in Progress. In 8th Americas Conference on Information Systems, Seattle, Washington.

Mayer, P., Kirchner, J., Volkamer, M., 2017. A Second Look at Password Composition Policies in the Wild: Comparing Samples from 2010 and 2016. In Symposium On Usable Privacy and Security, 13-28.

Miller, G. A. 1956. The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.

Nelson, D., 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), 705–715.

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

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

Notoatmodjo, G., Thomborson, C., 2009. Passwords and Perceptions. In Proceedings of the 7th Australasian Information Security Conference, AISC, Wellington, New Zealand.

Pahnila, S., Siponen, M., Mahmood, A., 2007. Which Factors Explain Employees' Adherence to Information Security Policies? In Proceedings of the Pacific Asia Conference on Information Systems, Auckland, New Zealand.

Proctor, R. W., Lien, M., Vu, K. L., Schultz, E. E., Salvendy, G. 2002. Improving computer security for authentication of users: influence of proactive password restrictions. Behavior Research Methods, Instruments, Computers 34, 163–169.

Ranganath, C., Libby, L. A. Wong, L. 2012. Human learning and memory, in: Frankish, K., Ramsey, W., The Cambridge Handbook of Cognitive Science. Cambridge University Press, Cambridge & New York, NY, pp. 112-130.

Renaud, K., De Angeli, A., 2004. My password is here! An investigation into visuo-spatial authentication mechanisms. Interacting with Computers, 16, 1017–1041.

Rundus, D., Atkinson, R. C. 1970. Rehearsal processes in free recall: A procedure for direct observation. Journal of Verbal Learning and Verbal Behavior, 9(1), 99-105.

Saastamoinen, A. 2014. Lomalla unohtuneet salasanat tulevat työnantajille kalliiksi – jopa satojen tuhansien kustannukset. http://yle.fi/ylex/uutiset/lomalla_unohtuneet_salasanat_tulevat_tyonantajille_kalliiksi__jopa_satojen_tuhansien_kustannukset/3-7580109. (accessed 24.09.15).

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

Sharma, S. K., Sefchek, J. 2007. Teaching information systems security courses: A hands-on approach. Computers & Security, 26(4), 290-299.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F. 2010. Encountering stronger password requirements: user attitudes and behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security, ACM, 2.

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

Tari, F., Ozok, A., Holden, S. H., 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In Proceedings of the second symposium on Usable privacy and security. ACM Press, New York, 56-66.

Thing, V. L., Ying, H. M. 2009. A novel time-memory trade-off method for password recovery. Digital Investigation, 6, S114-S120.

Vance, A., Eargle, D., Ouimet, K., Straub, D., 2013. Enhancing Password Security through Interactive Fear Appeals: A Web-based Field Experiment. In Proceedings of the 46th Hawaii International Conference on System Sciences, HICSS, Hawaii.

Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., Schultz, E.E., 2007. Improving password security and memorability to protect personal and organizational information. International Journal of Human-Computer Studies, 65, 744-757.

Weir, C. S., Douglas, G., Carruthers, M., Jack, M. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. Computers & Security, 28(1), 47-62.

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, 102-127.

Woods, N., Siponen, M., 2018. Too many passwords? How understanding our memory can increase password memorability. International Journal of Human-Computer Studies 111, 36-48.

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, 2799–2816.

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

Zhang, L., McDowell, M.C., 2009. Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. Journal of Internet Commerce, 8 (3-4), 180-197.

Vitae

Naomi Woods is a postdoctoral researcher at the University of Jyväskylä, Finland. She has a Ph.D. in Cognitive Science and an MSc. in Clinical Psychology. Her research focuses on password security and memorability. Woods has published studies in the field of Human-Computer Interaction and Information Systems.

Mikko Siponen is full professor of Information Systems. His degrees include Doctor of Social Sciences, majoring in Philosophy; Lic.Phil. in information systems; and Ph.D. in Information Systems. He has received over 10 million EUR of research funding from corporations and numerous other funding bodies. Besides leading industry-funded projects, Siponen has been a PI on projects for the Academy of Finland, the EU, and the Finnish Funding Agency for Innovation. His current H index is 43, and he has more than 8000 citations (Google Scholar). He has published more than 55 journal articles.