Author(s): Woods, Naomi; Siponen, Mikko

Title: Too many passwords? : How understanding our memory can increase password memorability

Year: 2018

Version:

Please cite the original version:

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. https://doi.org/10.1016/j.ijhcs.2017.11.002

Too many passwords? How understanding our memory can increase password memorability

Naomi Woods , Mikko Siponen

PII: S1071-5819(17)30158-1
DOI: 10.1016/j.ijhcs.2017.11.002
Reference: YIJHC 2166

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

Received date: 24 March 2017
Revised date: 13 October 2017
Accepted date: 17 November 2017

Please cite this article as: Naomi Woods , Mikko Siponen , Too many passwords? How understanding our memory can increase password memorability, *International Journal of Human-Computer Studies* (2017), doi: 10.1016/j.ijhcs.2017.11.002

Highlights

- There was no relationship between memory performance and correct password recall.
- General metamemory constructs could predict memory performance, but not password recall.
- The contextualized password metamemory constructs of Capacity, Locus, Achievement, and Task predicted correct password recall.
- There was a difference between the contextualized password metamemory constructs that predicted password recall, in comparison with the generalized metamemory constructs that predicted memory performance.

TOO MANY PASSWORDS? HOW UNDERSTANDING OUR MEMORY CAN INCREASE PASSWORD MEMORABILITY

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 common authentication mechanism, that are only increasing with time. Previous research suggests that users cannot remember multiple passwords. Therefore, users adopt insecure password practices, such as password reuse in response to their perceived memory limitations. The critical question not currently examined is whether users' memory capabilities for password recall are actually related to having a poor memory. This issue is imperative: if insecure password practices result from having a poor memory, then future password research and practice should focus on increasing the memorability of passwords. If, on the other hand, the problem is not solely related to memory performance, but to users' inaccurate perception of their memory, then future research needs to examine why this is the case and how such false perception can be improved. In this paper we examined this conundrum by contextualizing the memory theory of metamemory, to the password security context. We argue, based on our contextualized metamemory theory, that the recall of multiple passwords is not related to users' memory capabilities, and therefore users are able to actually remember more passwords than they think. Instead, we argue that users' perceptions of their memories abilities, in terms of password memory capacity; perceived control over their memory; motivation to remember; and their understanding of their memory, explains why users cannot remember their passwords. We tested our contextualized metamemory theory in the password security context through a longitudinal experiment, examining over 3500 passwords. The results suggest that our contextualized metamemory theory, rather than the general metamemory theory explains password recall. This study has important implications for research in password security, and practice.

Keywords: password security; memorability; human memory; metamemory; information security; authentication

1. Introduction

The number of passwords is set to rise, as users acquire more and more accounts in their everyday, personal and working lives (Chiasson et al., 2009; Lin et al., 2013; Zhang et al., 2009). This increase is resulting in an escalation in information security risks, as users adopt insecure password practices, such as password reuse, writing down passwords, sharing passwords, and choosing weak passwords (Adams and Sasse, 1999; Campbell et al., 2006; Guo, 2013; Inglesant and Sasse, 2010; Zhang et al., 2009), to cope with their inability to remember multiple passwords (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). However, in numerous cases users choose to continue these insecure behaviors even though they are aware of the security risks (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009). This situation may have arisen due to the fact that forgetting passwords can have high consequences if passwords need to be reset, in terms of money (e.g., IT helpdesk costs), time (e.g., when employees are unable to log on to work), and convenience (e.g., when users are unable to access their accounts, or have to create new passwords), (Brown et al., 2004, Hayashi et al., 2012, Inglesant and Sasse, 2010; Renaud and De Angeli, 2004; Tari et al., 2006; Vu et al., 2007).

As the number of accounts and passwords increase over time, this problem will only get worse (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009). Therefore, the security and memorability of passwords are an important concern. Previous research have so far examined the "password problem" (Wiedenbeck et al., 2005) in terms of understanding, predicting and changing users' insecure security behavior through behavioral models, such as the protection motivation theory (PMT) (Jenkins et al., 2014; Johnston et al., 2015; Pahnila et al., 2007; Vance et al., 2012; 2013; Workman, et al., 2008; Zhang and McDowell, 2009). Another stream of research has focused on memory theory to understand the memory processes and the users' behavior involved with password management; and to attempt to

increase password memorability (Adams and Sasse, 1999; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011; Nelson and Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007). However, even though previous studies have examined users' attitudes and perceptions towards their passwords and password management, the important questions that have not been explored are whether users' poor password recall is actually related to poor memory performance, that is, are users unable to remember their passwords because their memory cannot cope? Or, do users' perceptions of their memory capabilities in general terms, and in terms of remembering their passwords, affect their password recall performance? Answering these questions is essential for the future of password research and practice. If users cannot remember their passwords as a result from having a poor memory, then future research and practice should focus on increasing the memorability of passwords. If, on the other hand, the problem is not solely related to memory performance, but to users' inaccurate perception of their memory, then future research needs to examine why this is the case and how such false perception can be improved.

This study focuses on answering these issues. We argue based on our contextualized metamemory theory, that the recall of multiple passwords is not related to users' memory capabilities, and therefore users are able to actually remember more passwords than they think. Instead, we argue that users' perceptions of their memories abilities, in terms of password memory capacity; perceived control over their memory; motivation to remember; and their understanding of their memory, explains why users cannot remember their passwords. The next section will discuss the previous research in multiple passwords. Then we examine the theoretical background, looking at the human memory, metamemory and its influence on memory performance. The following section will modify the metamemory theory to the specific context of password recall. Based on the contextualized metamemory theory, we discuss the current study, its hypotheses, and the reasoning behind the password

metamemory framework. This paper will then later discuss the research methodology, including the experimental design, and then the results. The final sections of the paper will conclude with a discussion of the study's important findings and contributions.

2. Previous Research

Since the late 1990's, when Adams and Sasse (1999) suggested that users cannot remember more than 4-5 unique passwords successfully, the world has technologically changed, with increasing numbers of passwords being required to secure our accounts and information (Lin et al., 2013). Countless users have more than 10 passwords in use within their personal lives and at work (Zhang et al., 2009). Within most organizations users are required to change their passwords regularly; this impacts on users' password behavior as many choose weak passwords to compensate for the sheer number of them (Marquardson, 2012). Moreover, guidance and advice on managing them are normally aimed at just one password (Grawemeyer and Johnson, 2011). Many users rely solely on their memory to remember all their passwords, even though they believe they have too many accounts (Bang et al., 2012; Campbell et. al., 2011; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). However, if users cannot remember their passwords, the mechanism does not work successfully. Combined with the huge costs from forgetting passwords (Brown et al., 2004; Hayashi et al., 2012; Inglesant and Sasse, 2010; Tari et al., 2006; Vu et al., 2007), this influences users' password security behavior, and ultimately undermine the security of the password mechanism (Chiasson et al., 2009; Duggan et al., 2012; Gaw and Felten, 2006; Zhang et al., 2009). Without a solution, giving users an alternative or a way of coping with multiple passwords, insecure password behaviors will only rise as the number of accounts do so (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009).

3. Theoretical Background

With an increase in the number of passwords, users believe they cannot cope with remembering all their passwords (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). This may be the case; maybe users have no more space to retain anymore passwords; however, people still manage to learn and recall new information every day. Therefore, understanding fully how the memory functions is a necessity; but moreover, understanding how users' perceptions of their memories' capabilities affect their memory performance is pertinent to understanding how their perceptions of their memory for remembering passwords, affect their ability to correctly recall them.

3.1. Memory

There are several factors involved with remembering passwords. Firstly, the user has to learn the password successfully; then the user has to retain the password; and then finally, the user has to successfully recall the password. This process elicits a number of memory stores and functions dependent on the stage of the process. The Stages of Memory Theory (Modal Model) is one of the most influential multi-store models (Atkinson and Shiffrin, 1968). It suggests that are three memory stores: the sensory store is thought as the interface between perception and memory, holding information for a brief period of time, before it is passed to the short-term memory (STM). The STM is limited in its capacity and stores information for just a matter of seconds. The long-term memory (LTM) stores information over a long period of time, ready for retrieval, which is not currently held in the conscious awareness. Previous research suggests that users' claim that they cannot remember their passwords because their memories limitations (Grawemeyer and Johnson, 2011). However, the LTM is unlimited in its capacity (Baddeley, 2009[a]; Eysenck and Keane, 2010). This leads us to postulate that low

password correct recall, is not related to poor memory retrieval performance. We therefore propose a null hypothesis:

H1: There will be no significant correlation between memory performance and password correct recall.

There are several factors that can result in the password process failing. The password has to be learnt successfully in the first place (Zhang et al., 2009). Learning takes concentration and mental effort, which can be effected by many things, such as distractions (Adams and Sasse, 1999; Jenkins et al., 2014; Zhang and McDowell, 2009). Retrieving passwords also has its problems, with two main types of forgetting, trace decay (the gradual weakness of memory) and interference (caused by the confusion between similar memories) (Ling and Catling, 2012); this effect can be counteracted through frequent use of a password (Anderson, 2009; Baddeley, 2009[b]; Criss et al., 2011; Sasse, et al., 2001).

Another factor that can influence the password process is the users' beliefs of their own memory capabilities and functions, or as it is known as, metamemory (Dixon et al., 1988; Hertzog et al., 1987). This paper will discuss in the next section the important influence of metamemory and how it affects memory performance, and ultimately, password recall.

3.2. Metamemory

Metamemory has been studied since the 1970's (Glass et al., 2005), when it was introduced by Flavell and his colleagues (Flavell, 1971, Flavell and Wellman, 1977). Metamemory has been broadly defined as cognitions about memory (Wellman, 1983), but more specifically, as the knowledge and awareness of our cognitive processes (Flavell, 1971; 1979). Metamemory is a collective term for the multidimensional factors of knowledge, beliefs, and behaviors related to memory (Hertzog, 1992; Hertzog et al., 1990[b]; Hertzog et al.,

1987); i.e. the ability to reflect on one's own memory functioning and memory processes in general (Dixon and Hultsch, 1983[a]; Glass et al., 2005; Hertzog et al., 1990[b]; Pierce and Lange, 2000). Metamemory is important as it guides our choices in how we use our cognitive resources, e.g., if a person believes that some information is more difficult to learn, they may spend more time learning it (Besken and Mulligan, 2013). Over the years, researchers have shown an increased interest in the role that metamemory has in learning and recalling information, and memory performance (Hertzog, 1992; Schwartz, Benjamin and Bjork, 1997).

3.2.1. Measuring metamemory

The Metamemory in Adulthood (MIA) questionnaire (Dixon et al., 1988) is a standardized questionnaire with good psychometric properties, that is the most frequently used methods of measuring metamemory, and the seven constructs that represent it (Dixon and Hultsch, 1983[a]; Dixon et al., 1988; Glass et al., 2005; Hertzog et al., 1987). The seven constructs are: Strategy: knowledge and use of memory strategies; Task: knowledge of basic memory processes; Capacity: beliefs about one's own memory capacities; Change: perception of the change in one's own memory capabilities; Anxiety: anxiety, and/or perception of the relationship between anxiety and memory performance; Achievement: perception of one's own motivation to perform well in memory tasks; and Locus: perceived sense of control over memory skills (Dixon et al., 1988). These constructs have been extensively studied and used for measuring metamemory in different context for over 20 years (Bacon et al., 2011; Glass et al., 2005).

3.2.2. Metamemory and memory performance

How good is your memory? is an important and insightful question. When answered, it provides an understanding of a complex set of processes that influence a person in their behavior and how well they perform (Cavanaugh et al., 1998). Regardless if it is a memory of a name, face, event or fact, recalling the information may be affected by what the person's believes is necessary, to remember the information accurately. Furthermore, the person's self-believe system about memory – whether they believe they will remember the information, can influence how they behave in a memory-demanding situation, which can govern their performance (Hertzog et al., 1987). Researchers are interested in the role that metamemory plays in memory performance (Hertzog et al., 1990[a]), as although memory performance is effected by memory mechanisms, such as encoding and retrieval, it is also effected by prior knowledge – familiarity with information; and contextual influences on behavior (Dixon and Hertzog, 1988). Negative beliefs about one's own memory capabilities and poor memory functioning is highly related to memory performance (Bacon et al., 2011; Glass et al., 2005). Therefore, recognizing that metamemory is complex and multidimensional is imperative for understanding how it affects the human memory, and its performance (Glass et al., 2005; Hertzog, 1992). Several studies have found relationships between specific metamemory factors and memory performance: a study by Dixon and Hertzog (1988) suggested that motivational factors should be considered with memory knowledge in relation to memory performance. Further research found that specific metamemory factors such as strategy, capacity, task and motivation (achievement), could effected and predict memory performance; as through an understanding of retrieval strategies and how they can be used to aid one's memory, coupled with and understanding of one's own memory capacity, and the required effort and motivation needed to perform can predict memory performance (Dixon and Hultsch, 1983[a]; Hertzog et al., 1990[b]).

To investigate the relationship between memory capabilities and their effects on password recall, we include in our model factors of metamemory in relation to memory performance (scales from the Metamemory In Adult (MIA) questionnaire), to confirm the relationship between specific metamemory factors and memory performance for nomological validity (Straub et al., 2004). We therefore hypothesize the following:

H2a: Strategy (metamemory) will have a significant positive effect on memory performance.

H2b: Task (metamemory) will have a significant positive effect on memory performance.

H2c: Capacity (metamemory) will have a significant positive effect on memory performance.

H2d: Change (metamemory) will have a significant positive effect on memory performance.

H2e: Anxiety (metamemory) will have a significant positive effect on memory performance.

H2f: Achievement (metamemory) will have a significant positive effect on memory performance.

H2g: Locus (metamemory) will have a significant positive effect on memory performance.

4. Contextualizing metamemory and memory performance to the password context

In this section, we contextualize the metamemory constructs to the context of password security, to examine which password metamemory constructs predict correct password recall. The metamemory construct *Strategy* means what memory strategies a person can understand and use to aid learning and memory retrieval. For example, writing and using a shopping list is a memory strategy to aid one to remember which products the person needs to buy. For the password security context, the password metamemory construct of Strategy refers to the

knowledge and use of memory strategies to remember password correctly by users. Unfortunately, some of these memory strategies adopted by users, when contextualized for the password security context are considered insecure. Such common insecure memory strategies include writing passwords down, sharing passwords, and password reuse (Adams and Sasse, 1999; Duggan et al., 2012). Even though users are aware of these behaviors being insecure, they are still more concerned with remembering their passwords, and still adopt these strategies (Gaw and Felten, 2006). We therefore hypothesize:

H3a: Strategy (password metamemory) will have a significant positive effect on password correct recall.

The metamemory construct of *Task* signifies a person's understanding of their basic memory processes. An example of this is that most people are aware that information which is more interesting is easier to remember, than information that is less interesting (Bacon et al., 2011). In the context of password metamemory, Task refers to users' understanding how they remember passwords, e.g., passwords with more meaning are easier to remember. However, this understanding can sometimes lead to insecure password behavior, where weak passwords are chosen with biographical information, or are related to the service of the password (Helkala and Svendsen, 2011). Nonetheless, having an increased understanding of how one's memory functions positively effects memory performance (Dixon and Hultsch, 1983), we therefore, suggest:

H3b: Task (password metamemory) will have a significant positive effect on password correct recall.

Capacity, in terms of metamemory is a person's perceptions of their own memory capacity and performance. Several studies examining metamemory have found perceived

memory capacity to have an effect on memory performance (Dixon and Hultsch, 1983; Hertzog et al., 1990; Hertzog et al., 1994), be the perception to be accurate or inaccurate (Hertzog et al., 1987). Metamemory literature suggests that if a person thinks that their memory capacity is limited, then their memory performance will also be limited (Hertzog et al., 1987). Therefore, perceived memory capacity is important in the context of remembering passwords because it refers to the amount of passwords users believe they can remember, and the ability to recall correctly. Previous research has noted that users believe that they have too many passwords, and cannot remember so many passwords (Bang et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). We argue that the users' belief of their memory capacity limitations may affect their memory performance in the password context. Therefore, the users' perceptions of their capacity to recall passwords should be positively related to their password recall. More precisely, those users who perceive their memory capability as high have better recollection of their passwords than those users who perceive it to be low. Hence, it is hypothesized:

H3c: Capacity (password metamemory) will have a significant positive effect on password correct recall.

The metamemory construct of *Change* represents the perception of the change in one's own memory capabilities. When contextualizing this construct to password security it can refer to users' perception of the change in their capabilities in remembering passwords. Memory is affected by age; therefore, as people get older changes in memory capability occur with cognitive decline (Baddeley, 2009). The perceptions of this change have been found to be related to memory performance (Cavallini et al., 2013). *Anxiety*, and/or the perception of the relationship between anxiety and memory performance can refer to the users' perceived anxiety towards remembering their passwords, within the password security

context. Increased levels of anxiety have been found to be related to low memory performance (Lineweaver and Hertzog, 1998). Within the password context, due to the consequences of forgetting, users often develop a fear of forgetting their passwords (Ives et al., 2004) and consequently adopt insecure password behaviors to cope with the anxiety. We hypothesize the following:

H3d: Change (password metamemory) will have a significant positive effect on password correct recall.

H3e: Anxiety (password metamemory) will have a significant negative effect on password correct recall.

Achievement, metamemory construct refers to the perception of one's own motivation to perform well in memory tasks. Metamemory research has found that Achievement (motivation) can predict memory performance (Dixon and Hertzog, 1988). Achievement, in the context of password, would refer to the user's motivation towards remembering passwords. Previous password security research has found a relationship between motivation (in terms of motivation to protect) and insecure or secure password behaviors adopted (Jenkins et al., 2014; Zhang and McDowell, 2009). We therefore hypothesize:

H3f: Achievement (password metamemory) will have a significant positive effect on password correct recall.

Locus refers to the perceived sense of control over memory skills. If a person believes they have less control over their memory functioning, this can affect their memory performance (Lineweaver and Hertzog, 1998). Within the password security context, locus would refer to the perceived control over the users' ability to remember their passwords. We hypothesize the following:

H3g: Locus (password metamemory) will have a significant positive effect on password correct recall.

In this study we propose a conceptual framework that scrutinizes the perception that users' memories cannot cope; examining the users' perceptions towards their password recall, and their memory in general. Attempting to answer the question: can poor password recall really be explained by having a "poor" memory, or is it the inaccurate perception of users' password recalling abilities, affecting their performance? As illustrated in Figure 1, the password metamemory framework, it represents the relationships between memory performance, password correct recall, and metamemory.

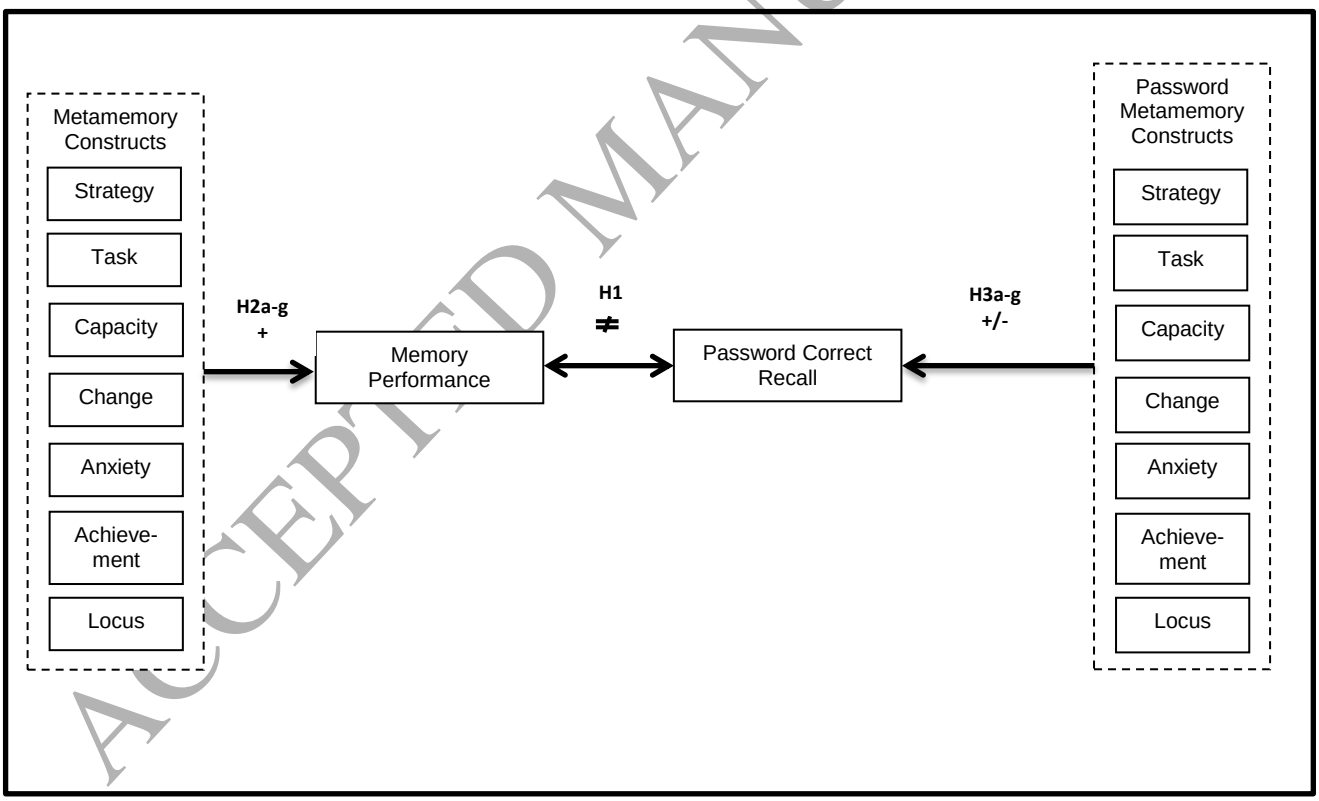

Fig. 1. Research model for testing the password metamemory framework

5. Research Methods

A two-part study was conducted including a longitudinal design, collecting password recall data (over 3500 passwords), data from memory performance tests, subjective data from the MIA questionnaire, and from an adapted (password context) version of the MIA questionnaire. This data was used to test the password metamemory framework, through examining the relationships between memory performance, password recall, and metamemory.

5.1. Participants

Participants were selected from staff and students from a university in Finland (*N*=48). The participants all had work experience, and were all experienced computer users. An advert was posted to all at the university with details about the study, asking them to sign up and answer a preliminary questionnaire. The questionnaire asked for demographic information which allowed the experimenters ensure the participants were of a range of ages, and within a range. Age is considered to be a factor that has an effect on memory and metamemory (Baddeley 2009[c]; Dixon and Hultsch, 1983[a]; Glass et al., 2005; Hertzog et al., 1990[b]). However, password users are not from one specific age group, and we felt that if older participants were not included in this study, this would undermine the ecological validity. Therefore, there was a distribution of ages, and although there were slightly more participants from the younger age groups, initial data analysis indicated that memory performance was marginally higher in the younger groups, but not significantly higher. Regarding the effect of the participants' age on metamemory results, studies have shown that metamemory is affected by age, and the constructs that predict memory performance are different dependent on the age group (Dixon and Hultsch, 1983[a]; Glass et al., 2005; Hertzog et al., 1990[b]). However, younger age groups and middle-age groups have been shown to have similar

results; the differences are only present in older age groups, which have been defined in many studies as 60 years + (Cavallini et al., 2013; Devolder et al., 1990; Dixon and Hultsch, 1983[a]; Hertzog, et al., 1994;). In this current study, the highest age range was from 45-54 years, which in terms of metamemory studies, is to be considered as middle-aged, and therefore should not show an effect of age. Demographic information is reported in Table 1.

Study credits were offered to the participants as an incentive to take part and to continue to take part in the study.

Table 1. Demographic Information

Age	Gender	Education level
18 to 24 years (count of 15; 32.3%)	Male (count of 31; 64.6%)	Bachelor's degree (count of 18; 37.5%)
25 to 35 years (count of 33; 32.3%)	Female (count of 17; 35.4%)	Master's degree (count of 22; 45.8%)
35 to 44 years (count of 9; 18.8%)		Doctoral degree (count of 8; 16.7%)
45 to 54 years (count of 9; 18.8%)		

5.2. Measures

For the first part of the study, password recall and password metamemory was examined. A website designed for creating and recalling passwords monitored password entries, and a password-version of the MIA questionnaire was created to collect password metamemory responses. The second part of the study examined participants' memory performance and metamemory, using memory performance tasks and the MIA questionnaire.

5.2.1. Password recall

A website with password generation and input capabilities was designed to collect password data. Over 12 weeks, participants created and recalled passwords, in which the website monitored correct input, and input errors. All passwords had to meet password guidelines (see Table 2), to ensure a minimum level of strength, and that participants didn't create passwords e.g. "123", that would have affected the results. These guidelines were

given to the participants before and during the creation of their passwords, and were imposed through system requirements.

Table 2. Guidelines 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 lower case letter (a-z).
4. contain at least one upper case letter (A-Z).
5. contain at least one special character (e.g. !, %, &).
6. not contain names (e.g. JussiH1#).

Two passwords were created every two weeks, then on average three passwords were recalled every week. This design was employed to firstly make the study as realistic as possible; and secondly to prevent cognitive overloading, as having to learn many items at once, could have affected recall results (Baddeley, 1992). Ten passwords were created and recalled for ten fictitious accounts, with varying importance of account types, from online banking, to social networking, to online gaming; again this design was to make the study as realistic as possible (see Table 3).

Table 3. Account types and names

Type	Name
Online banking	Danske Bank
	Nordea
Email account (personal)	Yahoo
	Gmail
Social Networking	Facebook (FB)
	Twitter
Online Shopping	Amazon
	Expedia
Online Gaming (free)	Forge of Empires (FoE)
	Tribal Wars

5.2.2. Password metamemory

Password metamemory was measured by means of an adapted version of the Metamemory. In Adulthood (MIA) questionnaire (Dixon et al., 1988). The seven constructs of metamemory were represented by 108 items. The questions were amended to be more specific in terms of the password management context (see Table 4). Like the original MIA, items were statements and questions followed by a 5-point Likert scale (for more details of

the MIA, please see below). All metamemory constructs were examined for construct validity, and showed to have a good internal consistency (Cronbach's alpha): Strategy (0.71), Task (0.84); Capacity (0.89); Change (0.84); Anxiety (0.92); Achievement (0.84); Locus (0.72). All results were computed by taking the mean score for each construct for each participant. All seven constructs were entered into the framework to keep the comparison between memory in general and memory in the password context, consist.

Table 4. Metamemory In Adulthood (MIA), and Password MIA constructs

Construct	Definition	Sample Item
Strategy	Knowledge and use of memory strategies (+ = high use)	When you are looking for something you have recently misplaced, do you try to retrace your steps in order to locate it?
Strategy (password)		If you have forgotten your password, do you use a lot of mental effort in trying to remember it?
Task	Knowledge of basic memory processes (+ = high knowledge)	For most people, facts that are interesting are easier to remember than facts that are not.
Task (password)		For most people, passwords that are meaningful are easier to remember than passwords that are not.
Capacity	Beliefs about one's own memory capacities (+ = high capacity)	I am good at remembering names.
Capacity (password)		I am good at remembering passwords.
Change	Perception of the change in one's own memory capabilities (+ = stability)	The older I get the harder it is to remember clearly.
Change (password)		The older I get the harder it is to remember my passwords clearly.
Anxiety	Anxiety and/or perception of the relationship between anxiety and memory performance (+ = high knowledge)	I feel anxious if I have to introduce someone I just met to another person.
Anxiety (password)		I feel anxious if I have to use a password I haven't used for a long time.
Achievement	Perception of one's own motivation to perform well in memory tasks (+ = high achievement)	It doesn't bother me when my memory fails.
Achievement (password)		It doesn't bother me when I can't remember my passwords.
Locus	Perceived sense of control over memory skills (+ = internal locus)	It's up to me to keep my remembering abilities from deteriorating.

Locus (password)	It's up to me to keep my password remembering abilities from deteriorating.

5.2.3. Memory performance

The human memory is incredibly complex; it encodes, retains and retrieves information, and plays an important role in our perception (Baddeley, 2009). Therefore, to represent participants' memory performance, three type of memory performance were examined: digit span, immediate recall, and long-term recall. Digit span and immediate recall represent the performance of the short-term memory, while long-term recall represents long-term memory performance (Baddeley, 2009). Digit span performance was tested using an increasing sequence of numbers presented for memorization. Free-recall memory tasks have been used often to test LTM performance, using word-lists presented for memorization, and then recalled in any order (Beaudoin and Desrichard, 2011; Dixon and Hultsch, 1983[a]; Glass et al., 2005; Hertzog et al., 1990[b]; Lineweaver and Hertzog, 2010).

The free-recall word-lists were taken from the Auditory-Verbal Learning Test (AVLT) (Rey, 1964). The word-lists are shown in English in Table 5. For the purposes of this study, this test was given as a visual test of memory, not verbal. Free-recall tests can be presented either visually or verbally (Baddeley, 2009[b]; Lezak, 1995); and as in this case, memory performance was being compared with password recall, therefore, a visual presentation was considered more appropriate, as passwords are visually learned. The second memory test, to measure digit span was taken from the Wechsler Memory Scale – Revised (WMS-R) (Wechsler, 1987). The list of number sequences is shown in Table 5.

Table 5. Free-recall word-lists and digit span number sequences

First word-list (in English)	Second word-list (in English)	Digit span number sequence
summer	table	6-2-9
curtain	bird	3-7-5
coffee	shoe	5-4-1-7
leaf	sample	8-3-9-6
school	mountain	3-6-9-2-5
factory	branch	6-9-4-7-1
track	church	9-1-8-4-2-7

jacket	glass	6-3-5-4-8-2
ship	cloud	1-2-8-5-3-4-6
treatment	wall	2-8-1-4-9-7-5
nose	food	3-8-2-9-5-1-7-4
home	car	5-9-1-8-2-6-4-7
color	village	
pike	step	
river	fish	

5.2.4. Metamemory

Metamemory was measured by means of the extensively used Metamemory In Adulthood (MIA) questionnaire (Bacon et al., 2011), developed by Dixon et al. (1988). It is a multifactor instrument presenting questions and statements followed by a 5-point Likert scale, measuring memory knowledge, memory beliefs, and memory-related affect, over seven scales with a total of 108 items (Dixon and Hultsch, 1983; Dixon, Hultsch and Hertzog, 1988; Hertzog et al., 1987). The seven scales include Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus (reported in Table 4). The MIA is well known for its psychometric properties, and several studies have reported that it is factorial valid and internally consistent (Dixon and Hultsch, 1983; Dixon et al., 1988; Glass et al., 2005; Hertzog et al., 1987). In this current study all metamemory constructs were examined for construct validity, and showed to a good internal consistency (Cronbach's alpha): Strategy (0.70), Task (0.79); Capacity (0.79); Change (0.89); Anxiety (0.84); Achievement (0.76); Locus (0.81). All results were computed by taking the mean score for each construct for each participant.

5.3. Procedure

Ethical approval was sought and approved by the university's ethics committee before recruitment for the study. The participants were asked to reply to an advert posted through the university; and while signing up for the study they were given information about what to expect, and that agreeing to take part included their formal consent. The participants were

informed that they could withdraw from the study at any point, and this option was available within the website that was used for the experiment, and via email to the experimenters.

All participants completed exactly the same tasks for the duration of the whole study. The study included a 12-week password recall stage, the completion of the Password MIA questionnaire, a memory performance test, and finally the completion of the original MIA questionnaire.

5.3.1. Password recall

During the 12 weeks, two passwords were created in weeks 1, 2, 4, 6, 8 (totaling 10 passwords) (see Table 6). Three passwords on average, (week 1 recalled 2 passwords, and in week 12, 10 passwords were recalled) were recalled every week (see Table 6). Participants were given three attempts to correctly recall their passwords each time – the website monitored all password input, including all errors. Over the 12 weeks, more than 3500 passwords were collected for these participants.

Table 6. Password (study) schedule

Week	Create Passwords (number)	Remembering Passwords (number)	Account Names
1 beginning	2		Danske Bank/Amazon
1 end		2	Danske Bank/Amazon
2 beginning	2		Facebook/Yahoo
2 end		3	Danske Bank/FB/Amazon
3 beginning			
3 end		3	Yahoo/FB/Amazon
4 beginning	2		Nordea/Forge of Empires
4 end		3	Danske Bank/Nordea/FoE
5 beginning			
5 end		3	Nordea/Yahoo/FB
6 beginning	2		Expedia/Gmail
6 end		3	Yahoo/Gmail/FoE
7 beginning			
7 end		3	Danske Bank/FB/Expedia
8 beginning	2		Tribal Wars/Twitter
8 end		3	Nordea/Twitter/Tribal Wars
9 beginning			
9 end		3	Gmail/FB/Expedia
10 beginning			
10 end		3	Yahoo/Amazon/FoE
11 beginning			
11 end		3	Twitter/FoE/Tribal Wars
12 beginning			
12 end		10	All

5.3.2. Password metamemory

The participants were asked to complete the Password MIA questionnaire after their password recall, and before they took part in the memory performance test. The questionnaire was sent electronically to participants, and was completed via their computer or in hard copy.

5.3.3. Memory performance test and metamemory

The participants were presented with a PowerPoint presentation with instructions about what they could expect from the test. PowerPoint was used as a convenient way of consistently presenting the test items, visually, and also for the same period of time, as the test was timed through the presentation of slides. The instructions were in English; however, the word-lists (free-recall) were in the participants' mother-tongue language, which was confirmed before the study started. The word-lists were in the participants' first language, so there would not be any unfair advantage given to Finnish participants. When the test began the first list of 15 words was presented to the participants for one minute (word-lists are reported in Table 3). During this time the participants were required to memorize the words. Immediately after, the screen would go blank and the participants would then have one minute to immediately recall as many words as possible, in any order (to measure STM). After the recalling minute, the same first word-list would appear again, and the participants had one minute to learn as many words as possible. Then the screen would go blank, and they would have, again one minute to recall as many words as possible. This was repeated four times, so in total, the participants would be presented with the same word-list five times, and asked to recall them five times; this repetition would show a learning curve. The sixth list represented to the participants was the second word-list. Again, like before, this list was shown for one minute, then the participants would have to recall as many words as possible,

just from the second list; this was to elicit memory interference. Following the recall of the second word-list, the participants were then asked to recall as many words from the first list as possible, again giving one minute for recall.

Following the free-recall task, the participants were presented with further instructions regarding the digit span test. When the test began the participants were presented with a sequence of three numbers, and given one second to memorize them. The screen would then go blank, and they would have one second to recall the numbers in the correct order. The participants would then be presented with another sequence of three numbers, again given one second to learn them, and one second to recall them in order. Every two sequences would increase in number from three to eight numbers (shown in Table 3). As the sequence of numbers increased, so did the amount of time the participants had to learn and recall the sequences.

After the memory tests, the participants were then asked to complete the MIA questionnaire. Following the questionnaire, the participants were asked to recall as many words from the first word-list as possible. This recall and the last one just before the digit span test, were measures of LTM recall.

6. Results

Both objective and subjective quantitative data collected during both parts of the study. Over 3500 passwords were collected and analyzed; and measured password correct recall. The memory performance data measured digit span, immediate recall, and long-term recall. For an overall memory performance score, immediate recall and long-term recall were totaled to give a generalized performance score, as recall scores were being compared to password recall performance. Although, there was an overall memory score, all three individual scores were analyzed separately, in connection to metamemory and password recall to gain a more

in-depth understanding of any potential effects. Metamemory was represented through the constructs of the MIA questionnaire; as were the Password metamemory scores, represented by the constructs of the Password MIA questionnaire.

6.1. Model Testing

To test the Password Metamemory Framework, a correlation design was used to analyze the relationship between memory performance and password correct recall. Multiple regression tests were employed to examine the predictive qualities of the metamemory constructs on memory performance, and the password metamemory constructs on password correct recall. The results of the correlational analyses between password recall and memory performance are presented in Table 7, and represented in Figure 2. The results of statistical analysis examining the constructs of metamemory and memory performance and passwords recall are presented in Table 8, and represented in Figure 3. The results of the hypotheses testing are shown in Table 9.

Table 7. Correlation analysis results

Factor correlation		**Pearson's r**	***p***
Memory performance	Password correct recall	-0.109	0.231

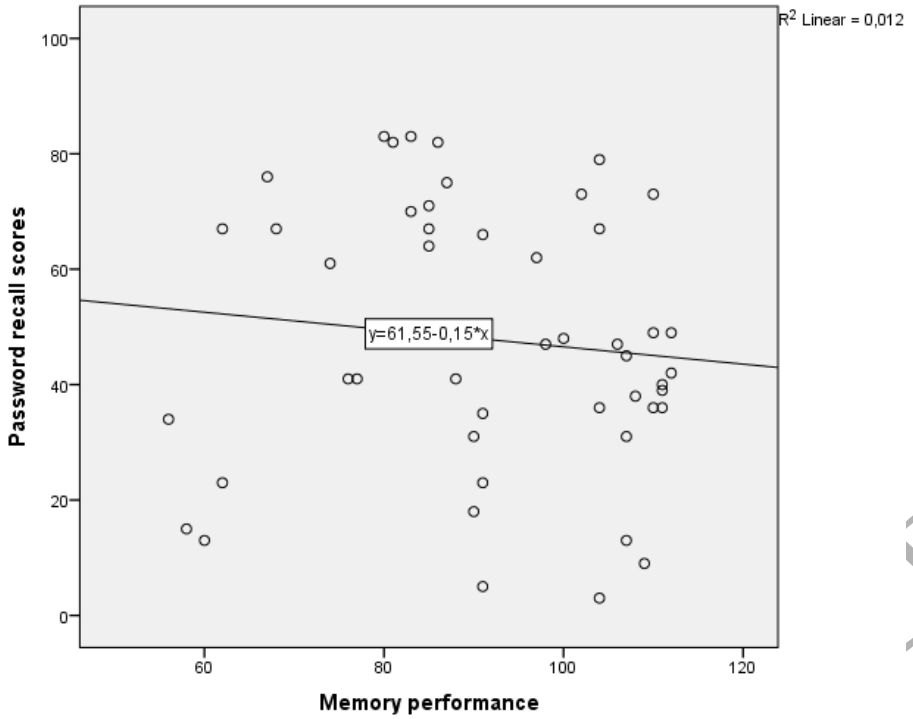

Fig. 2. Scatter plot showing no relationship between memory performance and password recall.

Table 5. Multiple regression analysis results

Factors	Significant predictor variables (metamemory)	Significant predictor variables (Password metamemory)	Std. β	Sig.
Memory performance	Adj R^2=0.519; F=17.91, p< 0.001			
	Strategy		0.391	< 0.001
	Capacity		0.315	0.011
	Task		0.241	0.044
Password correct recall		Adj R^2=0.838; F=61.56, p< 0.001		
		Capacity	0.310	< 0.001
		Locus	0.316	< 0.001
		Achievement	0.296	0.002
		Task	0.214	0.044

Table 6. Results of hypotheses testing

Hypotheses		
H1:	There will be no significant correlation between memory performance and password correct recall.	Supported
H2a:	Strategy (metamemory) will have a significant positive effect on memory performance.	Supported
H2b:	Task (metamemory) will have a significant positive effect on memory performance.	Supported
H2c:	Capacity (metamemory) will have a significant positive effect on memory performance.	Supported
H2d:	Change (metamemory) will have a significant positive effect on memory performance.	
H2e:	Anxiety (metamemory) will have a significant positive effect on memory performance.	
H2f:	Achievement (metamemory) will have a significant positive effect on memory performance.	
H2g:	Locus (metamemory) will have a significant positive effect on memory performance.	

H3a:	Strategy (password metamemory) will have a significant positive effect on password correct recall.	
H3b:	Task (password metamemory) will have a significant positive effect on password correct recall.	Supported
H3c:	Capacity (password metamemory) will have a significant positive effect on password correct recall.	Supported
H3d:	Change (password metamemory) will have a significant positive effect on password correct recall.	
H3e:	Anxiety (password metamemory) will have a significant negative effect on password correct recall.	
H3f:	Achievement (password metamemory) will have a significant positive effect on password correct recall.	Supported
H3g:	Locus (password metamemory) will have a significant positive effect on password correct recall.	Supported

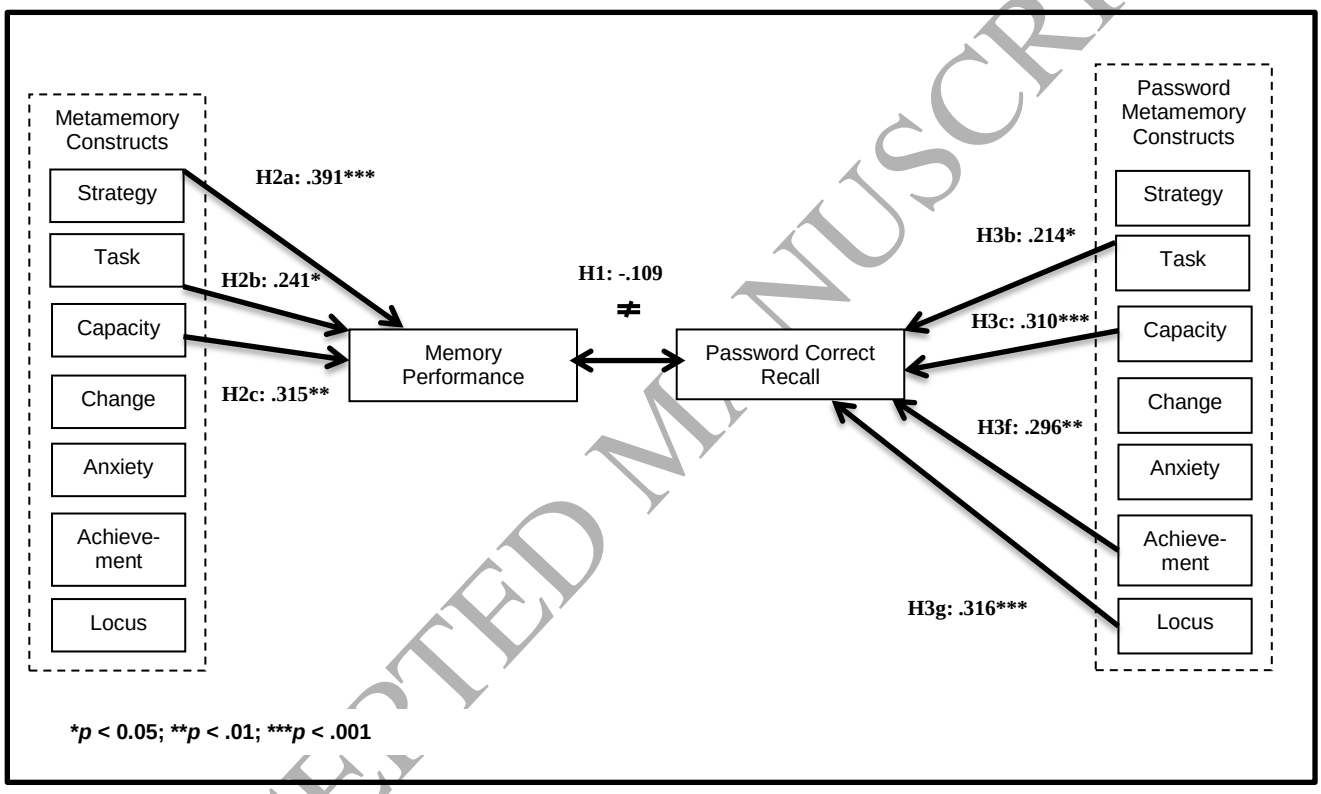

Fig. 3. The Password Metamemory Framework: summary of supported results

6.1.1. The relationship between memory performance and password correct recall

A correlation design was employed to examine the relationship between memory performance and password correct recall. Due to H1 being proposed as a null hypothesis, a *post hoc* power analysis was performed using R STUDIO (version 0.98.1103), and showed a good level of statistical power (0.82). The correlation analysis showed that there was no significant correlation between memory performance and password correct recall (p = 0.231),

supporting H1. With further analysis, there was also no relationship between digit span and password correct recall (p = 0.238), nor immediate recall (p = 0.215), nor long-term recall (p = 0.293), further supporting H1.

It is practically impossible to accept a null hypothesis where the correlation is exactly zero (Cortina and Folger, 1998); therefore, we calculated a confidence interval to assess the uncertainty of our correlation estimate. The question to answer is not whether the correlation between memory score and password recall score is exactly zero, but whether it is small enough to not make a difference. Therefore, we follow the recent guidelines by Aguirre-Urreta and Rönkkö (2017), and calculate and interpret the endpoints of the confidence intervals. We also applied a Bayesian analysis as it is recommended as an alternative when assessing the non-existence of an effect (Hoenig and Heisey, 2001). Due of lack of prior research on the relationship between memory performance and password recall, this analysis was implemented using uninformative priors. In this particular scenario, the frequentist confidence interval is equivalent with the Bayesian credible interval (Lu, Ye, and Hill, 2012), which was also confirmed by our Bayesian analysis. We assume that the readers are more familiar with confidence intervals than credible intervals, thus we have reported the former.

The estimated correlation between memory performance and password correct recall was -0.109 with a 95% confidence interval between [-0.38, 0.18]. The estimated value of -0.109 suggests that the memory performance score explains just over 1% of the variation of the performance test, which means that the two scores are largely independent. The upper limit of 0.18 similarly means just over 3% of explained variation, which implies that 97% of the password correct recall is mostly unrelated to users' memory capabilities if we assume that both scores are measured without errors. In interpreting the lower limit of -0.38, we observe that the effect is larger; however, the direction is counterintuitive, because if memory

performance had an effect on password correct recall, we would have expected it to be positive.

In summary, we did not find a relevant effect size. However, the correlation between memory performance and password recall was close enough to zero to be considered negligible. We therefore conclude that H1 is of no effect, which is supported by our analysis.

6.1.2. Metamemory predicting memory performance

To examine the constructs of metamemory and the predictive qualities towards memory performance, a stepwise multiple regression test was used. Based on the MIA questionnaire scales, the metamemory predictor variables were: Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus. Although previous research has established a relationship between Strategy, Task, Capacity (Dixon and Hultsch, 1983[a]) in predicting memory performance; for nomological validity all metamemory constructs were entered into the model.

The analysis reported that there were three significant predictors of memory performance: Strategy was the best predictor variable ($p < 0.01$), followed by Capacity ($p = 0.11$), and then Task ($p = 0.044$). These results were expected due to previous research (Dixon and Hultsch, 1983[a]), and therefore, H2a –c was supported.

6.1.3. Password metamemory predicting password correct recall

A stepwise multiple regression test was employed to investigate the predictive factors of password metamemory on password correct recall. Taken from the Password MIA questionnaire, the seven predictor variables were: Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus.

The results showed that there were four significant predictor variables of password correct recall: Capacity was the strongest predictor ($p < 0.01$), followed by Locus ($p < 0.01$),

then Achievement (p = 0.02), and finally, Task (p = 0.044). Therefore, H3b, c, f and g were supported, while H3a, d, and e were not supported, emphasizing a password security contextual difference in the relationship between metamemory and memory performance.

7. Discussion

Users claim they cannot remember all their passwords, and feel justified for adopting insecure password behaviors as a result of their memories limitations (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006). Hence, the focus of this study has been primarily to investigate whether poor password recall is related to poor memory capabilities. Regardless of what users' believe about their password memory capabilities, this study found no relationship between correct password recall and memory performance. The results suggest that poor password recall is not related to having a "poor" memory. These findings are important as they can provide users with valuable knowledge that could lead to an increase in password correct recall, and a decrease in insecure password behaviors.

Based on the discovery that there was no relationship between memory performance and correct password recall, this has resulted in the questioning of whether there are other factors involved in poor password recall. As metamemory is considered a significant factor in memory performance (Hertzog et al., 1990[a]), the second focus of this study was to investigate the involvement metamemory could have in password recall. The results first showed that there were no constructs from the metamemory (general memory) scale that could predict password correct recall (p = 0.062, overall). Therefore, metamemory was not related to password recall. This was an unexpected and important finding as the results from this study confirmed that the metamemory constructs of Strategy, Capacity and Task could predict memory performance. What this means is that an understanding of memory retrieval strategies, an understanding of the persons' memory capacity and performance, and an

understanding and knowledge of how the memory works in general, best predicts memory performance, but not password correct recall. These results established there was no relationship between the metamemory (general memory) constructs and password correct recall, which confirmed the need for a password security context-specific instrument.

With that last point in mind, the MIA questionnaire was adapted to represent operational measures of the conceptual framework presented for the password security context. The results showed that the password metamemory constructs of Capacity, Locus, Achievement, and Task could predict password correct recall. Therefore, users who believe they have more memory capacity to remember their passwords correctly, believe they have more control over remembering their passwords, who are more motivated to remember their password correctly, and understand what makes passwords more memorable, have a better password correct recall rate.

A surprising finding was that the password metamemory construct of Anxiety did not predict password recall. Many users develop a fear of forgetting due to the number of passwords (Ives et al., 2004). However, its absence in the predictive model could be explained by when users are anxious about remembering their passwords, it could affect their coping mechanism, i.e. they reuse their passwords or write them down. Anxiety does not necessarily predict the recall of passwords, just the security behavior they adopt.

Another interesting finding revealed from this study is the differences between predictive metamemory constructs in the password security and memory (in general) contexts. The constructs of password metamemory that could predict password recall were different than those found between metamemory (general memory) and memory performance. Both Capacity and Task were present in both models. However, with the application of metamemory to the password context, the predictive constructs diverged from what was expected. Locus and Achievement were present in the password context part of the

framework, while Strategy was absent. It could be argued that Locus and Achievement were present in the password context, as they represent control over the users' ability to remember their passwords, and their motivation towards remembering their passwords. Motivation and control have both been found to be related to password behavior (Zhang and McDowell, 2009). When users' believe they have less control, are less motivated to learn and remember stronger passwords (Zhang and McDowell, 2009). Strategy on the other hand was not found to predict password recall, whereas it was found to predict memory performance. Strategy has been discovered on numerous occasions to predict memory performance, so what is different about the password context? When you consider what password memory strategies are, and in relation to memory strategies, one can see why the results are different. With metamemory (general memory), making a note, writing down, making associations with other similar memories are considered *good* strategies, and aids memory performance. However, writing passwords down, sharing them, reusing them, is considered *bad* password security practices (Adams and Sasse, 1999; Duggan et al., 2012), although some security experts see these practices as a necessary evil in specific circumstances (for example, Kotadia, 2005). Therefore, whereas perceived capacity of ones' memory, knowledge of memory strategies, and understanding how the memory functions in general is related to memory performance; within the password context, there is a different picture. Perceived capacity of how many passwords can be remembered correctly, what level of control the users' perceives they have over remembering their passwords, their level of motivation to remember their password, and understanding what makes password more memorable are relevant factors in password correct recall, different to the general recall context. These differences are important as it emphasizes the need to focus on perceived control and motivation to remember passwords.

Overall, these results support the Password Metamemory Framework, bringing to light the complex relationships (or lack of relationships), between memory performance and password recall; and give an interesting insight into factors such as the components of metamemory, that contribute to password correct recall.

8. Conclusion

With every year, users are accumulating more and more accounts and services, which is leading to passwords being forgotten, and resulting in increased costs pertaining to password resetting, in terms of money, time and convenience (Brown et al., 2004; Gaw and Felten, 2006; Tari et al., 2006). Previous research suggests that users cannot cope with multiple passwords because of memory limitations (Chiasson et al., 2009; Duggan et al., 2012; Gaw and Felten, 2006). However, the results of this study suggest that correct password recall is not related to *good* or *bad* memory capabilities, but it is related to the perceptions of these capabilities. Therefore, if the problem is not solely related to memory performance, but to users' inaccurate perception of their memory, then future research needs to examine why this is the case and how such false perception can be improved. This could lead to implications for both organizations and the home-user, as an improvement in these false perceptions could result in increased policy compliance, with regards to creating stronger passwords; and reduce the need to adopt insecure password behaviors, such as writing passwords down (Biddle et al., 2012; Chiasson et al., 2009; Duggan et al., 2012; Gaw and Felten, 2006). From the results of this study, memory performance was shown to be predicted by specific metamemory constructs; whereas password recall had different metamemory contributing constructs. Future research also needs to examine the differences in contributing factors dependent on the password context, and to gain a better understanding of the complex relationships between password metamemory and password recall. Understanding the

complexity of metamemory in the password context, and the inaccurate perceptions of users could also lead to increased motivation to learn and recall passwords through users having a better understanding of their memories' capabilities, with the aim to reduce insecure password practices.

The main limitation of our study was that the sample population consisted of university staff and students. Although, the participants were of a varied education and demographic, it cannot be ignored that working and studying in a higher education institution could possibly lead many to be more aware of their memories or have a better understanding of them. However, we increased the variety of our population through including staff from various positions within the university.

In conclusion, this study proposed the Password Metamemory Framework, which offers a new perspective of examining password recall, and users' inabilities to recall multiple passwords. Our results show that correct password recall had no correlation to the memory capabilities of the user, but was correlated to the users' perceptions of their capacity to recall passwords correctly, their control over their memory for passwords, their level of motivation to remember passwords, and their understanding of how passwords can be made more memorable. This has new important implications for organizations and home-users alike. Through challenging users' perceptions of their memory capabilities towards remembering their passwords, it can lead to increased password memorability, and can therefore, reduce the consequences of forgetting passwords and adopting insecure password behaviors, such as security breaches.

Acknowledgments

The authors would like to thank Dr. Mikko Rönkkö for his guidance and comments. The authors would also like to thank the participants for taking part in such a long study. This research was supported by Tekes (the Finnish Funding Agency for Technology and Innovation) and ITEA (Information Technology for European Advancement) via the MERgE project, and the University of Jyväskylä.

References

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

Aguirre-Urreta, M., Rönkkö, M., 2017. Statistical inference with PLSc using bootstrap confidence intervals. MIS Quarterly, forthcoming.

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

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., 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.

Bacon, E., Huet, N., Danion, J., 2011. Metamemory knowledge and beliefs in patients with schizophrenia and how these relate to objective cognitive abilities. Consciousness and Cognition, 20 (4), 1315–1326.

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.

Beaudoin, M., Desrichard, O., 2011. Are Memory Self-Efficacy and Memory Performance Related? A Meta-Analysis. Psychological Bulletin, 137 (2), 211-241.

Besken, M., Mulligan, N.W., 2013. Easily perceived, easily remembered? Perceptual interference produces a double dissociation between metamemory and memory performance. Memory & Cognition, 41 (6), 897-903.

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.

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

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.

Cavallini, E., Bottiroli, S., Fastame, M.C., Hertzog, C., 2013. Age and subcultural differences on personal and general beliefs about memory. Journal of Aging Studies, 27, 71-81.

Cavanaugh, J.C., Feldman, J.M., Hertzog, C., 1998. Memory Beliefs as Social Cognition: A Reconceptualization of What Memory Questionnaires Assess. Review of General Psychology, 2 (1), 48-65.

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.

Cortina, J. M., Folger, R.G., 1998. When is it Acceptable to Accept a Null Hypothesis: No Way, Jose? Organizational Research Methods, 1(3), 334–350.

Criss, A., Malmberg, K., Shriffrin, R., 2011. Output interference in recognition memory. Journal of Memory and Language, 64 (4), 316-326.

Devolder, P.A., Brigham, M.C., Pressley, M., 1990. Memory Performance Awareness in Younger and Older Adults. Psychology and Aging, 5 (2), 291-303.

Dixon, R.A. (2000). The concept of metamemory: Cognitive, developmental, and clinical issues. In Berrios, G.E., Hodges, J.R., (Eds.), Memory disorders in psychiatric practice, Cambridge University Press, New York, pp. 47–57.

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

Dixon, R.A., Hultsch, D.F., 1983[a]. Metamemory and memory for text relationships in adulthood: A cross-validation study. Journal of Gerontology, 38, 689–694.

Dixon, R.A., Hultsch, D.F., 1983[b]. Structure and development of metamemory in adulthood. Journal of Gerontology, 38, 682–688.

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

Eysenck, M., Keane, M., 2010. Cognitive Psychology, sixth ed. Psychology Press, Hove & New York, NY.

Flavell, J.H., 1971. First discussant's comments: What is memory the development of? Human Development, 14, 272–278.

Flavell, J.H., 1979. Metacognitive and cognitive monitoring: A new area of cognitive developmental inquiry. American Psychologist, 34, 906–911.

Flavell, J.H., Wellman, H.M., 1977. Metamemory, in: Kail, R.V., Hagen, J.W., (Eds.), Perspectives on the development of memory and cognition. Erlbaum, Hilldale, NJ.

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.

Glass, J.M., Park, D.C., Minear, M., Crofford, L.J., 2005. Memory beliefs and function in fibromyalgia patients. Journal of Psychosomatic Research, 58, 263– 269.

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, pp. 997-1006.

Hertzog, C., 1992. Improving Memory: The Possible Roles of Metamemory, in: Herrmann, D.J., Weingartner, H., Searleman, A., McEvoy, C. (Eds.), Memory Improvement, Springer–Verlag, New York, pp. 61-78.

Hertzog, C., Dixon. R. A., & Hultsch, D. F. (1990[a]). Relationships between metamemory, memory predictions, and Memory Task performance in adults. Psychology and Aging, 5 (2), 215-227.

Hertzog, C., Dixon. R.A., Hultsch, D.F., 1990[b]. Metamemory in adulthood: differentiating knowledge, beliefs, and behavior. Advances in Psychology, 71, 161–212.

Hertzog, C., Dixon. R.A., Schulenberg, J.E., Hultsch, D.F., 1987. On the differentiation of memory beliefs from memory knowledge: The factor structure of the metamemory in adulthood scale. Experimental Aging Research, 13 (2), 101-107.

Hertzog, C., Lineweaver, T.T., & Hines, J.C., 2014. Computerized assessment of age differences in memory beliefs. Perceptual & Motor Skills: Physical Development & Measurement, 119 (2), 609-628.

Hertzog, C., McGuire, C.L., Lineweaver, T.T., 1998. Aging, attributions, perceived control, and strategy use in a free recall task. Aging, Neuropsychology, and Cognition, 5, 85–106.

Hertzog, C., Saylor, L.L., Fleece, A.M., Dixon. R.A., 1994. Metamemory and aging: Relations between predicted, actual and perceived memory task performance. Aging and Cognition, 1 (3), 203-237.

Hoenig, J.M., Heisey, D.M., 2001. The Abuse of Power: The Pervasive Fallacy of Power Calculations for Data Analysis. The American Statistician, 55(1), 19–24.

Hultsch, D.F., Hertzog, C., Dixon, R. A., Davidson, H., 1988. Memory self-knowledge and self-efficacy in the aged, in: Howe, M.L., Brainerd, C.J.,(Eds.), Cognitive development in adulthood: Progress in cognitive developmental research. Springer–Verlag, New York, pp. 65–92.

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, pp. 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., 1978. On interpreting the effects of repetition: Solving a problem versus remembering a solution. Journal of Verbal Learning & Verbal Behavior, 17, 649-667.

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.

Kotadia, M., 2005. Microsoft: Write down your passwords. ZDNet Australia 23.

Lezak, M.D., 1995. Neuropsychological Assessment, third ed., Oxford University Press, NewYork & Oxford.

Lin, S., Yen, D.C., Chen, P.S., Lin,W., 2013. Coding behavior of authentication code on the internet. Computers in Human Behavior, 29, 2090–2099.

Lineweaver, T.T., Bondi, M.W., Galasko, D., Salmon, D., 2014. Effect of knowledge of APOE genotype on subjective and objective memory performance in healthy older adults. American Journal of Psychiatry, 171 (2), 201-208.

Lineweaver, T.T., Hertzog, C., 1998. Adult efficacy and control beliefs regarding memory and aging: separating general from personal beliefs. Aging, Neuropsychology, and Cognition, 5 (4), 264-296.

Ling, J., Catling, J., 2012. Cognitive Psychology. Pearson Education Ltd., Harlow.

Lu, D., Ye, M., Hill, M.C., 2012. Analysis of regression confidence intervals and Bayesian credible intervals for uncertainty quantification: Regression confidence and Bayesian credible intervals. Water Resources Research, 48(9).

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

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.

Pierce, S.H., Lange, G., 2000. Relationships among metamemory, motivation and memory performance in young school-age children. British Journal of Developmental Psychology, 18, 121–135.

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

Rey, A., 1964. *L'examen clinique en psychologie*. Presses Universitaires de France, Paris.

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.

Schwartz, B.L., Benjamin, A.S., Bjork, R.A., 1997. The Inferential and Experiential Bases of Metamemory. Current Directions In Psychological Science, 6 (5), 132-137.

Straub, D.W., Boudreau, M., Gefen, D. (2004). Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems, 13(24), 380-427.

Tari, F., Ozok, A.A., Holden, S.H., 2006. A Comparison of Perceived and Real Shoulder surfing Risks between Alphanumeric and Graphical Passwords. In Proceedings in (SOUPS), Pittsburgh, PA, USA.

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.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49, 190-198.

Vu, K.L., Proctorb, 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.

Wechsler, D., 1987. Wechsler Memory Scale-Revised manual. The Psychological Corporation, San Antonio, TX.

Wellman, H.M., 1983. Metamemory revisited, in: Chi, M.T.H., (Ed.), Trends in memory development research. Karger, Basel, Switzerland, pp. 31 -51.

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.

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 post-doctoral researcher at the University of Jyväskylä, Finland. She has a Ph.D. in Cognitive Science, and a MSc. in Clinical Psychology. Her research focuses on password security and memorability.

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 40, and he has more than 6000 citations (Google Scholar). He has published 50 articles in journals such as MIS Quarterly and Information Systems Research.