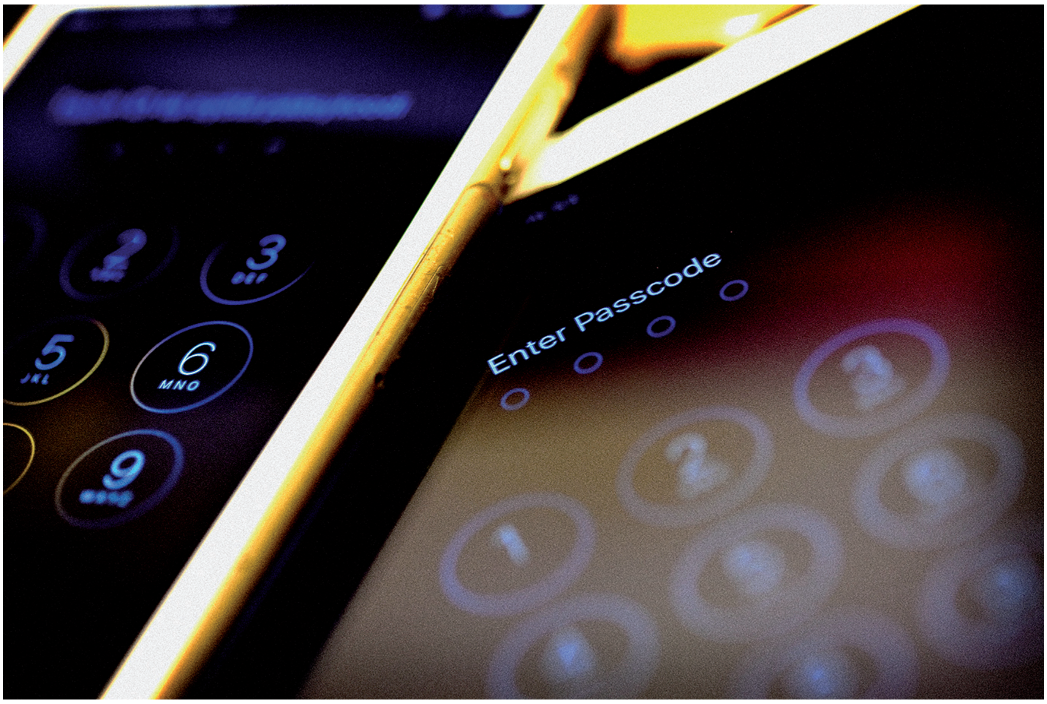
JYVÄSKYLÄ STUDIES IN COMPUTING
249

Naomi Woods

Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory



JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 249

Naomi Woods

Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 3
marraskuun 26. päivänä 2016 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 3, on November 26, 2016 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory

JYVÄSKYLÄ STUDIES IN COMPUTING 249

Naomi Woods

Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

Editors
Marja-Leena Rantalainen
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Ville Korkiakangas
Publishing Unit, University Library of Jyväskylä

URN:ISBN:978-951-39-6846-5
ISBN 978-951-39-6846-5 (PDF)

ISBN 978-951-39-6845-8 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2016

ABSTRACT

Woods, Naomi
Improving the Security of Multiple Passwords Through a Greater Understanding of the Human Memory
Jyväskylä: University of Jyväskylä, 2016, 151 p.
(Jyväskylä Studies in Computing
ISSN 1456-5390; 249)
ISBN 978-951-39-6845-8 (nid.)
ISBN 978-951-39-6846-5 (PDF)

Multiple passwords are an increasing security issue that will only get worse with time. One of the major factors that compromise multiple passwords is users' memory, and the behaviors they adopt to compensate for its failures. Through studying memory elements that influence users' password memorability, we may increase our understanding of the user and therefore make proposals to increase the security of the password authentication mechanism. This dissertation examines the human memory to understand password security behaviors; and moreover, develops new theories and revises prominent memory theories for the password context. This research employs memory theories to not only increase the memorability of passwords, but to also improve the security of them by means of three studies that examine users' beliefs and awareness (metamemory) about how their memory affects their password memorability and insecure password behavior; and look to increasing password memorability through improving learning (repetition through verification), and retrieval (through uniqueness). Empirical longitudinal studies collecting objective and subjective data measuring password recall (over 10000 passwords), memory interference, memory performance, memory beliefs, user convenience, and insecure password behavior. Through collecting objective password recall data, the results of these studies challenge users' preconceptions about justifying their adoption of insecure password behaviors. Furthermore, it challenges the assumption of trade-offs between password security, memorability and user convenience found in previous password research. In meeting the objectives of the dissertation, this research has significant practical implications for organizations and individual users. Through a greater understanding of the human memory this can inform users to adopt better password security practices. The implications of these results suggest how to increase password memorability, how to decrease password forgetting, and how to decrease insecure password behaviors and the consequences of such insecure behaviors (such as security breaches).

Keywords: password security; password memorability; user convenience; memory theories; user memory; metamemory; interference; repetition; password reuse; unique passwords

Author

Naomi Woods
Department of Computer Science and Information Systems
University of Jyväskylä
naomi.woods@jyu.fi

Supervisors

Professor, Ph.D., D.Soc.Sc., Mikko Siponen
Department of Computer Science and Information Systems
University of Jyväskylä

Professor, Ph.D., Pertti Saariluoma
Department of Computer Science and Information Systems
University of Jyväskylä

Reviewers

Professor, Ph.D., José J. Cañas
Department of Experimental Psychology
University of Granada

Professor, Ph.D., Huigang Liang
Center for Healthcare Management Systems
College of Business
East Carolina University

Opponents

Professor, Ph.D., José J. Cañas
Department of Experimental Psychology
University of Granada

Associate Professor, Ph.D., Miguel Gea
Language and Information System Department
University of Granada

ACKNOWLEDGEMENTS

I started my PhD in very different circumstances than I find myself today, professionally and personally. My whole life has changed over the past four years. The people mentioned below have contributed to that, and have made me who I am today. They have encouraged me, inspired me, and have contributed to the successes of my life. While writing this, I had to consider who to include and where to include them. I think I have included everyone in the world (well, in my world), because they all mean so much to me, and I appreciate everyone for their big or small contribution to my life.

My first supervisor Prof. Mikko Siponen has supported and encouraged me to be the best I can be, to step outside my comfort zone, through for instance lecturing and presenting. He has challenged me and provided intellectual inspiration and enthusiasm; while putting up with my hyperactivity and arguing with me, even when he and I both knew he was right. He has always believed in my work, and has provided me with the funding to achieve my success. My second supervisor Prof. Pertti Saariluoma has given me encouragement and advice through the process. Providing the support I needed from an academic from psychology/cognitive science, that understands my approach to research and the subject of my work. Thank you both so much.

Living in Finland has meant that several of my work colleagues have not only become my friends, but I consider them as family, my Finnish family. I would like to thank Dr. Kati Clements for her strength, support and being a truly inspirational friend – you are my Zena. Juuli Lintula, for her sweetness and particularity in everything, for reading through my work, and translating everything. Manja Nikolovska, for her amazing rockstar approach to saving the world and IS research. Dr. Rebekah Rousi, for inspiring me to think outside the box, and brining her beautiful family into my life. Cory Barker, for being one of the smartest guys I know, pushing my brain to its limits, reading through my work, and counting dots. But these guys have been so much more than that, they have been there for me unconditionally, and I know they always will be – thank you.

I would like to thank also Dr. Philipp Holtkamp for the challenging and stimulating questioning and conversations; and for going through my research and helping me work through so many complex problems. Dr. Henri Pirkkalainen, for his humor, but also someone I could turn to professionally and personally, for being my Finnish brother. (Soon to be Dr.) Johanna Silvennoinen, for her stimulating conversations, arguments about the existence of the mind, her silly voices that brighten my day and make academic conversations challenging and incredibly silly, and of course her co-authorship in research-based song creations, like "uncorn, or is it just a horse?"

I would also like to thank Prof. Tuure Tuunanen for his support through the process, I knew I could always look to him for reassurance in a presentation. Andy (Nan) Zhang, for his advice and for taking the time to read my work. Jussi P. P. Jokinen, for invaluable statistical advice, and Alexander Semenov for

translating what I needed a computer to do, into a website that could collect all the data for this dissertation. I would like to thank Sarah (Yixin) Zhang for her professional, academic and spiritual counsel. Hilkka Grahn, for reading through my work and translations, for just being the brightness first thing in the morning in the office opposite, and a good friend.

I would like to thank Hemin Jiang, Hadi Ghanbari, Alain Tambe Ebot, Aggeliki Tsochou for their inspiring conversations and for their friendship.

Special thanks go to Seija Paananen, and Tapio Tammi for your administrative support, but also being invaluable friends; and to Sami Kollanus for listening to me worry about my work progression, and every other academic worry.

I would like to thank Niina Ormshaw for being there for me and my partner in crime, and Niko Tuominen for always very interesting and stimulating conversations, you are both great friends.

I would also like to thank Antti Vuorenmaa, Jose J. Cañas, Tiina Koskelainen, Markus Salo, Eetu Luoma, Tuomo Kujala, Kate (Jungwon) Kuem, Jing Li, Teija Palonen, Panu Moilanen, Wael Soliman, Noora Hämäläinen, Samu Turunen, Arto Ojala, Tuomas Kari, Toni Taipalus and Ari Tuhkala, Patrick Grönlund, Pentti Koskela, Ugo Etudo, Olga Kushanova, Alexander Clements, and Arja Rousi (Elsa, my Frozen research assistant).

My warmest thanks go to my family and friends in England, for all their love and support - they might be a couple of thousand kilometers away, but they are never far: Jasmine Woods, John Bass, Carmen Mason, Oliver Mason, Claudia Mason, Alan Woods, Gavin Woods, and Sian Wilkinson. They have all supported me in so many wonderful ways.

I would like to thank Deepa Sutherland whose comments when I was a child made me believe in myself, and believe I could be a scientist and doctor – still need another six doctorates though to make it to Sam Beckett levels.

I would like to also thank Derek Chapman for his hours of patience, and Michael Angelo for his spiritual guidance.

And finally I would like to thank Carrie Allerton, my best friend, you have been there for me always, and have welcomed me into your home and family in my darkest hours. You are pink, and radiate a beauty that can only come from the purest of hearts. I am honored to know you and have you as my friend.

I dedicate this dissertation to all those named on this page, without your contributions, love, and support I would have not achieved my dreams.

Jyväskylä 6.11.2016
Naomi Woods

FIGURE

TABLE

ABBREVIATIONS

ANOVA - Analysis Of Variances
AVLT - Auditory-Verbal Learning Test
FB - Facebook
FOE – Forge Of Empires
GLMM - Generalized Linear Mixed Model
IS – Information Systems
IT – Information Technology
LTM – Long-Term Memory
LTWM – Long-Term Working Memory
MIA – Metamemory In Adulthood (questionnaire)
PMT – Protection Motivation Theory
STM – Short-Term Memory
TAM - Technology Acceptance Model
TRA - Theory of Reasoned Action
WM – Working Memory
WMS-R - Wechsler Memory Scale – Revised

LIST OF INCLUDED PUBLICATIONS

I. Woods, N., & Siponen, M. The password metamemory framework: a new perspective in examining password memorability and password reuse. (Under review).

II. Woods, N. Password verification: increasing password memorability, while not inconveniencing the user. (Under review).

III. Woods, N., & Siponen, M. The Unique Password Theory: better password memorability, better password security practice. (Under review).

CONTENTS

“Memory is the treasury and guardian of all things.”

(Cicero, 106-43 BC)

“The problem is that the average user can't and won't even try to remember complex enough passwords to prevent dictionary attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it on a Post-it and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications."

(Schneier, 2004)

1 INTRODUCTION

1.1 Background and research context

Passwords are the most commonly used authentication mechanism (Grawemeyer & Johnson, 2011; Vance et al., 2013; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009), and are thought to be the future of security (Grawemeyer & Johnson, 2011; Wiedenbeck et al., 2005), due to the cost, reliability and technical issues that pertain to password alternatives. Considering that cracking passwords can give open access to any sensitive information in an IS, the security of passwords has been an important priority in information security research (Crossler et al., 2013; Garrison, 2006; Bonneau & Preibusch, 2010; Grawemeyer & Johnson, 2011; Siponen & Vance, 2010). The password problems noted in the IS literature include insecure password behaviors, such as choosing weak passwords; reusing or modifying passwords for more than one account; writing passwords down; sharing passwords; and not changing passwords regularly (Adams & Sasse, 1999; Campbell et al., 2006; Guo, 2013; Zhang et al., 2009). It is widely reported that such insecure password behaviors stem from the users' inability to memorize multiple passwords; hence, they adopt these behaviors (Campbell et al., 2006; Duggan et al., 2012; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). The ramifications of forgetting passwords can be expensive in terms of time (e.g. when employees are unable to log on to work systems), money (e.g. IT helpdesk costs), and convenience (e.g. when users are unable to access their accounts), if passwords need to be reset (Brown et al., 2004; Vu et al., 2007). Given that the number of passwords and the amount of accounts and systems they protect are on the rise, this is a problem that will only get worse with time (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009).

There are several issues that affect the security of passwords. Previous research suggests there is a trade-off between password memorability and password security, and more recently user convenience (Tam et al., 2010; Vu et al., 2007; Weir et al., 2009; Zhang et al., 2009). However, users are more concerned with remembering passwords, and reducing any inconvenience caused by the password process, than securing their information (Grawemeyer & Johnson, 2011; Tam et al., 2010; Weir et al., 2009; Zhang, et al., 2009). And this is just one reason why users are still considered to be the weakest link in information security (Crossler et al., 2013; Ifinedo 2012; Sasse et al., 2001).

Therefore, to improve users' password behavior, password policies, guidance, and training is given on websites, and within corporations. Moreover, previous IS research has examined the problem from two research streams. The first stream approaches insecure password behavior as any other IS security behavior; applying theories such as deterrence, rational choice, and Protection Motivation Theory (PMT) (Guo & Yuan, 2012; Jenkins et al., 2014; Johnston et al., 2015; Vance et al., 2013; Willison & Warkentin, 2013; Workman, et al., 2008; Zhang & McDowell, 2009). These studies have their merits, and help us to understand why users adopt insecure password practices; however, they are not intended to solve memory issues. The second stream theorizes that insecure password behaviors stem from memory issues, and accordingly, focus on the memory aspect of the problem.

There is a deficit of studies that attempt to improve the memorability of passwords and fewer still that conduct laboratory experiments capturing actual password recall and behavior, instead of users' perceptions towards their memory and behavior. Therefore, the important direction of this password security research examines the human memory in more depth via means of analyzing objective data. This will give a better understanding of how memory affects the password process while suggesting ways in which to improve multiple password memorability, and increasing the security of the password authentication mechanism. Hence, this dissertation will attempt to answer: through applying different memory theories to understand the password problem, can we increase the memorability and the security of passwords simultaneously? Through increasing the memorability of passwords, do we have to compromise on the security of passwords? How can we increase the memorability of passwords using the existing password mechanisms and systems? Is password memorability just a memory capacity problem, or are there other factors involved?

The aim of this dissertation is to examine the human memory in more depth, and apply a cognitive science approach to scientifically explain insecure password behaviors within the password security context. Scientific explanation has been used to describe different facets of human thinking, including learning and memory (Thagard, 2012). Scientific explanation in cognitive science is within the same stream as philosophical explanation, and describes mechanisms that result in phenomena to be clarified (Abrahamsen & Bechtel, 2012). These mechanisms are a framework of factors that interact that result in changes and are associated with solutions (Saariluoma, 2003; Thagard, 2012). In cognitive science, explanations describe a variety of aspects of thinking (e.g. memory) that occurs mechanistically, due to interactions or computational procedures. A single general theory or framework of cognition would explain the mechanistic workings of all human thinking, including memory and learning (Thagard, 2012). In term of human behavior, “there is no single framework for explaining human behavior; instead different types of problems must be solved using very different types of explanatory frameworks” (Saariluoma, 2005). There are seemingly unendless different explanations for human behavior; however, it is crucial to examine different explanatory frameworks to attempt to resolve problems in human behavior resulting from cognitive issues (Saariluoma, 2005). Therefore, through applying memory theories to password security I make propositions to increase the memorability of passwords, while not compromising the security of passwords.

As a cognitive science dissertation, the main body is written in the style of cognitive science, while the studies themselves are written for the IS publishing forum; meaning that the structure is different, and it is written for a different audience. Therefore, this dissertation will start with a cognitive science approach to the study of memory with a brief description of the main theories and issues involved with it. Then it will discuss the password context: what makes a password strong, the password problem, and will then look to password security research focusing on IS security behavior, and more importantly considering the issue from a memory perspective. Next I will give an overview of the research conducted for this dissertation, and an overview for the three studies involved; before moving onto the individual chapters for each study, where I will discuss the research progression. Finally, this dissertation will discuss the overall key findings, contributions, limitations and suggested future research.

1.2 Cognitive science and approaches to the study of the human memory

Virtually every aspect and action in our everyday lives depends on our memory (Ranganath, et al, 2012), from remembering a person’s name to driving a car. Therefore, understanding how the human memory works and the processes involved is an important area of exploration within the field of cognitive science.

Cognitive science attempts to understand the mind and its processes: examining behavior and intelligence, and how information is processed in terms of language, perception, emotion, reasoning, learning and memory in humans (cognitive psychology) and in computers (artificial intelligence) (Abrahamsen & Bechtel, 2012; Thagard, 2008). As an interdisciplinary field, cognitive science embraces philosophy, psychology, neuroscience, linguistics, anthropology and artificial intelligence. The discipline’s origins date back to the Ancient Greek philosophers such as Aristotle exploring the nature of human knowledge, and from there the discipline remained a philosophical issue until the emergence of psychology in the late nineteenth century (Thagard, 2008). With the introduction of electronic computers around the 1940’s, artificial intelligence and neural networks gave rise to a "cognitive revolution" in psychology, and by the mid-1970s the discipline had been given its name (Abrahamsen & Bechtel, 2012).

The study of the human memory goes back nearly as far as the psychology discipline to Ebbinghaus in 1885. Ebbinghaus, through learning list of words and nonsense syllables (or verbal learning approach), was the first to demonstrate that memory could be studied experimentally (Baddeley, 2009a; Ranganath, et al, 2012). Since the late 1800s there have been countless developments in understanding the human memory. Bartlett (1932) while studying meaning and memory using complex material such as stories and folk tales proposed that remembering was not an exact replay of events, but an "imaginative construction", as we access bits of an experience to form and reconstruct memory and fill in the blanks with an internal representation about the world (schema) (Baddeley, 2009a; Ranganath, et al, 2012). Milner in the late 1950's developed another approach to examining the human memory, by studying patients. Her studies of amnesic patients demonstrated that damage to certain brain areas caused specific memory and cognitive dysfunctions while allowing other functioning to continue unaffected. These results led to the development of neuroscience and neuropsychological research, examining the different brain regions involved with specific memory processes (Ranganath, et al, 2012).

Having discussed some of the most important developments and approaches for the study of memory, the next section will look to the multi-store model which is one of the most significant memory theories.

1.2.1 Multi-store model

When comparing the human memory to a computer system, it is required to encode information, store information, and retrieve the stored information (Baddeley, 2009). There are many theorists that have described the fundamentals of the human memory system, how they interact, and how information is processed. The Stages of Memory Theory (Modal Model) proposed by Atkinson & Shiffrin (1968) (illustrated in Figure 1.) is considered one of the most influential multi-storage models, identifying three types of memory stores: sensory memory, short-term memory, and long-term memory (Eysenck & Keane, 2010). Information is first processed in the sensory memory, like an interface between perception and memory, before being passed along to the STM, a temporary store, and then it's stored in the LTM (Baddeley, 2009a). Even with a distinct sensory memory, STM and LTM, the flow of information is not assumed to be just in one direction from environment – sensory memory – STM – to the LTM, studies suggest that information flows in both directions (Baddeley, 2009a). For example, our own knowledge about the world held in the LTM may influence our motivation to learn and process information in the sensory or STM.
However, the model modal is based on many assumptions, which has led to the subsequent questioning and eventually elaboration and developments of the model.

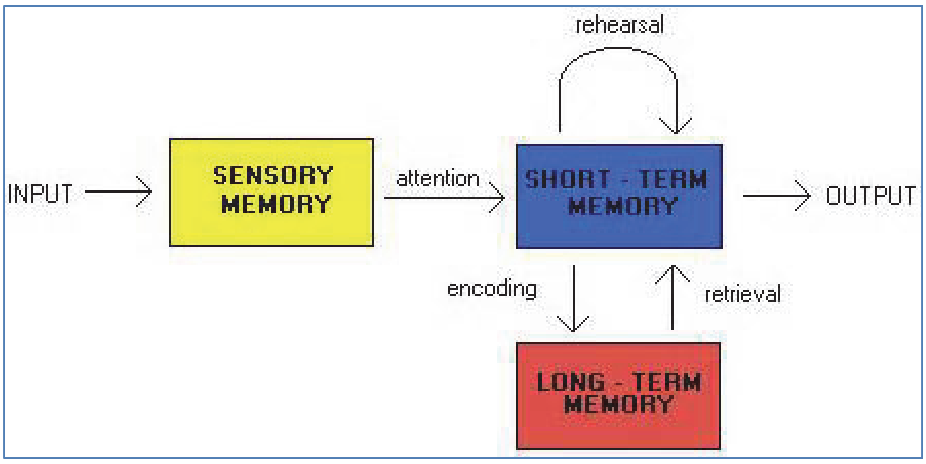


FIGURE 1: Stages of Memory Theory (Atkinson & Shiffrin, 1968)

The sensory memory was the focus of much research in the 1960s, examining the encoding, storage and retrieval of information (Eysenck & Keane, 2010). It refers to the fleeting storage of information being attended to before the information is processed in the STM, or just lost/forgotten. An example of how the sensory memory works is the trail left by a sparkler. The trail as an image, stays after the sparkler has passed being stored briefly, then rapidly fading and illustrating forgetting. This phenomenon is how we perceive films as moving images. The static image remains briefly in our sensory store until we are presented with the next static image, bridging the gap between images that are slightly different and changing gradually (Baddeley, 2009a).

The short-term memory is considered to store small amounts of information for a brief period of time (Baddeley, 2009b). It has a limited capacity (Ling & Catling, 2012), which was established by Miller (1956), with a recall rate being 7 ± 2 items (Miller, 1956). The model modal, although considered a working memory model, referred to mainly verbal STM. Criticisms of the model were based on its assumptions, that information was transferred from the STM to the LTM just through simple rehearsal; and that it didn't conclusively explain how patients with dysfunctional STM did not have general working memory dysfunctions. Baddeley & Hitch (1974) (illustrated in Figure 2.) in response to these criticisms proposed a multicomponent model of working memory. When referring to the STM, one is referring to the storage of information for a brief amount of time, whereas the working memory is assumed to combine storage with information manipulation, and to perform as a workspace for carrying out complex tasks. The working memory model consisted of three components: a modality-free central executive similar to an attentional controller; and two subsystems, the phonological loop which holds and manipulates speech-based information, and a visuospatial sketchpad, specialized for spatial and visual coding (Baddeley, 2009c; Ranganath, et al, 2012).

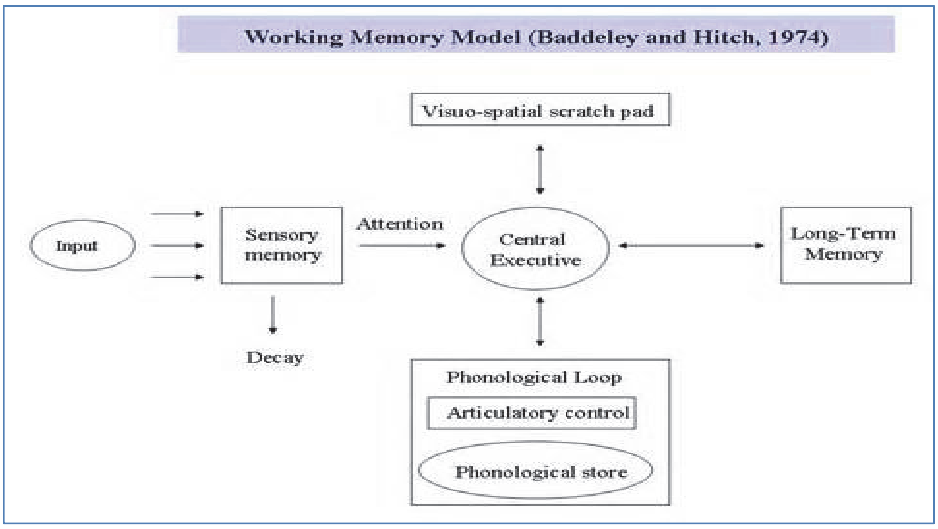


FIGURE 2: Working memory model (Baddeley & Hitch, 1974)

The episodic buffer was the most recent component to be added to the working memory model. Proposed by Baddeley (2000), it is the third subsystem controlled by the central executive, that is used to integrate information into a coherent whole and to store that information briefly from the visuospatial sketchpad, the phonological loop and the LTM (Eysenck & Keane, 2010; Ranganath, et al, 2012).

Individual differences in the working memory have been comprehensively examined using a variety of measures based on the storage and manipulation of information. These measures have shown to be capable of predicting cognitive performance successfully. Furthermore, neuropsychology cases and neuroimaging studies have played a critical role in providing evidence and supporting the multicomponent model (Baddeley, 2009d).

The long-term memory is referred to the systems in which information is stored over a long period of time, with unlimited capacity (Baddeley, 2009e; Eysenck & Keane, 2010). There are different component of LTM (proposed by Squire, 1992), however the most important distinction is between explicit or declarative memory, and implicit or nondeclarative memory. Explicit/declarative memory is the memory involved with intentional or conscious retrieval, of either or both specific events (episodic memory), such as passing an exam; or remembering facts (semantic memory), e.g. houseplants will die if you don't water them (Tulving, 1972). Implicit/nondeclarative memory does not depend on conscious recall and is demonstrated through performance, for example, riding a bike. There are different types of implicit memory and learning: procedural memory, classical conditioning and priming (Baddeley, 2009a).

1.2.2 Learning or encoding

“The capacity to learn is crucial for the development of both the individual and society.” (Baddeley, 2009d). Studying learning by scientific experimentation can be traced back to Ebbinghaus in the mid-1880s (mentioned previously). Nonsense syllables were studied and learned, and he found that learning occurs in a linear fashion, and was improved when practice was spread or distributed, compared to being concentrated (Baddeley & Longman, 1978). Testing has also found to be important for learning, to ensure successful retrieval (Landauer & Bjork, 1978). The expanding retrieval method is a learning schedule where items are tested after a short delay, then tested subsequently as the delay increases, this is an effective learning procedure with significant practical implications (Baddeley, 2009d).

1.2.2.1 Cognitive load

Cognitive load theory is refers to the amount of "mental energy" or effort required to process information (Feinberg & Murphy, 2000). Cognitive load increases as the amount of information increases that our mental resources have to process. When the amount of information exceed the capacity and limitations (as the working memory has a limited capacity in processing information), it can become overloaded (heavy cognitive load), and therefore learning reduces (Baddeley, 1992; Miller, 1956).

1.2.2.2 Capacity

Memory capacity was originally one of the defining characteristics distinguishing between the STM and LTM. All subcomponents of the working memory are limited in capacity (Baddeley & Hitch, 1974). The working memory has a limited capacity only being able to hold 7 ± 2 items (Miller, 1956). This limitation effects thought processes making it difficult to encode and learn new information, resulting in information being easily forgotten, sometimes even before it has been stored in the LTM (Baddeley, 2009b; Eysenck & Keane, 2010).

1.2.2.3 Repetition and rehearsal

Repetition in learning is an important part of general memory theories. Throughout the years, repetition and rehearsal was thought by many theorists as all that is needed to learn (Baddeley, 2009). A more contemporary view suggests learning can be increased through linking the 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 the STM for immediate use; for instance, until you make a call. Elaborative rehearsal is what is used to transfer information from the STM to the LTM as it incorporates thinking about the meaning of the information and relating it to what is already know (Goldstein, 2011). Furthermore, if recall of information is expected later after a delay, more retrieval cues will be formed while rehearsing (Jacoby & Bartz, 1972). What is more, Nilsson (1987) found that motivation and intention to learn is important for the focus of attention. More recent studies suggest that repetition without motivation from the learner to organize the information may not necessary result in learning (Baddeley, 2009).

1.2.2.4 Depth of processing

Craik and Lockhart (1972) believed that information is processed on several levels. For example, when processing a written word, the word is observed on a visual level, with how the letters are printed. The sound of the word is considered, and how we image it looks. The meaning of the word is contemplated, in general terms, e.g. an apple is a fruit; and personally, an apple is my favorite fruit. Several studies have shown that the more levels of processing and deeper levels of meaning would show better retention (Eysenck & Keane, 2010). Bartlett suggested that by adding meaning through a story or schema to information will also facilitate recall. As with elaborate processing, using information already known to attach to what is being learned this results in better memorability (Baddeley, 2009d).

1.2.2.5 Mnemonic technique

Mnemonics are learning techniques used to aid information retention, through adding meaning to and ordering the meaningful information so that our brain can retain it easier (Baddeley, 2009). There are several types of mnemonic aids: external aids, such as lists, calendars, and diaries have been found to be the most commonly used (Harris, 1980). Whereas internal aids are considered useful when a person cannot use external aids, such as in an examination, notes cannot be brought in (Harris, 1980). Examples of internal aids are for instance, visual imagery mnemonic techniques such as the method of loci, where information that needs to be remembered is associated with locations; e.g. a route to walk along (Eysenck, 2009). An example of verbal mnemonic techniques would refer to for instance, Bradshaw (1849), used a way in which to code historical dates into letters and then construct meaningful sentences. There are three components that most mnemonic techniques require, meaningful information (relating the new information to what is already known); retrieval structure (cues are formed and used to assist memory retrieval); and “speed-up” (practice and the quickening of retrieval allows the process to become quicker) (Eysenck, 2009).

1.2.2.6 Long-term working memory

Long-term working memory (LTWM) was a theory proposed by Ericsson & Kintsch (1995). This model suggested that the LTM was involved in temporarily storing information, and was inspired by the performance of people who were experts in remembering. The information stored in the LTM could be utilized to help prose recall, and therefore experts could learn to store relevant information that could be accessed easily using retrieval cues in the working memory resources (Eysenck & Keane, 2010).

Several studies have examined LTWM: one study by Chase & Ericsson (1982) tested a participant's impressive digit span and found that he was using mnemonic techniques that he had developed through his job as a runner. Another study, by Ericsson & Polson (1988) found that a waiter was employing a specific structure to remember customers' orders. These findings do not mean that experts have a better working memory capacity, they just more proficient at combining LTM and working memory resources (Eysenck & Keane, 2010).

1.2.3 Retrieval from the long-term memory

Many efforts have been made to describe the LTM retrieval process. Just because one fails to retrieve a memory, it doesn't mean that it has been forgotten or not encoded properly (Ling & Catling, 2012). Retrieval starts with the spread of activation of associated traces stored in the memory by means of least one cue. This process can fail for many reasons: the cues are not suitably related to the target, or they are weakly related to the target, when there is not enough cues, when they are not properly learned, when we do not give enough attention to retrieving the memory, or it can be down to just our frame of mind or emotional state. Retrieval can also be affected unintentionally by context (context cues) (McLeod, et al., 1998): it can be more successful if the context is the same of that when encoding the memory, e.g. mood (mood-state-dependent recall), environment. Retrieval failures can be caused by many factors, however on many occasions we assume that we have simply forgotten the information rather than it being a retrieval failure (Anderson, 2009a).

1.2.4 Forgetting

Forgetting is a loss of information already stored in the long-term memory. It has been extensively investigated for over a hundred years, dating back to Ebbinghaus (Eysenck & Keane, 2010). There are two type of forgetting: incidental and motivated. Incidental forgetting is referred to as unintentionally forgetting, and motivated forgetting not only refers to intentional forgetting, but also forgetting caused by motivation while not being conscious of the intention (Anderson, 2009b). However I am only going to discuss incidental forgetting here as motivated forgetting is not relevant to the password security context.

There are two main theories of forgetting; trace decay and interference lead to incidental forgetting (unintentional forgetting). Trace decay theory describes the gradual weakness or loss of memories over a period of time, due to the passage of time (Ling & Catling, 2012). Whereas interference theory defines the phenomenon as retrieving a memory that is disrupted or interfered with, by similar memory traces (Anderson, 2009b; Criss, et al., 2011). There are two main forms of interference that interact and impede the retrieval of memories, retroactive interference and proactive interference (Groome, 1999; Wiedenbeck, et al., 2005). Retroactive interference is when information recently learnt or recent memories hinder the retrieval of older similar memories (Anderson, 2009b). Proactive interference is when previously learnt information or older memories interfere with the retrieval of similar more recently learnt information or memories (Anderson, 2009b).

Uniqueness has an effect on recall and forgetting concerning the interference effect. With information being more unique, it increases the level of distinct memory traces (Eysenck & Eysenck, 1980); and therefore distinctiveness counteracts the effects of interference (Schmidt, 1991). Distinctiveness of a memory item is dependent on the relationship between the encoding of the item, and the amount of overlap of encoding. Eysenck suggested that distinctive memory items are better remembered because through being distinctive, they would be more thoroughly processed than non-distinctive memory items (Eysenck, 1979). Numerous studies have found that interference is mostly dependent on the similarity of the information being retrieved, regardless if it is retroactive or proactive interference. Therefore, if information is not similar to other information learnt, forgetting should not occur (Baddeley, 2009).

1.2.5 Motivation to learn and to recall

Motivation can influence a person's performance to succeed at a task. However, this is dependent on the interpretation of what success is in terms of the task, to how well it is performed. From the proposition of self-determination theory (Ryan & Deci, 2000), motivation can be divided into two different types: intrinsic motivation (internal) and extrinsic motivation (external). Intrinsic motivation is the internal drive to pursue new experiences, to gain knowledge, and learn new things to further one's own cognitive and social development. It is a result of an interest or enjoyment in the task, existing internally, not due to external pressures; e.g. learning a computer package to gain better skills. Extrinsic motivation is the bases on the pursuit of an activity due to external goals, for example rewards such as money, or sanctions when misbehaving (Ryan & Deci, 2000).

The motivation and intention to learn is important for the focus of attention, however, they are not essential factors in learning (Nilsson, 1987). Motivation has an indirect effect on learning as it establishes how much time and level of attention is focused on the material, which results in learning. If there is a lack of interest in the information attention will be diverted, and therefore, learning is less likely to occur (Baddeley, 2009d).

As motivation affects the level of attention given to a task (Nilsson, 1987), it therefore affects memory retrieval. The more attention given to retrieving a piece of information, and the greater the mental effort focused on the task, the higher the chances of recalling said information (Anderson, 2009a).

1.2.6 Metamemory

Flavell in the 1970's proposed studied metamemory as the knowledge and awareness of cognitive processes (Flavell, 1971; 1979). Metamemory is a collection of multidimensional factors that represent our knowledge, beliefs and behaviors about our memory; that allows us to reflect on our memory's functioning and processes in general (Dixon & Hultsch, 1983a; Glass et al., 2005; Hertzog, 1992; Hertzog, Dixon & Hultsch, 1990 b; Pierce & Lange, 2000). Metamemory influences 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, or decide not to expend the energy and not learn it (Besken & Mulligan, 2013). The seven factors that measure metamemory 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, Hultsch & Hertzog, 1988). Previous research has investigated the important role that metamemory has in learning and recalling information, and memory performance (Hertzog, 1992; Schwartz, Benjamin & Bjork, 1997).

1.2.7 Memory: summary

Examining the human memory is an important issue, as it reveals so much about our cognition and behavior (Eysenck & Keane, 2010). The human memory is incredibly complex, with so many factors affecting its processes, from several storage systems with different functionalities, to the processing of information, in terms of encoding, storing and retrieving (Baddeley, 2009a). This is even before we consider humans' perceptions of their own memory's functionality, and how that affects the memory process. However, through exploring the human memory and understanding how it functions we can clarify what it is capable of, and what it is not capable of. This is imperative when examining the learning and recalling multiple passwords, forgetting passwords, and the insecure password behaviors that are adopted by users. Especially as users often use their memory's (perceived) limitations to justify their insecure password behaviors (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011).

1.3 Password security context and the password problem

What makes a secure password is different from policy to policy. Although most policies impose three requirements: length, complexity, expiration period (Marquardson, 2012). The big password problem can be divided into a contextual issue and a user issue. There are a number of contextual issues that affect the demands placed on the user, e.g.: time (to remember the password or meet the policy requirements) (Marquardson, 2012), money (the cost of resetting a password, or losses through security breaches) (Brown et al., 2004; Ives et al., 2004), fear (of the consequence of forgetting) (Inglesant & Sasse, 2010; Tam et al., 2010), personal goals (work and leisure take preference over security goals)

Grawemeyer & Johnson, 2011). These are just some of the demands placed on the user; however, the user has his or her own issues to contend with. The user has to create, encode, and recall distinctly different passwords for many accounts, which can be extremely demanding (Grawemeyer & Johnson, 2011). Therefore, more often than not, insecure password behaviors are adopted, such as choosing weak passwords; writing passwords down (or making a record of them); password sharing; not changing passwords regularly; and reusing their passwords as a coping strategy for cognitive offloading (Grawemeyer & Johnson, 2011; Zhang et al., 2009).

1.3.1 Insecure password behavior: as IS security behavior

Previous IS research has examined the password problem from two different research streams. The first stream approaches insecure password behavior as any other IS security behavior, and applies theories such as deterrence theory, and Protection Motivation Theory (PMT) (Guo & Yuan, 2012; Jenkins et al., 2014; Johnston et al., 2015; Vance et al., 2013; Workman, et al., 2008; Zhang & McDowell, 2009) to passwords as any other insecure behavior. The second research stream theorizes that insecure passwords behaviors stem from memory issues, and accordingly, focus on the memory aspect of the problem. We initially discuss the first research stream, and demonstrate how they overlook the memory aspect of the password problem.

Within IS literature, researchers have turned to behavioral models to understand, predict and change insecure information security behaviors within different IS contexts. The most frequently used theories that explain password behaviors as other insecure behaviors, include Protection Motivation Theory (PMT) and fear appeals (Jenkins et al., 2014; Johnston et al., 2015; Vance et al., 2013; Willison & Warkentin, 2013; Workman, et al., 2008; Zhang & McDowell, 2009), and the deterrence theory (Guo & Yuan, 2012). PMT is a theory from health psychology that describes the protective behavior adopted in response to fear of a health threat, e.g. giving up smoking in response to a fear of cancer (Rogers, 1975). Deterrence theory emphasizes the role of threat of receiving sanctions and the compliant behavior that is in response to the threat (Siponen & Vance, 2010). Within the password context Workman et al. (2008) employed PMT to understand policy non-compliance, in terms of regularly changing passwords. They found that if the benefits of complying with a policy outweighed the costs, then security recommendations would be disregarded. Another study examined PMT in terms of users' password protection intentions conducted by Zhang and McDowell (2009). They found that certain factors measuring protection motivation such as fear, response costs, and response efficacy significantly affected password protection intentions, and were good predictors in intention to adopt good password behavior. They also found that when users believed that actions taken to protect passwords were effective, then there would be higher motivation to adopt secure password behavior. However, if the users believed that their passwords were vulnerable regardless of their actions, they had less motivation to learn and use strong passwords.

A study by Vance et al. (2013) found that fear appeals had an effect on users' motivation to create strong passwords. Jenkins et al. (2014) also employed fear appeals to reduce insecure password behavior. They found that through using "just-in-time" fear appeals, they were able to reduce password reuse by 88%. Even though they were able to reduce password reuse by 88%, this was only attained through password reuse monitoring, which in a real-world setting is impossible, as there is no global system that monitors all passwords. Finally, the role of sanctions in terms of deterrence theory has been used to examine insecure password behavior. For instance, Guo and Yuan (2012) examined how different types of sanctions explained users intentions to write down passwords. They found that users wrote down passwords, just in case they found it difficult to remember them.

Overall, these studies provide a valuable understanding of how fear or deterrents can be used to improve users' insecure password behaviors, such as password sharing (Siponen & Vance, 2010; Vance et al., 2013), choosing a weak password (Johnston et al., 2015), writing passwords down (Guo & Yuan, 2012), or password reuse (Jenkins et al., 2014). However, if users believe that they cannot cope with remembering multiple passwords, then PMT, fear appeals or deterrence theory may not be effective solutions to avoid insecure password behaviors, as they do not incorporate the human memory as a factor. Next, we discuss the research that approaches the password problem, multiple passwords, insecure behavior (including password reuse), and user convenience; from the memory perspective.

1.3.2 Insecure password behavior: a password memorability problem

Adams & Sasse (1999) suggested that users can only successfully remember five unique passwords. The problem is, is that since 1999, the world has technologically changed (Lin, et al., 2013). Nowadays, users are generally required to remember over 10 distinctively different passwords (Zhang, et al., 2009). Passwords are only effective if you can remember them (Duggan et al., (2012), and with the cost of forgetting them being high, this drives users to adopt insecure password behavior (Duggan et al., 2012; Zhang, et al., 2009).

There has been a range of studies examining memory and its effect on different aspects of the password problem: password reuse (Adams & Sasse 1999; Sasse et al., 2001; Vu et al., 2007; Zhang et al., 2009), and the contributing factors (Bang et al., 2012; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009); the perceived importance of information (Bubas et al., 2008; Grawemeyer & Johnson, 2011; Vu et al., 2007); and how policies can affect users' password choices (Campbell et al., 2011; Marquardson, 2012).

Multiple passwords are a significant issue for users to remember (Bang, et al. 2012; Campbell, et. al., (2011). This situation is not helped by the fact that organizations and service providers give guidance on managing just one password, not on managing multiple passwords (Grawemeyer & Johnson, 2011). However, several studies have found that users rely just on their memory for password management, even when electronic devices and software are available (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). They found that users preferred to rely mostly on their memory, and their memory alone, than to use password management tools as they were potentially vulnerable to attacks.

As a result of increasing numbers of passwords, previous research suggests that there is a trade-off between password security and password memorability (Vu et al., 2007; Zhang et al., 2009). Strong passwords versus weak passwords; and meaningful passwords are preferred over random passwords (Marquardson, 2012; Nelson & Vu, 2010; Sasse et al., 2001; Wiedenbeck et al., 2005). However, just because a password is random, and therefore strong, it does not mean that it isn't meaningful to the user (Sasse et al., 2001). Craik & Lockhart (1972) suggested that meaningful information is better remembered. Therefore, in a study by Nelson & Vu (2010), they suggested that by adding meaning to passwords through mnemonic techniques, would be easier for users to remember them. Through creating mnemonic passwords, this technique makes passwords more secure, and with more meaning to the users, it increases memorability (Grawemeyer & Johnson, 2011; Nelson & Vu, 2010).

However, there is still so much pressure put upon a user to remember their passwords, which creates a fear as a result from the consequences of forgetting passwords being high, in terms of cost for instance (Brown et al., 2004; Ives et al., 2004). Organizations can spend thousands each year on resetting passwords, and through the losses due to security breaches (Brostoff & Sasse, 2000; Hayashi et al., 2012, Ives et al., 2004; Saastamoinen, 2014), when insecure password behaviors are adopted (Adams & Sasse, 1999; Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011).

Users are solely responsible for their passwords for the personal and organizations' accounts (Grawemeyer & Johnson, 2011). Website restrictions and password policies require: complexity, length and an expiration period (Marquardson, 2012). Forcing users to obey these requirements influences password selection in terms of strength, but it also influences users to modify and reuse their password; even if policies advise users to choose unique passwords (Adams & Sasse, 1999; Gaw & Felten, 2006; Stanton, et al., 2005). Password policy may influence users to select weaker passwords due to constraints, and therefore it's easier to choose the bare minimum, and do not change them regularly if simpler, weak passwords are used (Marquardson, 2012). Selecting weaker passwords is thought to reduce the cognitive burden and can be better for recall (Nelson & Vu, 2010; Wiedenbeck, et al., 2005). However, when password system requirements prevent the selection of weaker passwords, then reuse can be adopted to compensate (Gaw & Felten, 2006).

Consequently, the implementation of password policies are not always successful due to the lack of understanding regarding the users' tasks, the mental effort involved in complying with the constraints of the policy (Guo, 2013; Marquardson, 2012), and the cognitive processes involved with generating, encoding and recalling multiple passwords. Some websites do not enforce strict password requirements, as they do not want to drive their users away through the inconvenience of spending time on password creation and recall (Gaw & Felten, 2006).

1.3.3 Insecure password behavior: a user convenience problem

More recent studies are recognizing that user convenience is also an important issue that can result in insecure password behavior (Jenkins et al., 2014; Tam et al., 2010). The user inconvenience experienced while using authentication mechanisms is due to the process being time-consuming, when creating passwords (including changing passwords), and recalling passwords (Jenkins et al., 2014; Renaud & De Angeli, 2004). Therefore, there is a trade-off between password security and convenience (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009). User convenience is very new as a concept in this area of research and therefore, is still in the process of being defined. However, so far several studies that discuss it and suggest that user inconvenience can be caused when trying to meet the requirements of a password policy while creating passwords (Inglesant & Sasse, 2010), when passwords are forgotten, when there are problems recalling passwords, and when passwords need to be changed (Bang et al., 2012; Furnell, 2013; (Gaw & Felten, 2006; Zhang & McDowell, 2009). The time and mental effort needed in the password process results in the user adapting their behavior, and adopting insecure password behaviors to avoid inconvenience (Duggan et al., 2012; Notoatmodjo & Thomborson, 2009; Tam et al., 2010; Weir et al., 2009).

1.3.4 Password security context: summary

Password security is an important but complicated issue for IS researchers (Crossler et al., 2013; Garrison, 2006; Bonneau & Preibusch, 2010; Grawemeyer & Johnson, 2011; Siponen & Vance, 2010). This is due to the human factor; that users are solely responsible for their passwords and the security of their and their organizations' information. There are several demands placed on the user to encourage them to adopt secure password behaviors. However, these demands do not often take into consideration the psychology of a user (Grawemeyer & Johnson, 2011). Previous IS research has examined password issues pertaining to 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), and memory limitations (Adams & Sasse, 1999; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Nelson & Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007). They have found that there is a trade-off between password security, password memorability, and user convenience (Bang et al., 2012; Tam et al., 2010; Vu et al., 2007; Weir et al., 2009; Zhang et al., 2009). However, through the collection of subjective data of users' perceptions towards their password management and behavior (Bang et al.; 2012; Duggan et al., 2012; Grawemeyer & Johnson, 2011; Notoatmodjo & Thomborson, 2009), and the fact that the human memory is so complicated with many factors that influence the password process; password research has not found a practical solution for the password problem.

1.4 Overview of research gap

There are numerous studies that examine password security, looking into several factors that influence it; memory being the most significant (Adams & Sasse 1999; Bang et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Nelson & Vu, 2010; Notoatmodjo & Thomborson, 2009; Sasse et al., 2001; Wiedenbeck et al., 2005; Vu et al., 2007; Zhang et al., 2009). However, due to the human memory being so complex; IS researchers have just scratched the surface of this area of focus. This dissertation examines cognition to understand password security behaviors; and moreover, develops new theories and revises prominent cognitive scientific theories for the IS context. Previous research has found that users are aware of their memory limitations in remembering their passwords (Adams & Sasse, 1999; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Nelson & Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007), questioning whether their memories are "good enough" to remember multiple passwords. This led me to question, if long-term memory has an unlimited capacity (Baddeley, 2009), how is it that users cannot remember multiple passwords; and through a lack of understanding of how their memory works, can this influence their passwords recall, and password behavior? The first study looked to answer these questions, through examining metamemory (the beliefs and understanding about one's own memory) (Dixon & Hultsch, 1983a), memory performance, password recall and insecure password behavior. One of the metamemory constructs that effects memory performance is strategy. Strategy refers to what memory strategies a person can understand and use to aid learning and memory retrieval. For example, external aids such as writing and using a shopping list is a memory strategy (Dixon, Hultsch & Hertzog, 1988). However, several common memory strategies or external aids are considered, in the password context to be insecure password behaviors, such as writing passwords down, and sharing passwords (Grawemeyer & Johnson, 2011; Zhang et al., 2009). Therefore, internal mnemonics are considered a good strategy for increasing password memorability and security (Nelson & Vu, 2010). However, it takes practice, with extra time and mental effort to create mnemonic passwords, and therefore, it could increase inconvenience. Hence, users are aware of issues with password memorability, yet being advised not to use simple memory strategies to help them due to security issues. So, what can be done to help this situation? There needs to be a solution to help the user: we need to increase password memorability while not decreasing security, and not affecting the convenience of the password process; and if we can, preferably not impacting the service provider also. This is where I look to repetition in learning through verification, and memory interference in password behavior. In the first study I had designed the experiment to ask the participants to verify their password three times to increase memorability. A couple of the participants had commented on how they thought that this was helping their memory, however, I was concerned as I didn’t want to cause too much inconvenience. This led me to question whether such a small change in verification could have a significant impact on memorability, and whether this would significantly impact on the users’ convenience. The second study therefore looked to increasing password learning to effect password memorability. However, recall is also a factor in the password process, so the third study looked to interference as a mechanism to develop a theory to explain password retrieval problems. Through applying the phenomena of interference to password behaviors, could adopting unique passwords instead of reusing or modifying passwords, lead to better memorability and concurrently increase password security? Ultimately, all three studies contribute to the important direction that this dissertation takes is to examine the human memory in more depth, to give a better understanding of how memory affects password creation, recall, and behavior; while suggesting ways in which to improve multiple password memorability, and increase the security of the password authentication mechanism.

In these studies, an online password system was developed to allow participants to create and recall passwords over a number of weeks. A large amount of data was collected, to test the hypotheses and research questions. These studies are some of the first to examine password security and memory employing a longitudinal laboratory experiment design. The objective data measured password recall, memory recall, and password memory interference; and was complimented by subjective questionnaires to collect data on users’ perceptions of their memory in general, password memory, verification convenience, and attitudes and perceived behavior towards their password security. By collecting objective data, the results challenge users’ preconceptions about insecure password behaviors. Moreover, it challenges the trade-offs between password security, memorability and user convenience proposed by previous password research (Bang et al., 2012; Tam et al., 2010; Vu et al., 2007; Weir et al., 2009; Zhang et al., 2009). This dissertation has significant practical implications for organizations and individual users, as it proposes that a greater understanding of the human memory can inform users to adopt better password security practices. The results of this dissertation suggest how to increase password memorability, decrease, password forgetting, decrease insecure password behaviors and the consequences of a lack of password security (such as security breaches). These findings could ultimately lead to the password problem being solved.

1.5 Overview of chapters

1.5.1 Study 1. The password metamemory framework: a new perspective in examining password memorability and password reuse

In this study I propose the Password Metamemory Framework. This study questions whether users have problems remembering their passwords because they have too many, or because their memories cannot cope. Through examining long-term memory performance, and metamemory (one's beliefs about our memory), the results suggest that password recall is not related to memory capacity. However, password recall is related to the users' perceptions of their memory capabilities. With further analysis, I also discovered that password reuse was not related to password recall or memory capabilities, but it was related to perceived anxiety towards users' memory capabilities. It seems that the security of the password mechanism is being undermined by users' memory beliefs and password coping strategies (Adams & Sasse, 1999; Gaw & Felten, 2006; Ives et al., 2004; Zhang et al., 2009). Therefore, understanding what drives users to form their perceptions of their password capabilities is important, and a useful tool to explain their password recall and password reuse behavior.

1.5.2 Study 2. Password verification: increasing password memorability, while not inconveniencing the user

In this study I will examine the effects of repetition on password recall. When users create passwords they are asked to re-enter their passwords for verification. If they were asked to re-enter a second time, would this increase their password memorability? Participants were asked to re-enter their passwords two and three extra times to see if it affects their password recall significantly. As expected, the more times the password is entered, the better it is remembered. However, I also took into consideration that user convenience may be affected by the increase in verification. Users cannot be expected in the real-world to re-enter their passwords five, ten, or fifteen times when creating them due to inconvenience of the process. Therefore, the study examined the balance between memory, security and convenience, and found that while password memorability increased through repetition, user inconvenience was not significantly affected. Consequently, these findings provide strong evidence that to increase password memorability, there does not need to be substantial changes in practices or devices; small changes are effective enough.

1.5.3 Study 3. The Unique Password Theory: better password memorability, better password security practice

In this study I propose the Unique Password Theory. The results of my study support the theory, that unique password are more memorable than reused or modified passwords. This is an important discovery, as many users adopt password reuse practices because they believe they cannot remember all their passwords, and that reusing will help them remember (Adams & Sasse, 1999; Gaw & Felten, 2006; Ives et al., 2004; Zhang et al., 2009). This also has significant security implications as unique passwords are considered more secure than reused and modified passwords (Adams & Sasse, 1999; Duggan et al., 2012; Gaw & Felten, 2006; Ives et al., 2004; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). Therefore, unique passwords increase password memorability, while encouraging a higher level of secure password practice.

1.6 Research process and dissertation structure

Each of the following chapters represent a research study focusing on one element of memory. All three studies have been submitted for review, and the details of their status are summarized in Table 1.

TABLE 1: Summary of study publication status

Chapter	First author	Co-author	Status
2	Naomi Woods	Mikko Siponen	Under review with the *Journal of the Association of Information Systems*
3	Naomi Woods	-----	Under review with the *European Journal of Information Systems*
4	Naomi Woods	Mikko Siponen	Under review with *Information Systems Research*

This dissertation will present these studies in order of users' memory awareness (Study 1. metamemory), then will examine how to increase password memorability through improving learning (Study 2. repetition), and retrieval (Study 3. uniqueness-interference). Finally, this dissertation will discuss the overall key findings from all three studies, with contributions, limitations and suggested future research.

2 THE PASSWORD METAMEMORY FRAMEWORK: A NEW PERSPECTIVE IN EXAMINING PASSWORD MEMORABILITY AND PASSWORD REUSE

2.1 Abstract

Passwords are the most common authentication mechanism which will only increase 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 examined by IS researchers 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. Similarly, we argue that password reuse has no relationship with memory performance, or password recall. We suggest that password reuse can be explained by the users' perceived anxiety towards their ability to remember their passwords. We tested our contextualized metamemory theory and general memory theories in the password security context through a laboratory experiment, examining over 3500 passwords. The

results suggest that our contextualized metamemory theory, rather than the general metamemory theories explains password recall and reuse. This study has important implications for research on password security, and practice.

2.2 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 & Sasse, 1999; Campbell et al., 2006; Guo, 2013; Inglesant & Sasse, 2010; Zhang et al., 2009), to cope with their inability to remember multiple passwords (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). However, in numerous cases users choose to continue these insecure behaviors even though they are aware of the security risks (Gaw & Felten, 2006; Notoatmodjo & 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), (Brown et al., 2004, Hayashi et al., 2012, Inglesant & Sasse, 2010; 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 & Felten, 2006; Notoatmodjo & Thomborson, 2009). Therefore, the security and memorability of passwords have been an important concern in Information Systems (IS) research. Previous IS studies have so far examined the password problem 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 & 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 & Sasse, 1999; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Nelson & 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? Furthermore, how does this affect their perceived justification for password reuse? Answering these questions is essential for the future of password research and practice. If insecure password practices 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 IS research into insecure password security behaviors, multiple passwords, and password reuse. 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, and its implications to IS practice.

2.3 Password Reuse and the Current Status of Password Research

Since the late 1990's, when Adams & 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 (Zhang et al., 2009); however guidance and advice on managing them are normally aimed at just one password (Grawemeyer & 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 & Felten, 2006; Grawemeyer & 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 & 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 & Felten, 2006; Zhang et al., 2009). Without a solution, giving users an alternative or a way of coping with multiple passwords, insecure password behaviors such as password reuse (using the same password for more than one account) and password modification (using the same password with small changes for more than one account), will only rise as the number of accounts do so (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009).

Password reuse is a significant security issue, costing millions of dollars, wasted on cyber security as a direct consequence (Infosecurity Magazine, 2014). The consequences of reuse can affect home-users and organizations as for example, hackers obtain lists of password hashes from websites with low security, and are then able to gain access to more secure websites and accounts (Ives et al., 2004, Zhang et al., 2009). For the home-user, there is another issue with password reuse, as within some organizations high-level managers may be able to see their employees' passwords; and if these are reused from employees' personal accounts, then these personal accounts become vulnerable. This vulnerability, works the other way round also, when personal account passwords are cracked, then hackers are able to gain access to company systems if the passwords are reused (Infosecurity Magazine, 2014; Ives et al., 2004).

There are several studies that have examined password reuse as an insecure password behavior, which many users admit to adopting regularly (Grawemeyer & Johnson, 2011; Ives, et al., 2004). Furthermore, some studies have shown that users feel justified for adopting this insecure password practice, believing that they have no alternative (Gaw & Felten, 2006; Infosecurity Magazine, 2010). User believe that reuse makes it easier to remember their passwords (Adams & Sasse, 1999; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009), and reuse their passwords as a coping strategy for their perceived memory limitations (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011), regardless, even if they are aware or unaware of the security risks (Gaw & Felten, 2006).

However, there is one thing all of these studies have missed: it is that these insecure behaviors occur due to users' lack of understanding and knowledge of how their memory functions. We argue that insecure password behaviors (e.g., reuse) are adopted because of users' beliefs about the capabilities and limitations of their memory, be it accurate or inaccurate. We maintain that this is just a belief, and actually, the memory is capable of recalling many passwords. To make our case, we will next discuss the human memory, then will examine metamemory and how users' memory knowledge, beliefs and awareness can affect their memory performance; more specifically, their password recall performance; which forms the theoretical background of the paper. We contextualize these theories to the password context and present formal hypothesis.

2.4 Theoretical Background: memory theories

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 & Felten, 2006; Grawemeyer & 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. Users' perceptions of what their memories are capable of, results in the adoption of insecure password behaviors. Therefore, understanding fully how the memory functions is a necessity; but moreover, understanding how users' perceptions of their memories' capabilities affect their memory performance (how accurate their memory is), is pertinent to understanding how their perceptions of their memory for remembering passwords, affect their ability to correctly recall them.

2.4.1 Memory theory

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 & 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 & Johnson, 2011). However, the LTM is unlimited in its capacity (Baddeley, 2009a; Eysenck & 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, e.g., people speaking, personal goals, or work tasks (Adams & Sasse, 1999; Jenkins et al., 2014; Zhang & McDowell, 2009). Also, the level of mental effort to learn the password also effects how well it is stored and eventually retrieved from the LTM (Nelson & Vu, 2010).

Furthermore, in terms of retrieving passwords, forgetting is another factor that affects the password process: there are two main types of forgetting, trace decay and interference. Trace decay is the gradual weakness of loss a stored memory over a period of time, due to the passage of time (Ling & Catling, 2012); this effect can be counteracted through frequent use of a password (Sasse, et al., 2001). Whereas interference is the effect of when attempting to retrieve a memory, a similar memory impedes or disrupts the retrieval (Anderson, 2009; Baddeley, 2009b; Criss et al., 2011). This is a common issue in password retrieval especially when passwords have been reused or modified, as the user becomes confused between similar passwords and/or accounts, and recalls the incorrect password (Grawemeyer & Johnson, 2011; Nelson & Vu, 2010; Wiedenbeck et al., 2005).

One final 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, Hultsch & Hertzog, 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.

2.4.2 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 & 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, Dixon & Hultsch, 1990b; Hertzog et al., 1987); i.e. the ability to reflect on one's own memory functioning and memory processes in general (Dixon & Hultsch, 1983a; Glass et al., 2005; Hertzog, Dixon & Hultsch, 1990b; Pierce & 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 & 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 & Bjork, 1997).

2.4.3 Measuring metamemory

The Metamemory in Adulthood (MIA) questionnaire (Dixon, Hultsch & Hertzog, 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 & Hultsch, 1983a; Dixon, Hultsch & Hertzog, 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, Hultsch & Hertzog, 1988). These constructs have been extensively studied and used for measuring metamemory in different context for over 20 years (Bacon, Huet & Danion, 2011; Glass et al., 2005).

2.4.4 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, Feldman & Hertzog, 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, Dixon & Hultsch, 1990a), 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 & Hertzog, 1988). Negative beliefs about one's own memory capabilities and poor memory functioning is highly related to memory performance (Bacon, Huet & Danion, 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 (Dixon & Hultsch, 1983a; Hertzog, Dixon & Hultsch 1990b). 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.

2.4.5 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 & 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 & 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, Huet & Danion, 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 & Svendsen, 2011). Nonetheless, having an increased understanding of how one's memory functions positively effects memory performance (Dixon & 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 & 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 & Felten, 2006; Grawemeyer & 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 has 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 & 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 & 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 & 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 & 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.

2.4.6 Password metamemory, password recall and password reuse

Previous research has reported that password reuse behavior is adopted as a result of users being unable to remember their passwords correctly (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). However, if there is no relationship between memory performance and password correct recall, could there be no relationship between password reuse too? Users adopt password reuse as a coping strategy due to their perceived memory limitations, we therefore hypothesize:

> H4a: There will be no significant correlation between memory performance and password reuse.

> H4b: There will be no significant correlation between password correct recall and password reuse.

Password reuse is considered as coping strategy for memory limitations (Adams & Sasse, 1999; Duggan et al., 2012). This behavior is adopted based on users' perceptions of their memory capabilities or more specifically, their password recall capabilities. Therefore, we propose that password metamemory could play a part in the adoption of this insecure password behavior. Therefore, all password metamemory constructs are entered into the model, and we hypothesize the following:

> H5a: Strategy (password metamemory) will have a significant positive effect on password reuse.

H5b: Task (password metamemory) will have a significant negative effect on password reuse.

H5c: Capacity (password metamemory) will have a significant negative effect on password reuse.

H5d: Change (password metamemory) will have a significant negative effect on password reuse.

H5e: Anxiety (password metamemory) will have a significant positive effect on password reuse.

H5f: Achievement (password metamemory) will have a significant positive effect on password reuse.

H5g: Locus (password metamemory) will have a significant negative effect on password reuse.

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. Moreover, we will examine these perceptions in terms of password reuse behavior, and as well as comparing the differences between the general memory context to the password security context. 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 3, the password metamemory framework, it represents the relationships between memory performance, password correct recall, password reuse and metamemory.

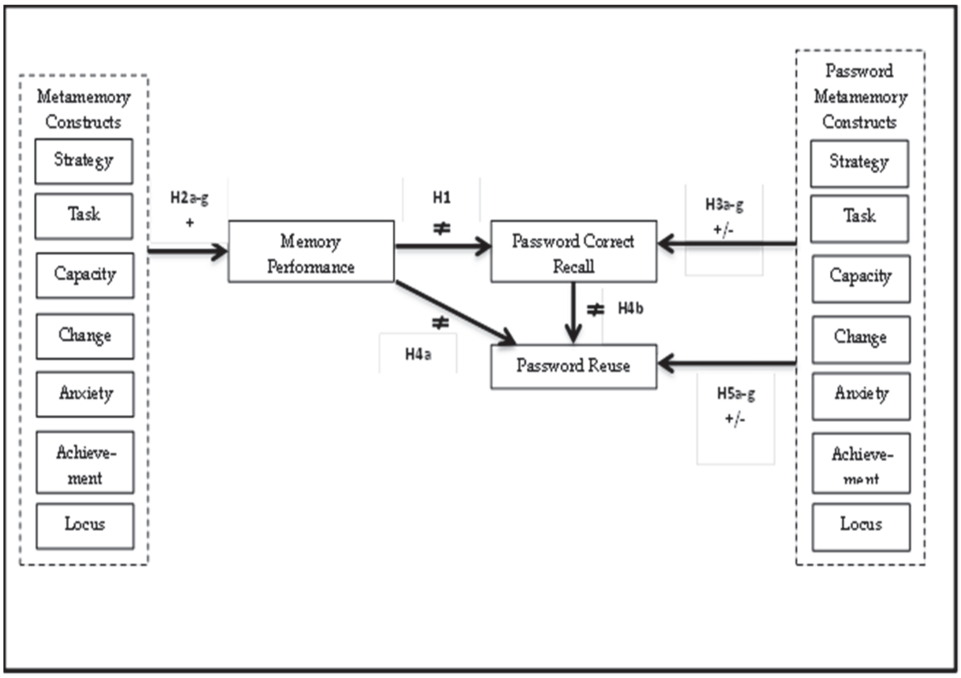


FIGURE 3: Research model for representing the proposed relationships between metamemory, memory performance, password recall, password metamemory, and password reuse

2.5 Research Methods

In this study, a laboratory experimental design was employed to collect data. Laboratory experiments are a common method of data collection used in IS research, due to the precision it offers in measuring independent variables (Liu & Myers, 2011), imperative to analyzing memory recall, and password recall. Through employing this type of design, it did not mean that realism was not incorporated into the study. Several features of the study matched the everyday password management experience, e.g., how many passwords were created at one time. Furthermore, examining password recall in a realistic setting would be a security issue, with limitations to what details could be studied. Therefore, several password studies of this type usually employ a laboratory experiment design (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009).

A two-part study was conducted, 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, metamemory, and password reuse.

2.5.1 Participants

Participants were selected from staff and students (with work experience) from a university in Finland (*N*=48). All computer users who engage in the use of passwords in ISs were considered suitable participants, as the human memory is not related to factors such as gender, culture or student versus worker. The participants all had work experience, and were all experienced computer users. Age is considered to be a factor that has an effect on memory and metamemory (Baddeley 2009c; Dixon & Hultsch, 1983a; Glass et al., 2005; Hertzog, Dixon & Hultsch, 1990b). 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 & Hultsch, 1983a; Glass et al., 2005; Hertzog, Dixon & Hultsch, 1990b). 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, Brigham & Pressley, 1990; Dixon & Hultsch, 1983a; 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 2.

TABLE 2: Demographic Information

Age	Gender	Education level
18 to 24 years	Male	Bachelor's degree
(count of 15; 32.3%)	(count of 31; 64.6%)	(count of 18; 37.5%)
25 to 34 years	Female	Master's degree
(count of 33; 32.3%)	(count of 17; 35.4%)	(count of 22; 45.8%)
35 to 44 years		Doctoral degree
(count of 9; 18.8%)		(count of 8; 16.7%)
45 to 54 years		
(count of 9; 18.8%)		

2.5.2 Measures

For the first part of the study, password recall and password metamemory was examined by a website designed for creating and recalling passwords, and a password-version of the MIA questionnaire.

2.5.2.1 Password recall

A website with password generation and input capabilities was designed to collect password data. Over 12 weeks, participants created and recalled passwords, and the website monitored correct input, and input errors. 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, can affect 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.

2.5.2.2 Password metamemory and password reuse

Password metamemory was measured by means of an adapted version of the Metamemory In Adulthood (MIA) questionnaire (Dixon, Hultsch & Hertzog, 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 Appendix 1 and Table 3). 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). Password reuse was an additional construct that was measured through items from the Password MIA, and additional password related questions; this construct too, showed good internal consistency (0.77). 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 3: 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	It doesn’t bother me when my memory fails.
Achievement (password)	(+ = high achievement)	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.
Password reuse	Perceived rates of password reuse (+ = high rates of reuse)	Do you reuse passwords (use exactly the same password) for more than one account?

The second part of the study examined participants’ memory performance and metamemory, using memory performance tasks and the MIA questionnaire.

2.5.2.3 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 is 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 & Desrichard, 2011; Dixon & Hultsch, 1983a; Glass et al., 2005; Hertzog, Dixon & Hultsch, 1990b; Lineweaver & 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 4 and Appendix 2. 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, 2009b; 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 4 and Appendix 2.

For analysis, the total memory score for each participant was calculated, which included the immediate recall and the long-term recall, as an overall score for the participants' general memory recall performance. However, all three memory performance scores (digit span, immediate recall, and long-term recall) were analyzed separately, in connection to metamemory, password recall and password reuse to gain a more in-depth understanding of any potential relationships.

TABLE 4: 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	

2.5.2.4 Metamemory

Metamemory was measured by means of the extensively used Metamemory In Adulthood (MIA) questionnaire (Bacon, Huet & Danion, 2011), developed by Dixon, Hultsch and Hertzog (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 & Hultsch, 1983; Dixon, Hultsch & Hertzog, 1988; Hertzog et al., 1987). The seven scales include Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus (reported in Table 3). The MIA is well known for its psychometric properties, and several studies have reported that it is factorial valid and internally consistent (Dixon & Hultsch, 1983; Dixon, Hultsch & Hertzog, 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.

2.5.3 Procedure

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.

2.5.3.1 Password recall

During the 12 weeks, two passwords were created in weeks 1, 2, 4, 6, 8 (totaling 10 passwords). Three passwords on average, (week 1 recalled 2 passwords, and in week 12, 10 passwords were recalled) were recalled every week. 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.

2.5.3.2 Password metamemory

The participants were asked to complete the Password MIA questionnaire (see Appendix 1) after their password recall, and before they took part in the memory performance test. The questionnaire was sent out electronically, and was completed via their computer or in hard copy.

2.5.3.3 Memory performance test and metamemory

The participants were presented with a PowerPoint presentation with instructions about what they could expect from the test (see Appendix 2). 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 4). 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 4). As the sequence of numbers increased, so did the amount of time the participants had to learn and recall the sequences.

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.

2.6 Results

There was a large amount of quantitative (objective and subjective) 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 to see if there was any effect. 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.

2.6.1 Model Testing

To test the Password Metamemory Framework, a correlation design was used to analyze the relationships between memory performance, password correct recall, and password reuse. To examine the predictive qualities of the metamemory constructs on memory performance; the password metamemory constructs on password correct recall; and the password metamemory constructs on password reuse, multiple regression tests were employed. The results of the statistical analyses are presented in Table 5 and Table 6; and the results of the hypotheses testing are shown in Table 7. All results are represented in Figure 4.

TABLE 5: Correlation analysis results

Factor correlation		Pearson's r	*p*
Memory performance	Password correct recall	-0.109	0.231
Memory performance	Password reuse	-0.193	0.208
Password correct recall	Password reuse	0.205	0.266

TABLE 6: 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
Password reuse	Adj R^2=0.082; *F*=5.18, *p*=0.028	Adj R^2=0.178; *F*=2.46, *p*=0.034		
	Anxiety	Anxiety	0.318/ 0.313	0.028/ 0.048
		Capacity	-0.663	0.033

TABLE 7: Results of hypotheses testing

Hypotheses		
1:	There will be no significant correlation between memory performance and password correct recall.	Supported
2a:	Strategy (metamemory) will have a significant positive effect on memory performance.	Supported

2b:	Task (metamemory) will have a significant positive effect on memory performance.	Supported
2c:	Capacity (metamemory) will have a significant positive effect on memory performance.	Supported
2d:	Change (metamemory) will have a significant positive effect on memory performance.	
2e:	Anxiety (metamemory) will have a significant positive effect on memory performance.	
2f:	Achievement (metamemory) will have a significant positive effect on memory performance.	
2g:	Locus (metamemory) will have a significant positive effect on memory performance.	
3a:	Strategy (password metamemory) will have a significant positive effect on password correct recall.	
3b:	Task (password metamemory) will have a significant positive effect on password correct recall.	Supported
3c:	Capacity (password metamemory) will have a significant positive effect on password correct recall.	Supported
3d:	Change (password metamemory) will have a significant positive effect on password correct recall.	
3e:	Anxiety (password metamemory) will have a significant negative effect on password correct recall.	
3f:	Achievement (password metamemory) will have a significant positive effect on password correct recall.	Supported
3g:	Locus (password metamemory) will have a significant positive effect on password correct recall.	Supported
4a:	There will be no significant correlation between memory performance and password reuse.	Supported
4b:	There will be no significant correlation between password correct recall and password reuse.	Supported
5a:	Strategy (password metamemory) will have a significant positive effect on password reuse.	
5b:	Task (password metamemory) will have a significant negative effect on password reuse.	
5c:	Capacity (password metamemory) will have a significant negative effect on password reuse.	Supported
5d:	Change (password metamemory) will have a significant negative effect on password reuse.	
5e:	Anxiety (password metamemory) will have a significant positive effect on password reuse.	Supported
5f:	Achievement (password metamemory) will have a significant positive effect on password reuse.	
5g:	Locus (password metamemory) will have a significant negative effect on password reuse.	

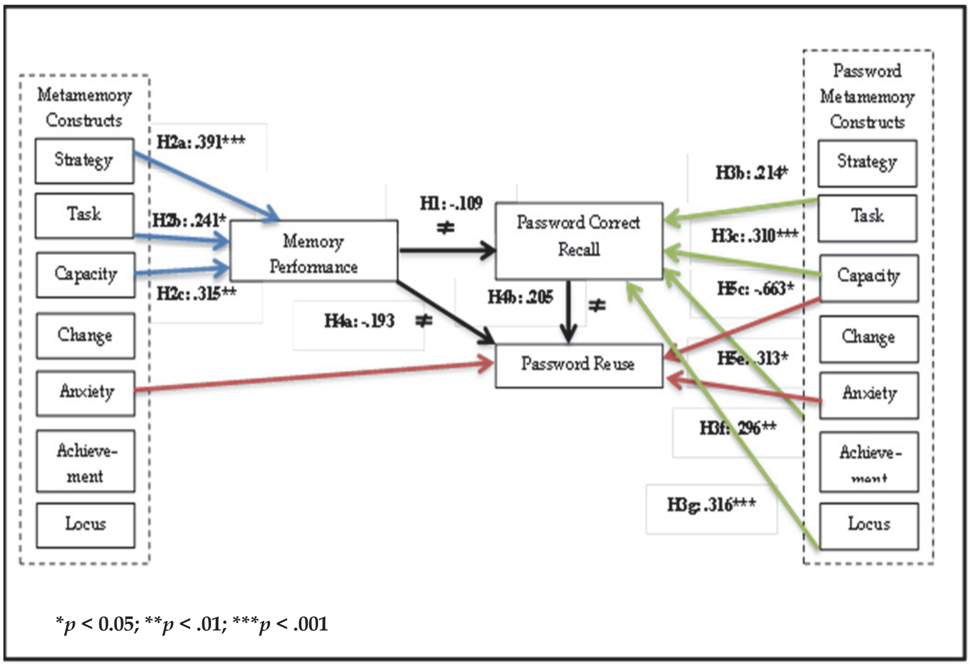


FIGURE 4: Summary of the results showing the relationships between metamemory, memory performance, password recall, password metamemory and password reuse.

2.6.1.1 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 (r = -0.109, *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.

2.6.1.2 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 & Hultsch, 1983a) 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 & Hultsch, 1983a), and therefore, H2a – c was supported.

2.6.1.3 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.

2.6.1.4 The relationship between memory performance and password reuse

To analyze the relationship between memory performance and password reuse, a correlation design was employed. As H4a was proposed as a null hypothesis, a post hoc power analysis was conducted using R STUDIO, and showed a good level of statistical power (0.80). The correlation analysis revealed that there was no relationship between memory performance and password reuse (r = -0.193, $p = 0.208$), supporting H4a. When examining the individual memory performance scores, there was no correlation between password reuse and digit span ($p = 0.374$), immediate recall ($p = 0.063$), and long-term recall ($p = 0.190$), further supporting H4a.

2.6.1.5 The relationship between password correct recall and password reuse

A correlation design was employed to examine the relationship between password correct recall and password reuse. H4b was proposed as a null hypothesis, and therefore, a post hoc power analysis was conducted using R STUDIO, and revealed a good level of statistical power (0.84). The correlation analysis showed that there was no significant correlation between password correct recall and password reuse (r = 0.205, $p = 0.266$), supporting H4b.

2.6.1.6 Password metamemory predicting password reuse

To examine the constructs of password metamemory to show any predictive value towards password reuse, a multiple regression test was performed. The scales from the Password MIA were examined in relation to password reuse, and were measured as predictor variables: Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus.

The analysis revealed that there were two significant predictor variables of password reuse: Anxiety was the best predictor ($p = 0.048$), followed by Capacity ($p = 0.033$). H5c and e were supported, whereas, H5a, b, d, f, and g were not supported.

With further analysis, the constructs of the (memory) metamemory were examined to investigate any relationship with password reuse. The results showed that there was one predictor variable of password reuse, and this was

Anxiety from the MIA questionnaire (p = 0.028), revealing that anxiety plays a key role in reusing passwords.

2.7 Discussion

2.7.1 New contributions

Users claim they cannot remember all their passwords, and feel justified for adopting insecure password behavior as a result of their memories limitations (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006). Hence, the focus of this study has been primarily to investigate whether poor password recall is related to poor memory capabilities. Therefore, the first contribution of this study was that there was no relationship found between correct password recall and memory performance. These results demonstrate 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 reduce password reuse behavior.

Based on the results 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, Dixon & Hultsch, 1990a), the second focus of this study was to investigate the involvement metamemory could have in password recall. The second new finding was that there were no constructs from the (memory) metamemory scale that could predict password correct recall (p = 0.062, overall). Therefore, (memory) metamemory was not related to password recall. This was an unexpected and important finding as the results from this study confirmed that the (memory) metamemory constructs of Strategy, Capacity and Task together, 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 showed there was no relationship between the (memory) metamemory constructs and password correct recall. This illustrates the need for password security context-specific instruments, especially when examining factors as complex as the human memory and metamemory, within the IS context.

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, which revealed the next new finding. This new finding showed that together, 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.

The next new contribution highlights 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 (memory) metamemory 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 & McDowell, 2009), when users' believe they have less control, are less motivated to learn and remember stronger passwords. 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. In (memory) metamemory, 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. 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 emphases the need for IS-specific measurements, and secondly, it illustrates to the need to focus on perceived control and motivation to remember passwords.

Users adopt insecure password behaviors such as password reuse as a result of being unable to remember all their passwords (Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). However, this study has found no relationship between password recall and memory performance. This has led us to question the involvement of memory capabilities in the justification of password reuse. This study's third focus was to investigate the relationship between password reuse, password recall, and memory performance; and whether metamemory, or more specifically password metamemory was involved. The next new contributions were that the results revealed there was no relationship between memory performance and password reuse, and there was no relationship between password correct recall and password reuse. These findings are against the current wisdom in the literature: users belief that they have to adopt insecure password reuse, because they cannot remember their passwords, or there are too many passwords for their memory to cope with (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006). The findings of this study show that memory performance, and password correct recall are not the reasons for incidences of password reuse (not directly, anyway); thus, there must be another cause. Therefore, further analysis of metamemory (memory and password) and password reuse, revealed some very interesting results: the constructs of password metamemory were initially examined in reference to password reuse; we then looked to (memory) metamemory to see if there were any other effects. The fourth new finding from his study was that two of the password metamemory constructs had an impact on password reuse. Both Anxiety and Capacity significantly predicted password reuse. This means that users with higher levels of anxiety towards their memory for passwords, and perceived lower memory capacity for remembering passwords, are more likely to reuse their passwords. Furthermore, the analysis of the (memory) metamemory constructs with password reuse, revealed that the only construct related to password reuse was also Anxiety. These finding highlight the important role that metamemory plays, in not only password correct recall, but also password reuse.

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 that contribute to password correct recall and password behaviors, such as password reuse.

2.7.2 Implications for practice

Password memorability is reported as one of the key issues in IS practice (Siponen & Vance, 2010). Password memorability problems lead to passwords being forgotten, which results in increased costs pertaining to password resetting, in terms of money, time and convenience (Brown et al., 2004; Tari et al., 2006). Second, password memorability problems, and a fear of forgetting passwords result in insecure password practices such as password reuse, which increases the risk of accounts being hacked (Ives et al., 2004). Previous research suggests that users cannot cope with multiple passwords because of memory limitations (Chiasson et al., 2009; Duggan et al., 2012; Gaw & Felten, 2006). However, the results of this study suggest that correct password recall is not related to good or bad memory capabilities, nor does password reuse, but it is related to the perceptions of these capabilities. If users were made aware of these findings, the implications for practice would impact on both organizations and the home-user.

The implications are similar for both organizations and home-users. Awareness that password memorability is not related to how good users memories are could result in increased policy compliance, with regards to creating stronger passwords, and the reduced need to write passwords down (Biddle et al., 2012; Chiasson et al., 2009; Duggan et al., 2012; Gaw &Felten, 2006); as users have more motivation to learn and recall their passwords, and through passwords becoming more memorable. Second, through passwords being more memorable, there would be fewer instances of passwords being forgotten and the consequences of password resetting, in terms of money, time and convenience. The third implication is that due to the increased memorability of passwords, and reduction of insecure password behaviors, information assets would be more secure, and organizations would be less vulnerable to security breaches; while home-users could also be more secure, and reduce the consequences of security breaches.

2.7.3 Limitations and future research

For this study a laboratory experimental design was chosen due to the precision needed to test the human memory and objective password recall. Laboratory experiments are considered to have their strengths and weaknesses (Dennis &Valacich, 2001); whereas they can be strong in terms of precision and control (Dennis & Valacich, 2001; Liu & Myers, 2011), they can be weak in terms of generalizability (to populations) and realism (for the participant), (McGrath, 1982). However, many scientists regard realism to be not as important as precision (Friedman, 1953), and therefore, laboratory experiments are a popular method of data collection in IS research (Liu & Myers, 2011). Furthermore, as creating and recalling passwords in a realistic setting would have issues pertaining to security, in terms of what could be monitored; previous password studies often employ a laboratory methodology (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009).

Another limitation was that password reuse was measured by means of participants reporting their perceived rates of reuse. The reasons for this were that if participants were allowed to reuse their passwords, this would have had an effect on password recall, due to type of passwords rather than memory performance.

Previous research suggests that users' password memorability problems are based on the users' memory capabilities to cope with multiple passwords (Chiasson et al., 2009; Duggan et al., 2012; Gaw & Felten, 2006). However, this critical assumption has not been examined empirically in terms of if users' memories are actually unable to cope or not. This issue is central to future password research because if insecure password practices result from poor memory, then future research should put premium on the development and use of memory techniques or password management systems to cope with the memory problem. If, on the other hand, the problem is not related to memory performance, but users' inaccurate perception of their memory limitations, then future research need to examine why this is the case and how such false perception can be improved. In this study we solved this riddle: password correct recall is not related to good or bad memory.

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 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, to eventually increase the memorability of passwords and reduce insecure password practices.

This study finally examined password reuse and its relationships to password recall, memory recall and password metamemory. These results revealed a surprising relationship with anxiety, as an important contributing factor to password reuse. Further investigation of anxiety is warranted as a predicting factor in password reuse, from both metamemory in general, and within the password context, to gain a better understanding of the users' beliefs, and ways in which to reduce password reuse behavior.

2.8 Conclusions

It is widely believed that users' adoption of insecure password behaviors, such as password reuse, is a result of users' memory capabilities, and their inability to cope with multiple passwords. In this study the Password Metamemory Framework was proposed which not only argues that this is a misconception, but offers a new perspective on examining password recall, users' inabilities to recall multiple passwords, and password reuse. 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. Furthermore, password reuse is not related to memory performance or password recall. When the users' claim they reuse their passwords because "they have too many passwords", or "their memory cannot cope", the results of this study suggests that it is not about their actual memory capabilities, but due to their perceptions towards their capacity to remember passwords, their anxiety towards remembering them, and their anxiety towards their memory in general. Therefore, users' with high levels of anxiety towards remembering their passwords, regardless of the memories actual capabilities, are more likely to reuse their passwords.

The Password Metamemory Framework and the results from this study have new important implications for IS password practice as through challenging users' perceptions of their memory capabilities towards remembering their passwords, it can first, undermine their justification for adopting insecure password practices, such as password reuse. Second, it can lead to increased password memorability. Third, it can therefore, reduce the consequences of forgetting passwords, in terms of money, time and convenience (e.g., employees being unable to log on to work systems, increased IT helpdesk costs, new passwords being sent without email encryption).

3 PASSWORD VERIFICATION: INCREASING PASSWORD MEMORABILITY, WHILE NOT INCONVENIENCING THE USER

3.1 Abstract

An increase in the number of passwords needed in users' lives is increasing insecure password behaviors (such as password reuse). Although, there are alternatives such as biometrics, due to costs and insufficient technology, passwords are preferred as the main form of security authentication. Therefore, there is a need for ways in which password memorability and security can be increased. This would help elevate the consequences of forgetting passwords and security breaches. In this study we turn to password verification – a part of the password process. In the majority of services and websites, users are required to verify their passwords once after creating them by re-entering them immediately. In this study, participants were allocated into three groups where they were asked verify their passwords once (control group); twice, and three times (two experimental groups). Through applying repetition in learning to the password process, the literature would suggest that this would have significant effects on password memorability. However, as previous IS research has discovered password behavior is not that straightforward. Previous research has found a trade-off between password security and memorability. More recently, studies are suggesting that user convenience is also an important factor. Therefore, simply increasing the number of password verification times would not necessarily reduce insecure password behavior, as user inconvenience could also be affected. We therefore, also examine user convenience, and the effects of increasing password verification times on convenience levels. The results suggest as to be expected, that password memorability increased with the number of verification times. However, the level of user inconvenience did not equally respond; in fact user inconvenience was similar across groups. What this means is that small changes to the password process, such as addition verification

times, can have significant results on password memorably while not significantly inconveniencing the user. The implications are that these results and practical suggestions could ultimately have a positive effect on password security.

3.2 Introduction

Passwords are the most prevalent method of authentication (Bang et al., 2012; Vu et al., 2007). Over the past few years, as the number of accounts users have accumulated has risen, so too has the number of passwords (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Despite the fact that users are more aware of security issues pertaining to password cracking; as a result of the struggle users have to remember multiple passwords, they often employ insecure password behaviors as coping strategies to aid password memorability (Biddle et al., 2012; Campbell et al., 2006; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). This is a result from that the consequences of forgetting passwords can be high, in terms of money for instance (Brown et al., 2004; Ives et al., 2004). Organizations spend thousands each year on, not only resetting passwords, but through the losses due to security breaches (Brostoff & Sasse, 2000; Hayashi et al., 2012, Ives et al., 2004; Saastamoinen, 2014), when insecure password behaviors are adopted (Adams & Sasse, 1999; Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). These insecure password behaviors include, password reuse, writing passwords down, sharing passwords, choosing weak passwords, and not changing passwords regularly (Adams & Sasse, 1999; Campbell et al., 2006; Guo, 2013; Zhang et al., 2009). Furthermore, with users forgetting passwords, and adopting insecure password behaviors, these actions are bringing into question the ultimate security of passwords and future of the mechanism (Grawemeyer & Johnson, 2011). There are alternatives to passwords, such as biometrics, and security tokens (Florêncio & Herley, 2007; Keith et al., 2009). However, these alternatives are not as popular as passwords, due to the cost of implementation, etc. Therefore, currently increasing the security and memorability of passwords is an important area of research in Information Systems (IS) (Bonneau & Preibusch, 2010; Grawemeyer & Johnson, 2011).

Previous IS research has approached investigating the issues pertaining to password security through examining the password problem being a memory problem (Adams & Sasse, 1999; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Nelson & Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007), and generalizing password security behavior as 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 found that there is a trade-off between password security and password memorability (Vu et al., 2007; Zhang et al., 2009); for example, users will choose easily cracked passwords as they may have meaning to the user, and therefore be more memorable (Nelson & Vu, 2010; Wiedenbeck et al., 2005). However, researchers are finding that convenience is also a factor that is influencing password security and memorability (Bang et al., 2012; Hoonakker et al., 2009; Jenkins et al., 2014; Tam et al., 2010; Thing & Ying, 2009). Inconvenience caused to the user within the password context, would refer to the inconvenience experienced when time and mental effort is spent on the password process (creating, learning, and recalling passwords) (Jenkins et al., 2014; Renaud & De Angeli, 2004; Zhang & 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 password policy requirements of the service. In previous research user convenience is a very new concept in this area of research and therefore, is still in the process of being defined. Nevertheless, they suggest that the inconvenience experienced by the user while engaging in the password process can lead to the adoption of insecure password behaviors, e.g. not changing their passwords regularly. Therefore, when considering ways in which to increase password memorability and/or security, one has to consider the convenience factor, as it can have an effect the users' memory and security behavior (Duggan et al., 2012; Notoatmodjo & Thomborson, 2009; Tam et al., 2010; Weir et al., 2009).

In this study, we turn to password verification – a part of the password creation stage – where the user is asked after creating their password, to re-enter it. Can we exploit a stage in the password process to increase the memorability of passwords? Through increasing the number of times in which a user is required to verify their password, could it have an effect on the memorability of that password? However, through increasing the number of times of password verification, this would increase the amount time given to the password process, which would surely increase user inconvenience. Therefore, we will examine the balance between memory and convenience, to see whether a small increase in the number of verification times has a significant effect on password memorability, and on user convenience.

We test our hypotheses using a laboratory 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 of verifying their passwords at the creation stage. Our findings suggest that through increasing the number of times a password is verified will have a positive effect on password memorability, while not having a considerable effect on the users' convenience levels.

The rest of the paper is organized as follows: Section 2 we discuss the previous research in examining password security, memorability and user convenience. In section 3 we examine memory theories and more specifically theories of learning and retention, and develop our hypotheses. In section 4 we describe the methodology used. Then present our findings in section 5. Finally, we discuss our findings and their implications in section 6 and 7.

3.3 Previous research

Password authentication is the most popular security (Keith et al., 2009; Zhang et al, 2009). This is due to alternatives, such as biometrics being costly and not widely accepted (Florêncio & Herley, 2007; Keith et al., 2009). Hence, password security is still an important issue that needs addressing, in terms of making passwords more secure, more memorable, and managing password security behavior that users adopt. One of the major issues with the mechanism is the number of passwords in which a user requires in their every-day life (Chiasson et al., 2009; Lin et al., 2013; Zhang et al., 2009). With an increase in internet usage, the number of accounts, and therefore passwords, has just exploded over the past few years (Sharma & 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 numbers of passwords to learn and remember (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). These insecure password behaviors can include password reuse, writing passwords down, sharing passwords, creating weak passwords, and not changing passwords regularly (Adams & Sasse, 1999; Campbell et al., 2006; Guo, 2013; Inglesant & Sasse, 2010; Zhang et al., 2009). Many users employ these behaviors as they see them as coping strategies to help them remember their passwords, regardless of the potential security risks to their accounts and their employers' accounts (Gaw & Felten, 2006; Notoatmodjo & 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 & Sasse, 2010; Tari et al., 2006; Vu et al., 2007).

3.3.1 Trade-off: password security vs. password memorability

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 & Vu, 2010; Sasse et al., 2001; Wiedenbeck et al., 2005). The security of passwords is compromised for more memorable passwords. However, just because a password is random, and therefore strong, it does not mean that it isn't meaningful to the user (Sasse et al., 2001). Nonetheless, users are more concerned with remembering their passwords than securing information (Grawemeyer & 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 & Johnson, 2011; Zhang et al., 2009).

3.3.2 Trade-off: password security, password memorability, user convenience

The authentication mechanism should be: secure, memorable, usable, and convenient, i.e. not too time-consuming (Renaud & De Angeli, 2004). Inconvenience experienced as a result of the authentication mechanism is due to the process being time-consuming, when creating passwords (including changing passwords), and recalling passwords (Jenkins et al., 2014; Renaud & De Angeli, 2004).

Studies are beginning to observe that convenience is also an important contributing factor in insecure password behavior (Jenkins et al., 2014; Tam et al., 2010); and that there is a trade-off between password security and convenience (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009). A study by Tam et al. (2010), reported users saying "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". 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 & Thomborson, 2009; Tam et al., 2010; Weir et al., 2009). Moreover, password policy requirements increase the effort users expend on the password process (Inglesant & Sasse, 2010). Therefore, the inconvenience experienced by the user can result in insecure password practices (Tam et al., 2010). Examples of these insecure behaviors are that users will frequently create passwords that are easy to remember, as they are considered more convenient, and therefore aids memory limitations (Campbell et al., 2011; Zhang & McDowell, 2009). Changing passwords is also considered inconvenient, and therefore, user will not change their passwords regularly (Bang et al., 2012; Furnell, 2013; (Gaw & Felten, 2006; Zhang & McDowell, 2009). Another insecure password behavior is password sharing; users will sometimes share passwords, not necessarily because they are incapable of remembering them, but because it is a convenient practice, 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 & McDowell, 2009). Therefore, more research is needed to examine the trade-off between convenience, memorability, and security (Hoonakker et al., 2009; Weir et al., 2009).

3.4 Theoretical background

IS researchers have studied memory theory to attempt to make passwords more memorable, and easier for our brains to process while learning and remembering (Nelson & Vu, 2010; Sasse, et al., 2001; Vu, et al., 2007; Zhang et al., 2009). In this section we will examine several memory theories to gain an understanding of some of the processes involved in learning and recalling, including repetition and rehearsal, and how they affect the password process.

3.4.1 Memory theories

Atkinson and Shiffrin (1968) proposed the stages of memory theory. This prominent theory suggests that the human memory is composed of three memory stores, the sensory memory, the short-term memory (STM), and the 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 it is being processed. The LTM stores information indefinitely after it has been processed, ready for retrieval. When referring this theory to the password process, the password would be observed and attended to by the sensory memory, it would be learned and rehearsed in the STM/working memory, and stored (long-term) in the LTM, ready for it to be retrieved.

When looking to memory theory to help with the issues of password memorability, researchers have examined the LTM for storage and retrieval, in terms of remembering and recalling multiple passwords (Adams & Sasse, 1999; Nelson & Vu, 2010; Wiedenbeck et al., 2005; Vu et al., 2007; Zhang et al. 2009). There have also been some studies that have examined the STM, with regards to learning passwords and factors that affect it, such as cognitive load (Jenkins et al., 2014; Marquardson, 2012), depth of processing (Nelson & 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 (WM/STM) model was proposed by Baddeley and Hitch (1974) which consists of several components that manipulate information before it is transferred to the LTM, or is just forgotten. This processing and manipulation of information is what is considered as learning. However, the STM has a limited capacity (Ling & Catling, 2012), this was first established 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, as through ordering information into "chunks", e.g., USA is one chunk of three larger items: "United States of America", this recoding of information allows more to be encoded and learnt (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 & 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, e.g. the word "apple", is processed visually, as the image, as the word, in terms of it being a fruit, in specific terms as, maybe a person's favorite fruit, etc. This information is processed more deeply, and hence would be retained better. Several studies have shown that the more levels of processing and deeper levels of meaning would show better retention (Baddeley, 2009; Craik & Lockhart, 1972; Craik & Tulving, 1975). In terms of passwords, Nelson & Vu (2010) suggested that through mnemonic techniques meaning could be added to a password while keeping it still secure.

Cognitive load theory is refers to the amount of "mental energy" or effort required to process information (Feinberg & 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 (heavy cognitive load), and therefore learning reduces (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 which add to the cognitive load, as this information is processed concurrently (Adams & Sasse, 1999; Jenkins et al., 2014; Notoatmodjo & Thomborson, 2009; Zhang & McDowell, 2009). The number of passwords being learnt at one time can also affect cognitive load; although this rarely happens in real life, as passwords are generally learned one at a time. The level of mental effort expended to learn the password also effects how well it is stored and eventually retrieved from the LTM (Nelson & Vu, 2010). Nelson and Vu (2010) found that users were not putting enough effort, with no in-depth consideration, into creating their passwords; and as a consequence, this would negatively affect their password recall.

Therefore, capacity refers to the limitation in the amount of information the STM/WM can process at one time; depth of processing involves increasing the amount of areas in the brain involved with information processing and memory consolidation; whereas, cognitive load refers to the mental energy required to coordinate these areas of the brain to process information and consolidate a memory. And so, having discussed these factors that affect learning, and learning passwords; we will now look to how information is transferred from the STM to the LTM in terms of repetition/rehearsal, and how repetition can be incorporated into the password process to encourage this transfer.

3.4.2 Repetition/rehearsal, learning and transferring information to the LTM

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). Repetition in learning is an important part of general memory theories. Atkinson & Shiffrin (1968) emphasized in their stages of memory theory, the role of repetition in improving memorability.

“The process of rehearsal is repeating information over and over” (Goldstein, 2011, pp.173). There is a relationship between rehearsal and storage in LTM (Jacoby & Bartz, 1972; Rundus & Atkinson, 1970). Through repetition or rehearsal, information is kept or maintained for longer in the STM and subsequently transferred to the LTM (Atkinson & Shiffrin, 1968; Jacoby & Bartz, 1972; Nelson 1977; Rundus & Atkinson, 1970).

However, over the years of psychological research, the understanding that rehearsal alone, as means of transferring information from the STM to the 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 insure that information is held in the STM; the transfer of information from the STM to the LTM may be considered as a different process (Jacoby & Bartz, 1972). Furthermore, Craik and Lockhart also (1972) with their depth of processing approach argued that repetition does not affect memorability if the depth of processing is constant. Only rehearsal which leads to increased depth of processing will have an effect on memory performance (Craik & Lockhart, 1972).

In response to the criticism of repetition and rehearsal, Nelson (1977) found that contrary to the findings of Craik & Lockhart, recall increased with the number of repetitions. Nelson (1977) examined distributed repetition and massed repetition; he found that repetitions even when massed have an effect on recall. Nelson concluded that same-depth repetition doesn’t facilitate memory recall was not supported, and that the number of “rote” repetitions is correlated to the memory recall.

Throughout the years, repetition and rehearsal was thought by many theorists as all that is needed to learn (Baddeley, 2009). A more contemporary view suggests learning can be increased through linking the 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 the STM for immediate use; for instance, until you make a call. Elaborative rehearsal is what is used to transfer information from the STM to the LTM as it incorporates thinking about the meaning of the information and relating it to what is already know (Goldstein, 2011). Furthermore, if recall of information is expected later after a delay, more retrieval cues will be formed while rehearsing (Jacoby & Bartz, 1972). What is more, Nilsson (1987) found that motivation and intention to learn is important for the focus of attention. More recent studies suggest that repetition without motivation from the learner to organize the information may not necessary result in learning (Baddeley, 2009).

3.4.3 Repetition as password verification

"We are often asked to produce a password under hurried circumstances … with no opportunity for rehearsal" (Brown, et al., 2004). Several studies in IS have noted that repetition and rehearsal have an effect on password memorability (Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al. 2009), and can also be beneficial when creating passwords (Helkala & Svendsen, 2011). Zhang et al. (2009) suggested that rehearsal is a successful method in learning passwords, as it keeps them in the STM longer, and therefore would have a higher chance of entering the LTM.

A study by Wiedenbeck et al. (2005) believed that passwords are only learned through rote, repetition learning, and this would affect password security. As a result of this being the only method of learning them, and that random passwords have a lack of meaningful content; weak passwords are created because rote learning is considered not always the best way to learn especially when the content doesn't have meaning. They proposed that due to the meaningful content in graphical passwords, that meaning would aid learning through repetition or rehearsal. Although meaning increases memorability, we disagree with the first suggestion that random passwords have no meaning; as passphases or mnemonic alphanumeric passwords are random meaningful passwords (Sasse, et al., 2001).

Another study by Vu, et al. (2007) found that when they added a verification stage (one extra time to re-enter) to their study design, as the passwords were being generated; participants felt that the login repetitions helped them remember their passwords. Furthermore, their results suggested that logging in several times after the password had been generated increased password memorability, incorporating a delay between creation and initial recall. Whereas they found that re-entering the password as verification at the generation stage had an effect, but not a significant effect on password memorability. This supports the results found by Nelson (1977) when he examined distributed and massed repetition. Distributed over time, repetition has a stronger effect on learning; however Nelson (1977) still found that massed repetition also had an effect on memorability. Nevertheless, 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. Hence massed repetition in terms of verification, at the stage of password creation would be more beneficial.

These studies have noted the importance of repetition in password learning; however this has not been the focus of their studies. Vu et al. (2007) added a re-entry stage when participants created their passwords into their study design, 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 would have an effect on the participants' cognitive load. Jacob and Bartz

(1972) although argued that repetition did not necessarily lead to improved memorization, they did acknowledge that when learning shorter lists of words, they would be held in the STM longer than longer lists of words, hence a higher probability of entering the LTM. Therefore, learning many passwords at once would affect password recall, and moreover, this situation would not occur in the "real-world", as multiple passwords are rarely created at the same time. Furthermore, Wiedenbeck et al. (2005) used repetition in learning passwords as an argument for the use of graphical passwords. However, they 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 (Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al. 2009). However, all these studies have not considered the practical application of using verification for learning through repetition, while incorporating the effect of repetition on convenience, and inconvenience on password memorability and security.

3.5 Current study

In this study we will examine the effects of repetition on password recall. When users create passwords they are asked to re-enter their passwords for verification (Vu et al., 2007). If they were asked to re-enter a second time would this increase their password memorability? We will ask participants to re-enter their passwords two and three extra times to see if it affects their password recall significantly. The literature suggests that the more times passwords are entered, the better they are remembered. However, we will also look to the issue of convenience too – users cannot be expected when creating passwords in the real-world to enter their passwords five, ten, or fifteen times when creating them. Therefore, we will examine the balance between memory and convenience, with the prospect of increasing password security. We therefore propose the following hypotheses:

> H1: Increasing the number of password verification times will have a positive effect on password recall.
>
> H2: Increasing the number of password verification times will have negative effect on user convenience.

3.6 Methodology

To test our hypotheses we employed a longitudinal laboratory experimental design, collecting objective data in terms of password recall, and subjective data in the form of questionnaire answers measuring user convenience. A laboratory design was preferred due to the precision that this type of design offers in measuring independent variables (Liu & Myers 2011).

3.6.1 Participants

Ninety participants were selected from staff and students (with work experience) from a Finnish university. All participants had work experience and were experienced computer users. Due to the effect of age on memory, all participants were matched on age (Baddeley 2009c). The 90 participants were randomly allocated into three groups: control group (verification x1 (*N*=30)), and two experimental groups: (verification x2 (*N*=30), and verification x3 (*N*=30)) (reported in Table 8). Study credits were offered to the participants as an incentive for taking part in the study.

TABLE 8: Verification groups

Control group	Verification x1 (re-enter once)
Experimental groups	Verification x2 (re-enter twice) Verification x3 (re-enter three times)

3.6.2 Measures

A website was created for the purposes of collecting all data for this study. The website allowed participants to create and recall passwords, and answer questionnaires measuring their experience. However, for the purposes of this study, we are only examining the user convenience construct related to password verification.

3.6.2.1 Objective data

The objective password recall data was collected via the website regardless if the participants entered their passwords correctly or incorrectly. Over five weeks, the participants created five passwords for five fictitious accounts, and recalled them 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 amount (Nelson & 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 & Sasse, 1999). This longitudinal design was employed to prevent cognitive overloading, as the increased cognitive load would affect the learning and recalling process (Baddeley, 1992). The type of design was also 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 guidelines imposed length, complexity, and variety to ensure a minimum level of password strength across all groups (reported in Table 9.).

TABLE 9: Guidelines and system requirements 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. to 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:

1. more than eight characters consisting of the English alphabet A-Z, a-z
2. at least one upper case and one lower case letter
3. at least one number 0-9
4. at least one special character !,”#¤. etc.
5. no words or names
6. all passwords to have less than 3 of the same characters in the same sequence

The system should not allow more than 4 letters to be in sequence, regardless if they are capitals or lowercase

3.6.2.2 Subjective data

The subjective user convenience data was collected via questionnaires on the website, taken by the participants after creating and recalling passwords. A pilot study was conducted where the reliabilities of the questionnaire items were calculated. When analyzing reliability, in both the pilot and the current study (for each of the three weeks of password creation and the overall scores), all questionnaire items showed to have a good level of reliability (Cronbach alpha score of 0.70 and above). For the purposes of this study, the questions that only referred to measuring user convenience of verifying passwords after creation were included in the final analysis (see Table 10 and Appendix 3.). These questions were adapted to be more specific to password verification, from questions used by Shay et al. (2010) and Workman et al. (2008) in their studies in password and security behavior.

TABLE 10: Questionnaire items to measure user convenience of password verification

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

3.6.3 Procedure

All participants completed the same tasks throughout the study. However, depending on which group the participants were allocated to, determined the number of times in which they would verify 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 creating their passwords, participants were asked to verify them, however if they were verified incorrectly then the password would be reset. The website also monitored all input errors when the participants were recalling their passwords; they were given three attempts to enter them correctly. 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, all at the end of each week (creation and recall schedule illustrated in Table 11.). Over 4000 passwords were input into the website and over 800 questionnaires were completed over the five weeks.

TABLE 11: Password (study) schedule

Week	Create 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

3.7 Results

We collected a large amount of objective and subjective data, including over 3000 passwords, and questionnaire responses measuring user convenience. To test our hypotheses we used analysis of variances (ANOVAs) to show differences between the groups, and independent t-tests to further confirm our results with in more detail.

3.7.1 Password recall

Correct password recall could be categorized by the total number of passwords correctly recalled over the five weeks, and 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 password verification group on total correct password recall. There was a significant effect of password verification group on total correct password recall ($F_{(2,90)}$ = 11.600, $p < 0.001$), supporting H1. Another between-subjects ANOVA showed there was also a significant effect of password verification on correct first time password recall ($F_{(2,77)}$ = 10.807, $p < 0.001$), further supporting H1. Total correct password recall and correct first time password recall were highest in the three-times verification group, followed by two-times, and then the control (one-times) group (shown in Figure 5). The descriptive and inferential results are summarized in Tables 12 and 13.

3.7.2 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 password verification group on user convenience ($F_{(2,120)}$ = 2.512, p = 0.087), not supporting H2, however, these results supported the objectives of this study. With further analysis, an independent t-test was performed, showing 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 examining the descriptive statistics, the results revealed that user inconvenience was (when comparing all three groups), the lowest in the two-times verification password group, then secondly, the control group, and the highest was the three-times verification password group (shown in Figure 6). Therefore, further 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 inconvenience was higher in the three-times group, which was to be expected. However, a t-test showed that there was not a significant difference in user inconvenience between the one-times group and the two-times group (t = -1.154, df = 58, p=0.127), and user inconvenience was actually lower in the two-times password verification group than the one-time group. Although, this does not support the hypothesis, it could support the objectives of this study. The descriptive and inferential results are summarized in Tables 12 and 13.

TABLE 12: Descriptive results

		Verification group	
Mean (Standard deviation)	Control group – verification x1 (*N*=30)	Experimental group - verification x2 (*N*=30)	Experimental group - verification x3 (*N*=30)
Total Password correct recall	5.00 (2.92)	7.10 (2.77)	8.43 (2.65)
Correct first time 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)

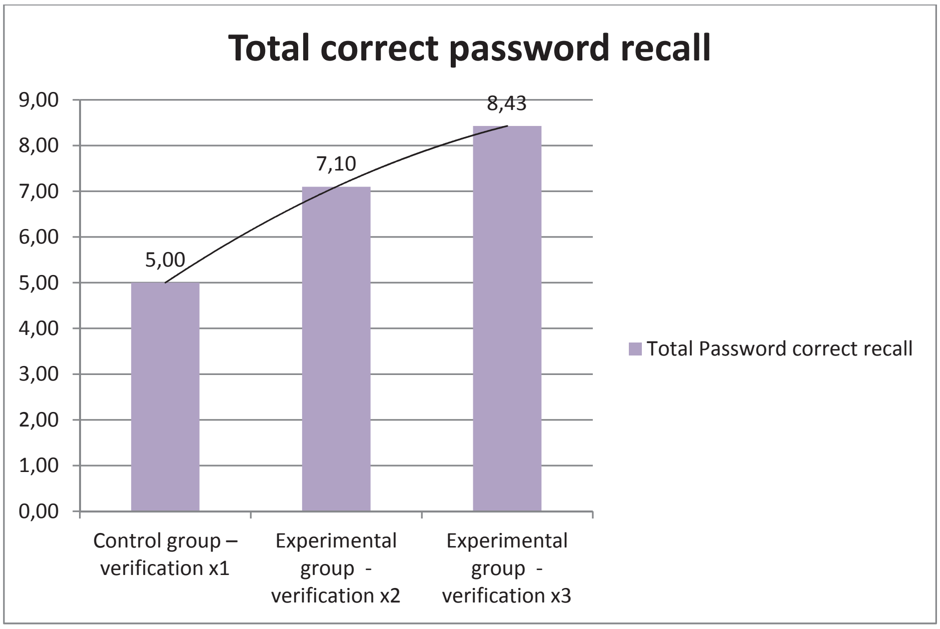


FIGURE 5: The mean score of total correct password recall

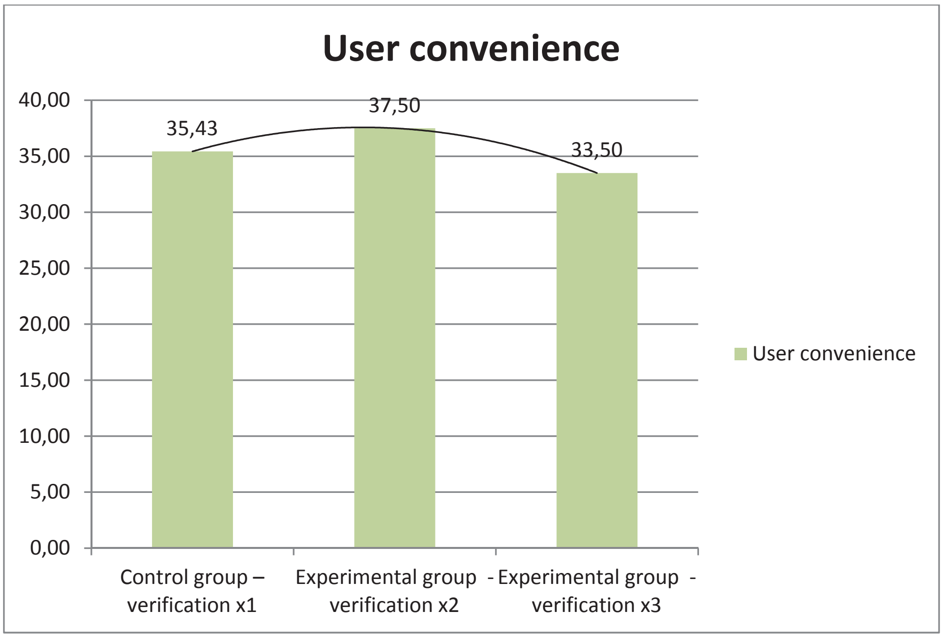


FIGURE 6: The mean score of user convenience

TABLE 13: Inferential results

Dependent variable	Hypothesis	sig
Correct password recall	H1: Increasing the number of password verification times will have a positive effect on password recall	$p < 0.001$ (total correct) $p < 0.001$ (correct first time)
User convenience	H2: Increasing the number of password verification times will have negative effect on user convenience.	$p = 0.087$

3.7.3 Further analysis

Through further analysis a correlation design revealed there was no significant relationship between the two dependent variables: password recall and user convenience, which was to be expected.

3.8 Discussion

3.8.1 New contributions

The results of our study make several important contributions. First, our results showed that increased numbers of password verification, increases password memorability. Verifying passwords three times increases password memorability by 28% when compared with current practices in use (verifying passwords just once); from 42% correct password recall to 70%. Even by increasing the verification to just two times, increased the password memorability by 17%, from 42% correct password recall to 59%. 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 strong evidence that to increase password memorability, there does not need to be substantial changes in practices or devices; small changes are effective enough.

The second new contribution was that even though previous research suggests that the more time users spend on the password process, the higher their inconvenience level (Renaud & De Angeli, 2004; Zhang & McDowell, 2009); we found that this was not necessarily the case. Not only did we find that user convenience levels were similar across all three groups (51%-58%); we also found that with the number of times of verification did not equate to an increase in user inconvenience levels. The highest level of user inconvenience was experienced by the three-times password verification group, with one-times group being only 3% lower. The two-times password verification group had the lowest user inconvenience levels, being 7% lower than the three-times group, and 4% lower than the one-times group. Although there was no significant difference across the three groups, the inconvenience result in the second group was unexpected. With further 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 it was time-consuming. These findings are interesting as it suggests that user convenience is not directly affected by time on the password process, as previous research suggests (Renaud & De Angeli, 2004; Zhang & McDowell, 2009), or changes in practices, i.e. increasing verifications.

The third new contribution is that the "trade-off" that previous research suggests (Bang et al., 2012; Tam et al., 2010; Vu et al., 2007; Weir et al., 2009; Zhang et al., 2009), is not as dynamically inflexible as is proposed. What this means is where previous research suggests that you can have one or the other, security vs. memorability (Vu et al., 2007; Zhang et al., 2009), security vs. convenience (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009); one, our findings show that if one factor increases, the other doesn't automatically decrease; and two, 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.

3.8.2 Implications for practice

The implications of our results are for both organizations and service providers. Password problems, such as insecure password behaviors (reusing passwords, writing passwords down, sharing passwords, choosing weak passwords, and not changing passwords regularly) stem from users being required and finding it challenging to remember multiple passwords; and their fear of forgetting them (Inglesant & Sasse, 2010; Tam et al., 2010). Users' insecure behaviors and forgetting passwords have serious consequences for both organizations, and service providers in terms of money, loss of employee productivity, and convenience (Inglesant and Sasse 2010, Sasse et al., 2001). Therefore, our findings have vital implications for, first, making passwords more memorable; second, for reducing the consequences of forgetting passwords; and third, reducing insecure password behaviors and the outcomes of them; while at the same time not significantly changing the password process.

3.8.3 Limitations and future research

The first limitation of this study is that as a laboratory experiment, realism (for the participant) and generalizability (to populations) are not strong facets in this type of methodological approach (McGrath, 1982). However, what this study lacked in realism and generalizability, it made up for in precision and control (Dennis & Valacich, 2001; Liu & Myers, 2011). When measuring the human memory and collecting objective data, precision is the extremely important, and therefore laboratory experimental designs are often employed in this type of study in IS research (Liu & Myers, 2011). Besides, when collecting password data, it would have been a security issue if the data collection was actually within the "real-world", and therefore, only a laboratory experiment could have been employed.

By employing a laboratory experimental design, the study was designed in such a way to eliminate as many confounding variables as possible. However, we still attempted to incorporate as much realism into the design as possible. This resulted in more limitations such as the participants having the opportunity to write their passwords down. The study was completed online, and although there were instructions and warnings of security breaches if participants took note of their passwords, they still could have broken the rules.

Another limitation is with respect to the verification process in this study. Verifying passwords two or three times is novel and different to the normal process in users' everyday lives. Just for the fact that the process was novel could have affected the memorability of the passwords, as novelty increases memorability (Baddeley, 2009). However, with careful consideration, it was decided that the design could not have been adapted to exclude such an effect, but has to be duly noted.

The final limitation refers to the construct of user convenience. There are several studies that examine user convenience in the password context (Bang et al., 2012; Jenkins et al., 2014; Renaud & De Angeli, 2004; Tam et al., 2010; Weir et al., 2009), and have found that it is a key factor effecting password security (Bang et al., 2012; Tam et al., 2010; Weir et al., 2009). However, it is still not fully defined, nor examined in terms of its theoretical grounding. Therefore, in future research, user convenience needs to be examined in more depth, properly defined as a concept, and in terms of a psychological backing; and just as importantly, it needs to be operationalized, possibly from the motivation perspective for consistent measurement.

There are several other directions in which future studies could take. There needs to be more longitudinal designs incorporated into password studies. Longitudinal studies of password recall, first makes the study more realist as users rarely create, learn and recall several passwords at one time. Second, this type of approach would increase cognitive load and undermine the measurement of password recall (Baddeley, 1992). Future studies also need to 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. Finally, future studies should look to measuring increased amounts of verification attempts (such as five or even ten times), on memorability and user convenience.

3.9 Conclusion

Users are increasingly finding it hard to recall their passwords as the amount of accounts continue to rise (Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). As users push their memory capabilities, they adopt insecure password behaviors to cope with inability to remember their passwords (Grawemeyer and Johnson 2011, Notoatmodjo and Thomborson 2009, Zhang et al. 2009). Coupled with the fear of forgetting, these insecure password behaviors result in severe consequences for not only the user, but organizations also; in terms of money, loss of employee productivity, and inconvenience (Brown et al., 2004; Inglesant & Sasse, 2010; Sasse et al., 2001). There have been several studies looking to the human memory to understand the password problem, and attempt to solve it. However, like with the adoption of biometrics, cost and familiarity win out over a mechanism that could possibly solve these issues (Florêncio & Herley, 2007; Keith et al., 2009). In this study, we look to adapt small changes to the already existing password process. Through increasing password verification times, could this increase password memorability, as repetition is suggested to increase memory performance? However, 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. Therefore, we examine user convenience while increasing password verification times, to see if one affects the other.

Our results are very promising. We find that increased verification increases password memorability, however, it does not affect user convenience proportionately. This study and its results have important implications for IS password practice, as through simple adjustments to the password process via increased verification times, it first makes passwords more memorable while not concurrently increasing user inconvenience. Second, it reduces the consequences of forgetting passwords. Finally, it reduces insecure password behaviors and the security issues pertaining to them. Future research should examine the interaction between security, memorability and convenience in more depth, to gain a greater understanding of the relationships between these important factors involved in the password process.

4 THE UNIQUE PASSWORD THEORY: BETTER PASSWORD MEMORABILITY, BETTER PASSWORD SECURITY PRACTICE

4.1 Abstract

Users believe that their memories cannot cope with multiple passwords. This is a misconception that can lead to adopting insecure password security practices/behaviors, such as reusing passwords (using exactly the same password), or modifying passwords (using the same password with slight amendments), for more than one account. These behaviors are widespread amongst users and can result in hackers gaining easier access to high-level security sites, by stealing passwords from sites with lower levels of security. Many users suffering from "password overload" turn to password reuse as they believe it will aid their memory. This research proposes the Unique Password Theory, based on a cognitive-psychological memory theory; which argues in contrary to users' beliefs, that unique passwords have a greater effect on password recall, than modified or reused passwords. This theory not only challenges the users' misconception, it also promotes good password behavior and practice through adopting unique passwords. Furthermore, it emphases the need for new IS theories for understanding password recall, as passwords only exist in the IS context. A 12-week empirical longitudinal study collecting over 6000 passwords test the Unique Password Theory by examining password recall and memory interference. The results of this study demonstrate that, with the application of the Unique Password Theory, unique multiple passwords are more memorable than modified or reused passwords.

This theory has important implications for IS practice as it proposes that as unique passwords increase the memorability of passwords, this potentially reduces some other insecure password behaviors, such as writing passwords down. Second, password reuse and modification does not increase password memorability, and should not be adopted to cope with multiple passwords

memorability. Finally, as multiple unique passwords are not as easily forgotten as reused or modified passwords, unique passwords minimize the ramifications of forgetting passwords (e.g. increased IT helpdesk costs).

4.2 Introduction

User authentication is a key defense against information security breaches (Zhang et al., 2009). Despite advances in biometric authentication mechanisms (Renaud & De Angeli, 2009), passwords remain by far the most common means of user authentication (Florêncio & Herley, 2010; Keith et al., 2009). Moreover, users accumulate more and more passwords as the number of accounts rise (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Given that cracking passwords can give open access to any sensitive information in an IS, the security of passwords has been an important priority in IS security research (Crossler et al., 2013; Garrison, 2006; Bonneau & Preibusch, 2010; Grawemeyer & Johnson, 2011; Siponen & Vance, 2010). Insecure password behaviors include choosing weak passwords; reusing or modifying passwords for more than one account; writing passwords down; and sending new passwords without encryption in emails (Adams & Sasse, 1999; Campbell et al., 2006; Guo, 2013; Zhang et al., 2009). It is widely reported that such insecure password behaviors stem from the users' inability to memorize multiple passwords; hence, they adopt these behaviors as coping strategies for perceived memory limitations (Biddle et al., 2012; Campbell et al., 2006; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). With the number of passwords and the amount of accounts and systems they protect are on the rise, this is a problem that will only get worse with time (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009).

In this study the Unique Password Theory is proposed, founded on the cognitive-psychological memory theory of interference. The Unique Password Theory argues that using unique, distinctively different passwords will have a greater effect on password recall than modified, similar, or reused passwords. This theory emphasizes that by following password security guidance, unique passwords are actually more memorable than previously thought (Duggan et al., 2012; Grawemeyer & Johnson, 2011). The adoption of the Unique Password Theory improves the memorability of passwords, which in turn can result in a reduction of some other insecure password behaviors, such as writing passwords down. This study collected empirical data (over 6000 passwords), measuring the effect of password behavior on password recall and interference, during a 12-week longitudinal study of multiple passwords.

This has important implications as it: 1. challenges user preconceptions that insecure password behavior (reusing the same password or modifying passwords) cues to aid memory, and should be adopted to compensate for memory limitations. 2. The Unique Password Theory contravenes IS security research, arguing that good security practice can lead to higher multiple passwords memorability, and not the contrary. 3. These findings can be further used to advice users and corporations on the management and security of multiple passwords.

The rest of this paper is structured as follows: the next section will discuss the previous IS research in insecure security behaviors, multiple passwords, and password reuse. Then we examine the theoretical background, looking at the human memory and interference. The following section discusses the development of the Unique Password Theory and its hypotheses. Later in this paper, we will discuss the research methodology, including the experimental design, and then the results. The remaining sections of the paper will conclude with a discussion of the study's important findings, and the contributions and implications of the Unique Password Theory to both IS research and practice.

4.3 Previous research

Previous IS research has examined the password problem from two research streams. The first stream focuses on the memory aspect of the problem, and the second research stream focuses on insecure password behavior as any other IS security behavior. However, the second stream of research is not intended to solve memory issues, which is considered the central issue in password security. It is important to examine the human memory in more depth, to give a better understanding of how memory affects password recall, forgetting passwords, and insecure password behavior, such as password reuse. This paper will now discuss these issues, and previous attempts to address the password problem.

4.3.1 Forgetting passwords and its consequences

Password security is an important issue, which is being undermined by the increasing amount of passwords needed to secure all our accounts and services (Chiasson et al., 2009). With multiple passwords to remember, users are more prone to forgetting, with substantial costs to the user (home-user) and organization (Brostoff & Sasse, 2000; Brown, et al., 2004; Hayashi et al., 2012; Inglesant & Sasse, 2010; Vu, et al., 2007). For a home-user, this causes inconvenience and disruption due to loss of account access; and information security risks as resetting procedures are sent within emails (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009; Tam et al., 2010). To an organization, the costs of password resetting can be in terms of money, time and loss of services. When a user forgets their password, they can temporarily lose access to their organization's systems, causing inconvenience, disruption, and can lead to reduced productivity (Inglesant & Sasse, 2010, Sasse et al., 2001). Again, like the home-user, security is also an issue, as many workers create weak passwords due to the inconvenience of resetting and remembering new passwords (Inglesant & Sasse, 2010, Notoatmodjo & Thomborson, 2009, Tam et al. 2010). The money lost to companies for resetting passwords as a consequence of passwords being forgotten, can be in its hundreds of thousands (Brostoff & Sasse, 2000; Hayashi et al., 2012; Saastamoinen, 2014). As a result of the considerable pressure put upon users to remember their passwords, many have developed a fear of forgetting (Inglesant & Sasse, 2010, Tam et al., 2010), and therefore use coping strategies, such as password reuse, to deal with their memory failures (Adams & Sasse, 1999; Biddle et al., 2012; Duggan et al., 2012; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011).

4.3.2 Password reuse and modification problems: why should each password be unique?

Password reuse (using the same password for more than one account) and password modification (using the same password with small changes for more than one account) are insecure password behaviors, users adopt as coping strategies for forgetting passwords (Adams & Sasse, 1999; Biddle et al., 2012; Duggan et al., 2012, Gaw & Felten, 2006; Grawemeyer & Johnson, 2011). This behavior is considered to be a serious security problem that is not only worse than first thought (Bang et al., 2012), but will get worse with time, as the number of accounts increase (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Hackers obtain lists of password hashes from websites with low security, crack them using password-cracking software, then gain access to more secure websites and accounts with reused or modified passwords (Ives et al., 2004; Zhang et al., 2009).

Research by Ives et al. (2004) highlighted the security problem of reusing passwords, from a home-user perspective and from an organizational perspective. They reported an incident of home-users' personal vulnerabilities, when a journal editor could have gained access to his employees' personal accounts easily because as a high-level manager, he was able to see hundreds of his employees' passwords for their organizational accounts. Research by Swivel secure (2014) also illustrated the vulnerabilities of password reuse but within the organizational context. They found that 63% of business owners reuse their passwords and continue to believe that their systems are secure, and that 73% of US workers admitted to password reuse. A statement from the VP of Swivel Secure reported that password reuse was "rife", and that a substantial amount of money was being spent on the consequences of password reuse every year. Password reuse is a significant problem as it would only take an employees' online shopping account to be hacked, for unauthorized and undetectable access to company accounts and systems (Infosecurity Magazine, 2014).

It is extremely important to have a unique (distinctively different) password for each account (Nelson & Vu, 2010). There are several elements to password security, while users are advised to create unique passwords because they are considered to provide better security than reused or modified passwords, there are limitations to this increased security. Increased levels of security provided by unique passwords does not refer to password strength. Users can create weak passwords using dictionary words, or choosing characters that meet the bare minimum of the policy criteria (Marquardson, 2012), that are easily cracked, but are still different from each other. The increased security that unique passwords provide refers to multiple passwords, not the individual password; and the security issues pertaining to password reuse. There are serious issues with password reuse, and through unique passwords not being reused, they automatically improve levels of password security.

4.3.3 Previous research: responding to the password problem

Previous IS research have approached the password problem from two research perspectives. The first theorizes that insecure password behaviors stem from memory issues, and accordingly, focus on the memory aspect of the problem. The second approaches insecure password behavior as any other IS security behavior; applying theories such as deterrence, rational choice, and Protection Motivation Theory (PMT) (Jenkins et al., 2014; Vance et al., 2013). These studies have their merits, and help us to understand why users adopt insecure password practices. However, none of the prominent theories in IS security, namely sanctions in terms of deterrence theory (D'Arcy et al., 2009; D'Arcy & Herath, 2011) or fear in terms of PMT (Pahnila et al., 2007), are intended to solve memory issues. Therefore, an important direction in password research should examine the human memory in more depth, to give a better understanding of how memory affects password recall and password reuse.

Research examining memory and its effect on different aspects of the password problem, have included the study of: password reuse (Adams & Sasse, 1999; Sasse et al., 2001; Vu et al., 2007; Zhang et al., 2009); and the contributing factors (Bang et al., 2012; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009); the perceived importance of information (Bubas et al., 2008; Grawemeyer & Johnson, 2011; Vu et al., 2007); and how policies can effect users' password choices (Campbell et al., 2011, Marquardson 2012). Furthermore, many studies have examined password reuse and its contributing factors (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Key reasons for user justification for reusing their passwords were that reuse made it easier to remember them, and they had too many accounts (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Subsequently, users believe that through using password reuse and modified passwords, they will better remember their passwords (Adams & Sasse, 1999; Bang et al., 2012; Campbell et al., 2011). However, scholars also suggest, based on memory inference studies that it has the opposite effect (Adams & Sasse, 1999; Chiasson et al., 2009).

IS researchers have applied several memory theories to password recall. However, we have to consider that passwords as a stimuli are not present in their form in any other real-world situation, they are specific just to the IS context. Therefore, can we apply these memory theories directly to password recall?

4.3.3.1 The research gap

Adams and Sasse (1999) advised that users would be able to successfully remember between four and five unique passwords, but since then, the world has technologically changed (Lin et al., 2013). Nowadays, users are generally required to remember over 10 distinctively different passwords (Zhang et al., 2009). Passwords are only effective if you can remember them (Duggan et al., 2012), and as the cost of forgetting them is high, this drives users to adopt insecure password behavior (Duggan et al., 2012, Zhang et al., 2009). One of the most significant issues with password security is that users believe they have a problem remembering too many passwords (Bang et al., 2012; Campbell et al., 2011). The research gap is two-fold:

First, users believe that password reuse will aid their password memorability. Several studies have reported this, such as Bang et al. (2012), Duggan et al. (2012), and Notoatmodjo and Thomborson (2009), as they have collected subjective data from users. It is intuitive to think that reused or modified passwords are easier to remember than many unique passwords. However, Bang et al. (2012) and Notoatmodjo and Thomborson (2009) unfortunately based their study on the short-term memory, which has a limited capacity (Miller, 1956), and not the long-term memory, which has an unlimited capacity (Baddeley, 2009a; Eysenck & Keane, 2010), where passwords are stored. We argue that reused and modified multiple passwords can be in fact, less memorable than unique passwords. The Unique Password Theory argues that using unique, distinctively different passwords will have a greater effect on password recall than modified or reused passwords, due to less interference. This is contrary to the perceptions of the users and some researchers.

Second, previous studies have turned to interference theory, but do not specifically examine interference in alphanumeric passwords and its effect on password recall. There are several studies that apply different memory theories to the password context, examining password security behavior, such as reuse; memory techniques to make passwords more memorable, and a few have even referred and used interference theory. Chiasson et al. (2009) and Wiedenbeck et al. (2005) used interference theory to examine graphical password memorability. These studies have found that graphical passwords are not necessarily easier to recall than alphanumeric passwords. Furthermore, graphical passwords are different to alphanumeric passwords to recall. Graphics and pictures as stimuli exist in the real-world, whereas alphanumeric passwords do not exist in any other context except information security. However, Zhang et al. (2009) turns to interference theory also, but applies interference techniques to improve password recall. All these studies have important findings; however, there is a considerable research gap, as they do not specifically examine interference in alphanumeric passwords and its effect on password recall. This article will now discuss the human memory, how reused and modified multiple passwords are in fact, less memorable than unique passwords, and the development of the Unique Password Theory.

4.4 Theory Building

Before building a theory, it is important to explain what a theory is. Theories in natural sciences are used to denote one or more hypothesis, principles or propositions (Laudan, 1996). Similarly, in management science, Colquit and Zapata-Phenan (2007) defines theory as a relationship between the elements of the theory, often expressed as variables in management science. In turn, DiMaggio (1995) defined theory as accounts and narratives of social processes. In natural sciences (at least), theory is also used to describe a set of individual theories (Laudan, 1978). For example, "atomic theory" does not refer to one specific theory, but a set of different doctrines (Laudan, 1978, pp. 71-72). To simplify, there are two approaches for theory building. Natural and social sciences have long tradition of theory development based on qualitative observation (Godfrey-Smith, 2003; Nagel, 1979), for example performed through microscope or telescope. In IS and management science such qualitative observation driven theory development is often called 'inductive' theory development (Colquit & Zapata-Phenan, 2007). Alternative approach is the hypothetical approach (or hypothetical deductive). In IS, the hypothetical approach is often literature or theory based, while in natural sciences, scholars' imaginations and speculative argumentation have also a key role in hypothesis formulation (Einstein, 1930; Popper, 1980). This article follows the hypothetical approach to develop a Unique Password Theory. Often new theories are based on existing theories or some part of them. For example, Unified Theory of Acceptance and Use of Technology are based on eight IT use theories. Also, new theories can be based on existing theories by specifying or adding something new that the extant theories have not originally proposed (Niiniluoto, 1993). For example, TAM, based on TRA, proposes that ease of use explain IT use, while ease of use is not originally included in TRA (Davis, 1987). The Unique Password Theory is based on a multi-store memory model and interference. In order to understand and test the Unique Password Theory, we first need to understand these two memory theories, which will be discussed next.

4.4.1 The information-processing approach and the multi-store memory model

The problem with multiple passwords and their memorability is thought to be related to information retrieval, by means of retrieving passwords from the long-term memory (Zhang et al., 2009). To understand why password retrieval is an issue, and why many users believe password reuse increases memorability (Adams & Sasse, 1999; Duggan et al., 2012), one needs a basic understanding of how the human memory functions.

The Stages of Memory Theory (Modal Model) proposed by Atkinson and Shiffrin (1968) is considered one of the most influential multi-storage models, identifying three types of memory stores: sensory memory, short-term memory, and long-term memory. The sensory memory stores information for a brief period of time and is thought of as an interface between perception and memory. The short-term memory (STM) or working memory (WM) (updated by Baddeley & Hitch (1974)), attends to and processes information, stores it for only a matter of seconds, and has a limited capacity. The long-term memory (LTM) has an unlimited capacity to hold information which is not currently in the conscious awareness; this information is held ready for retrieval for over a very long period of time (Baddeley, 2009a; Eysenck & Keane, 2010). In terms of password management, the password is observed and attended to by the sensory memory, is learned and rehearsed in the STM, and is stored (long-term) in the LTM, ready for retrieval.

One of the issues preventing users from remembering their passwords is if they have learnt them properly in the first place. Learning a password requires mental effort and concentration to ensure the correct storage for its eventual retrieval (Zhang et al., 2009). The LTM issues with password memorability are storage and retrieval problems; coupled with the limitations of learning passwords. We argue that this leads users to believe that their memories cannot cope with too many passwords, and therefore adopt password reuse. This article will discuss these long-term memory retrieval issues in the next section.

4.4.2 Interference Theory: a theory of forgetting

Interference is a phenomenon, a mechanism to explain forgetting (Anderson, 2009), which has been studied in psychology for over a hundred years (Eysenck & Keane, 2010). Interference theory is a set of principles from the field of human learning and memory (Crowder, 1976), that views forgetting as an information retrieval error – retrieving a memory (from the LTM), that has been disrupted or interfered with, by similar memory traces (Anderson, 2009; Criss et al., 2011). Interference occurs because we accumulate experiences over our life-time, and these memories amass, sharing several common traits due to the fact that people are creatures of habit and enjoy routine. Routine actions like eating an evening meal is a less memorable experience, unless we do something different making it unique, such as meeting a friend for dinner. The uniqueness of the experience makes it more memorable (Crowder, 1976). With an increase number of similar memory traces gathered over time, demonstrates a forgetting curve as the presence of these similar traces compromise the retrieval of the target memory (Anderson, 2009). There are different retrieval cue-target item relationships, if one retrieval cue is used for more than one target memory it interferes with the retrieval process and therefore errors occur; this is referred to as Competition Assumption (Anderson et al., 1994). This is also the case for the complexity of the target memory. Cue-overload principle is when a memory has different components to it with more complexity, it will have more retrieval cues which will be possibly shared with other memories, and therefore making it harder to retrieve (Watkins, 1978). When the retrieval cue becomes associated with more than one memory or item, this is when the interference occurs (Eysenck & Keane, 2010). A cue activates all associated items to some degree, and the items compete or fight with the target item for "access to awareness". These are known as competitors, and with more competitors fighting against the target item, the stronger the interference will be (Anderson et al., 1994).

There are several theories of interference. Competition assumption and cue-overload principle are just two that explain in more depth, the specifics of the phenomenon. Additionally, interference also has two main forms that effect and impede the retrieval of memories: retroactive and proactive (Wiedenbeck et al., 2005). Retroactive interference is when a more recently learnt memory/information hinders the retrieval of older similar memories/information; and proactive interference is when older memories/information interferes with the retrieval of similar, more recently learnt information or memories (Anderson, 2009). With regards to password management, retroactive interference would affect the recall of older passwords as newer passwords are learnt. Whereas, proactive interference occurs when users learn a new password, but have problems recalling it as the previous password impedes on the new one (Bunting, 2006).

"Qualitatively distinct situations produce interference" (Anderson, 2009, pp.201), these situations include for example experiences such as parking a car to recalling a list of words. However, even though these situations can be very different, the fundamental mechanism that results in forgetting is the same – interference. Interference has been studied in different contexts. One example is that Baddeley and Hitch (1977) found that rugby players had difficulty recalling the names of the teams that they had played earlier in the season. With further investigation they discovered that, while the time between the games was not important, the number of games played had an effect on the players' recall of the teams' names. When we consider these findings in terms of password management, the results would suggest that the time between learning, for instance, the second password and the first password would not cause greater interference if the time was greater. However, the number of passwords would have an effect on retrieving older passwords.

In the Unique Password Theory it applies the interference mechanism to explain why multiple passwords undermine the whole password mechanism. The Unique Password Theory proposes that multiple unique passwords, which are considered to be more secure, can be more memorable than reused and modified passwords; and argues that due to passwords only existing in the IS context, a general memory theory cannot be simply applied to explain password recall. Next, we will discuss this, and the development of the theory.

4.4.3 Developing the Unique Password Theory: understanding multiple password interference

4.4.3.1 Password security: an IS specific context

Authentication mechanisms used for smart phones, tablets, most of the web services, and so on, are IT artefacts, or more precisely software artefacts. Passwords are a set of different random characters, which have one key feature: to that allow users' access to their accounts. Therefore, remembering multiple different alphanumeric passwords is not only specific, but only exists uniquely to software authentications systems.

Interference presents itself in recalling passwords when a user is required to retrieve one password from a choice of multiple passwords, and when considering the structure or complexity of the password in terms of capitals, letters, numbers and special characters. When applying a theory such as interference theory to recalling passwords, one has to consider how passwords are different in terms of the stimuli used in interference research, and the context of everyday situations in which it occurs. Passwords are different. First, in structure, even if words are included in passwords, there are still numbers, capitals, and special characters. There is no other situation in which people are required to recall these combinations, with the significance or meaning that they carry. Second, meaning also plays a part, the importance, the consequences and the motivation to recall passwords will affect the memorability of them. Third, how the memory cues are formed in terms of what they are used for, but the situations in which they are created. Fourth, the way in which in any other situation, memory strategies would be employed to aid memorability; however, these strategies are considered insecure password behaviors. Fifth, different password behaviors (e.g., adopting unique, modified and reused passwords) will have a different and specific effect on the cue-target password relationship. This means that remembering multiple passwords, are not general memory problems that can be addressed by the direct application of extant memory theories. Having said that, the previous general memory theories provide the best explanations of to how memory works, which is useful for building specific theories for passwords.

4.4.3.2 The Unique Password Theory: a theory of password retrieval

Interference theory is a theory of forgetting (Eysenck & Keane, 2010). It examines retrieval to explain why forgetting occurs. The Unique Password Theory examines forgetting, and employs interference to explain password retrieval. Interference as mechanism has been the framework and incorporated into several memory theories, such as theories of learning (Crowder, 1976). As with competition assumption and cue-overload principle, where these theories examine the interference mechanism in more depth; the Unique Password Theory examines the specifics of the interference mechanism in different password behaviors (such as adopting unique, modified and reused passwords). So why is the Unique Password Theory different to Interference theory? First, interference theory has been researched using stimuli such as words, images, and everyday experiences and memories to support it. These are fundamentally different to passwords. When considering everyday experiences in terms of password recall, an everyday same routine could be compared to reusing a password. In our everyday lives these similar or same routines are considered as being not as memorable, for instance eating an evening meal. The uniqueness of the event, such as going out with a friend for dinner makes it more memorable. However, comparing this to password reuse, if users had just one password for all their accounts, then there would be less chance of forgetting it. This comparison shows that interference theory cannot be directly applied to explain why users forget their passwords, due to the nature of the password context (detailed in the previous section). In the real world, users generally create a set of unique passwords then reuse them several times (Brown et al., 2004). This is due to password reuse being a security risk, and password requirements being different for different services (Campbell et al., 2011); this means the use of one universal password that is unchanging is not possible. Therefore, the uniqueness of multiple passwords needs to be exploited to increase memorability, and while concurrently increasing security. Thus, the Unique Password Theory looks to retrieval to support the recall of passwords, instead of just explaining why users forget them.

4.4.4 The Unique Password Theory: assumptions and arguments

As a new theory of explaining password recall, and incorporating the mechanism of interference we argue the followings:
1. Unique passwords are more memorable than reused and modified passwords. Indeed, we argue contrary to the previous password literature, that unique passwords, owing to being different from each other, makes them less exposed to memory retrieval problems caused by interference. Therefore we hypothesize the following:

> H1a: Adopting multiple unique passwords will negatively affect password interference compared with modified passwords or reused passwords.
>
> H2a: Adopting multiple unique passwords will positively affect password correct recall compared with modified passwords or reused passwords.

2. Similarity in password composition causes interference due to the number of competitor passwords and the number of retrieval cues.
3. Unique passwords have less competitor items for each retrieval cue, and less retrieval cues for each target item, causing lower levels of interference when retrieving the target password.
4. Modified passwords (using the same password with small changes for more than one account, e.g., 386firstnamelastname1 and 386firstnamelastname2), have several competitor items for each retrieval cue, which causes higher levels of interference when retrieving the target password. Giving a practical example, let us presume that a number of passwords are modified as the following:
Account 1 password: 386firstnamelastname1
Account 2 password: 386firstnamelastname2
Account 3 password: 386firstnamelastname3, and so on.
We argue that due to the similarity between the passwords, the interference when retrieving the correct password from the long-term memory, for the right account leads to incorrect password recall.

5. Reused passwords (using the same password for more than one account), have several retrieval cues for each target item, which causes higher levels of interference when retrieving the target password for the right account. The user may confuse which accounts the reused password belongs to.
6. Different password behavior (e.g. adopting unique, modified or reused passwords) results in a different cue-target password relationship. Although there will be several retrieval cues for each password, Figure 7 illustrates in its simplest form the cue-target password interference relationship, with the account as the retrieval cue:

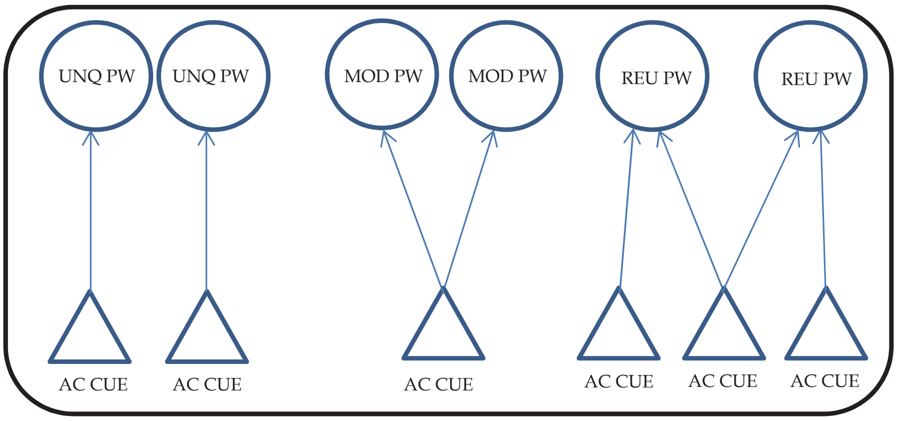


FIGURE 7: Cue-target password interference relationship

7. Increasing numbers of accounts/passwords increases interference, and therefore, 8. increasing numbers of accounts/passwords decreases the level of passwords recall. Previous memory research suggests that interference increases as the number of items to remember increases (Baddeley & Hitch, 1977). This suggests that as the number of passwords rise, so does password interference and incorrect password recall (Vu et al., 2007). We argue that interference will be higher between modified passwords, and reused passwords compared with unique passwords; and therefore, correct password recall will be lower in the modified and reused password groups compared with the unique password group, due to similarity between the passwords and accounts. We hypothesize the following:

> H1b: The increase of password interference will be stronger as the number of passwords increase when adopting multiple modified or reused passwords compared with multiple unique passwords.
>
> H2b: As the number of passwords increase, the decrease in password correct recall will be stronger when adopting multiple modified or reused passwords compared with multiple unique passwords.

4.4.4.1 Unique passwords, total login errors, account-password matching errors, and login failures

The interference effect “initiates a dramatic decline in memorability and performance” (Everitt et al., 2009) in password recall. Moreover, forgetting passwords can be attributed to the interference between the correct matching of passwords to the right accounts (Nelson & Vu, 2010), and/or to the interference between the passwords themselves (Grawemeyer & Johnson, 2011; Zhang et al., 2009). These two types of password recall errors can be categorized into account-password matching errors, and login failures. Account-password matching errors would occur when a user would get confused between accounts. This could be caused if there is one retrieval cue for more than one item, or in this case password. Therefore because of the interference between the passwords, users may remember a password correctly, but find it hard to recall which account it belongs to. On the other hand, login failures are not only caused by confusion between passwords and misremembering, but also by mistyping, interruptions, and completely forgetting the password entirely (Grawemeyer & Johnson, 2011). An example of login failures would be when a user would have one password: “386Djtovghnbm3”, but may recall it as “368Djtovghnbm3”, or “386djtovghnbM3”, and so on. When the item (or password) is complex enough to warrant many cues to recall it, these cues may be associated with other items, and therefore confusion in their structure will ensue. Hence, based on these types of password recall errors we hypothesize the following:

> H3a: Adopting multiple unique passwords will negatively affect total password recall errors compared with modified passwords or reused passwords.
>
> H3b: The increase in total password recall errors will be stronger as the number of passwords increase when adopting multiple modified or reused passwords compared with multiple unique passwords.
>
> H3c: Adopting multiple unique passwords will negatively affect account-password matching errors compared with modified passwords or reused passwords.
>
> H3d: Adopting multiple unique passwords will negatively affect password login failures compared with modified passwords or reused passwords.

In summary (illustrated in Figure 8), The Unique Password Theory argues that reused and modified password behavior will have a positive effect on interference, which will have a negative effect on password correct recall, and a positive effect on recall errors. Therefore, against users’ preconceptions, adopting unique passwords can not only lead to better password security practices, but can also increase correct password recall.

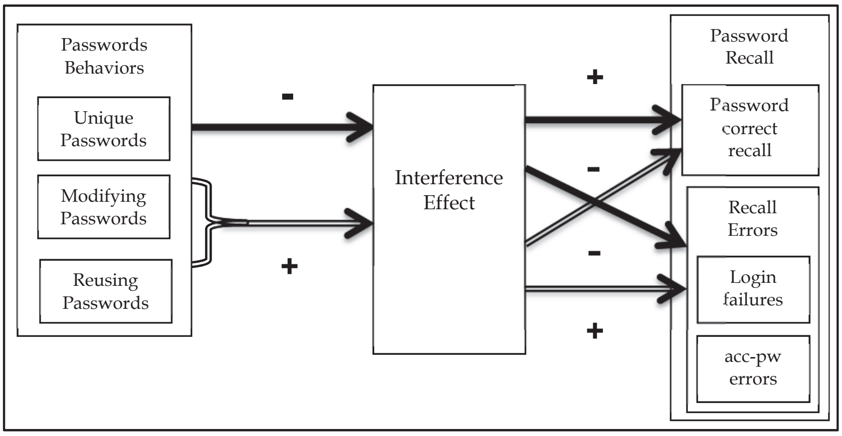


FIGURE 8: Unique Password Theory

TABLE 14: Summary of Hypotheses

Dependent Variables	Password behavior and password increase
Password interference	H1a: Unique passwords < modified passwords or reused passwords H1b: Interaction: number of passwords x unique passwords < modified or reused passwords
Password correct recall	H2a: Unique passwords > modified passwords or reused passwords H2b: Interaction: number of passwords x unique passwords < modified or reused passwords
Total password recall errors:	H3a: Unique passwords < modified passwords or reused passwords H3b: Interaction: number of passwords x unique passwords < modified or reused passwords
Account-password matching errors	H3c: Unique passwords < modified passwords or reused passwords
Login failures	H3d: Unique passwords < modified passwords or reused passwords

4.5 Research Methods

A longitudinal experiment was conducted for 12 weeks, using a web-based password creation and recall system that allowed participants to create passwords, recall passwords, and monitor password recall errors, and password behavior. The experiment collected over 6400 passwords, and examined password recall, password interference, and their relationship with three different types of multiple passwords: unique passwords, reused passwords, and modified passwords.

4.5.1 Participants

Given that the human memory is not associated with factors such as gender, culture or student versus worker; any computer user who engages in the use of passwords in ISs is considered a suitable participant. Participants were selected from the staff and students from a university in Finland. The participants were all experienced computer users and all had work experience. They were randomly allocated into three groups: the unique password group (*N*=27), the reuse password group (*N*=27), and the modified password group (*N*=27), totaling 81 participants. The participants were matched on age, as age has an effect on memory (Baddeley, 2009c). Demographic information is reported in Table 15. Study credits were offered to the participants as an incentive for taking part in the study.

TABLE 15: Demographic Information

Age	Gender	Education level
18 to 24 years (count of 24; 29.6%)	Male (count of 52; 64.2%)	Further education (count of 1; 1.2%)
25 to 34 years (count of 33; 40.7%)	Female (count of 29; 35.8%)	Bachelor's degree (count of 35; 43.2%)
35 to 44 years (count of 14; 17.3%)		Master's degree (count of 37; 45.7%)
45 to 54 years (count of 5; 6.2%)		Doctoral degree (count of 8; 9.9%)
55 to 64 years (count of 5; 6.2%)		

4.5.2 Measures

A website with password generation and input capabilities was created and employed for the participants to generate and recall passwords, and to monitor any input errors. The website also held information about the study, the schedule, and guidelines for creating passwords.

4.6 Experimental Design to test the Unique Password Theory

Laboratory experiments have been found to be between the second to third most commonly used method of data collection in the AIS basket of top academic journals, due to the level of control measuring the independent variables (Liu & Myers, 2011). In this study a laboratory experimental design was chosen for many reasons, as although it has its limitations in terms of its realism, it, on the other hand, allows for precision over the creation and recalling of passwords, and password input monitoring. Several aspects of the design of the experiment intended to match the everyday password management experience, e.g. how many passwords were created at one time. Furthermore, studying password creation and recall in a realistic setting would be a security issue, with limitations of what detail could be monitored, especially in relation to password interference. Therefore, password studies of this type are normally laboratory experiments (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009).

4.6.1 Defining groups and passwords

The effects of interference on memory recall is what defined the password groups (unique, reused, and modified). As interference is based on similarity of information retrieval (Baddeley, 2009b), therefore, one group would create unique passwords; one group would create modified passwords, where passwords would be similar in characters; and a third group where the passwords would be the same for several accounts. The passwords created by each group were imposed by the password creation guidelines, reported in Table 16; these guidelines had six rules that every password had to meet. These six rules imposed complexity and length, to ensure a minimum level of password strength across all groups. Rule 7 defined the group based on the interference phenomena. After the first password was created, the rules remained the same for all passwords created in the unique password group and the modified password group. The reused groups' rule 7 changed during the study (see Table 16.); if it had remained the same, the participants would have created only one password, and this would have not been a test of memory. Therefore, the reused group created three unique passwords, which were reused for seven accounts. This is a more "true to life" situation, as many users have a set of unique passwords, but reuse them for many accounts (Shay et al. 2010, Zhang, et al. 2009). The password rule schedule is shown in Table 17.

Rule 7 defined each group and therefore the system had to be programmed to recognize this rule for each group. The system group criteria are reported in Table 16.

TABLE 16: Guidelines and system requirements 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#).		
Unique group	Modified group	Reused group
7. be unique = different from every other password created, preferably different in meaning too (e.g. Bookcase1# and iloveTV1!).	7. contain between four – six characters in common with the other passwords created (e.g. Redbag1# and Redbag2&) – this is to help anonymously identify you.	7. be the same as one of the previous passwords – this is to help anonymously identify you.
System Criteria	System Criteria	System Criteria
all passwords to have less than 3 of the same characters in the same sequence.	all passwords to have between 4-6 characters in common in the same sequence.	passwords to be the same as one of the previous passwords created.

TABLE 17: Creating passwords rule schedule

Pass words/ week	Unique group		Modified group		Reused group	
	1st	2nd	1st	2nd	1st	2nd
1	No Rule 7	Unique Rule	No Rule 7	Modified Rule	No Rule 7	Reused Rule
2	Unique Rule	Unique Rule	Modified Rule	Modified Rule	Unique Rule	Reused Rule
4	Unique Rule	Unique Rule	Modified Rule	Modified Rule	Reused Rule	Reused Rule
6	Unique Rule	Unique Rule	Modified Rule	Modified Rule	Unique Rule	Reused Rule
8	Unique Rule	Unique Rule	Modified Rule	Modified Rule	Reused Rule	Reused Rule

In previous research, different types of passwords such as reused and unique passwords, were not defined as specifically as within this study. In a study by Zhang et al. (2009, pp.170) the rule imposed to create unique passwords was: 'use a password with the first two letters different from your other accounts'. With further analysis of the passwords created within our study, users that were creating modified passwords would have met this rule, while still reusing the main body of previous passwords. Therefore, this rule has been found to not impose password uniqueness, and within this study, it would affect the results. In a diary study by Duggan et al. (2012, pp.421), the study authors stated, "Passwords that reused only part of another password were treated as unique." From the perspective of interference, this would affect the results because this modification would lead to confusion; therefore, this type of password is referred to as a "modified" password for the purposes of this study. Gaw and Felten (2006) examined password reuse and referred to related passwords as being in the same category as reused passwords. Although there is an element of reuse in modified passwords (a user is essentially reusing a part of the password again), to fully understand the effects of interference on password recall, it is necessary to distinguish between simply reusing a password and actually modifying it, as similarity plays a significant part in its effect (Baddeley, 2009b).

4.6.2 Password Schedule

Participants from all groups completed the same experiment. As a longitudinal study, this experiment was conducted 1-2 times per week during a three month period. The passwords were not only recalled several times during the three months, but were also learned over this period of time (the password schedule for the study is shown in Table 18.). Several previous studies required their participants to learn several passwords all at once to test password memorability (Nelson & Vu, 2010; Vu et al., 2007; Zhang et al., 2009). However, learning many passwords all at once would not be a realistic situation: there are not many occasions when a person is required to learn many passwords at one time. Furthermore, learning several items or passwords can have an effect on the participants' cognitive load, and further recall could be measuring the cognitive load effect not the interference effect. For these reasons a longitudinal design was preferred. The schedule in terms of creating and recall passwords within the week were chosen for regularity, and for enough time to pass between creating and recalling passwords for recall to really represent long-term recall. The account order and frequency of recall was chosen to represent different levels of frequency of recall, and time between recall, to see if there was an effect.

TABLE 18: 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

4.6.3 Number and type of passwords

Ten accounts and passwords was chosen for this study because although Adams and Sasse (1999) advised that users could only learn and successfully remember between four to five passwords, users are nowadays often required to learn and successfully remember more than 10 passwords, which is more realistic (Zhang et al., 2009). Since this experiment investigated interference, then pushing the participants' memory capabilities would illustrate the point at which the interference effect would become a significant issue for password memorability.

Each participant created passwords for 10 accounts (as detailed in Table 19), and recalled them 42 times (up to 3 attempts each) over 12 weeks. Therefore, the recalled data that was used to analyze the password recall and password interference totaled over 6400 passwords.

TABLE 19: Details of passwords and accounts

Unique group	10 unique passwords for 10 accounts
Modified group	10 modified passwords for 10 accounts
Reused group	3 unique passwords for accounts, and reused for 7 accounts

4.6.4 Types of accounts

A number of studies have used systems where the participants selected or were presented with accounts, and entered the corresponding passwords (Nelson & Vu, 2010; Vu et al., 2007; Zhang et al., 2009). In this study, a similar design was employed and participants were asked to enter passwords for five fictitious different account types: online banking, email (personal), social networking, online shopping, and free online gaming. These types of accounts were chosen because of their range of importance and data sensitivity. For each account type, two accounts were chosen to represent them (account names and types are shown in Table 20). This account-password design was preferred because it is used in users' everyday lives, and therefore, would be familiar to them.

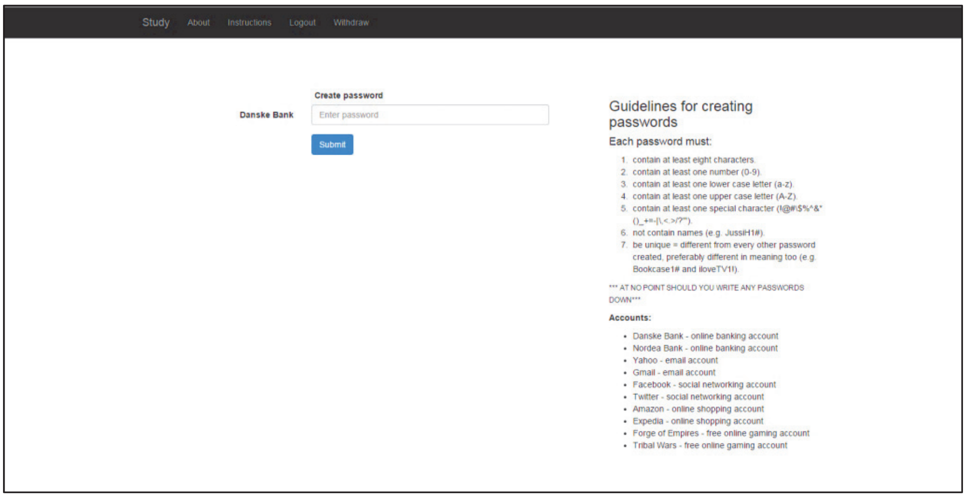
TABLE 20: Account types and names

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

4.6.5 Procedure

All participants in the three groups completed exactly the same procedure for the duration of the study. When the participants were recruited, they were given information about the study and told what was required of them. This included instructions that asked them not to write down their passwords, and told them not to discuss their passwords, their password choices, or the study information with others, as it would be a security breach. They also completed a questionnaire that asked for their demographic details (as shown in Table 15).

When creating passwords, the participants were taken to a series of web pages to undertake the task (shown in Figure 9). If the passwords did not meet the criteria, an error message would appear saying which rule was not met. The participants were asked to learn the newly generated passwords and were told not to write them down. After the participants created a password, they were asked repeatedly to re-enter the password until they had successfully entered it three times, to ensure that it had been learned and to reinforce the memory. For the password creation schedule, see Table 18.



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 (!@#\$%^&*()_+=-[|\,<.>/?'").
6. not contain names (e.g. JussiH1#).
7. be unique = different from every other password created, preferably different in meaning too (e.g. Bookcase1# and iloveTV1!).

*** AT NO POINT SHOULD YOU WRITE ANY PASSWORDS DOWN***

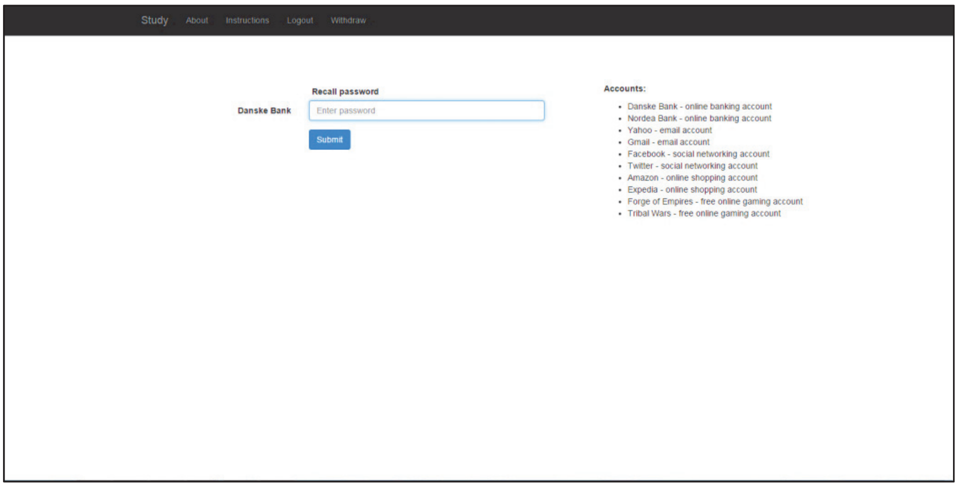
Accounts:

- Danske Bank - online banking account
- Nordea Bank - online banking account
- Yahoo - email account
- Gmail - email account
- Facebook - social networking account
- Twitter - social networking account
- Amazon - online shopping account
- Expedia - online shopping account
- Forge of Empires - free online gaming account
- Tribal Wars - free online gaming account

FIGURE 9: Password creation web page

At the password recall stage, the participants were taken to a series of web pages to recall their passwords (shown in Figure 10). These pages were visually the same as the creating pages; however, the password guidelines were not present, as they were not relevant at this point. The participants were given three attempts to recall the password. If they failed, this message appeared: “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 given this message because their lapse in memory may have been temporary, and since they may have thought that they would not need to use the password again, this would have had an effect on the password’s retention.

Regardless if they entered the passwords correctly or not, they were then taken to the next password page to recall the next password, and so on until all three passwords had been attempted. This password recall process reoccurred in all weeks. For the final session in week 12, the recalling process was the same as previous weeks; however, the participants were asked to recall all 10 passwords.



Recall password

Danske Bank

Accounts:

- Danske Bank - online banking account
- Nordea Bank - online banking account
- Yahoo - email account
- Gmail - email account
- Facebook - social networking account
- Twitter - social networking account
- Amazon - online shopping account
- Expedia - online shopping account
- Forge of Empires - free online gaming account
- Tribal Wars - free online gaming account

FIGURE 10: Password recall web page

4.7 Results

A large amount of quantitative data was collected during the 12 week study. This data could be categorized into three types that represent the each dependent variable: the total score (i.e. the total amount for the whole 12 weeks); the week 12 score (as all 10 passwords were recalled in week 12, it would be interesting to see how the participants recalled all the passwords at once); and thirdly, the overall or mean score for the whole study (week 1-11, these results do not include the week 12 scores, as they would be seen as outliers because of the amount of passwords recalled that week). The descriptive results are summarized in Table 21.

TABLE 21: Descriptive results

Mean (std. dev.)	Password group Unique group (*N*=27)			Modified group (*N*=27)			Reused group (*N*=27)		
Dependent variable	Total score (wk 1-12)	Week 12 score	Mean score (wk 1-11)	Total score (wk 1-12)	Week 12 score	Mean score (wk 1-11)	Total score (wk 1-12)	Week 12 score	Mean score (wk 1-11)
Password interference	23.19 (29.06)	6.11 (8.49)	1.29 (0.13)	41.44 (38.49)	11.52 (11.61)	2.92 (0.13)	37.00 (17,79)	9.46 (9.30)	1.85 (0.13)
Password correct recall	25.74 (12.10)	6.00 (3.40)	1.75 (0.06)	16.40 (10.49)	3.77 (2.85)	1.20 (0.06)	22.14 (7.25)	5.00 (2.25)	1.56 (0.06)

Total password recall errors	41.52 (34.21)	9,68 (7.87)	2.71 (0.17)	64.81 (31.44)	16.07 (8.86)	3.96 (0.17)	47.67 (18.62)	10.07 (5.52)	2.78 (0.17)
Acc-pw matching errors	5.11 (10.62)	0.35 (3.05)	0.34 (0.07)	12.55 (18.24)	1.04 (4.15)	0.74 (0.07)	19.62 (8.39)	1.04 (2.08)	0.91 (0.07)
Login failures	37.44 (30.69)	9.33 (9.12)	2.39 (0.15)	52.25 (29.44)	13.11 (8.12)	3.19 (0.15)	28.14 (15.91)	4.96 (4.94)	1.79 (0.15)

Initial tests were conducted to check that age did not have an effect on password interference, correct password recall, or password recall errors, between the password groups. This was confirmed through employing an analysis of variance test (ANOVA), (p = 0.16; p = 0.39; p = 0.48, respectively).

4.7.1 Coding data

The website monitored all of the creation and recall attempts, which allowed for the coding of every password entered. The system would recognize the correct password for the right account, the correct password for the wrong account, and all others errors. The password recall errors were categorized into account-password matching errors (where the correct password was recalled, but for the wrong account), and login failures (which included all other incorrect recall). Password interference included errors that were associated with other created passwords, such as in the case of account-password matching errors, and password similarities (where errors were partially associated with other created passwords – these were categorized under login failures).

4.7.2 Theory Testing

The password interference, the correct password recall, and the password recall errors were tested by analysis of variances (ANOVAs), to examine the differences between the password groups. These results included the total scores (weeks 1-12) and the week 12 scores for all of the dependent variables. Generalized linear mixed models (GLMMs) were employed to analyze the differences between the password groups as the amount of passwords increased, to represent the linear nature of the increase. The results included the mean scores (weeks 1-11) for all dependent variables. The hypotheses testing results are shown in Table 22.

TABLE 22: Inferential results

Dependent variable	Hypothesis	sig.
Password interference	H1a: Unique passwords < modified passwords or reused passwords	p = 0.009 (total score) p = 0.013 (wk12)
	H1b: Interaction: number of passwords x unique passwords < modified or reused passwords	p < 0.0005 (mean score)
Password correct recall	H2a: Unique passwords > modified passwords or reused passwords	p = 0.004 (total score) p = 0.021 (wk12)
	H2b: Interaction: number of passwords x unique passwords < modified or reused passwords	p < 0.0005 (mean score)
Total password recall errors:	H3a: Unique passwords < modified passwords or reused passwords	p = 0.013 (total score) p = 0.017 (wk12)
	H3b: Interaction: number of passwords x unique passwords < modified or reused passwords	p < 0.0001 (mean score)
Account-password matching errors	H3c: Unique passwords < modified passwords or reused passwords	p < 0.0005 (total score) p < 0.05 (wk12)
Login failures	H3d: Unique passwords < modified passwords or reused passwords	p = 0.024 (unique x modified) p = 0.166 (unique x reused)

4.7.2.1 Total Interference

Kruskal-Wallis between-subjects (ANOVA) tests were employed to test the differences in total interference between the password groups. This non-parametric test was used because of the distribution of the data. The tests showed that there was a significant effect of the password group on the total password interference, for the total study (χ^2 = 9.470, df = 2, p=0.009), and week 12 (χ^2 = 8.747, df = 2, p=0.013). Password interference was significantly higher in the modified and reused groups compared with the unique group, these results support H1a.

Using a generalized linear mixed model, total interference was analyzed as the number of passwords increased. There was a significant main effect of the password group on total interference ($F_{(2,876)}$ = 13.419, p < 0.0005). There was also a significant main effect of the number of passwords on total interference

($F_{(4,876)}$ = 104.618, p < 0.0005). The two-way interaction between the password group and number of passwords was also significant ($F_{(8,876)}$ = 5,638, p < 0.0005), supporting H1b. The total amount of interference increased as the amount of passwords increased (shown in Figure 11). By eight passwords, there was a significant difference between the unique group and the modified and reused group. However, there was no significant difference between the modified and reused group, suggesting that the unique group was affecting total interference, and further supporting the hypothesis.

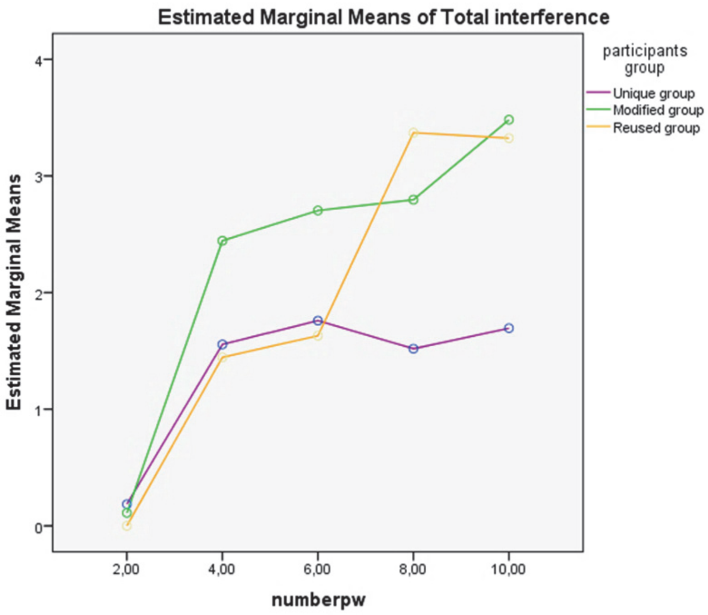


FIGURE 11: Mean scores of total password interference for each password group as the amount of passwords increases

4.7.2.2 Password correct recall

Between-subject ANOVAs were conducted to examine the effect of the password group on the password correct recall; both for the total study and in week 12. There was a significant effect of the password group on password correct recall for the total study ($F_{(2,78)}$ = 5.810, p = 0.004), and a significant effect of password group on password correct recall in week 12 ($F_{(2,78)}$ = 4.047, p = 0.021), supporting H2a. Password correct recall was the highest in the unique group, followed by the reused group, and was lowest in the modified group; this was the case for the total study scores and week 12 scores.

A generalized linear mixed model was employed to analyze the linear nature of the increasing number of passwords during the study, and its effect on password recall for all three groups. The main effect of the password group on password correct recall was significant ($F_{(2,876)}$ = 6.074, p < 0.0005). However, there was no significant main effect of the number of passwords on password correct recall ($F_{(4,876)}$ = 1.555, p = 0.184). Although, there was a significant effect between 6 and 8 passwords (p = 0.03), and 6 and 10 passwords (p = 0.028).

We believe this is due to the fact that the reused group only had two unique passwords to recall until six passwords; at that point, the number of passwords increased enough to increase the confusion between accounts – this is supported by the password interference data.

There was a gradual increase in the significance between the password groups on password correct recall as the number of passwords increased. The significant difference between the unique group and the two other groups increased when the password amount increased to eight, and continued through to ten passwords. This illustrates that the effect of the password group would be stronger in the modified and reused group compared with the unique group, decreasing the amount of password correct recall more severely as the amount of passwords increased. Therefore, as the amount of passwords increased, the effects of the password group increased too. Thus, there was a significant two-way interaction between the password group and the number of passwords ($F_{(8,876)}$ = 4.133, p < 0.0005), supporting H2b, (shown in Figure 12).

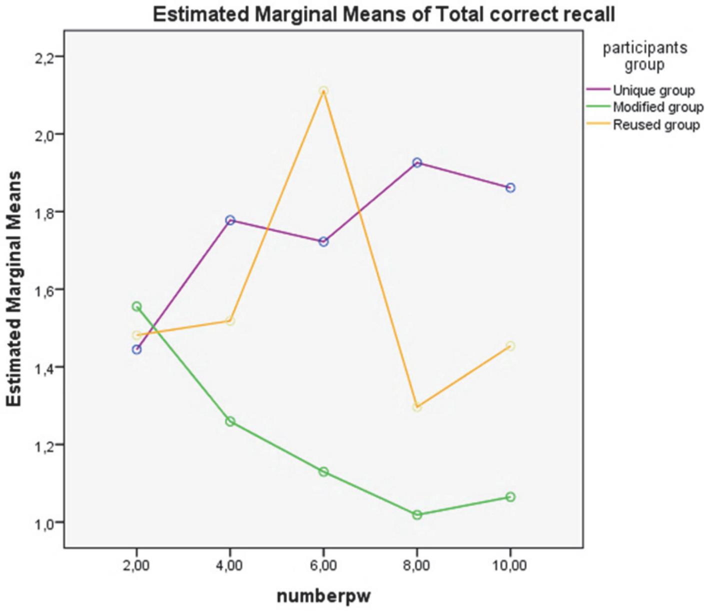


FIGURE 12: Mean scores of total password correct recall for each password group as the amount of passwords increases

4.7.2.3 Total password recall errors

Kruskal-Wallis between-subjects tests were employed to examine the effects of the password group on total password recall errors. There was a significant effect of password group on total password recall errors for the total study (χ^2 = 8.685, df = 2, p = 0.013), and for week 12 (χ^2 = 8.097, df = 2, p = 0.017), as the unique group had the lowest total password recall errors, and the modified group having the highest. These results support H3a.

A generalized linear mixed model was employed to test the effect of the number of passwords on total password recall errors in between each password group. There was a significant main effect of the password group on total password recall errors ($F_{(2,876)}$ = 17.572, p < 0.0001). There was also a significant main effect of the number of passwords on total password recall errors ($F_{(2,876)}$ = 27.777, p < 0.0001). The two-way interaction between the password group and number of passwords was also significant ($F_{(2,876)}$ = 4.104, p < 0.0001), supporting H3b (shown in Figure 13). The increase of total password recall errors was stronger in the modified and reused group compared with the unique group as the amount of passwords increased.

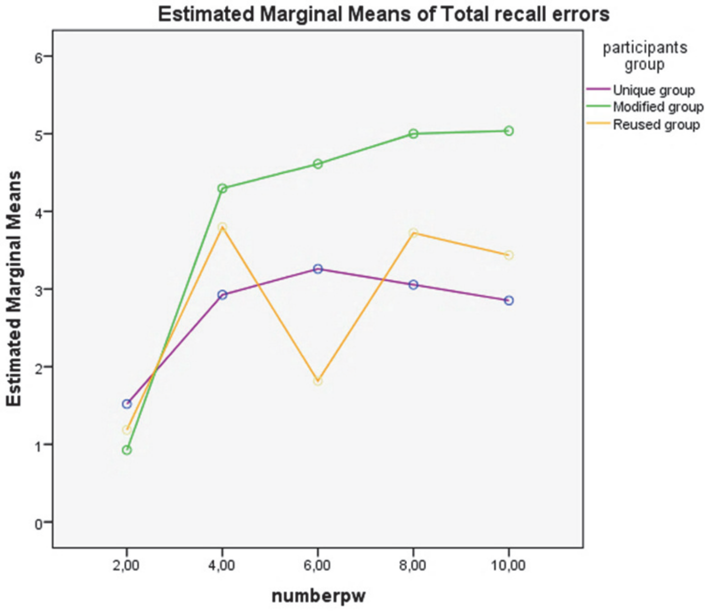


FIGURE 13: Mean scores of total password recall errors for each password group as the amount of passwords increases

Total password recall errors can be divided into account-password matching errors and login failures. These sub-factors of password recall errors are examined to fully understand the effects of password group on these errors.

Account-password matching errors

Kruskal-Wallis between-subjects tests were conducted to analyze the effect of the password group. The unique password group had the lowest score of account-password matching errors, followed by the modified group, and the reused group had the highest level of these errors (shown in Table 21). The password group had a significant effect on account-password matching errors for the total study (χ^2 = 21.642, df = 2, p < 0.0005), and in week 12 (χ^2 = 29.074, df = 2, p < 0.0005), supporting H3c.

Login failures

The unique password group had a lower login failure rate when compared with the modified group. The reused group had the lowest rate of login failures across all three groups. Mann-Whitney U tests (non-parametric t- test) were performed to analyze the differences between the unique group and the modified group, and the unique group and the reused group. There was a significant difference between the unique group and the modified group in login failures (U=250.500, N_1=27, N_2=27, p = 0.024, one-tailed), which supports H3d. Even though the reused group had a lower login failure score, it was not significantly lower than the unique group (U=308.500, N_1=27, N_2=27, p = 0.166, one-tailed). We believe that the reused group had a low score due to the high level of account-password matching errors. Having a lower login failure rate does not mean that the reused group had a higher level of total password correct recall. It indicates that, out of the total number of incorrect password recall errors, the reused group had a higher level of account-password matching errors than login failures when compared with the other groups. This would make sense as the reused group had three unique passwords for seven accounts, which could cause confusion between accounts, whereas the modified group had similar passwords which could cause confusion between the passwords themselves. Although, H3d is not supported, the overall total password recall errors are significantly higher in the modified and reused groups compared with the unique group. Analyzing the account-password matching errors and login failures sub-factors just illustrate the different effects of adopting different password behaviors (such as adopting unique, modified or reused passwords) has on the total password recall and errors.

4.7.3 Further analysis

When designing the study, several aspects of password creation and recall were taken into consideration. To ensure that cognitive load would not be a factor in learning passwords, the maximum of two passwords were created at one time, over eight weeks. Similarly, a longitudinal design was used for password recall as well, to reflect the long period of creation of passwords, but also to allow for the manipulation of password recall frequency and the time between recall tasks.

Further analysis was performed to see whether there was an effect of the number of times in which the passwords were recalled (or frequency of password recall), and the time between the recall tasks on password correct recall and password interference. Passwords were recalled for each account between 3-6 times over the 12 weeks, with a variety of time between recall tasks.

Although the frequency of password recall showed to have a significant effect on password correct recall and password interference, it did not have a meaningful effect, i.e. as the frequency increased. To confirm these findings, deeper analysis was performed. The Facebook account had the highest number of times in which the passwords were recalled (six times), and Gmail had one of the lowest (three times). The results showed there was no significant difference in password correct recall, or password interference between the two accounts. To further confirm this, Facebook and Twitter (also recalled three times) were examined, and the results showed that there was a difference between the two accounts, in this instance. When looking at the schedule, the Twitter passwords had been recalled twice in succession, which led to the questioning if the time between recall tasks had an effect. The results showed that, for instance, between Nordea (which had three weeks between the recall task) and Yahoo (one week), there was no difference in password correct recall or interference. Between Forge of Empires and Tribal Wars, there were no weeks between recall tasks from week 11 to 12, and there was no difference; and between Expedia (two weeks) and Forge or Empires (zero weeks) there was no difference either. This would suggest that the time between recall tasks or possibly the frequency of recall within a period of time would not have an effect on password correct recall or interference. To confirm this further an analysis of the week 12 password correct recall and interference was performed. There was no significant effect. One would think that the recall performance would be greater in the Forge of Empires passwords as there were three successive recall tasks, weeks 10, 11, 12, and the passwords had been recalled five times over the 12 weeks; however in comparison with Danske passwords, they had been recall also 5 times, but there had been four week between recall tasks in week 7 and week 12. Danske account had a higher password correct recall.

These results suggest that the amount of times in which you recall your passwords or the time between recalling passwords does not have an effect of password correct recall. However, as this was not the main focus of this paper, a much more in-depth study of this will give more precise findings.

4.8 Discussion

4.8.1 New Contributions

Previous IS security research suggests that unique passwords are harder to remember than reused or modified passwords, and therefore insecure password behaviors (such as reusing and modifying passwords) are considered a reasonable coping strategy (Biddle et al., 2012; Chiasson et al., 2009; Duggan et al., 2012; Gaw & Felten, 2006). This study proposed the Unique Password Theory, which demonstrates that multiple unique passwords are actually easier to remember than reused or modified passwords. The theory maintains that password reuse and modification should not be used as a memory coping strategy, especially as it can reduces password security. Next, we discuss the new contributions of the study in more detail.

As the first contribution, the empirical results support the Unique Password Theory suggesting that, by adopting multiple unique passwords, each password will be more memorable than modified or reused passwords. The unique password group had a significantly higher level of password correct recall then the modified and reused groups. So too, as the number of passwords increased, the unique group's correct recall rate was 10% higher than the reused group for the total study, as well as in week 12. This was surprising, as the reused group (in theory) only had three passwords to recall (but had to recall them for seven other accounts). The unique group also correctly recalled 25% more passwords than the modified group in week 12, and 22% for the whole study. These findings challenge some previous studies and users' beliefs that password reuse increases memorability (Duggan et al., 2012; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). Moreover, Grawemeyer and Johnson (2011) found that unique passwords were associated with login failures and mismatching the correct password to the right account. We explain these conflicting results through the acknowledgment of the different research methodologies and settings. For example, Duggan et al. (2012) and Grawemeyer and Johnson (2011) used interviews and diary studies, while Notoatmodjo and Thomborson (2009) used surveys to report participants' difficulty in remembering their passwords. Such methods basically express the users' subjective beliefs and are not based on observing users' actual password behaviors directly from the system, as adopted in our study. The results of our study demonstrate that users can remember unique passwords better than reused or modified passwords.

The second new finding was that adopting multiple unique passwords has a negative effect on total password recall errors compared with reused and modified passwords. The unique group had a lower level of total password recall errors, when compared to the reused group (5% lower for the total study). The modified group's total password recall errors rate was 15% higher than the unique group for the total study. When examining the results in more detail, there are some surprising findings that showed that different types of multiple passwords (unique, reused, or modified) affected different types of recall errors (account-password matching errors or login failures). Adopting unique passwords had a negative effect on account-password matching errors (correct password, but wrong account), and as the amount of passwords increased so did the significance between the three password groups. The reused group had a significantly higher level of account-password matching errors, being 39% more than the unique group, and the modified group was also 20% higher than the unique group. The login failures (which included all other incorrect recall) however, had a different distribution as the modified group had 13% higher login failures than the unique group; but the reused group had an 8% lower level of login failures compared with the unique group. This type of recall error distribution would make sense when considering that modified passwords, comprise of characters that are similar to each other, e.g. Password1! and Password2&. Therefore, the amount of login failures for modified passwords would be higher than account-password matching errors, as the interference would be between the password details. When considering reused passwords, there were only three unique passwords reused for seven accounts, and therefore the interference would be higher between the accounts, causing a higher level of account-password matching errors. Because reused passwords are more affected by high levels of account-password matching errors, there was no significant difference in login failures between the reused group and the unique group. Despite the fact that the hypothesis regarding the login failures was not supported, the total password recall errors (overall) was still significantly lower in the unique group compared with both other password groups. Further to that point, higher levels of total password recall errors in the reused group compared with the unique group, highlights that interference has a stronger effect on password recall, than the effect of the frequency that the password is recalled.

The third new finding revealed that there was a significant effect across all of the dependent variables, from unique passwords as the amount of passwords increased. These results are important, as with time, users will continue to accumulate more accounts and therefore, more passwords (Gaw & Felten, 2006). This will lead to further insecure password practices and the resulting security risks if the relationship between this increase in the amount of passwords and the effect on correct recall, interference, and recall errors is not fully understood. Password correct recall was significantly affected by adopting unique passwords; however, the number of passwords was not solely a significant factor. This finding could suggest that there is no limitation to the amount of passwords a user can store, and potentially recall, as the long-term memory is unlimited. Furthermore, as the amount of password increased the significance level also increased, demonstrating that by adopting reused or modified passwords, password correct recall will decline more strongly as the amount of passwords increase compared with multiple unique passwords. Additionally, password interference was significantly affected by the number of passwords, which supports the findings of Baddeley and Hitch (1977), when they examined interference and the memorability of the number of items, in other contexts than password security. Likewise, the total password recall errors was significantly affected by the increase in the number of passwords, showing that an increase in passwords can also result in an increase in errors too.

Overall, the results of this study support the proposed Unique Password Theory. This theory demonstrates that through a greater understanding of the functionality of the human memory, this can lead to increased memorability of passwords, which can ultimately lead to better password security practices.

4.8.2 Implications for practice

Previous research suggests that users frequently modify (Adams & Sasse, 1999), and reuse passwords (Duggan et al., 2012; Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009). This is because users believe that they will increase password memorability (Bang et al., 2012; Duggan et al., 2012; Notoatmodjo & Thomborson, 2009). The results of this study support the Unique Password Theory that actually suggests the opposite, proposing that unique passwords are more memorable than reused or modified passwords. However, if users were made aware of why password reuse and modification does not increase password memorability, they could understand that memory limitations are no longer an excuse for adopting insecure password practices. The implications for practice are two-fold: for organizations and for home-users. Within an organization, increased password memorability and memory awareness could result in increased policy compliance, with regards to creating unique passwords (required in a number of password policies); creating stronger passwords, and the reduced need to write passwords down (Biddle et al., 2012; Chiasson et al., 2009; Duggan et al., 2012; Gaw & Felten, 2006). Other implications for organizations are that their information assets would be more secure; and through a reduction in password reuse and increased better password security practices, organizations are less likely to have security breaches, and the security risks that accompany them. Further implications for organizations stem from the increased memorability of unique passwords: if passwords are more memorable, then less time and money would be spent on the consequences of forgetting them, such as when passwords are reset.

For home-users, the practical implications of increased password memorability and memory awareness could first lead to reduced insecure password behaviors, such as reuse and writing passwords down. It could also increase secure password practices, such as creating stronger passwords. Second, less time, inconvenience and money would be spent on the consequences of forgetting passwords. Third, through adopting unique passwords, personal and organizational information could be more secure, and reduce the consequences of security breaches, through the reduction of reuse behavior and forgetting passwords.

4.8.3 Limitations and future research

Quantitative methodology is considered to be beneficial in the pursuit of a greater understanding of IS phenomena, with both strengths and weaknesses. However, it is believed that “all methods of science are flawed” (Dennis & Valacich, 2001, pp. 4). Research studies may have different and sometimes conflicting goals, which include generalizability (to populations), realism (for the participant), and precision (control over what is being measured) (McGrath, 1982). For example, Nobel Prize winner Friedman (1953) regarded precision to be more important than realism in science. In IS research, laboratory experiments rank between the second and third most popular method of data collection in the AIS basket of top academic journals (Liu & Myers, 2011). This methodology is commonly used due to the level of precision it offers when measuring independent variables (Dennis & Valacich, 2001; Liu & Myers, 2011). In this current study, a laboratory methodology was chosen as participants' memories were being tested; and therefore, an experiment with high precision was seen as important. Furthermore, previous password studies usually employ a laboratory methodology (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009), as creating and recalling passwords in a realistic setting would have security issues. These issues are in relation to unauthorized access to participants' accounts, and limitations in what details could be monitored, in terms of password interference. When designing the experiment, we considered many issues that would increase the realism of the design. The longitudinal design was employed to not only study how passwords were recalled over a period of time, but so that not all passwords were learned at the same time, as this would have an effect on cognitive load. Ten passwords were created and recalled, as five (used in many studies, (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009)) are not similar to the real-world situation, as many users have more than ten passwords (Zhang et al., 2009). A range of accounts were used to mimic the real-world setting, and to represent the different levels of importance and sensitivity of accounts. A website with an account-password design was employed to collect the data, as this is generally used by users on a daily basis. These elements of the design increased the realism of the study; however, it would, for security reasons, have been impossible to conduct this study in a real-world setting and still capture the precision in our data.

Another limitation of this study refers to password strength. Although the password rules did impose a level of strength across all groups: length (more than eight characters), and complexity (upper and lower case letter, numbers, and punctuation); additional password strength from random passwords, or a maximum length was not monitored or imposed between groups, as this study was a test of memorability.

Notwithstanding all the meticulous considerations in the development and design of this experiment, it was not without its shortcomings. The participants, after they had created their passwords could have written them down. However, within the instructions they were asked not to write down their passwords, and were told not to discuss their passwords, their password choices, or the study information with others, as it would be considered a security breach. In addition, on the password creation screen, they were reminded not to write their passwords down for security purposes. Furthermore, the exact purpose of the study was not revealed to the participants: they were told that they were taking part in a study that was testing a new password input system. This deception was employed so that the participants were aware that it was important to remember the passwords, but they were not overly conscious of the fact that their memory was the focus of the study. If they had known, this may have led to a bias in the results.

There is a deficiency of empirical studies examining multiple password behavior over a longer period of time. This study is one of the first longitudinal password studies that not only included creating many passwords over many weeks, but also recalling them several times over those weeks too. It can be argued that this is a more realistic setting than those studies in which the passwords are created all at once (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009). Learning all the passwords at one time increases cognitive load, which, in-turn decreases memorability (Baddeley, 1992). This said, it is arguable whether these studies were ultimately testing password memorability or the effect of cognitive load on password learning.

We propose the following future studies to examine password recall with a longitudinal design: within our study, several participants were able to learn and recall their 10 passwords with reasonable success; in week 12, 45% of the unique group recalled all 10 passwords correctly. These results suggest that we should have considered using 15 passwords, or even more, to really push the participants' memories, to demonstrate password memorability and the effects of password interference. Future studies can look to having larger numbers of passwords, because as we accumulate more and more accounts, the number of passwords is only set to rise. With this in mind, future studies should not only look at multiple password recall for higher numbers of passwords, but also to increasing numbers of passwords, and the effects on password recall as these numbers increase. This will give a more deep understanding of how change from increasing numbers of passwords affect password memorability.

The next proposal for future research concerns how previous password studies have categorized passwords. Previous studies have used less stringent definitions, for example, modified passwords being defined as reused passwords (Gaw & Felten, 2006), or even unique passwords (Duggan et al., 2012). The strict categorization of password types/adopted behavior (i.e. unique, modified and reused) in this study was imperative, to fully test the effect of password interference, because of the nature of the interference effect. This was also apparent when examining the level of password recall errors in each group. Future research should categorize their passwords more carefully, especially if they are examining the interference effect, as it may affect their results.

We finally propose, based on our initial results of password recall frequency and time, that these elements should be investigated further. Our findings suggest that frequency of recall or time between recalling passwords does not have an effect on password correct recall, or password interference. However, this was not the focus of the study, and it is necessary to examine these factors in much more detail.

4.9 Conclusions

As the amount of passwords increase over time, users believe that their memory cannot cope. This can influence their password behavior, for example, resulting in password reuse and writing down passwords. This study provides a new perspective in understanding the password problem, by looking to the interference effect to manipulate the memorability of multiple passwords, while not concurrently compromising user security. The Unique Password Theory states that unique multiple passwords are more memorable than modified or reused passwords. The results from a 12-week study suggest that not only were the unique passwords more memorable, they reduced password recall errors and password interference.

The Unique Password Theory and the results of this study have new important implications for IS password practice. First, while unique passwords are not necessarily stronger, they are still considered more secure when compared with reused or modified passwords; as discussed in the password reuse literature (Adams & Sasse, 1999; Duggan et al., 2012; Gaw & Felten, 2006; Ives et al., 2004; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). However, many users chose to adopt password reuse and modification to aid their password memorability. The results reveal that password reuse and modification does not increase password memorability, and should not be adopted to cope with multiple password memorability. Second, unique passwords increase the memorability of passwords, which potentially could lead to the reduction of some other insecure password behaviors, such as choosing weak passwords or writing passwords down. Finally, multiple unique passwords are less easily forgotten than reused or modified passwords, and therefore unique passwords minimize the consequences of forgetting passwords (e.g. increased IT helpdesk costs). Future research should examine the effects of multiple passwords (more than 10 passwords), and increasing numbers of passwords (such as the effects as the amount of passwords rise), and apply a longitudinal research setting.

5 SUMMARY

5.1 Key findings

This dissertation contributes to the field of Information Systems Security, as it studies password security, an important part of information security. Through examining cognition, it allows us to understand password security behaviors; and more importantly, develops new theories and modifies significant cognitive scientific theories, for the IS context.

Several password studies have collected their data through means of subjective surveys or diary studies, asking users to give their opinions of their password management and behavior (Bang et al.; 2012; Duggan et al., 2012; Grawemeyer & Johnson, 2011; Notoatmodjo & Thomborson, 2009). This subjective data does not capture the "true" picture, because all users have some opinion, story, or experience about using passwords. In my studies the data was objectively driven, collecting and measuring password recall. This objective data gave an interesting and insightful picture into password behavior. However, it was still complimented by subjective survey data. The findings of these studies make counterintuitive suggestions based on not what users believe, but on what they actually do, which will hopefully contribute towards solving the password problem.

From the first study, the results showed that there was no relationship between password recall and memory performance; and there were no relationships between password recall or memory performance and password reuse. What this means is that password recall is not based on how good a user's memory is. It also means that not being able to recall passwords is no excuse for password reuse. Furthermore, there were differences in the metamemory constructs that predict memory performance, compared to password recall performance, supporting that password recall cannot be considered like other memory recall. Moreover, password reuse could be predicted by the metamemory construct of anxiety, which suggests that users reuse their passwords, not because they cannot remember them but because they have an anxiety about remembering them. From the second study, it was found that as the number of verification times increased, so too did password recall, while not compromising user convenience. The key finding was that, although previous research suggests that there is a "trade-off" between memory and convenience, my results does not support that. There were several key findings from the third study. The results showed that unique passwords were more memorable than reused and modified passwords; that there was less login errors; and as the number of passwords increased so too did the benefits of using unique passwords compared with reused and modified passwords. Furthermore, due to reused and modified passwords being a security risk, through using unique passwords, users could be more secure than if they adopted reuse and modification. The key findings supported the Unique Password Theory, making counterintuitive suggestions that the "trade-off" between memory and security is not as inflexible as previous research suggests; and that password reuse is in fact not a good coping strategy for users wanting to increase their password memorability.

The overall key findings of this dissertation is that through collecting predominately objective password recall data, interesting and counterintuitive results suggest that users' preconceptions of their password management and behavior is not based on their subjective understanding of their memory and security behavior. Furthermore, the trade-off that researchers suggest is not supported by this body of research. This could due to several studies being based on subjective user data (Bang et al.; 2012; Duggan et al., 2012; Notoatmodjo & Thomborson, 2009), and/or not fully understanding or applying memory theory correctly (Bang et al., 2012; Notoatmodjo & Thomborson, 2009).

5.2 Practical Implications

There are important practical implications for this dissertation and all three studies. This is through providing empirical evidence to support better security practice guidelines (e.g. creating unique passwords); through providing practical suggestions for increasing the memorability of passwords (e.g. repetition, and creating unique passwords); and through providing a more deep understanding of how users' memories effect their password recall (unique passwords), and how users' perceptions of their memory affect their password recall (metamemory).

All three studies have the same objectives, and therefore have the same implications for both organizations and to individual users. The findings support that through a better understanding of the human memory can inform users to adopt better password security practices. The results suggest how to make passwords more memorable; how to reduce password forgetting, which will reduce the consequences of forgetting (such as IT helpdesk costs), and the fear of forgetting which results in users adopting insecure password behaviors:

So too, it will therefore reduce insecure password behaviors adopted and the consequences of these behaviors (such as security breaches).

5.3 Limitations

Although the studies of this dissertation were designed meticulously, they were not without their limitations. All three studies had similar limitations: through them being laboratory experiments, they may have had higher levels of precision and control over the variables (Dennis & Valacich, 2001; Liu & Myers, 2011); however, they (like most laboratory experiments), lacked realism and generalizability (McGrath, 1982). Nevertheless, as objective memory data was being collected and measured, the precision from the laboratory design was of most importance. On the other hand, it would have also been difficult to run these studies in the "real-world" setting, as collecting password data would have been a security issue, and would have ultimately affected the results. Even so, while designing the studies, realism was taken into consideration, by means of employing a longitudinal design. Several password studies require their participants to learn and recall several passwords all at once (Nelson & Vu, 2010; Vu et al., 2007; Wiedenbeck et al., 2005; Zhang et al., 2009). This would, firstly, effect cognitive load and therefore learning and recall; and secondly, it is rare that users are required to learn and recall several passwords in the real-world, and hence, a longitudinal design being more realistic.

The second limitation arose from attempting to make the studies more realistic. The studies were completed online, and although there were instructions and warnings of security breaches if participants took note of their passwords, they still could have broken the rules. However, even if they had untaken the tasks with researcher supervision, there could have still been the possibility that the participants could have written the password down after leaving the researchers' supervision.

A third limitation would refer to password strength. This research was interested in testing password memorability. And although, password strength was imposed throughout all three studies via password guidelines and restrictions; it was not the focus of the work, and no further measurement was taken.

5.4 Future research

Due to the complexity of the human memory and the complexity of the password process, and its effect on password behavior, there are a number of future studies, I will suggest.

Firstly, based on methodological design, all three studies noted the importance of longitudinal methodology, and propose that future research adopts the same approach to measuring objective password recall.

Further suggestions for future research from each study include examining the effects of increasing numbers of verification when creating passwords on passwords recall and user convenience, this to see whether password verification can actually be increased enough where password memorability is no longer a problem while it not being inconvenient. Another suggestion would be to increase the number of passwords participants have to learn and recall, and their effect on interference. This would give a really good indication to the significance of the problem of password interference, especially when considering that the number of passwords is rising. Another suggestion is to look at the effect of frequency and recall times of passwords on password memorability. There is the assumption that the amount of times in which you recall your passwords or the time between recalling passwords has an effect of password correct recall; however, our results suggest otherwise. Therefore, objective data needs to be collected to verify these assumptions. Future research could examine user convenience in more depth, looking to develop a model, and possibly operationalize it from the perspective of motivation.

This dissertation looked to a variety of elements of memory that could affect password memorability and behavior. Suggestions for future research from the perspective of the thesis as a whole, examining cognitive scientific theories to increase password memorability, while not decreasing password security should look to alternative memory theories, and psychological/cognitive science theories to explain and examine the interaction between password memorability and behavior. These could include examining cognitive load more deeply and its effect on learning passwords; enhancing long-term working memory to increase learning and recalling passwords; motivation in learning and recalling passwords; user personality, especially in terms of risk-taking behavior; the effects of attention on password creation; stress caused by the password process on password memorability; user emotional states on password memorability and behavior. Furthermore, research could look more closely at the effect of user anxiety on password recall, and insecure password behavior. These are just some suggestions; but ultimately, future research should examine in more detail the interactions between password security, memorability and user convenience.

6 CONCLUSION

With a rise in internet usage, social networking and ecommerce, passwords have become an essential mechanism for ensuring the security of our personal and organizational information, finances, and communication (Bang, et al. 2012; Vu, et al., 2007). However, as the number of passwords rise, so do users' insecure password practices to cope with the memorability of multiple passwords (Gaw & Felten, 2006; Notoatmodjo & Thomborson, 2009; Zhang et al., 2009). This research has examined memory theories to not only increase the memorability of passwords, but to improve also the security of them. This dissertation examined metamemory to gain a better understanding of how users' beliefs about their memory can affect their password memorability and insecure password behaviors. It then looked to increase the memorability of passwords through improving learning (repetition through password verification), and retrieval (through uniqueness); while not compromising the security of passwords. By collecting objective password recall data, the results of these studies challenge users' preconceptions about justifying their adoption of insecure password behaviors. Furthermore, it challenges the assumption of trade-offs between password security, memorability and user convenience. In meeting the objectives of the dissertation, this research has significant practical implications for organizations and individual users. Through a greater understanding of the human memory this can inform users to adopt better password security practices. The implications of these results suggest how to increase password memorability, how to decrease password forgetting, and how to decrease insecure password behaviors and the consequences of such insecure behaviors (such as security breaches).

YHTEENVETO (FINNISH SUMMARY)

Useiden salasanojen käyttäminen on kasvava turvallisuusriski, joka vain pahenee ajan kuluessa. Yksi merkittävimmistä useiden salasanojen käyttämisen vaaratekijöistä on ihmisen muisti ja käyttäytymismallit, joilla kompensoidaan salasanojen muistamisen ongelmia. Tutkimalla muistin aspekteja, jotka vaikuttavat käyttäjien salasanojen muistamiseen, voidaan lisätä ymmärrystä käyttäjistä ja tehdä ehdotuksia siitä, miten salasanojen todentamismekanismien turvallisuutta voisi parantaa. Tässä väitöskirjatutkimuksessa tutkitaan ihmisen muistia, jotta voitaisiin ymmärtää salasanojen tietoturvallisuuteen liittyvää käyttäytymistä. Tavoitteena on myös luoda kokonaan uusi teoria ja kehittää jo olemassa olevia, yleisesti hyväksyttyjä muistiteorioita salasanakontekstissa. Tutkielma käsittelee muistiteorioita tavoitteenaan kehittää salasanojen tietoturvan tasoa ja lisätä salasanojen muistettavuutta. Väitöskirja pohjautuu löydöksiin kolmesta eri tutkimuksesta, joissa tutkitaan käyttäjien uskomuksia ja tietoisuutta (metamuistia) oman muistinsa vaikutuksista salasanojen muistamisessa ja heikon turvallisuustason salasanakäyttäytymisessä sekä pyritään parantamaan salasanojen muistettavuutta kehittämällä oppimista (vahvistuksen toistot), ja helpottamaan muistihakuja (ainutlaatuisuus). Empiirisillä pitkittäistutkimuksilla mitataan salasanojen (yli 10 000 salasanaa) muistamista, muistin väliintuloa, muistin suorituskykyä, muistiuskomuksia, käytön mukavuutta sekä heikon tietoturvatason salasanakäyttäytymistä. Keräämällä objektiivista tietoa salasanamuistikokemuksista tutkimukset haastavat käyttäjien ennakkokäsityksiä, jotka osaltaan ovat toimineet oikeutuksena heikon tietoturvatason käyttäytymismallien omaksumiselle. Löydökset haastavat myös yleistä olettamusta siitä, että tietoturvatasoltaan kehittyneet salasanat ovat muistettavuudeltaan sekä käyttömukavuudeltaan heikkoja. Tämän väitöskirjatutkimuksen tuottamalla syvällisellä ymmärryksellä on merkittäviä organisaatio- ja yksilötason vaikutuksia, joiden perusteella käyttäjät voivat kehittää salasanakäyttäytymisensä tietoturvatasoa. Tulokset ohjaavat käyttäjiä parantamaan salasanojen muistettavuutta, vähentämään salasanojen unohtamista, luopumaan heikon tietoturvatason salasanakäyttäytymisestä sekä ymmärtämään tietoturvapuutteiden, kuten tietoturvarikkeiden, seuraamuksia.

REFERENCES

Abrahamsen, A., & Bechtel, W. (2012). History and core themes. In K. Frankish & W. Ramsey (Eds.), *The Cambridge handbook of Cognitive Science* (pp. 9-28). Cambridge & New York, NY: Cambridge University Press.

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, April). Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. In *Enhanced Security with Passwords & CAPTCHAs – CHI '15*, (pp. 2315-2324). Seoul, Republic of Korea.

Anderson, M. (2009^{a}). Retrieval. In A. Baddeley, M. Eysenck & M. Anderson, *Memory*. Hove & New York, NY: Psychology Press.

Anderson, M. (2009^{b}). Incidental forgetting. In A. Baddeley, M. Eysenck & M. Anderson, *Memory*. Hove & New York, NY: Psychology Press.

Anderson, M., Bjork, R. A., & Bjork, E. L. (1994). Remembering can cause forgetting: Retrieval dynamics in long-term memory. *Journal of Experimental Psychology: Learning, Memory and Cognition, 20*, 1063-1087.

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

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.

Baddeley, A. (1992). Working memory. *Science*, *255*, 556–559.

Baddeley, A. (2000). The episodic buffer: A new component of working memory? *Trends in Cognitive Sciences, 4*(11), 417-423.

Baddeley, A. (2009^{a}). What is Memory? In A. Baddeley, M. Eysenck & M. Anderson, *Memory* (pp.1-18). Hove & New York, NY: Psychology Press.

Baddeley, A. (2009^{b}). Short-term Memory. In A. Baddeley, M. Eysenck & M. Anderson, *Memory* (pp.19-40). Hove & New York, NY: Psychology Press.

Baddeley, A. (2009^{d}). Learning. In A. Baddeley, M. Eysenck & M. Anderson, *Memory* (pp. 69-92). Hove & New York, NY: Psychology Press.

Baddeley, A. (2009^{e}). Episodic memory: organizing and remembering. In A. Baddeley, M. Eysenck & M. Anderson, *Memory* (pp. 93-112). Hove & New York, NY: Psychology Press.

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

Baddeley A., & Longman, D. (1978). The influence of length and frequently of training sessions on the rate of learning to type. *Ergonomics, 21,* 627-635.

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.

Bartlett, F. C. (1932). *Remembering: A Study in Experimental and Social Psychology*. New York: Cambridge University Press.

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.

Bonneau, J., & Preibusch, S. (2010, June). The password thicket: Technical and Markey failures in human authentication on the web. In *9th Workshop on the Economics of Information Security - WEIS 2010,* (pp.1-40). Boston, MA.

Brostoff, S., & Sasse, M, (2000). Are Passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV – Usability or Else!* (pp. 405-424). Springer London.

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, January). Password Composition Policy: Does Enforcement Lead to Better Password Choices? In *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.

Chase, W., & Ericsson, K. (1982). In A. Baddeley, M. Eysenck & M. Anderson, *Memory*. Hove & New York, NY: Psychology Press.

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., Forget, A., Stobert, E., Van Orschot, P. C., & Biddle, R. (2009, November). Multiple password interference in text passwords and click-based graphical passwords. In *16th ACM conference on Computer and communications security* (pp. 500-511). ACM.

Colquitt, J. A., & Zapata-Phelan, C. P. (2007). Trends in theory building and theory testing: A five decade study of the Academy of Management Journal. *Academy of Management Journal 50*(6), 1281.

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.

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

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.

Crowder, R. G. (1976). *Principles of learning and memory.* (Lawrence Erlbaum Associates, Hillsdale, NJ).

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems (20)*, 643–658.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence perspective. *Information Systems Research 20*(1), 79–98.

Davis, F. (1987). User acceptance of information systems: the technology acceptance model (TAM). *University of Michigan Business School*.

Dennis, A., & Valacich, J. (2001). Conducting research in information systems. *Communications of the AIS, 7*(5), 1–41.

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

DiMaggio, P. J. (1995). Comments on 'What Theory is Not. *Administrative Sciences Quarterly, 40*(3), 391-397.

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

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.

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

Einstein, A. (1930). *Religion and science*. New York Times Magazine. (Nov 9).

Emm, D. (2010). How secure are your passwords? *Infosecurity Magazine*. Retrieved October 01, 2013, from http://www.infosecurity-magazine.com/view/13175/comment-how-secure-are-your-passwords.

Ericsson, K., & Kintsch, W. (1995). Long-term working memory. *Psychological Review, 102*(2), 211-245.

Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. (2009, April). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *SIGCHI Conference on Human Factors in Computing Systems* (pp. 889-898). ACM.

Eysenck, M. W. (1979). Depth, elaboration, and distinctiveness. In L. S. Cermak & F. I. M. Craik (Eds.), *Levels of processing in human memory* (pp. 89-118). Hillsdale, NJ: Erlbaum.

Eysenck, M. W. (2009). Improving your memory. In A. Baddeley, M. Eysenck & M. Anderson, *Memory* (pp.357-380). Hove & New York, NY: Psychology Press.

Eysenck, M. W., & Eysenck, M. C. (1980). Effects of processing depth, distinctiveness, and word frequency on retention. *British Journal of Psychology, 71*, 263–274.

Eysenck, M. W., & Keane, M. (2010). *Cognitive Psychology* (6th ed.). Psychology Press, Hove & New York, NY.

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

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 R. V. Kail & J. W. Hagen (Eds.), *Perspectives on the development of memory and cognition*. Hilldale, NJ: Erlbaum.

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

Friedman, M. (1953). The Methodology of Positive Economics. In D. M. Hausman (Ed.). *The Philosophy of Economics: An Anthology*, (3rd Eds.) (pp. 145-178). Cambridge & New York, NY: Cambridge University Press.

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

Garrison, C. (2006, September). Encouraging good passwords. In *3rd annual conference on Information security curriculum development* (pp. 109-112). ACM.

Gaw, S., & Felten, E. (2006, July). Password management strategies for online accounts. In *second symposium on Usable privacy and security* (pp. 44-55). ACM.

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.

Godfrey-Smith, P. (2003). *Theory and Reality*. University of Chicago Press, Chicago.

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

Gottschalk, P. (1999). Implementation predictors of strategic information systems plans. *Information & Management, 36*, 77-91.

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

Groome, D., with H. Dewart, et al. (1999). *An Introduction to Cognitive Psychology: Processes and Disorders.* London & New York, NY: Psychology Press.

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

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*, 320–326.

Harris, J. E. (1980). Memory aids people – 2 interview studies. *Memory and Cognition, 8*, 31-38.

Hayashi, E., Pendleton, B. A., Ozenc, F. K., & Hong, J. I. (2012, May). WebTicket: account management using printable tokens. In *SIGCHI Conference on Human Factors in Computing Systems* (pp. 997-1006). ACM.

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

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

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.

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

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

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*, 83-95.

Infosecurity Magazine, (2014). Password Misuse is Rampant at US Businesses. Retrieved August 01, 2014, from http://www.infosecurity-magazine.com/news/password-misuse-is-rampant-at-us/.

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

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.

Laudan, L. (1978). *Progress and Its Problems: Towards a Theory of Scientific Growth*. University of California Press, London.

Laudan, L. (1996). Beyond positivism and relativism: Theory, method, and evidence. Westview Press.

Landauer T. K., & Bjork, R. A. (1978). In A. Baddeley, M. Eysenck & M. Anderson, *Memory*. Hove & New York, NY: Psychology Press.

Lezak, M. D. (1995). *Neuropsychological Assessment* (3rd ed.), New York & Oxford: Oxford University Press.

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*. Harlow: Pearson Education Ltd.

Liu, F., & Myers, M. D. (2011). An analysis of the AIS basket of top journals. *Journal of Systems and Information Technology 13*(1), 5 – 24.

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

McLeod, P., Plunkett, K., & Rolls, E. (1998). The Attraction of Parallel Distributed Processing for Modelling Cognition in *Introduction to Connectionist Modelling of Cognitive Processes*, Oxford University Press.

McGrath, J. E. (1982). Dilemmatics: The Study of Research Choices and Dilemmas. In J. E. McGrath, (Ed.), *Judgment Calls in Research* (pp. 69-80). Beverly Hills, CA: Sage.

McMurtrie, H., Baxter, J. S., Obonsawin, M. C., & Hunter, S. C. (2012). The relationship between memory beliefs, compliance and response change within a simulated forensic interview. *Personality and Individual Differences, 52*, 591-595.

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.

Morris, R., & Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM, 22*(11), 594-597.

Nagel, E. (1979). *The Structure of Science.*, Indianapolis, IN: Hackett Publishing Co.

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

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.

Niiniluoto, I. (1993). The aim and structure of applied research. *Erkenntnis, 38*(1), 1-21.

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

Notoatmodjo, G., & Thomborson, C. (2009, January). Passwords and perceptions. In *Seventh Australasian Conference on Information Security-Volume 98* (pp. 71-78). Australian Computer Society, Inc.

O'Sullivan, J. T., & Howe, M. L. (1995). Metamemory and memory construction. *Consciousness and Cognition, 4,* 104-110.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which Factors Explain Employees' Adherence to Information Security Policies? In *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.

Popper, K. (1980). *The Logic of Scientific Discovery*. Unwin Hyman, London.

Proctor, R., Lien, M., Vu, K., & et al. (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 K. Frankish & W. Ramsey (Eds.), *The Cambridge Handbook of Cognitive Science*. Cambridge & New York, NY: Cambridge University Press.

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. Paris: Presses Universitaires de France.

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.

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

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.

Saariluoma, P. (2003). Apperception, content-based psychology and design. In U. Lindeman, (Ed.), *Human Behavior in Design* (pp.72-78). Berlin: Springer.

Saariluoma, P. (2005). Explanatory frameworks for interaction design. In A. Pirhonen, H. Isomäki, C. Roast, & P. Saariluoma (Eds.), *Future Interaction Design* (pp.67-83). London: Springer.

Saastamoinen, A. (2014). Lomalla unohtuneet salasanat tulevat työnantajille kal liiksi – jopa satojen tuhansien kustannukset. Retrieved September 24, 2015, from http://yle.fi/ylex/uutiset/lomalla_unohtuneet_salasanat_tulevat_tyonantajille_kalliiksi__jopa_satojen_tuhansien_kustannukset/3-7580109.

Schmidt, S. R. (1991). Can we have a distinctive theory of memory? *Memory & Cognition 19*(6), 523-542.

Schneier, B. (2004). *Secrets and lies: digital security in a networked world*. New York, NY: Wiley Computer Publishing.

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.

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, July). Encountering stronger password requirements: user attitudes and behaviors. In *Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly 34*(3), 487-502.

Squire, L. R. (1992). Declarative and nondeclarative memory: Multiple brain systems supporting learning and memory. *Journal of Cognitive Neuroscience, 4*, 232-243.

Stanton, J. M., Stama, K. R., Mastrangelo, P., & et al. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-33.

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.

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.

Thagard, P. (2008). Cognitive Science. *The Stanford Encyclopedia of Philosophy.* Retrieved July 01, 2014 from http://plato.stanford.edu/archives/fall2008/entries/cognitive-science/.

Thagard, P. (2012). Cognitive architectures. In K. Frankish & W. Ramsey (Eds.), *The Cambridge Handbook of Cognitive Science*. Cambridge & New York, NY: Cambridge University Press.

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

Tulving, E. (1972). Episodic and semantic memory. In A. Baddeley, M. Eysenck & M. Anderson, *Memory*. Hove & New York, NY: Psychology Press.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013, January). Enhancing password se web-based field experiment. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 2988-2997). IEEE.

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.

Watkins, M. J. (1978). Engrams as cuegrams and forgetting as cue-overload: A cueing approach to the structure of memory. In C. R. Puff (Ed.), *The Structure of Memory*. (pp. 347-372). New York: Academic Press.

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

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.

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

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.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20.

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.

APPENDICES

Appendix 1: Password Metamemory Questionnaire

Participant Code: ____________________

Password Questionnaire
In this questionnaire, we would like you to tell us how you use your memory to remember your passwords, and how you feel about it. There are no right or wrong answers to these questions because people are different. Please take your time and answer each of the following questions as truthfully as possible, and to the best of your ability.

Each question is followed by five choices. Draw a circle around the number corresponding to your choice. **Mark only one for each statement**.

1. For most people, passwords that are meaningful are easier to remember than passwords that are not.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
2. I am good at remembering passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
3. Do you keep a list or note down important passwords?	5. never 6. rarely 7. sometimes 8. often 9. always
4. It is important to me to remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
5. I get upset when I cannot remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
6. If you have forgotten your password, do you use a lot of mental effort in trying to remember it?	1. never 2. rarely 3. sometimes 4. often 5. always
7. I think remembering my passwords are something of which to be proud of.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
8. I find it harder to remember my pass-	1. agree strongly

words when I am upset.	2. agree 3. undecided 4. disagree 5. disagree strongly
9. I am good at remembering which password belongs to which account.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
10. I can remember my passwords as well as always.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
11. Do you share your passwords with friends/family members/colleagues to help you remember them?	1. never 2. rarely 3. sometimes 4. often 5. always
12. I get anxious when I have to remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
13. It bothers me when I have to ask for my password to be reset.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
14. I'm less efficient at remembering my passwords now than I used to be.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
15. I have difficulty remembering my passwords when I am anxious.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
16. The older I get the harder it is to remember my passwords clearly.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
17. Do you use a memory technique such as mnemonics, to help you remember your passwords? Example of mnemonics: "There's no place like home" becomes "T'snp1h"	1. never 2. rarely 3. sometimes 4. often 5. always
18. I am just as good at remembering my passwords as I ever was.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly

19. I have trouble keeping track of which password belongs to which account.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
20. For most people, it is easier to remember passwords they need to use frequently than passwords they will not use for a long time.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
21. Most people find it easier to remember passwords for accounts they know they need to use than accounts they know they will never be using again.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
22. I am usually uneasy when I attempt to remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
23. I feel anxious if I have to use a password I haven't used for a long time.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
24. Having a better memory for passwords would be nice but it is not very important.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
27. Do you write down your passwords and put them in a prominent place, such as on your monitor or on your desk?	1. never 2. rarely 3. sometimes 4. often 5. always
28. It doesn't bother me when I can't remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
29. I am poor at remembering my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
30. I am much worse now at remembering my passwords than I was 10 years ago.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
31. Do you reuse your passwords for more than one account, to help you remember them?	1. never 2. rarely 3. sometimes 4. often

	5. always
32. Compared to 5 years ago, I am much worse at remembering my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
33. For most people it is easier to remember passwords they want to use than passwords they know they will never use.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
34. I remember my passwords much less now than 10 years ago.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
35. I can't expect to be good at remembering all my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
36. Most people find it easier to remember passwords for accounts that are more important to them than accounts that hold less importance.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
37. I have little control over my memory ability for remembering passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
38. When you want to remember your passwords, do you make a note of it or keep it in an electronic document on your computer or mobile device?	1. never 2. rarely 3. sometimes 4. often 5. always
39. I think it is important to work at sustaining my memory abilities for remembering passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
40. I forget my passwords more frequently now than when I was younger.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
41. As people get older they tend to forget their passwords more frequently.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
42. I work hard at trying to improve my memory for passwords.	1. agree strongly 2. agree 3. undecided

	4. disagree 5. disagree strongly
43. Compared to 10 years ago, I now forget many more passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
44. If I am suddenly required to remember my passwords, I know I will have difficulty doing it.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
45. For most people, it is easier to remember the right password for accounts they especially like than accounts that haven't made much of an impression on them.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
46. Most people find it easier to remember passwords that have more meaning than passwords that don't mean very much to them.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
47. Remembering to regularly change my passwords has improved over the last 10 years.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
48. I admire people who have a good memory for passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
49. My friends/colleagues often notice my memory abilities for remembering my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
50. When you try to remember your passwords, do you associate the passwords with their accounts?	1. never 2. rarely 3. sometimes 4. often 5. always
51. I am good at remembering the order of the characters of my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
52. For most people, passwords they have used before are easier to remember than passwords that are totally new to them.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
53. Familiar passwords are easier to remember than unfamiliar passwords.	1. agree strongly 2. agree

	3. undecided 4. disagree 5. disagree strongly		
54. a. I am good at remembering **random** passwords. 54. b. I am good at remembering **unique** passwords. 54. c. I am good at remembering **strong** passwords.	a. 1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly	b. 1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly	c. 1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
55. I would feel on edge right now if I had to recall all my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
56. My memory for passwords will decline as I get older.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
57. I often notice my friends'/colleagues' memory abilities for remembering their passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
58. My memory for passwords has greatly declined in the last 10 years.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
59. When you have trouble remembering your passwords, do you try to remember another similar password in order to help you remember?	1. never 2. rarely 3. sometimes 4. often 5. always		
60. My memory for passwords has declined greatly in the last 10 years because of an increase in the amount of passwords I need.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
61. I often forget which password belongs to which account.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
62. Do you try to remember what you were doing when creating your passwords, to help you remember them?	1. never 2. rarely 3. sometimes 4. often 5. always		
63. As long as I exercise my memory for remembering passwords, it will not decline.	1. agree strongly 2. agree 3. undecided 4. disagree		

	5. disagree strongly
64. I am good a remembering the accounts I have.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
65. I know if I keep using my passwords, I will never forget them.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
66. Do you try to relate your passwords to something else hoping this will increase the likelihood of remembering them later?	1. never 2. rarely 3. sometimes 4. often 5. always
67. It's important that I am very accurate when remembering my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
68. When I am tense and uneasy, I cannot remember my passwords very well.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
69. Do you try to concentrate hard on remembering your passwords?	1. never 2. rarely 3. sometimes 4. often 5. always
70. It's important that I am very accurate when remembering which password belongs to which account.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
71. It's up to me to keep my password remembering abilities from deteriorating.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
72. When using an account I don't know very well, I get nervous remembering the password.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
73. I have no trouble remembering all my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
74. It is easier for most people to remember passwords that are unrelated to each other than passwords that are related.	1. agree strongly 2. agree 3. undecided

	4. disagree 5. disagree strongly
75. Even if I work on it, my memory ability for remembering passwords will go downhill.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
76. Most people find it easier to remember meaningful passwords than random passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
77. Do you make mental images or pictures to help you remember your passwords?	1. never 2. rarely 3. sometimes 4. often 5. always
78. I know of someone in my family whose memory for passwords improved significantly as they got older.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
79. I am good at remembering lists of passwords and their accounts.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
80. I get anxious when I have to remember a password I haven't used for a long time.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
81. It bothers me when I forget a password.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
82. Most people find it easier to remember passwords that are related to other passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
83. Do you mentally repeat your password when you are trying to remember it?	1. never 2. rarely 3. sometimes 4. often 5. always
84. My memory for passwords has improved greatly in the last 5 years.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
85. I like to remember passwords on my own, without relying on coping strate-	1. agree strongly 2. agree

gies, such as writing passwords down.	3. undecided 4. disagree 5. disagree strongly		
86. I get tense and anxious when I feel my memory for passwords is not as good as other people's.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
87. Do you ask service providers to remind you or reset your passwords?	1. never 2. rarely 3. sometimes 4. often 5. always		
88. a. I'm highly motivated to remember **all** my passwords. 88. b. I'm highly motivated to remember my **most frequently used** passwords. 88. c. I'm highly motivated to remember all my **personal** passwords.	a.1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly	b. 1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly	c. 1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
89. I do not get nervous when I am suddenly required to remember my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
90. I find it difficult to remember my passwords and their accounts.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
91. My memory for passwords has got better in the last 10 years.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
92. For most people it is easier to remember passwords for accounts they are most interested in than passwords for accounts which they are less interested in.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
93. I have trouble remembering all my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
94. My memory for passwords will get better as I get older.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly		
95. It is easier for most people to remember strong passwords than weak passwords.	1. agree strongly 2. agree 3. undecided 4. disagree		

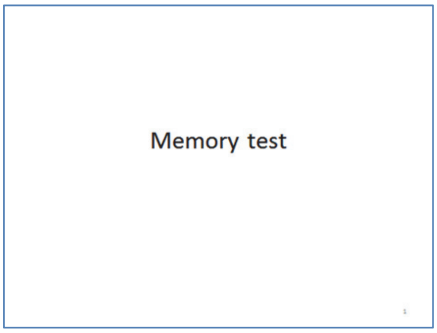
	5. disagree strongly
96. Do you write your passwords down?	1. never 2. rarely 3. sometimes 4. often 5. always
97. With more and more passwords I create, the harder it is to remember all my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
98. Most people find it easier to remember graphical passwords than text-based (alphanumerical) passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
99. After I have created a password, I have no difficulty remembering it.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
100. Do you write your passwords down or keep them in an electronic document to help you remember them?	1. never 2. rarely 3. sometimes 4. often 5. always
101. I would feel very anxious if I visited a website and had to remember the password.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
102. I am good at remembering the content and order of the characters of my passwords.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
103. No matter how hard a person works on his/her memory for passwords, it cannot be improved very much.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
104. If I were to work on my memory for passwords, I could improve it.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
105. It gives me great satisfaction to remember passwords I thought I had forgotten.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
106. Remembering the sequence of the characters of my passwords is easy for me.	1. agree strongly 2. agree 3. undecided

	4. disagree 5. disagree strongly
107. I am usually able to remember exactly which password belongs to which account.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
108. I think a good memory for passwords comes mostly from working on it.	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
109. Most people find it easier to remember random passwords than dictionary passwords. (Dictionary passwords are passwords that contain actual words.)	1. agree strongly 2. agree 3. undecided 4. disagree 5. disagree strongly
110. Do you create passwords that are related to personal information about yourself, such as using your date of birth or using a pet's name?	1. never 2. rarely 3. sometimes 4. often 5. always
111. Do you use unique passwords (completely different from any other password) for your accounts?	1. never 2. rarely 3. sometimes 4. often 5. always
112. Do you reuse passwords (use exactly the same password) for more than one account?	1. never 2. rarely 3. sometimes 4. often 5. always
113. Do you modify passwords (use an existing password with small amendments) for more than one account?	1. never 2. rarely 3. sometimes 4. often 5. always
114. Why do you reuse or modify your passwords for more than one account?	**If more than one answer is applicable, please circle more than one.** 1. convenience (it is difficult to think of a new password) 2. I like my passwords 3. it is easier to remember 4. there are too many passwords, my memory cannot cope 5. other (please tell us why):

	Please write clearly, thank you!
113. If you were told that reused and modified passwords increase security risks, as it makes it easier for hackers to access your accounts, would you change all your passwords to unique passwords?	Yes, why? …..
	No, why? ……
114. If you were told that it is easier to remember your passwords if they were all unique and completely different from each other, rather than reused or modified passwords, would you change your passwords to be all unique?	Yes, why? …..
	No, why? ……

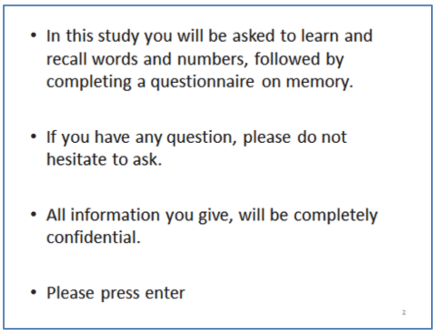
Many thanks for taking the time to complete this questionnaire.
If you have any queries, please contact: Naomi Woods (naomi.woods@jyu.fi).

Appendix 2: Memory test (in English)



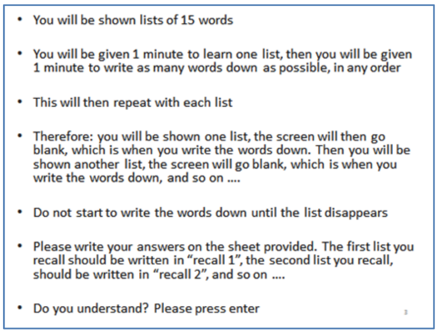
Memory test

1



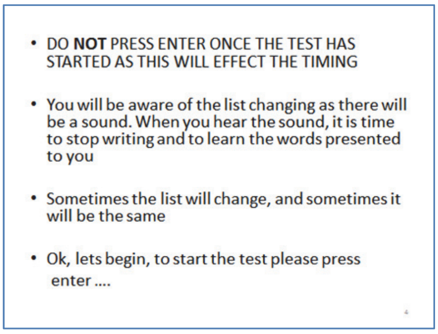
- In this study you will be asked to learn and recall words and numbers, followed by completing a questionnaire on memory.
- If you have any question, please do not hesitate to ask.
- All information you give, will be completely confidential.
- Please press enter

2



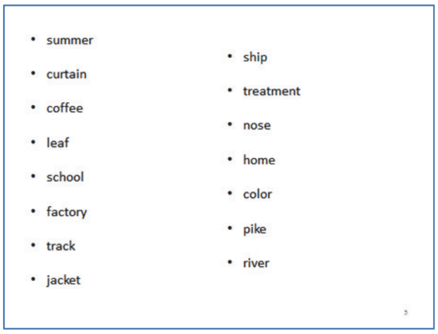
- You will be shown lists of 15 words
- You will be given 1 minute to learn one list, then you will be given 1 minute to write as many words down as possible, in any order
- This will then repeat with each list
- Therefore: you will be shown one list, the screen will then go blank, which is when you write the words down. Then you will be shown another list, the screen will go blank, which is when you write the words down, and so on ....
- Do not start to write the words down until the list disappears
- Please write your answers on the sheet provided. The first list you recall should be written in "recall 1", the second list you recall, should be written in "recall 2", and so on ....
- Do you understand? Please press enter

3



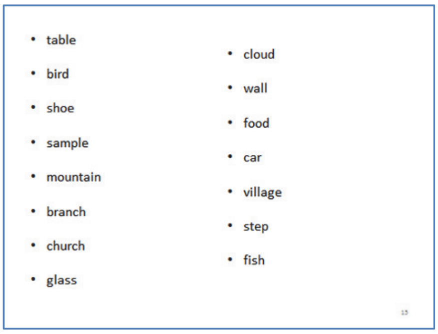
- DO **NOT** PRESS ENTER ONCE THE TEST HAS STARTED AS THIS WILL EFFECT THE TIMING
- You will be aware of the list changing as there will be a sound. When you hear the sound, it is time to stop writing and to learn the words presented to you
- Sometimes the list will change, and sometimes it will be the same
- Ok, lets begin, to start the test please press enter ....

4



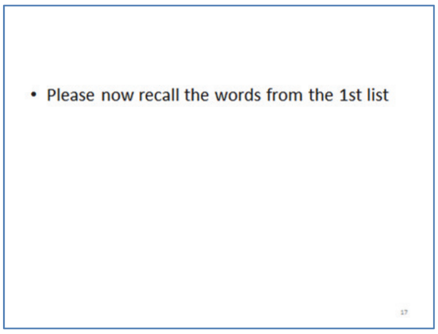
- summer
- curtain
- coffee
- leaf
- school
- factory
- track
- jacket
- ship
- treatment
- nose
- home
- color
- pike
- river

5



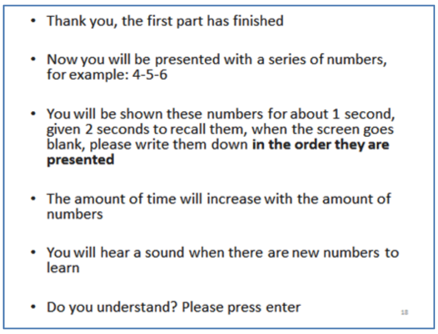
- table
- bird
- shoe
- sample
- mountain
- branch
- church
- glass
- cloud
- wall
- food
- car
- village
- step
- fish

15



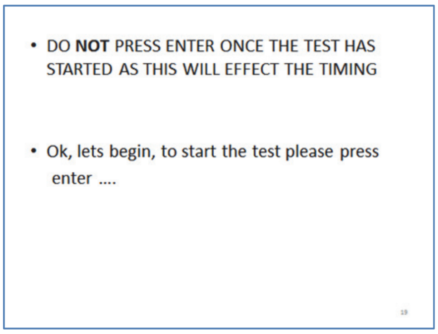
- Please now recall the words from the 1st list

17



- Thank you, the first part has finished
- Now you will be presented with a series of numbers, for example: 4-5-6
- You will be shown these numbers for about 1 second, given 2 seconds to recall them, when the screen goes blank, please write them down **in the order they are presented**
- The amount of time will increase with the amount of numbers
- You will hear a sound when there are new numbers to learn
- Do you understand? Please press enter

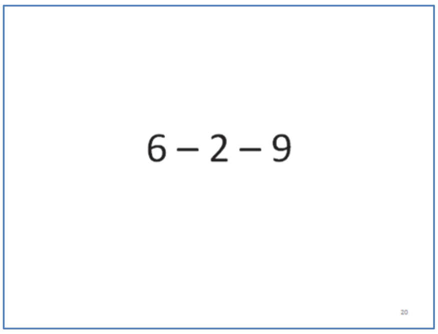
18



- DO **NOT** PRESS ENTER ONCE THE TEST HAS STARTED AS THIS WILL EFFECT THE TIMING

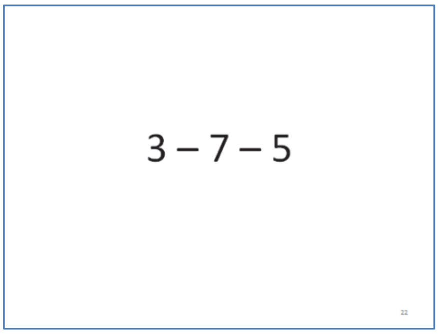
- Ok, lets begin, to start the test please press enter ....

19



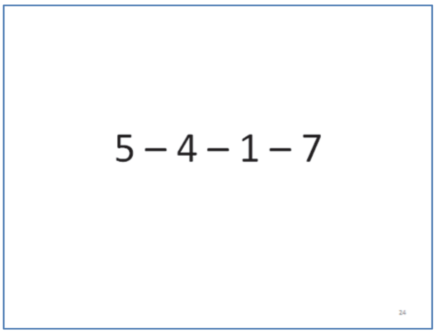
6 – 2 – 9

20



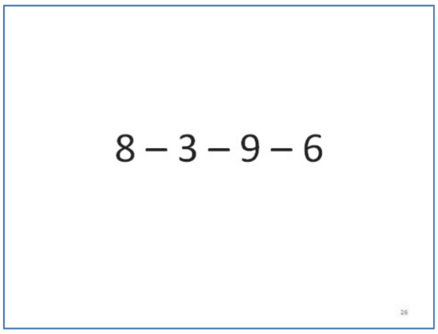
3 – 7 – 5

22



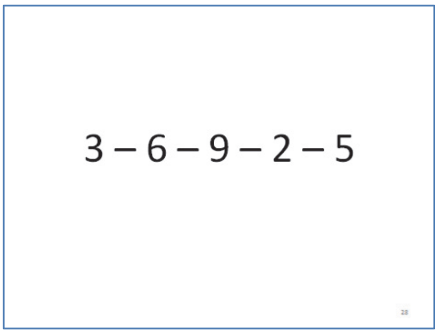
5 – 4 – 1 – 7

24



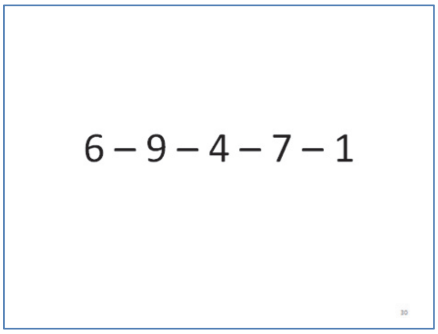
8 – 3 – 9 – 6

26



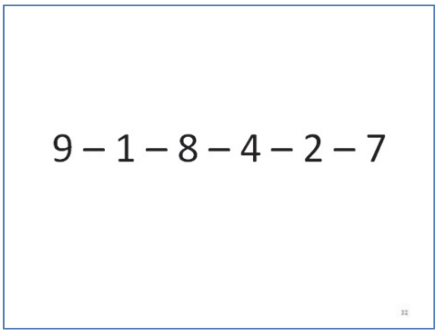
3 – 6 – 9 – 2 – 5

28



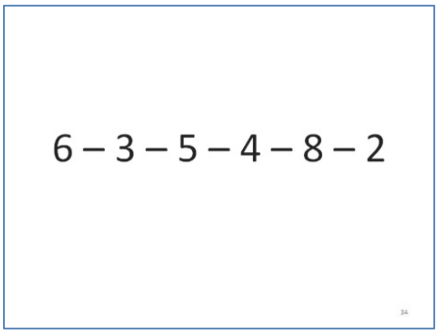
6 – 9 – 4 – 7 – 1

30



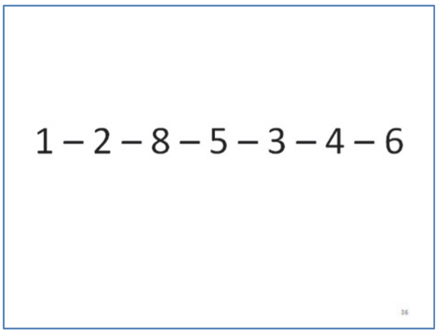
9 – 1 – 8 – 4 – 2 – 7

32



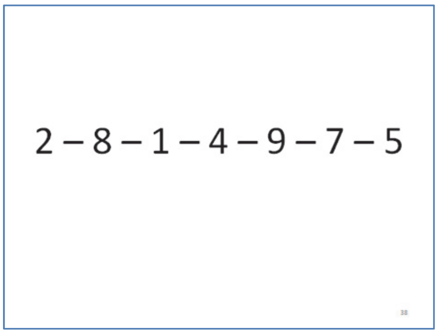
6 – 3 – 5 – 4 – 8 – 2

34



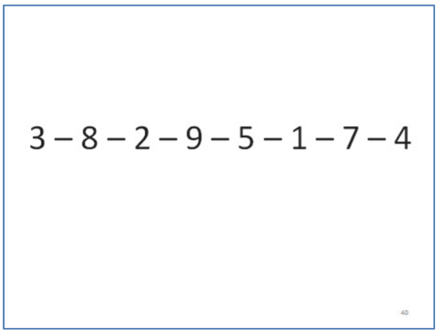
1 – 2 – 8 – 5 – 3 – 4 – 6

36



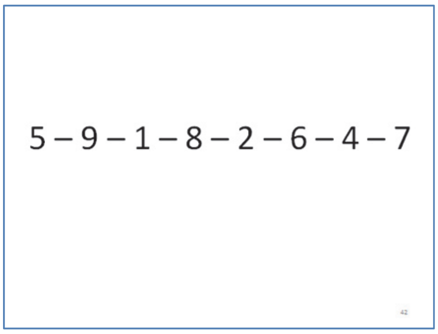
2 – 8 – 1 – 4 – 9 – 7 – 5

38



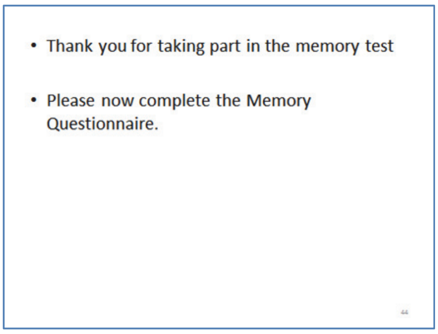
3 – 8 – 2 – 9 – 5 – 1 – 7 – 4

40



5 – 9 – 1 – 8 – 2 – 6 – 4 – 7

42



- Thank you for taking part in the memory test
- Please now complete the Memory Questionnaire.

44

Appendix 3: Questionnaire items to measure user convenience of password verification

TABLE 10: Questionnaire items to measure user convenience of password verification

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