Computers & Security 137 (2024) 103589

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# How memory anxiety can influence password security behavior

Naomi Woods [*], Mikko Siponen [†]

*University of Jyväskylä, Faculty of Information Technology, Agora, Mattilanniemi 2, Jyväskylä 40100, Finland*

ARTICLE INFO

*Keywords:*
Password security behavior
Password reuse
Password modification
Password metamemory
Memory anxiety
Security behavior
Password recall

ABSTRACT

Password reuse and modification are insecure password behaviors that are becoming increasingly prevalent as users are obliged to remember more passwords to access various digital services. Many users adopt these risky behaviors as a memory strategy in the belief that they have too many passwords for their memories to cope with. One important avenue in password research is metamemory, which encompasses the knowledge and understanding of memory capabilities and strategies. Previous research on password metamemory has examined the role that metamemory plays in memory performance (i.e., how well memory performs) and password recall. However, no previous research to date has investigated whether password reuse and modification are adopted as memory strategies due to an increase in knowledge and understanding of metamemory. To address this gap, two survey studies (Study1: $N = 50$, Study 2: $N = 303$) were implemented to examine the role that password metamemory plays in reusing and modifying passwords. Our findings suggest that of all metamemory constructs, users' anxiety regarding their perceived ability to remember passwords can influence them to reuse and modify their passwords. These findings have potentially important implications because with an enhanced understanding of how users' anxiety towards remembering passwords influences their security behavior, this could identify means of reducing password reuse and modification, thereby increasing password security and ultimately reduce some of the consequences of insecure password behaviors.

## 1. Introduction

Users are often overwhelmed by the number of passwords they are obliged to remember in their everyday (work and personal) lives (Das et al., 2014; Grawemeyer and Johnson, 2011; Ur et al., 2016; Zhang et al., 2009). To cope with the sheer numbers of passwords, many users create weak passwords, write their passwords down, and/or reuse the same password for multiple accounts (Cram et al., 2017; Guo, 2013; Vance et al., 2022; Yildırım and Mackie, 2019; Zimmermann and Gerber, 2020).[1] These behaviors are regarded as risky because they increase the likelihood of information security breaches within organizations and for individual home-users (Ives et al., 2004; Merdenyan and Petrie, 2022). For example, hacked or leaked reused passwords can be exploited to access other (and sometimes more highly sensitive) accounts. In turn, patterns in modification can be used to guess future passwords and passwords for other accounts (Das et al., 2014).

Many users adopt insecure password behaviors in the belief that they will be unable to remember unique passwords for different accounts (Brown et al., 2004; Inglesant and Sasse, 2010; Ives et al., 2004; Tam et al., 2010). Forgetting one's passwords can come at a high price as it leads to, for instance, inconvenience in terms of the time and effort that must be invested in resetting and creating new passwords. More alarmingly, it may also cause financial risk due to security breaches and repeated password resets (Brown et al., 2004; Chenchev et al., 2021; Ives et al., 2004; Morgan et al., 2021; Vu et al., 2007). Moreover, many users are not fully aware of the risks associated with these insecure behaviors and freely admit to reusing their passwords regularly (Grawemeyer and Johnson, 2011; Ives et al., 2004), feeling justified in doing so as they believe that there is no or little alternative, even when they are made aware of the seriousness of the consequences (Brown et al., 2004; Gaw and Felten, 2006; Infosecurity Magazine, 2018; Ives et al., 2004; Merdenyan and Petrie, 2022).

Previous research has examined the password problem and password security from various angles, including users' compliance with security

* Corresponding author.
*E-mail address:* naomi.woods@jyu.fi (N. Woods).
† Mikko Siponen (present address) Information Systems, Statistics, and Management Science, Culverhouse College of Business, The University of Alabama, AL, US.

[1] Password reuse = use of the exact same password for more than one account. Password modification = using the same password with only small changes for more than one account.

https://doi.org/10.1016/j.cose.2023.103589
Received 30 June 2023; Received in revised form 3 October 2023; Accepted 6 November 2023
Available online 10 November 2023

policies, to explain security behaviors (Barlow et al., 2018; Crossler et al., 2013; Jenkins et al., 2014; Johnston et al., 2015; Siponen and Vance, 2014; Warkentin et al., 2016; Willison and Warkentin, 2013; Workman et al., 2008; etc.). Another perspective has included several studies that have applied memory theories in a bid to understand password memorability and to explain users' security behavior and the trade-off between password memorability and security (Adams and Sasse, 1999; Chiasson et al., 2009; Duggan et al., 2012; Gaw and Felten, 2006; Wiedenbeck et al., 2005; Woods, 2017; Woods and Siponen, 2019; Zhang et al., 2009). One relevant framework in psychology is the theory of metamemory. Metamemory refers to knowledge and understanding of memory capabilities and strategies (Flavell, 1979). Metamemory has been studied extensively since the 1970s (Dixon, 2000; Dixon and Hultsch, 1983a, 1988; Flavell, 1971; Hertzog, 1992; Pierce and Lange, 2000; etc.). However, although password behavioral issues may be memory-related, metamemory has only recently been applied to the password context (Woods and Siponen, 2018). More specifically, password metamemory research has only examined the role that metamemory plays in memory performance (i.e., whether one has a good or bad memory) and password recall (Woods and Siponen 2018), while the influence that metamemory characteristics may have on password reuse and modification—as password memory strategies—remains unstudied, despite its clear importance. Many users reportedly adopt insecure password behaviors, such as password reuse and modification, because they believe they will be unable to remember their passwords (Brown et al., 2004; Inglesant and Sasse, 2010; Ives et al., 2004; Tam et al., 2010). Examination of metamemory characteristics in this context may shed new light on the reasoning behind these user behaviors.

In two studies, metamemory (knowledge, understanding, and self-belief about one's own memory and memory in general) is applied to the password context and examined users' password reuse and modification security behaviors. We argue that users engage in password reuse and modification due to their anxiety towards their memories' capabilities to remember multiple passwords rather than their actual memory capabilities. This has several important implications. For example, an enhanced understanding of how users' anxiety regarding their password recall influences their security behavior may help identify fruitful approaches to reducing password reuse and modification. One suggestion could include, designing cybersecurity awareness training that provides guidance on how users' cognition can affect password behavior. Through understanding the relationship between cognition and behavior, and understanding themselves better, users may in turn improve their password security behaviors.

To make our case, we will next discuss the previous password research, focusing on password reuse and modification in work and home settings. Next, we will examine the memory theory of metamemory, and how users' memory knowledge, beliefs and awareness can affect their how well their memory performs (memory performance). Then, we will examine the previous research on password memorability and password metamemory and then use the contextualization of metamemory in relation to password security behavior to form the basis of our hypotheses. The subsequent sections will discuss the research methodology and the results for both studies. Finally, the paper will conclude with a discussion of the studies' findings and implications for research and practice.

## 2. Previous research

### 2.1. The password context and insecure password behavior

Passwords are the most commonly used authentication mechanism (Al-Ameen et al., 2022; Ur et al., 2016; Yang et al., 2016; Zhang et al., 2009). However, they have their strengths and weaknesses. The former includes the lack of need for customized software and simplicity of use (Bonneau et al., 2012). The latter comprises of risky password behaviors. Although various alternatives to passwords are available (such as biometrics) (Renaud and De Angeli, 2009), passwords remain the most popular choice (Florêncio and Herley, 2010; Keith et al., 2009). It is thus imperative that we examine the ways in which users interact with passwords, in light of their criticality across a wide variety of work and personal settings (Das et al., 2014).

Password security is often undermined by users (Adams and Sasse, 1999; Gaw and Felten, 2006; Ives et al., 2004; Zhang et al., 2009). As a result of the pressure on users to remember multiple passwords, many develop a fear that they will forget them (Inglesant and Sasse, 2010; Tam et al., 2010) and thus adopt insecure password behaviors as a strategy to cope with the increasing amount of passwords required to secure their various accounts and services. Insecure password behaviors can include choosing weak passwords, writing passwords down and storing them in vulnerable locations, and reusing and modifying passwords (Chiasson et al., 2009; Duggan et al., 2012; Vance et al., 2022; Woods, 2017; Woods and Siponen, 2018; 2019). These issues arise because in everyday life, if people were to have a problem remembering something, they would generally use external memory aids – memory techniques and strategies, such as writing a shopping list (Dixon et al., 1988). In the password context, however, these memory strategies are unfortunately regarded as security risks, for example, writing passwords down (Woods and Siponen, 2018). However, not all memory strategies are considered risky when being employed to remember passwords; internal memory aids or techniques, such as mnemonics, are considered a secure memory technique to apply in creating, learning, and recalling strong passwords (Nelson and Vu, 2010; Woods, 2019). Nevertheless, it is the user's personal responsibility to invest greater time and effort in using the technique which can be a daunting task, and many are unwilling to do so (Duggan et al., 2012; Nelson and Vu, 2010; Notoatmodjo and Thomborson, 2009; Tam et al., 2010; Weir et al., 2009). Therefore, many users will prioritize convenience over security in their password management (Bang et al., 2012; Tam et al., 2010; Vu et al., 2007; Weir et al., 2009; Zhang et al., 2009).

### 2.2. Password reuse and password modification

Two insecure password behaviors include 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) (Bang et al., 2012; Das et al., 2014; Gaw and Felten, 2006; Seitz et al., 2017; Woods and Siponen, 2018). Although they are similar, password reuse and modification are different and should be distinguished, as they can be adopted for different reasons, and can affect memorability differently (Das et al., 2014; Stobert and Biddle, 2014; Woods, 2016). Nonetheless, some password security studies have approached them as the same insecure behavior (Gaw and Felten 2006; Zhang et al., 2009; etc.), perhaps because they ultimately lead to the same consequences.

#### 2.2.1. Password reuse

Password reuse (using the same password for more than one account) is a substantial security issue that directly leads to millions of dollars being wasted on cyber security measures (Infosecurity Magazine, 2014). The consequences of reuse can affect both home-users and organizations as, for example, hackers obtain lists of password hashes from websites with low-level security, enabling them to gain access to more secure websites and accounts (Ives et al., 2004; Zhang et al., 2009). This poses a substantial problem, for example, millions of passwords were leaked from large companies such as Twitter, LinkedIn, and Yahoo; when personal account passwords were cracked, the hackers were able to gain access to company systems when the passwords were reused (Das et al., 2014; Infosecurity Magazine, 2014; 2018; Ives et al., 2004).:

Previous research has ascertained that the top reasons for password reuse are that users believe that they will remember them more easily and that they have too many passwords to remember (Notoatmodjo and Thomborson, 2009). This highlights the trade-off between password

memory, security, and usability: users compromise the security of their passwords so that they might remember them (Zhang et al., 2009). In an attempt to encourage users to practice greater security, many organizations and online services implement password composition policies designed to increase password strength by imposing a minimum set of rules (for example, passwords must include upper- and lower-case characters, a number, and a special character) (Campbell et al., 2011; Shay et al., 2016; Woods and Silvennoinen 2022; Woods and Siponen, 2019). The imposition of different password composition policies can also discourage users from reusing their passwords (Campbell et al., 2011). Often, however, this leads users to simply modify their passwords as an alternative, which is considered to be equally hazardous (Das et al., 2014).

#### 2.2.2. Password modification

Das et al. (2014) reported that the top reason that users modify their passwords (i.e., using the same password with small changes for more than one account) were due to different password policies being imposed across different systems and services. However, they also have found that many users also modify their passwords (like password reuse) to support password memorization. Interestingly, however, they noted that users also modify their passwords in the belief that it can enhance their security.

Many users make small changes to their passwords, such as adding or removing a number or a special character, following simple rules. However, these simple rules can be used against the user to gain access to their other accounts in the future (Das et al., 2014; Zhang et al., 2010). A study by Zhang et al. (2010) noted that future passwords can be more easily guessed based on the users' modification behavior. Furthermore, Das et al. (2014) conducted an extensive study into password reuse and modification and found that they could successfully guess 30 percent of modified passwords within 100 attempts, based on the small changes with simple rules. They have also discovered that 98 percent of insertions and deletions in password modification happened at either the beginning or end of the password.

Overall, password reuse and modification cannot ultimately be prevented, as service providers cannot have access to all users' passwords from all other services. Therefore, it remains the user's responsibility to consider the trade-off between password memorability and security and decide whether or not to reuse or modify their passwords (Das et al., 2014).

### 2.3. Previous research on password memorability and password metamemory

Users typically engage in password reuse and modification based on the belief that they cannot remember all their passwords (Adams and Sasse, 1999; Campbell et al., 2006; Stobert and Biddle, 2014). One of the main reasons why users have problems remembering their passwords is due to the considerable number that they must remember (Nelson and Vu, 2010; Tam et al., 2010). Even with technology that facilitates secure password storage, such as password managers, many users choose to memorize all their passwords in comparison to storing them or using a password manager (Amft et al., 2023; Das et al., 2014; Grawemeyer and Johnson, 2011 Pearman et al., 2019). For those who do choose to use technologies such as password managers, often they are used in conjunction with passwords (Chenchev et al., 2021; Vance et al., 2022), and therefore, there is still the need to securely manage passwords. With large numbers of passwords to memorize, passwords may easily be forgotten due to memory interference (caused by the confusion between similar memories) and memory decay (deterioration of the memory over time) (Anderson, 2009; Baddeley, 2009). To avoid forgetting their passwords, therefore, users often adopt password behaviors, deemed insecure as a memory coping strategy (Adams and Sasse, 1999; Duggan et al., 2012).

According to memory theories, users' actual memory capacity and performance (how well their memory performs) may differ from what they believe them to be (Adams and Sasse, 1999; Campbell et al., 2006; Stobert and Biddle, 2014). This casts password memory issues in a new light—for example, suggesting that a number of password-related security issues may in fact stem from users' perceptions of their memory capabilities. The field of memory psychology boasts an extensive body of literature on metamemory, which refers to individuals' beliefs about their own memory functionality and capabilities (Dixon et al., 1988; Hertzog et al., 1987). Despite the potential relevance of metamemory in the password context, information security scholars have only recently begun to consider the potential importance of metamemory. The existing research on password metamemory studied the role of metamemory on memory performance and password recall (Woods and Siponen 2018) and found that users' actual memory performance (i.e., whether they had a good or poor memory) and correct password recall were unrelated (Woods and Siponen 2018). This finding raises an interesting question for password security research: if password recall is affected by users' beliefs about their memory capabilities rather than by their actual memory performance, might these beliefs influence their use of password-related coping strategies, such as password reuse and modification? To date, no study has examined whether an increased knowledge and understanding of metamemory will influence the adoption of password reuse and modification as password memory strategies. The objective of this paper, therefore, is to address this question using the metamemory theory framework.

## 3. Theoretical background

### 3.1. On metamemory

Metamemory is a collective term for the knowledge, beliefs, and awareness about the functioning, development, use, capacities, and limitations of one's own memory and memory in general (Dixon & Hultsch, 1983b; Flavell, 1971; Hertzog, 1992; Pierce and Lange, 2000). Metamemory is thus the explicit knowledge of and beliefs about one's own cognitive strengths and weaknesses as well as cognitive functioning in general. For example, most people find things that are more interesting easier to remember than things that hold less interest for them. The same applies to things that carry more meaning versus things that have less meaning (Bacon et al., 2011). Metamemory, as a multidimensional construct, explains why memory performance can be affected by many factors, including motivation, beliefs and perception, prior knowledge and skills, practice, and mood states (Bacon et al., 2011).

Measured by the Metamemory in Adulthood (MIA) questionnaire (Dixon et al., 1988), the constructs of metamemory are represented by seven scales, as follows: *Strategy*: the knowledge and ability to use memory strategies and techniques; *Task*: the knowledge and understanding of basic memory processes; *Capacity*: beliefs and perceptions about our own memory capacities; *Change*: perception of the change in our own memory capabilities; *Anxiety*: anxiety towards our memory performance and/or the perception of the relationship between anxiety and memory performance; *Achievement*: perception of our motivation to perform well in memory tasks; and *Locus*: the perception of our level of control over our own memory skills (Dixon et al., 1988). These scales have been used for over 30 years to measure the sub-constructs of metamemory and their relationship with memory performance (Hertzog et al., 1987).

### 3.2. Metamemory and memory performance

Metamemory plays a key role in determining how well the human memory performs (O'Sullivan and Howe, 1995). Several studies have investigated the role that metamemory plays in learning and recalling information (Hertzog, 1992; Hertzog et al., 1990a) and, more specifically, have examined the individual metamemory constructs and the two underlying metamemory categories: memory knowledge and

memory beliefs.

Memory beliefs about one's own memory abilities can be referred to as Memory Self-Efficacy (MSE) (Hertzog et al., 1990a; 1990b; Lineweaver and Hertzog, 1998; McMurtrie et al., 2012). There have been several studies that have found a relationship between memory beliefs or self-efficacy and memory performance (Cavallini et al., 2013; Hertzog et al., 1990b, 2014, 1987; O'Sullivan and Howe, 1995). Memory beliefs have been found to govern memory behavior and performance, and form an important understanding of one's self (Cavanaugh et al., 1998). Negative beliefs about one's own memory capabilities and poor memory functioning are strongly related to memory performance (Bacon et al., 2011; Glass et al., 2005).

Memory knowledge is thought, like any other knowledge, to be a personal construction that represents a person's understanding of the world or, in this case, their memory. More recent studies examining metamemory have found that memory knowledge is not associated with accuracy. Nonetheless, whether accurate or not, memory knowledge is still thought to influence memory performance (O'Sullivan and Howe, 1995). A recent study by Pierce and Lange (2000) observed a predictive relationship between metamemory and memory performance, through strategic behavior. Moreover, metamemory knowledge has resulted in strategies being used in learning that were subsequently used in information retrieval, ultimately resulting in good memory performance (Pierce & Lang, 2000).

## 4. Password metamemory, password recall and password reuse

Drawing on key literature in metamemory, we continue the discussion of how it can be contextualized to the password security context. We shall examine the relationship between password metamemory and password recall and propose its application to insecure password behavior, leading to the presentation of our hypotheses.

### 4.1. Applying the metamemory constructs to the password context

Based on previous metamemory research examining the link between metamemory and memory performance, Woods and Siponen (2018) applied drew on metamemory to examine whether they could predict password recall, adapting the metamemory constructs from the MIA questionnaire (Dixon et al., al.,1988) for the password context (Password Metamemory). The password metamemory construct of *Strategy* denotes users' knowledge and use of memory strategies to remember passwords correctly—for example, by creating mnemonic passwords. The password metamemory construct of *Task* concerns the user's understanding of how they remember passwords—for example, passwords that are more meaningful are easier to remember. The password metamemory construct of *Capacity* concerns the number of passwords users believe they can remember and their ability to recall them correctly. *Change* as a password metamemory construct represents the users' perception of the changes in their capabilities to remember passwords. *Anxiety* and/or the perception of the relationship between anxiety and memory performance within the password security context can represent the anxiety that surrounds successfully learning and correctly recalling passwords, with a fear of forgetting sometimes developing in relation to the consequences of forgetting passwords (Inglesant and Sasse, 2010; Tam et al., 2010). *Achievement*, in the password security context, represents the user's motivation towards learning and remembering passwords. Finally, the password metamemory construct of *Locus* concerns the user's perceived control over their ability to remember their passwords.

Using the Password Metamemory in Adulthood (P-MIA) questionnaire, adapted from Dixon et al. (1988), Woods and Siponen (2018) found that four password metamemory constructs—Capacity, Task, Achievement and Locus—could significantly predict correct password recall. Meaning that users who believe they have greater memory capacity to remember their passwords correctly; who understand what makes passwords more memorable; who are more motivated to remember their passwords correctly; and who believe they have more control over remembering their passwords are more likely to successfully recall their passwords (Woods and Siponen, 2018). These specific password metamemory constructs differed from the original metamemory constructs that predicted memory recall (Woods and Siponen, 2018; Hertzog et al., 1990b). Woods and Siponen (2018) suggested the inclusion of Achievement and Locus in the password metamemory model for predicting password recall was due to users' concerns about their ability to remember their passwords and their motivation towards learning and remembering them. Motivation and control have both been shown to impact password behavior (Zhang and McDowell, 2009). However, they further suggest that the absence of Strategy in the model could be explained by the fact that many good memory strategies—for example, making lists—are considered security risks when used in the password context, such as writing passwords down, reusing passwords, etc. (Woods and Siponen, 2018).

### 4.2. Password metamemory and insecure password behavior

Prior metamemory research has found that increased knowledge and understanding of metamemory have resulted in the use of memory strategies for learning and recall (Pierce and Lange, 2000). Within the password context, the knowledge and use of memory strategies (Password Strategy) have not been found to predict successful password recall (Woods and Siponen, 2018). However, no research to date has investigated whether enhanced knowledge and understanding of metamemory results in the adoption of password memory strategies, bearing in mind that password reuse and modification are regarded as strategies to overcome memory limitations (Adams and Sasse, 1999; Duggan et al., 2012). Therefore, we investigate whether users with increased knowledge and beliefs in their cognitive strengths and weaknesses are more likely to engage in password reuse and modification. We propose that password metamemory could be instrumental in the adoption of insecure password behavior, such as password reuse and modification, and hypothesize the following (in Table 1, and illustrated in Fig. 1):

## 5. Research methodology

Two studies employing a survey design collected subjective data from two different samples by means of an adapted version of the MIA questionnaire (P-MIA) (Woods and Siponen, 2018), which was used to measure password metamemory. Additional items concerning insecure password behaviors were appended to the questionnaire to measure password reuse and modification. The data were used to analyze the relationships between password reuse and modification, and password metamemory.

**Table 1**
Password metamemory hypotheses.

| Hypotheses | Password Reuse | Password Modification |
|---|---|---|
| Strategy (password metamemory) will have a significant positive effect on … | **H1a** | **H2a** |
| Task (password metamemory) will have a significant negative effect on … | **H1b** | **H2b** |
| Capacity (password metamemory) will have a significant negative effect on … | **H1c** | **H2c** |
| Change (password metamemory) will have a significant negative effect on … | **H1d** | **H2d** |
| Anxiety (password metamemory) will have a significant positive effect on … | **H1e** | **H2e** |
| Achievement (password metamemory) will have a significant positive effect on … | **H1f** | **H2f** |
| Locus (password metamemory) will have a significant negative effect on … | **H1g** | **H2g** |

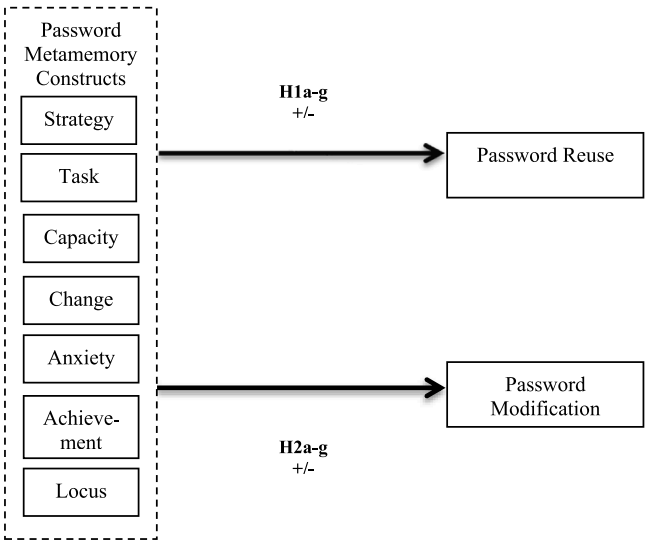


**Fig. 1.** Research model for examining the relationships between password security behaviors and password metamemory.

### 5.1. Participants

Two different samples were employed to maximize the findings' generalizability, and confirm the findings. The first study had a sample size of 50 which is considered a smaller sample size. However, it achieved the level of statistical power of just under 0.70 (calculated using RStudio). Therefore, as to achieve a good level of statistical power (0.80) (Cohen, 1992) in the second study, the sample size was assessed and was surpassed by 303 participants being recruited. An age limitation was imposed in both studies, as advanced age can have an effect on metamemory (Baddeley, 2009; Dixon and Hultsch, 1983a; Glass et al., 2005; Hertzog et al., 1990b). The younger age groups had more participants; however, preliminary analyses showed no effect for age. Given that password users represent a range of different age groups, for ecological validity, we did not want to exclude participants unless they were of an age that would be considered to affect the metamemory results. Existing research indicates that the younger and middle-aged groups show similar results and that differences emerged only for participants aged over 60 (Cavallini et al., 2013; Devolder et al., 1990; Dixon and Hultsch, 1983a; Hertzog et al., 1994). Therefore, the maximum age range was up to 54 years. Table 2 presents the participants' demographic information.

In Study 1, the 50 participants were selected from staff and students from a university. All participants had work experience and were experienced computer users. In Study 2, the 303 participants were recruited from Amazon's Mechanical Turk (MTurk) crowdsourcing services. Several studies have utilized the benefits of collecting data via MTurk (Jia et al., 2017; Lowry et al., 2016; Merdenyan and Petrie, 2022; Owens and Hawkins, 2019). It has been acknowledged that, like any other data collection method, it has its strengths and limitations. Nevertheless, there is a growing consensus that concerns surrounding the integrity of the data are unfounded and that the results can be more generalizable (Jia et al., 2017; Lowry et al., 2016). Study 2 imposed a set of inclusion criteria to ensure that the data were of good quality. The participants needed to have a Human Intelligence Task (HIT) approval rating higher than 90 % with more than 100 HITs approved (Merdenyan and Petrie, 2022).

### 5.2. Measures

#### 5.2.1. Password metamemory

Password metamemory was measured using an adapted version of the Metamemory In Adulthood (MIA) questionnaire, developed from Dixon et al. (1988). The password metamemory questions were amended from the original MIA questionnaire specifically for the password security context (Woods and Siponen, 2018) (see Table 3). The

**Table 2**
Demographic information.

| Study 1: $N = 50$ | | |
|---|---|---|
| Age | Gender | Education level |
| 18 to 24 years (count of 15; 30 %)<br>25 to 35 years (count of 15; 30 %)<br>35 to 44 years (count of 10; 20 %)<br>45 to 54 years (count of 10; 20 %) | Male (count of 31; 62 %)<br>Female (count of 19; 38 %)<br>Other (count of 0; 0 %) | Bachelor's degree (count of 18; 36 %)<br>Master's degree (count of 23; 46 %)<br>Doctoral degree (count of 9; 18 %) |
| Study 2: $N = 303$ | | |
| Age | Gender | Education level |
| 18 to 24 years (count of 65; 21 %)<br>25 to 35 years (count of 137; 45 %)<br>35 to 44 years (count of 51; 17 %)<br>45 to 54 years (count of 50; 17 %)<br>45 to 54 years (count of 50; 17 %) | Male (count of 171; 56 %)<br>Female (count of 131; 43 %)<br>Other (count of 1; 1 %) | High school certificate (count of 81; 27 %)<br>Bachelor's degree (count of 172; 57 %)<br>Master's degree (count of 37; 12 %)<br>Doctoral degree (count of 5; 2 %)<br>Other (count of 8; 2 %) |

**Table 3**
Example items representing the password metamemory in adulthood (P-MIA) constructs (Woods and Siponen, 2018).

| Password Metamemory Construct | Definition | Sample Item |
|---|---|---|
| Strategy | Knowledge and use of memory strategies to remember passwords (+ + high use) | 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 to remember passwords (+ + high knowledge) | For most people, passwords that are meaningful are easier to remember than passwords that are not. |
| Capacity | Beliefs about one's own memory capacities to remember passwords (+ + high capacity) | I am good at remembering passwords. |
| Change | Perception of the change in one's own memory capabilities to remember passwords (+ + stability) | The older I get the harder it is to remember my passwords clearly. |
| Anxiety | Anxiety and/or perception of the relationship between anxiety and recalling passwords correctly (+ + high knowledge) | 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 remembering passwords (+ + high achievement) | It doesn't bother me when I can't remember my passwords. |
| Locus | Perceived sense of control over one's own ability to remember passwords (+ + internal locus) | It's up to me to keep my password remembering abilities from deteriorating. |

Password-MIA (P-MIA) questionnaire uses 108 questions to represent the seven constructs of password metamemory, and participants report their answers on a 5-point Likert scale. All password metamemory constructs were examined for construct validity and showed good internal consistency (Cronbach's alpha) for both Studies 1 and 2: Strategy (0.71) (0.74); Task (0.84) (0.83); Capacity (0.89) (0.93); Change (0.84) (0.94); Anxiety (0.92) (0.93); Achievement (0.84) (0.88); and Locus (0.72) (0.82).

#### 5.2.2. Password reuse and modification

Password reuse and modification were measured through the additional items added to the P- MIA questionnaire (shown in Table 5). In both studies, participants were asked to report their password reuse and modification activities using a 5-point Likert scale. Some of the P-MIA questionnaire's items could have contributed to the measurement of password reuse and modification. However, they were not included in the measurement of these factors as they were written to represent the password metamemory constructs, and therefore could have influenced the results. For example, in response to the question, "Do you modify your passwords for more than one account, to help you remember them?", the participants could have responded based on their reasoning for password modification – high if they modify as a memory strategy and low if they modify for "security" purposes. Therefore, only direct questions relating to password behavior were used to measure these factors (see Table 4).

### 5.3. Procedure

In both studies, ethical considerations were taken into account. The participants were informed as to what they might expect from the study, that any information would be kept confidential, and that agreement to participate included their formal consent. They were also informed that they could withdraw from the study at any time. After both studies were closed, all data were anonymized using participant codes.

In Study 1, the participants were asked to sign up for the study by replying to an advert with preliminary details that was posted throughout the university with a link to the online questionnaire. The questionnaire included information about the study, the confidentiality of the data being collected, withdrawal information, and contact information. The participants were then asked to complete the P-MIA questionnaire (including password reuse and modification questions).

In Study 2, the online questionnaire was adapted for Mturk purposes, for example, adding a completion code for workers to confirm that they had completed the questionnaire. The online questionnaire link was distributed via MTurk, and potential participants who accepted the HIT were provided with a short introduction to the study. As with Study 1, full information about the study, confidentiality, the option to withdraw, and contact information were provided with the online questionnaire. The questionnaire included the P-MIA and password questions. All participants who completed the questionnaire received 3 USD as remuneration.

**Table 4**
Password reuse and modification questions.

| Construct | Definition | Sample Item |
|---|---|---|
| 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? Always, often, sometimes, rarely, never |
| Password modification | Perceived rates of password modification (+ = high rates of modification) | Do you modify passwords (use an existing password with small amendments) for more than one account? Always, often, sometimes, rarely, never |

## 6. Results

Subjective questionnaire data measuring password metamemory and password reuse and modification were collected by means of the participants' questionnaire responses. All password metamemory results were computed by the mean score for each construct for each participant (Table 5 reports descriptive statistics for Studies 1 and 2).

### 6.1. Password metamemory predicting password reuse and modification

Stepwise multiple regression tests were used to examine the predictive factors of password metamemory on password reuse and modification. The seven password metamemory constructs—Strategy, Task, Capacity, Change, Anxiety, Achievement, and Locus—were entered into the model for analysis.

The analyses in both Studies 1 and 2 revealed one significant predictor variable for both dependent variables (password reuse and password modification): Anxiety was the only password metamemory construct that could predict both password reuse (Study 1: $p = 0.008$; Study 2: $p < 0.001$) and password modification (Study 1: $p = 0.036$; Study 2: $p < 0.001$). Therefore, H1e and H2e were supported. Table 6 and Fig. 2 present the results of the analyses.

### 6.2. Further analysis

Hypothetico-inductive-statistical research settings facilitate post hoc examination and theorizing of interesting results (Siponen and Klaavuniemi, 2020). Following this approach, here, we shall take a further look at password metamemory anxiety.

#### 6.2.1. A deeper look at password metamemory anxiety

The password metamemory construct of *Anxiety* was the only significant predictive factor in password reuse and modification in both studies; as such, we decided to examine the construct in greater detail.

Since the late 1970s, researchers have emphasized a distinction between metamemory knowledge (knowledge and understanding of how the memory functions and awareness of memory strategies) and metamemory beliefs (a set of beliefs regarding one's own memory capabilities), which constitute metamemory (Flavell, 1979). Several researchers have found that self-beliefs about one's own memory can be independent of memory knowledge and awareness but can still influence our memory performance (Hertzog et al., 1987). In a study by Hertzog et al. (1987), while examining the MIA constructs, they reported that the items on the Anxiety scale could be attributed to two separable factors: questions regarding how anxious the respondent is in memory-demanding situations (affect/self-belief) and how higher levels of anxiety can affect memory performance (knowledge). Based on this division, we isolated the two sub-factors of the P-MIA and ran further

**Table 5**
Descriptive statistics for studies 1 and 2.

| Study 1: $N = 50$, Study 2: $N = 303$ | | | | |
|---|---|---|---|---|
| Construct | Study 1: Mean | Study 2: Mean | Study 1: SD | Study 2: SD |
| Strategy | 3.24 | 3.07 | 0.42 | 0.43 |
| Task | 4.10 | 4.11 | 0.33 | 0.46 |
| Capacity | 3.03 | 3.11 | 0.56 | 0.80 |
| Change | 2.93 | 2.87 | 0.68 | 0.86 |
| Anxiety | 3.09 | 3.10 | 0.77 | 0.87 |
| Achievement | 3.37 | 3.43 | 0.47 | 0.62 |
| Locus | 3.67 | 3.28 | 0.55 | 0.68 |
| Password reuse | 3.14 | 2.73 | 0.95 | 1.15 |
| Password modification | 3.26 | 2.92 | 1.01 | 1.05 |

**Table 6**
Multiple regression analysis results from studies 1 and 2.

| Factors | Significant predictor variables of Password metamemory | Std. $\beta$ | $p$ |
|---|---|---|---|
| **Study 1** | | | |
| Password reuse | Adj $R^2 = 0.211$; $F = 7.751$, $p = 0.008$ | | |
| | Anxiety | 0. 380 | 0.008 |
| Password modification | Adj $R^2 = 0.172$; $F = 4.651$, $p = 0.036$ | | |
| | Anxiety | 0.303 | 0.036 |
| **Study 2** | | | |
| Password reuse | Adj $R^2 = 0.090$; $F = 15.975$, $p <$ 0.001 | | |
| | Anxiety | 0.287 | $< 0.001$ |
| Password modification | Adj $R^2 = 0.061$; $F = 16.744$, $p <$ 0.001 | | |
| | Anxiety | 0.230 | $< 0.001$ |

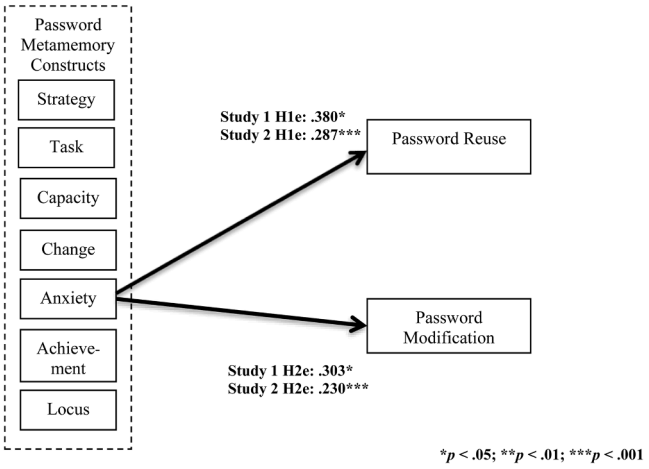


**Fig. 2.** Summary of supported results.

analyses to determine whether there was any effect on password reuse and modification.

The password anxiety metamemory constructs were examined for construct validity and showed good internal consistency (Cronbach's alpha): Study 1 Anxiety Affect (0.91) and Anxiety Knowledge (0.79); and Study 2 Anxiety Affect (0.89) and Anxiety Knowledge (0.75).

Stepwise multiple regressions were performed to examine the anxiety sub-constructs and reveal any predictive value toward password reuse, and password modification. The analyses revealed that in both studies, the Anxiety Affect was the only significant predictor variable of password reuse (Study 1: $p = 0.018$; Study 2: $p = 0.021$), and password modification (Study 1: $p = 0.013$; Study 2: $p = 0.015$).

*6.2.2. A deeper look at password reuse and modification, and the justification for insecure password behavior*

Although, the focus of these studies was to examine whether password metamemory could predict password reuse and modification, further analyses were conducted to provide a more enriched understanding of password reuse and modification and the participants' reasoning for engaging in such behaviors.

Combining the results of both studies, we found that 98 percent of the participants reported that they reuse and/or modify their passwords. Furthermore, 42 percent reported that they "often" reuse their passwords, whereas 50 percent reported that they "always" (4 %) and "often" (46 %) modify their passwords, as illustrated in Fig. 3a and 3b.

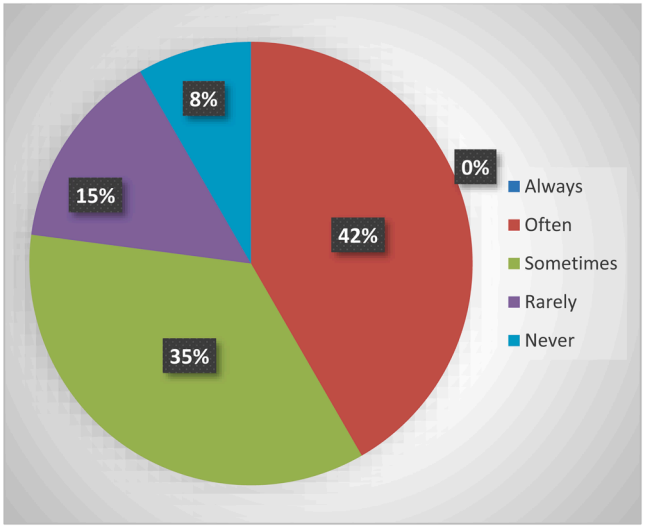


**Fig. 3a.** Percentages of frequency of password reuse.

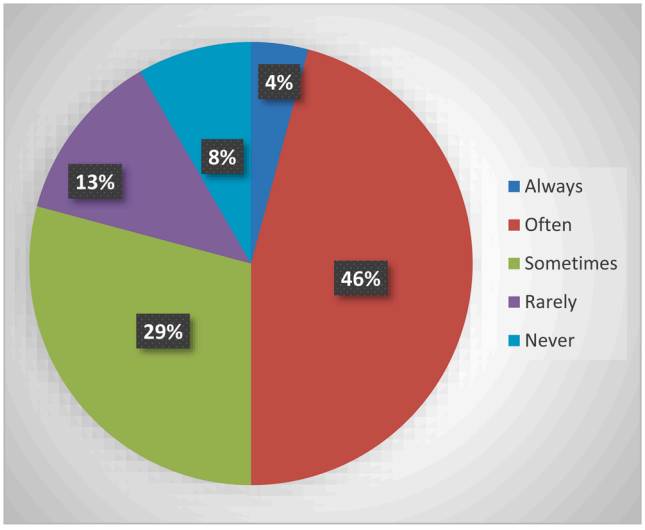


**Fig. 3b.** Percentages of frequency of password modification.

We then dove deeper and asked the participants about password reuse and modification for work accounts and personal accounts. Thirty-four percent reported they would "never" reuse or modify their work account passwords. Three percent said they would "always", 17 percent said they would "often", and 30 percent said they would "sometimes" reuse or modify their work account passwords (see Fig. 4a). By comparison, the same three percent of participants said that they would "always" reuse or modify their personal account passwords, whereas 30 percent reported that they would "often" and 45 percent reported that they would "sometimes" reuse and modify their personal account passwords. Only two percent said that they would "never" reuse or modify their personal account passwords (see Fig. 4b). When asked further, what accounts would you not reuse or modify the password for, 97 percent of the participants mentioned some sort of banking or financially-related account type. The distributions of frequency of reuse and modification when comparing work and personal accounts, paired with the percentage of participants reporting that they do not reuse/modify their banking/financial accounts, highlights their understanding that this type of password behavior is not necessarily secure.

When asked why they reuse and/or modify their passwords, the participants' responses ranged from convenience, preference, security to

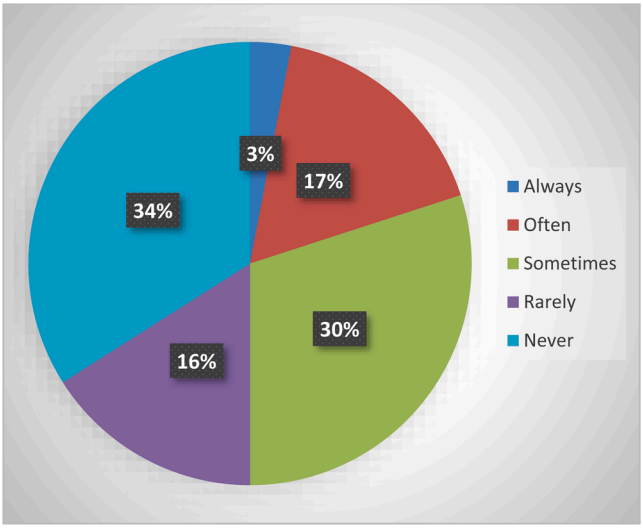


**Fig. 4a.** Percentages of frequency of password reuse and modification for work accounts.

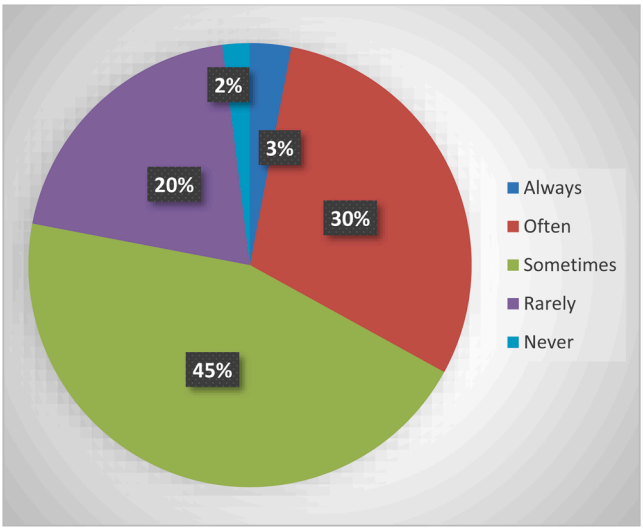


**Fig. 4b.** Percentages of frequency of password reuse and modification for personal accounts.

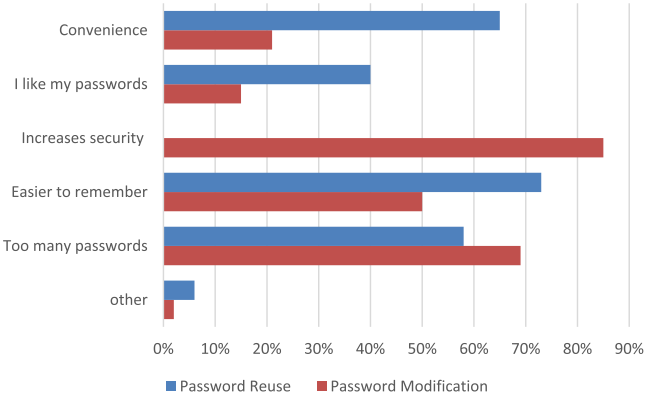


**Fig. 5.** Participants' responses: reasons for reusing and modifying passwords. *Participants were allowed to give more than one response.

memorability (see Fig. 5).

The participants' responses regarding their reasons for password reuse and modification showed different distributions: in particular, notable differences emerged between password reuse and modification in terms of security and memorability. No participants reported that they reuse their passwords for security reasons, but 85 percent reported that they modify their passwords because of security; and 73 percent reported that they reuse their passwords to help them remember, whereas 50 percent modify their passwords for the same reason. These results emphasize the variance in motivations for modifying and reusing passwords, which is important, as many researchers often regard these two behaviors as the same (Gaw and Felten 2006; Zhang et al., 2009; etc.). These findings also highlight that many users are aware that reuse is a security issue but nonetheless do it for perceived memory limitation reasons. Whereas, these results suggest that many users are unaware of the security risks of password modification and do not necessarily use it as a memory strategy.

## 7. Discussion

Users often justify the adoption of insecure password behaviors, such as password reuse and modification, as a strategy to help them recall multiple passwords, as they believe that they cannot cope with the number of passwords they are required to remember (Biddle et al., 2012; Das et al., 2014; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). Previous research has found no relationship between password recall and memory performance but found that users' perceptions, knowledge, and understanding of their memories affect password recall (Woods and Siponen, 2018). These findings, along with those showing that increased metamemory promotes the adoption of memory strategies (Pierce and Lange, 2000), have led us to question whether users' perceptions of their memories' capabilities result in the adoption of insecure password behavior, such as password reuse and modification. Based on our results, we shall proceed to discuss our findings and their implications, acknowledge the study's limitations, and offer suggestions for future research.

### *7.1. Predicting password reuse and modification from password metamemory*

If users' metamemory (perceptions, knowledge, and understanding of their memories) affects password recall, can it predict insecure password behaviors, such as password reuse and modification, as these behaviors have been reported in previous research to be strategies? (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011). Our examination of password metamemory in relation to password reuse and modification yielded compelling results. Only one password metamemory construct could significantly predict password reuse and modification: Anxiety. Passwords play an important role in our everyday lives—they keep our organizational and personal information secure, protect our companies' and our own finances, and grant us access to the systems and services that we use both at work and at home. Consequently, many users develop a fear that they will forget their passwords (Inglesant and Sasse, 2010; Tam et al., 2010). This fear is heightened by the consequences that will invariably ensue—loss of money and time and increased inconvenience when users are unable to access their online systems/services (Brown et al., 2004; Inglesant and Sasse, 2010; Ives et al., 2004; Tam et al., 2010). Understandably, this fear may turn to anxiety and, more specifically, anxiety about trusting one's own memory to remember passwords. There is a plethora of research that has acknowledged the relationship between negative perceptions of memory and memory performance (Bacon et al., 2011) and how anxiety relates to memory performance (Lineweaver and Hertzog, 1998), given that anxiety may escalate when one contemplates their potential failure to successfully complete a memory-based task (Davidson et al., 1991). One such theory

suggests that the working memory can get distracted by irrelevant thoughts about failure to perform, leading to diminished memory performance (Eysenck, 1992).

Within this study a more thorough investigation was performed of the password metamemory construct Anxiety due to it alone predicting password reuse and modification. The results revealed that Anxiety Affect (self-belief) rather than Anxiety Knowledge significantly predicted password reuse and modification. Previous research has identified the relationships between MSE (Memory Self-Efficacy or self-belief) and memory performance (Lineweaver and Hertzog, 1998). Moreover, there is research that recognizes that a anxiety about one's perceived memory capabilities can promote the adoption of behavioral strategies and memory strategies, irrespective of whether the anxiety is justifiable (Hertzog et al., 1987; Stöber and Esser, 2001).

From this research, we can surmise that being anxious about one's memory, regardless if it is justified or not, does not necessarily lead people to perform better. However, if being anxious about one's memory can result in the adoption of behavioral and memory strategies, why does memory performance (and thus, password recall) not improve? (Woods and Siponen, 2018). Previous findings suggests that MSE can affect motivation, effort, and persistence in memory-based tasks/memory performance (Beaudoin and Desrichard, 2011; Lineweaver et al., 2014). Moreover, a study by Stöber and Esser (2001) that examined metamemory in test-anxious participants found that participants with higher levels of anxiety were more likely to choose external memory storage (e.g., external memory aids, such as writing notes) over internal memory storage (i.e., their own internal memory systems). Therefore, users who are anxious about their ability to remember their passwords could, for example, adopt external memory strategies (such as writing a list), that takes less mental effort, rather than trusting and adopting internal memory strategies (using a memory technique, e.g., mnemonic) using more effort. It is unfortunate however, that the majority of external memory strategies used within the password context are generally considered insecure password behaviors, which lead many users to choose between security or memorability or attempt to strike a balance (Zhang et al., 2009).

Overall, our results confirmed that those who were more anxious about their memories' capabilities (self-belief) to recall passwords were more likely to reuse and modify their passwords.

### 7.2. Password metamemory strategy and adopting password reuse and modification

Another interesting finding was that the password metamemory construct of Strategy did not predict password reuse and/or modification, in fact there was no correlation at all (Study 1: $p = 0.443$ reuse, $p = 0.491$ modification, and Study 2: $p = 0.249$ reuse, $p = 0.086$ modification). These results were surprising, particularly given that password reuse and modification are regarded as memory strategies (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011) and that metamemory research suggests that increased metamemory is related to employing memory strategies (Pierce and Lange, 2000). The findings that Password Strategy does not predict password reuse or modification is even more surprising in light of the participants' reports that they reuse and modify their passwords to make them easier to remember. However, the participants' responses suggest that enhanced security was a more prominent motive for modifying their passwords than improved memorability. With varied motivations for both behaviors and variations in the perceived security of both behaviors and taking into account that many memory strategies are regarded as risky security behaviors in the password context, this would suggest the reasoning for Password Strategy was not included in the model. Therefore, the adapted questions that measure the password metamemory construct of Strategy (measuring memory strategy use and knowledge in the password context) could have been considered and responded to from a different perspective to that of the original metamemory strategy questions (in the MIA) due to their security nature.

### 7.3. Implications

Password reuse and modification lead to serious consequences, such as security breaches and loss of money (Brown et al., 2004; Gaw and Felten, 2006; Infosecurity Magazine, 2018; Ives et al., 2004). Our findings have important research implications as well as practical implications for both organizations and individual home-user that could help reduce these insecure password behaviors.

*Password reuse and modification distinction:* When attempting to mitigate risky security behavior, it is imperative that its underlying motivations be understood. Several studies have examined password reuse and modification but have regarded these as fundamentally the same behavior with the same motives (Gaw and Felten, 2006; Zhang et al., 2009; etc.). Not only do password reuse and modification affect password memorability differently (Woods, 2016) but if they stem from different motives (Das et al., 2014), then their reduction may warrant distinct approaches. If these differences are understood, they will improve the applicability of future research findings and can be applied to guidance, cybersecurity awareness training, and security policies that follow. To reduce both password reuse and modification, users could be made more aware of the consequences of these behaviors, and targeting the misconception of improved security with regards to modifying passwords. Furthermore, information and training could be provided to users to provide easy-to-use memory techniques that will encourage users to move from applying external memory strategies to internal memory strategies, that especially meet the different requirements of different password policies and in a more effortless way.

*Password Metamemory Anxiety:* The discovery that a specific construct of password metamemory could predict password reuse and modification is important as it highlights the important role that metamemory plays in password security behaviors. Furthermore, these results are new in that memory anxiety alone can predict password reuse and modification. Through acknowledging these results, security awareness training and guidance for users could be adapted to incorporate information about trusting one's memory and aspects that can reduce memory anxiety. This, in turn, could lead to changes in users' perceptions towards their memory and remembering password. Consequently, this could result in users choosing not to reuse and modify their passwords, leading to increased security policy compliance, enhancing password security, decreasing security breaches, and saving money lost to such breaches. Furthermore, these results also suggest that users' anxiety (state or trait) could potentially have an effect on their other security behaviors, not just their password security behaviors.

### 7.4. Study limitations

Our study has limitations. The first was that password reuse and modification were subjectively measured by means of participants reporting their perceived rates of reuse and modification in their everyday lives (at work and at home). We did not take an objective measure or monitor incidences of these behaviors on the grounds that it would be considered a security breach had we asked the participants to provide the passwords they actually used in real life. Moreover, when asked how many passwords the participants reused and modified in real life, many reported that they could not say for sure, as many reused their passwords on what they regarded as low-security websites, which were generally too many to count. Therefore, a sum of the number of passwords reused or modified would inevitably be a subjective response. The second limitation was the length of the P-MIA questionnaire (over 100 questions), which could potentially have resulted in questionnaire fatigue. As the P-MIA was based on the original MIA questionnaire (Dixon et al., 1988), to measure the constructs of metamemory, all items were required. However, to help counteract fatigue, the participants were

informed that the questionnaire was long so that they could manage their expectations. Furthermore, the statements were short and the questions were jumbled, so that any fatigued responses toward the end of the questionnaire would not affect specific constructs.

### 7.5. Future research

The results of this study highlight the need for further investigation of the metamemory construct of anxiety as a predicting factor in password reuse and modification. Future research should also investigate users' emotional responses to password security and how they influence it. We propose that types of anxiety should be examined along with fear, frustration, and motivation. Future research could investigate how a fear of forgetting could influence password security and memorability in greater detail. Since the password metamemory construct of strategy was not found to be related to password reuse or modification, we propose that it should be further investigated. We also recommend examining whether password reuse and modification are really adopted as a memory strategy (to enhance learning) or as a coping strategy to avoid the inconvenience of learning passwords. We also propose that further research should examine the relationship between password metamemory and other insecure password behaviors, such as choosing weak passwords, writing passwords down, and sharing passwords. Finally, we propose that anxiety and other psychological states should be examined for their effect on other security behaviors.

## 8. Conclusion

It is widely believed that users' adoption of insecure password behaviors, such as password reuse, both at home and in the workplace, stems from users' memory limitations, and their inability to cope with multiple passwords (Biddle et al., 2012; Duggan et al., 2012; Gaw and Felten, 2006; Grawemeyer and Johnson, 2011; Merdenyan and Petrie, 2022; Woods and Siponen, 2018; Zimmermann and Gerber, 2020). Users defend their password reuse and modification because they regard the behavior as a means of remembering their passwords more easily (Adams and Sasse, 1999; Duggan et al., 2012; Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009), not necessarily realizing the security risks (Gaw and Felten, 2006). Even when they are aware of the risks (Gaw and Felten, 2006; Notoatmodjo and Thomborson, 2009); due to a fear of forgetting, many will justify this behavior with a trade-off between password security and memorability (Gaw and Felten, 2006; Inglesant and Sasse, 2010; Tam et al., 2010; Zimmermann and Gerber, 2020). Previous research has found that password metamemory can affect password memorability (Woods and Siponen, 2018). Based on findings that suggest that increased metamemory can also result in the use of memory strategies to learn and recall (Pierce and Lange, 2000), the two studies examined the role that password metamemory plays in adopting password reuse and modification. The results have revealed a surprising relationship with anxiety as an important contributing factor to password reuse and modification. This represents a new perspective on the issue that suggests that users who are more anxious about remembering their passwords (regardless of their memories' actual capabilities) are more likely to reuse and modify their passwords. These findings have significant implications for both organizations and home-users. With a better understanding of how users' anxiety towards remembering passwords influences their security behavior, we may hope to identify and implement successful approaches to increase password security, for examine by developing cybersecurity awareness training that includes information about how users' cognition can affect their security behavior. With increased password security awareness, this may reduce password reuse and modification, and ultimately reduce the consequences of insecure password behaviors.

## CRediT authorship contribution statement

**Naomi Woods:** Conceptualization, Investigation, Methodology, Formal analysis, Resources, Writing – original draft, Writing – review & editing. **Mikko Siponen:** Conceptualization, Investigation, Methodology, Writing – review & editing.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Data availability

Data will be made available on request.

## Acknowledgments

The authors would like to thank the participants for taking part in the study. The research was supported by the Faculty of Information Technology at the University of Jyväskylä, Finland.

## References

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Commun. ACM 42 (12), 41–46. https://doi.org/10.1145/322796.322806.

Al-Ameen, M.N., Marne, S.T., Fatema, K., Wright, M., Scielzo, S., 2022. On improving the memorability of system-assigned recognition-based passwords. Behav. Inf. Technol. 41 (5), 1115–1131. https://doi.org/10.1080/0144929X.2020.1858161.

Amft, S., Höltervennhoff, S., Huaman, N., Acar, Y., Fahl, S., 2023. "Would you give the same priority to the bank and a game? I do {not!}" exploring credential management strategies and obstacles during password manager setup. In: Nineteenth Symposium on Usable Privacy and Security, pp. 171–190 (SOUPS 2023).

Anderson, M., 2009. Incidental forgetting. In: Baddeley, A., Eysenck, M., Anderson, M. (Eds.), Memory. Psychology Press, Hove and New York, NY.

Bacon, E., Huet, N., Danion, J., 2011. Metamemory knowledge and beliefs in patients with schizophrenia and how these relate to objective cognitive abilities. Conscious. Cogn. 20 (4), 1315–1326. https://doi.org/10.1016/j.concog.2011.02.017.

Baddeley, A., 2009. Memory and aging. In: Baddeley, A., Eysenck, M., Anderson, M. (Eds.), Memory. Psychology Press, Hove and New York, NY, pp. 293–316.

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. Int. J. Inf. Manage. 32, 409–418. https://doi.org/10.1016/j.ijinfomgt.2012.01.001.

Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2018. Don't even think about it! the effects of antineutralization, informational, and normative communication on information security compliance. J. Assoc. Infor. Syst. 19 (8), 689–715.

Beaudoin, M., Desrichard, O., 2011. Are memory self-efficacy and memory performance related? A meta-analysis. Psychol. Bull. 137 (2), 211–241. https://doi.org/10.1037/a0022106.

Biddle, R., Chiasson, S., Van Orschot, P.C., 2012. Graphical passwords: learning from the first twelve years. ACM Comput. Surv. 44 (4), 1–41. https://doi.org/10.1145/2333112.2333114, 19.

Bonneau, J., Herley, C., van Oorschot, P.C., & Stajano, F. (2012). The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, 553–567. DOI: 10.1109/SP.2012.44.

Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K., 2004. Generating and remembering passwords. Appl. Cogn. Psychol. 18 (6), 641–651. https://doi.org/10.1002/acp.1014.

Campbell, J., Kleeman, D., Ma, W., 2006. Password composition policy: does enforcement lead to better password choices?. In: Proceedings of the 17th. Australasian Conference on Information Systems Password Composition Policy. Adelaide, Australia. ACIS, p. 60.

Campbell, J., Ma, W., Kleeman, D., 2011. Impact of restrictive composition policy on user password choices. Behav. Infor. Technol. 30 (3), 379–388. https://doi.org/10.1080/0144929X.2010.492876.

Cavallini, E., Bottiroli, S., Fastame, M.C., Hertzog, C., 2013. Age and subcultural differences on personal and general beliefs about memory. J. Aging Stud. 27, 71–81. https://doi.org/10.1016/j.jaging.2012.11.002.

Cavanaugh, J.C., Feldman, J.M., Hertzog, C., 1998. Memory beliefs as social cognition: a reconceptualization of what memory questionnaires assess. Rev. General Psychol. 2 (1), 48–65. https://doi.org/10.1037/1089-2680.2.

Chenchev, I., Aleksieva-Petrova, A., Petrov, M., 2021. Authentication mechanisms and classification: a literature survey. In: Intelligent Computing: Proceedings of the 2021 Computing Conference. Springer International Publishing, pp. 1051–1070. Volume 3.

Chiasson, S., Forget, A., Stobert, E., Van Orschot, P.C., Biddle, R., 2009. Multiple password interference in text passwords and click-based graphical passwords. In: Proceedings of the 16th. ACM Conference on Computer and Communications Security, CCS '09. New York, NY. ACM, pp. 500–511. https://doi.org/10.1145/1653662.1653722.

Cohen, J., 1992. Quantitative methods in psychology: A power primer. Psychol. Bull. 112, 1155–1159.

Cram, W.A., Proudfoot, J.G., D'arcy, J, 2017. Organizational information security policies: a review and research framework. Eur. J. Infor. Syst. 26, 605–641.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 3 (2), 90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. In Proceeding of NDSS'14, San Diego, CA, 23–26.

Davidson, H.C., Dixon, R.A., Hultsch, D.F., 1991. Memory anxiety and memory performance in adulthood. Appl. Cogn. Psychol. 5 (5), 423–433. https://doi.org/10.1002/acp.2350050504.

Devolder, P.A., Brigham, M.C., Pressley, M., 1990. Memory performance awareness in younger and older adults. Psychol. Aging 5 (2), 291–303. https://doi.org/10.1037/0882-7974.5.2.291.

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

Dixon, R.A., Hultsch, D.F., 1983a. Metamemory and memory for text relationships in adulthood: a cross-validation study. J. Gerontol. 38, 689–694. https://doi.org/10.1093/geronj/38.6.689.

Dixon, R.A., Hultsch, D.F., 1983b. Structure and development of metamemory in adulthood. J. Gerontol. 38, 682–688. https://doi.org/10.1093/geronj/38.6.682.

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

Duggan, G.B., Johnson, H., Grawemeyer, B., 2012. Rational security: modelling everyday password use. Int. J. Hum.–Comput. Stud. 70, 415–431. https://doi.org/10.1016/j.ijhcs.2012.02.008.

Flavell, J.H., 1971. First discussant's comments: what is memory the development of? Hum. Dev. 14, 272–278.

Flavell, J.H., 1979. Metacognitive and cognitive monitoring: a new area of cognitive developmental inquiry. Am. Psychol. 34, 906–911.

Florêncio, D., Herley, C., 2010. Where do security policies come from?. In: Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS' 10). New York, NY, 10. ACM. https://doi.org/10.1145/1837110.1837124.

Gaw, S., Felten, E., 2006. Password management strategies for online accounts. In: Proceedings of the Second Symposium on Usable Privacy and Security, (SOUPS). New York, NY. ACM, pp. 44–55. https://doi.org/10.1145/1143120.1143127.

Glass, J.M., Park, D.C., Minear, M., Crofford, L.J., 2005. Memory beliefs and function in fibromyalgia patients. J. Psychosom. Res. 58, 263–269. https://doi.org/10.1016/j.jpsychores.2004.09.004.

Grawemeyer, B., Johnson, H., 2011. Using and managing multiple passwords: a week to a view. Interact. Comput. 23, 256–267. https://doi.org/10.1016/j.intcom.2011.03.007.

Guo, K.H., 2013. Security-related behavior in using information systems in the workplace: a review and synthesis. Comput. Secur. 32, 242–251. https://doi.org/10.1016/j.cose.2012.10.003.

Hertzog, C. (1992). Improving memory: the possible roles of metamemory. In D. J. Herrmann, H. Weingartner, A. Searleman, and C. McEvoy (Eds.), Memory Improvement, (pp. 61–78). New York: Springer–Verlag.

Hertzog, C., Dixon, R.A., Hultsch, D.F, 1990a. Relationships between metamemory, memory predictions, and memory task performance in adults. Psychol. Aging 5 (2), 215–227. https://doi.org/10.1037/0882-7974.5.2.215.

Hertzog, C., Dixon, R.A., Hultsch, D.F, 1990b. Metamemory in adulthood: differentiating knowledge, beliefs, and behavior. Adv. Psychol.. 71, 161–212. https://doi.org/10.1016/S0166-4115(08)60158-2.

Hertzog, C., Dixon, R.A., Schulenberg, J.E., Hultsch, D.F, 1987. On the differentiation of memory beliefs from memory knowledge g: the factor structure of the metamemory in adulthood scale. Exp. Aging Res. 13 (2), 101–107. https://doi.org/10.1080/03610738708259308.

Hertzog, C., Lineweaver, T.T., Hines, J.C., 2014. Computerized assessment of age differences in memory beliefs. Perceptual Motor Skills: Phys. Develop. Measure. 119 (2), 609–628.

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 Cogn. 1 (3), 203–237. https://doi.org/10.1080/13825589408256577.

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

Infosecurity Magazine, 2018. How Much do Passwords Cost Your Business? Infosecurity Magazine. Retrieved from. https://www.infosecurity-magazine.com/opinions/how-much-passwords-cost/.

Inglesant, P., Sasse, M.A., 2010. The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2010. New York, NY. ACM, pp. 383–392.

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

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. Infor. Technol. Develop. 20 (2), 196–213.

Jia, R., Steelman, Z.R., Reich, B.H., 2017. Using mechanical Turk data in is research: risks, rewards, and recommendations. Commun. Assoc. Info. Syst. 41. https://doi.org/10.17705/1CAIS.04114. Article 14.

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

Keith, M., Shao, B., Steinbart, P., 2009. A behavioral analysis of passphrase design and effectiveness. J. Assoc. Infor. Sys. 10 (2), 63–89.

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. Am. J. Psychiatr. 171 (2), 201–208. https://doi.org/10.1176/appi.ajp.2013.12121590.

Lineweaver, T.T., Hertzog, C., 1998. Adult efficacy and control beliefs regarding memory and aging: separating general from personal beliefs. Aging, Neuropsychol. Cognit. 5 (4), 264–296. https://doi.org/10.1076/anec.5.4.264.771.

Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D, 2016. "Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including mechanical Turk and online panels. J. Strat. Infor. Syst. 25 (3), 232–240.

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. Pers. Individ. Dif. 52, 591–595. https://doi.org/10.1016/j.paid.2011.12.002.

Merdenyan, B., Petrie, H., 2022. Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours. Behav. Inf. Technol. 41 (12), 2514–2527. https://doi.org/10.1080/0144929X.2021.2019832.

Morgan, M.D., Chowdhury, M.M., Latif, S., 2021. Protecting business from data breach. In: 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, pp. 1–5.

Nelson, D., Vu, K.L., 2010. Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. Comput. Hum. Behav. 26 (4), 705–715.

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

O'Sullivan, J.T., Howe, M.L., 1995. Metamemory and memory construction. Conscious. Cogn. 4, 104–110.

Owens, J., Hawkins, E.M., 2019. Using online labor market participants for nonprofessional investor research: a comparison of MTurk and qualtrics samples. J. Infor. Syst. 33 (1), 113–128. https://doi.org/10.2308/isys-52036.

Pierce, S.H., Lange, G., 2000. Relationships among metamemory, motivation and memory performance in young school-age children. Br. J. Develop. Psychol. 18, 121–135.

Renaud, K., De Angeli, A., 2009. Visual passwords: cure-all or snake-oil? Commun. ACM 52 (12), 135–140. https://doi.org/10.1145/1610252.1610287.

Seitz, T., Hartmann, M., Pfab, J., Souque, S., 2017. Do differences in password policies prevent password reuse?. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA '17. New York, NY. ACM, pp. 2056–2063. https://doi.org/10.1145/3027063.3053100.

Shay, R., Komanduri, S., Durity, A.L., Huh, P., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N., Cranor, L.F., 2016. Designing password policies for strength and usability. ACM Trans. Infor. Syst. Secur. (TISSEC) 18 (4), 13. https://doi.org/10.1145/2891411.

Siponen, M., Klaavuniemi, T., 2020. Why is the hypothetico-deductive (HD) method in information systems not an HD method? Infor. Organiz. 30 (1), 100287 https://doi.org/10.1016/j.infoandorg.2020.100287.

Siponen, M., Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. Eur. J. Infor. Syst. 23 (3), 289–305.

Stobert, E., Biddle, R., 2014. A password manager that doesn't remember passwords. In: Proceedings of the 2014 New Security Paradigms Workshop, NSPW '14. New York, NY. ACM, pp. 39–52.

Stöber, J., Esser, K.B., 2001. Test anxiety and metamemory: general preference for external over internal information storage. Pers. Individ. Dif. 30 (5), 775–781. https://doi.org/10.1016/S0191-8869(00)00069-6.

Tam, L., Glassman, M., Vandenwauver, M., 2010. The psychology of password management: a tradeoff between security and convenience. Behav. Infor. Technol. 29 (3), 233–244.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F., 2016. Do users' perceptions of password security match reality?. In: Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI'16. New York, NY. ACM, pp. 3748–3760.

Vance, A., Eargle, D., Eggett, D., Straub, D., Ouimet, K., 2022. Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength. MIS Q. 46 (3), 1721–1738.

Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., Schultz, E.E., 2007. Improving password security and memorability to protect personal and organizational information. Int. J. Hum.–Comput. Stud. 65, 744–757. https://doi.org/10.1016/j.ijhcs.2007.03.007.

Warkentin, M., Walden, E., Johnston, A.C., Straub, D.W., 2016. Neural correlates of protection motivation for secure IT behaviors: an fMRI examination. J. Assoc. Infor. Sys. 17 (3), 194–215.

Weir, C.S., Douglas, G., Carruthers, M., Jack, M., 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. Comput. Secur. 28 (1), 47–62. https://doi.org/10.1016/j.cose.2008.09.008.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N., 2005. PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum.–Comput. Stud. 63, 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010.

Willison, R., Warkentin, M., 2013. Beyond deterrence: an expanded view of employee computer abuse. MIS Q. 37 (1), 1–20.

Woods, N., 2017. Frequently using passwords increases their memorability—A false assumption or reality?. In: Proceedings of the 23rd Americas Conference on Information Systems (AMCIS 2017). Boston, MA. AISeL, pp. 1–5.

Woods, N. (2019). The light side of passwords: turning motivation from the extrinsic to the intrinsic. In Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy (WISP 2019), Munich, Germany, 23.

Woods, N., Silvennoinen, J., 2022. Enhancing the user authentication process with colour memory cues. Behav. Inf. Technol. 1–20. https://doi.org/10.1080/0144929X.2022.2091474.

Woods, N., Siponen, M., 2018. Too many passwords? How understanding our memory can increase password memorability. Int. J. Hum.–Comput. Stud. 111, 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002.

Woods, N., Siponen, M., 2019. Improving password memorability, while not inconveniencing the user. Int. J. Hum.–Comput. Stud. 128, 61–71. https://doi.org/10.1016/j.ijhcs.2019.02.003.

Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. 24, 2799–2816.

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

Yildırım, M., Mackie, I., 2019. Encouraging users to improve password security and memorability. Int. J. Info.Secur. 18, 741–759.

Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J., 2009. Improving multiple password recall: an empirical study. Eur. J. Infor. Syst. 18 (2), 165–176. https://doi.org/10.1057/ejis.2009.9.

Zhang, L., McDowell, M.C., 2009. Am I really at risk? Determinants of online users' intentions to use strong passwords. J. Internet Comm. 8 (3–4), 180–197.

Zhang, Y., Monrose, F., Reiter, M.K., 2010. The security of modern password expiration: an algorithmic framework and empirical analysis. In: Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10). New York, NY. ACM, pp. 176–186. https://doi.org/10.1145/1866307.1866328.

Zimmermann, V., Gerber, N., 2020. The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes. Int. J. Hum. Comput. Stud. 133, 26–44.

**Naomi Woods** is an Assistant Professor in Cyber Security. She has a Ph.D. in Cognitive Science and an MSc. in Clinical Psychology. Her research centers around the usability and security of authentication, and information security behavior. More specifically, it focuses on password security and memorability, inclusivity and accessibility of cyber security, and security-related technostress. Reflecting this multidisciplinary perspective, Woods has published studies in international journals and conferences in the fields of Human-Computer Interaction and Information Systems. Woods has received over 1 million EUR in external research funding, and has been the PI on several security-related projects.

**Mikko Siponen** is a Professor of Information Systems at the University of Jyväskylä, Finland. He has a Ph.D. in Philosophy from the University of Joensuu, Finland and a Ph.D. in Information Systems from the University of Oulu, Finland. Siponen is ranked among the top 30 scholars in Information Systems discipline. His-research interests include IS security, cybercrimes, IS development, computer ethics, IT use, and philosophical aspects of IS. In addition, Siponen has held managerial and leadership positions such as, Head of Department and Vice Dean for Research at the University of Jyväskylä. He has been PI for research projects funded by the Academy of Finland, the EU, Business Finland, and the Finnish Funding Agency for Technology and Innovation.