Forgot Your Password?

Motivating the Adoption of a Password Manager

Sophie Graf

Department of Psychology of Conflict, Risk & Safety

Faculty of Behavioural, Management and Social Sciences, University of Twente

Under the supervision of Dr. Iris van Sintemaartensdijk and Dr. Jan-Willem Bullee

July 7, 2022

Abstract

Hacking attacks pose one of the most common threats online. While strong passwords effectively protect online accounts from such attacks, users often resort to weak passwords due to the burden of remembering secure passwords. While password managers can solve this problem, adoption rates are still low. This experimental study was conducted to test the effectiveness of coping nudges (i.e., self-efficacy, response efficacy, response cost) based on Protection Motivation Theory to raise behavioural intention to adopt a password manager and facilitate password manager adoption. For this purpose, a randomized controlled trial was implemented with a pre-post measurement of behavioural intention. I controlled for the potential influence of other variables on behavioural intention (i.e., initial trust in password managers, password management practices and knowledge, security attitudes). In a follow up study after two weeks, it was assessed whether participants followed through on their behavioural intention. The results demonstrate that coping nudges did not encourage PM adoption or increase behavioural intention to adopt a PM. However, initial trust in password managers significantly predicted the intention to adopt a password manager. Based on the findings, I suggest that advertisements for password managers should highlight their trustworthiness, and future studies could research effective ways to foster the user's trust in password managers. The main conclusion is that password manager adoption appears to be substantially different from the implementation of other cyber security measures.

Keywords: password manager, cyber security, coping messages, nudging, self-efficacy, response efficacy, response cost, Protection Motivation Theory

Forgot Your Password? Motivating the Adoption of a Password Manager

Digital technologies are transforming our lives at a speed that no other milestone invention has done before. With the internet many of our everyday tasks have become more convenient, as working, shopping, communication, and the like, all take place online. We can access Facebook, Google Drive, our LinkedIn profile and favorite streaming platforms, online banking, and plenty more from anywhere in the world. All that is possible as our data is stored online, and we access it through our accounts.

Naturally, just as we would protect the valuables in our home, we must also guard our sensitive data. In 2019, 13% of Dutch citizens aged 15 and above, stated to have fallen victim to cybercrime (Centraal Bureau voor de Statistiek [CBS], 2020), with 42% of those crimes being hacking attacks. Cybercrime is defined as any crime that is either supported by technology (i.e., sending abusive texts) or exists only because of computer technology (i.e., unauthorizedly accessing a computer to gain financial information) (Bossler & Berenblum, 2019). International cybercrime records produce even higher numbers. In a survey from 2018 among U.S. adults, 32.7% of respondents reported having experienced a hack of their social media or e-mail account (Johnson, 2021). Cybercrime caused a financial loss of 621.45 million US dollars only in the state of California in 2020, further showcasing the severity of this issue (Johnson, 2021).

As these statistics prove, there is an urgent need for smart solutions to reduce the threat posed by a hacking attack. Those examples also raise the question where the security gap is in user's current protection strategies. At the moment, passwords are still the most common authentication method, although they are a highly flawed method (Kudale & Hemaltha, 2021).

Cyber criminals use a range of techniques to get hold of passwords, one of them is hacking attacks. Hackers will often guess passwords based on personal information of the target

or by randomly using words from a dictionary (Pedreira et al., 2021). Such hacking attempts can successfully be warded off by using secure passwords. Numerous websites have implemented strategies to nudge users to create a safe password, for instance through the use of a color code that indicates password strength, and by providing instructions about what constitutes a good password (Furnell & Esmael, 2017). Yet, problematically, most people use passwords that are easy to guess (Yildrim & Mackie, 2019). Remembering strong and unique passwords is cumbersome and takes a strain on the memory of the user, which is why many people resort to weak passwords and reusing passwords. Among cyber security professionals such issues are widely known and are referred to as the human factor (Herley et al., 2009; Summers & Bosworth, 2004). A quickly viable solution to this issue is a password manager (PM), as they relieve the memory burden by storing passwords for the user (Alkaldi & Renaud, 2016). Precisely, password managers are digital tools designed to increase the user's cyber safety by managing and generating passwords for the user. Passwords are stored within the manager as encrypted (i.e., unreadable) versions and can be decrypted (i.e.., converted into readable format) only by the master key, which is a master password created by the user. As password managers represent a form of informational risk mitigation, research in that field belongs to the branch of information security (Andress, 2019). Despite PMs offering an effective method to protect against cyber-attacks by improving password hygiene, adoption rates are still low (Farooq, 2019).

Determinants of PM Adoption and Adoption Intention

Pearman et al. (2019) offer a comprehensive overview of barriers for PM adoption. They recruited 30 participants for a semi-structured interview from a variety of password management strategies: not involving password-specific tools (e.g., notebooks, an Excel spreadsheet), built-in

password managers (e.g., iCloud KeyChain, Google Chrome Password Manager), and separately installed password managers (e.g., LastPass, KeePass). They confirmed and added depth to multiple previously identified barriers, which can be classified as security concerns, lack of need, and lack of awareness.

Security Concerns

Possibly the most prominent concern addresses the security of PMs (Pearman et al., 2019). This finding fits the picture drawn by previous research. An overwhelming body of research identified trust in password managers, or broadly speaking, security concerns as a main determinant for password manager adoption (Alkaldi & Renaud, 2016; Alodhyani et al., 2020; Aurigemma et al., 2017; Bahmanziari et al., 2003; Farooq et al., 2021; Karole et al., 2011; Maclean & Opphoff, 2018; Pearman et al., 2019). Trust relates to security concerns in that some users believe that password managers are not secure, unreliable, susceptible to security breaches, or sell the user's passwords to third parties (Fagan et al., 2017). Apart from numerous interviews that explored adoption factors and recognized trust as a key element (Alkaldi & Renaud, 2016, Alodhyani et al., 2020, Aurigemma et al., 2017, Pearman et al. 2019), it is also incorporated in models within cyber security literature that aim to explain technology adoption. Particularly, Maclean and Ophoff (2018) demonstrated the predictive power of trust for PM adoption intention within the framework of the Unified Theory of Acceptance and Use of Technology 2 with trust as an additional construct. Likewise, initial trust as proposed by the initial trust model plays a significant role in adoption intention, while personal predisposition to trust does not have an effect (Farooq et al., 2021). Furthermore, a salient security concern revolved around storing all passwords in the same place (Pearman et al., 2019). This distress with a single point of failure was previously established in studies about PM adoption (Fagan et al., 2017; Alkaldi & Renaud,

2016). Lastly, users may feel inhibited to use a PM if they do not know where their passwords are stored and how they are processed (Pearman et al, 2019). This is underlined by the fact that transparency about data storage, processing and usage was identified as a focal point for PM adoption (Alodhyani et al., 2020).

Lack of Need

The second major rationale for refraining from using password managers, may be summarized as a form of lack of need for it (Pearman et al, 2019). It is worth noting that this is almost exclusively a perceived lack, and not an actual lack. Specifically, some users may perceive their accounts as not valuable to require a PM. Other users report preferring to remember their passwords (Pearman et al., 2017). Recent discoveries shed a different light on this finding. Renaud and Zimmermann (2019) attempted to encourage PM use by placing a short explanation video about PMs on a student enrolment page next to the password entry field. When students enrolled through that website by creating an account, choosing a password, and enrolling, they also had to indicate whether they currently use a PM. The researchers found that the password strength of students who used a password manager was significantly higher than passwords chosen by students who did not (Renaud & Zimmermann, 2019). Naturally, if one uses easy-to-remember passwords, likely they are simple and easy to hack as well.

Indeed, many people wrongly believe their current password practices are safe (Alkaldi & Renaud, 2016). The assumption is further supported by the finding that individuals who score higher in password management knowledge are more likely to use a password manager (Kennison & Chan-Tin, 2021). A perceived lack of need may also derive from the mistaken impression that the user would not be at risk of a cyber-attack (Pearman et al., 2019).

Lack of Awareness

The third major barrier to adoption represents the lack of awareness of PMs (Pearman et al., 2019). Some users simply do not know that there is a tool available that safely stores passwords. This issue was echoed by numerous scholars (Alkaldi & Renaud, 2016; Fagan et al., 2017). Similarly, a lack of awareness on how password managers work may prevent users from using such tools (Aurigemma et al., 2017). For this reason, research on this subject has occasionally incorporated short videos explaining PMs before the main experimental manipulation to ensure that awareness is given (Aurgiemma et al., 2019). On a similar note, other scholars have used explanation videos to specifically investigate how awareness influences PM adoption (Renaud & Zimmermann, 2019; Albayram et al., 2021). Precisely, Albayram et al. (2021) compared a text message to a video-based message and found that both were comparable in raising understanding of PMs. However, outside of the context of a study, users may not be willing to watch an explanatory video about PMs. When Renaud and Zimmermann (2019) provided this kind of video next to the password entry field of a student enrolment page, 6% started the video, only .73% watched the video until the end, and just 4% indicated afterwards that they planned to install a PM.

In conclusion, to facilitate PM adoption in a fruitful way, multiple barriers need to be tackled. First and foremost, it appears that security concerns associated with PMs play a central part in keeping PM adoption rates low. For instance, some users do not feel that PMs are trustworthy, or they are worried about the fact that PM represent a single point of failure. Similarly, more transparency on how data is stored and processed was demanded. Second, users often believe that they do not need a password manager, largely due the several misbeliefs. Specifically, many users think their current password practices (i.e., reusing passwords, using weak passwords, sharing passwords) are secure when they are in fact unsafe (Alkaldi & Renaud,

2016). In addition, people tend to believe they are not at risk for a cyber-attack, or their accounts would not be valuable enough to require the extra security offered by a PM (Pearman et al., 2019). Third, there is no sufficient public awareness of PMs and how to use them (Alkaldi & Renaud, 2016; Aurigemma, 2017; Fagan et al., 2017).

Protection Motivation Theory

So far, researchers had some success with incorporating and applying these insights in models and interventions aiming to predict and encourage behavioural intentions to adopt a PM. Specifically, the implementation of Protection Motivation Theory (PMT) in this field of research yields promising results. PMT is one of the major motivational theories in Psychology with a background of extensive research (Menard et al., 2017a). Given that PMT has also been commonly and successfully adopted in the information security sector, it is a worthwhile endeavor to examine to what extent it applies to PM adoption (Menard et al., 2017a).

PMT views protection motivation as a result of a coping appraisal and a threat appraisal. The threat appraisal consists of threat severity and threat susceptibility, while the coping appraisal comprises self-efficacy, response efficacy, and response cost (Menard et al., 2017a). Threat severity is the perceived severity of the threat, whereas a person's perceived vulnerability to a threat or perceived likelihood of that threat is described by threat susceptibility. Both concepts positively affect protection motivation. Concerning the coping appraisal, self-efficacy refers to someone's belief in their capabilities to perform a given task (Bandura, 1977). Response efficacy on the other hand describes the belief that the recommended action will prevent the threat, while response cost is defined by the perceived costs (i.e., money, time) associated with performing the recommended action (Menard et al., 2017a). Self-efficacy and response efficacy positively influence protection motivation and thereby ultimately protective behavior, perceived

response cost on the contrary diminishes protection motivation (Menard et al., 2017a).

Applying Protection Motivation Theory to Password Manager Adoption

In an experiment, Menard et al. (2017a) used short messages based on PMT constructs to facilitate PM adoption. Participants randomly received one out of six messages each appealing to a different construct from PMT. They identified response efficacy as the most important and only significant determinant of PMT. A stronger influence of PMT was established by Aurigemma et al. (2019), as they compared the core PMT against the full PMT in terms of their explanatory power for PM adoption. As defined by Aurigemma et al., (2019), the predictors in the core model are self-efficacy, response efficacy, threat severity, and threat susceptibility, whereas the full model includes response cost, maladaptive rewards, and fear as additional predictors. Importantly, in the core model, self-efficacy was the most powerful facilitator, besides a weak predictive power of response efficacy. On the other hand, in the full model, response efficacy turned out to have the greatest impact, together with a moderate negative relationship between response cost and PM adoption (Aurigemma et al., 2019). While response cost has often been ignored in information security research (Floyd et al., 2000), it was noted by Aurigemma et al. (2019) that its contribution may be caused by the high set up cost associated with password managers. Regardless, it appears that the coping appraisal plays a vital role in the decision to adopt a PM. Other researchers supported the relevance of PMT constructs outside of models. For instance, Aurigemma et al. (2017) conducted an interview in which they identified perceived costs and benefits as an important reason for PM adoption. For participants that intended to use a PM but ended up not doing so, to a large extent insufficient time caused the inaction.

While the application of PMT produces not entirely coherent results, it confirms and

complements the empirically derived facilitators as well as core issues that keep users from installing a PM. Namely, self-efficacy, response efficacy, and concerns related to perceived response cost (e.g., lack of time, high set up cost) were raised (Aurigemma, 2019; Aurigemma, 2017; Menard, 2017a).

Coping Nudges

Even though interventions applying PMT to PM adoption are still scarce, the theory has been successfully used as framework for other security interventions. For instance, PMT has been adopted to investigate compliance with security policies (Herath & Rao, 2009), the use of antimalware programs (Johnston, 2010), and other behaviour with the goal of protecting PCs and home networks (Crossler & Belanger, 2014). For that purpose, nudging interventions have been commonly employed. They can be described as the systematic design and use of subtle messages to modify behaviour. Nudges are unique in that they are less strict than policies for instance, since they do not force but rather encourage a certain (desirable) behaviour (Thaler & Sunstein, 2008). Therefore, an advantage of nudging interventions is that they do not require timely investment of the users due to their short nature. A recently published research agenda for the field of cybercrime underlines and promotes the importance and usefulness of measures that do not interfere with the daily life of users (Leukfeldt, 2017). The implementation of nudges may be especially useful in the context of PM adoption, as nudges could simultaneously increase awareness of PMs – one of the main obstacle for PM use – while ensuring optimal cost-effectiveness.

Van Bavel et al. (2019) conducted an experiment to test the effect of PMT nudges on consumer behaviour in e-commerce. Right before making a mock purchase, participants received either a coping nudge, a fear appeal nudge, a combined nudge, or none (i.e., control).

Subsequently, they navigated through a website to do the online purchase. The results indicate that users who received a nudge navigated significantly safer than users in the control condition. In addition, participants in the coping condition navigated safer than the ones in the fear appeal condition and equally safe as participants in the combined condition (van Bavel et al., 2019). Other studies too support the conclusion that coping elements are more effective than threat elements in motivating protective action (Burns, 2017; Hanus & Wu, 2016; Jansen & Van Schaik, 2017; LaRose et al., 2005). An explanation may be that within information security, attacks are often directed towards organizations, and thus threats such as a data breach may not be relevant to the user at a personal level (Burnkrant & Unnava,1989; Johnston, 2015). Information security refers to the methodologies and practices with the purpose of protecting sensitive data, often in digital form, from unauthorized access and alteration (Andress, 2019). Nevertheless, other cyber threats tend to be perceived as relevant to the individual, leading to inconsistent outcomes of PMT within information security (Boss et al., 2015). Thus, even though users should feel that the threat of an account compromise applies to them, still the suitability of PMT for information security must be closely examined and verified.

Coping Appraisal

Further underscoring the importance of the coping appraisal, Aurigemma (2019) found that the threat appraisal did not influence intentions to adopt a PM, while coping appraisal constructs did (i.e., self-efficacy, response efficacy). These findings were replicated for compliance with password guidelines (Mwagwabi et al., 2018). The role of self-efficacy and response efficacy as the most influential determinants for protective action, and thus coping appraisal as a whole, is sustained by other work (Boehmer et al., 2015, Jansen & Van Schaik, 2017). A meta-analysis by Floyd et al. (2000) provides more evidence in favor of this argument.

The analysis comprised 65 studies assessing one or more PMT constructs with intention or behaviour as dependent variable. Of these 65 studies, 27 investigated only intention, 22 assessed only behavior, and 16 evaluated both behavior and intention. Notably, the effect sizes of the threat appraisal varied between small and medium, while the effect sizes of the coping appraisal constructs ranged from medium to large (Floyd et al., 2000). Additionally, all PMT constructs had larger effect sizes with intention compared to behavior (Floyd et al., 2000). A study by Milne et al. (2000) mostly replicated these findings.

Generally, the coping appraisal constructs of PMT evidently have a strong impact on protective actions and protection intention. Hence, nudges that entail a coping element are expected to perform excellent at predicting protection motivation as demonstrated by van Bavel et al. (2019). It follows that they are a compelling solution for security interventions.

The Present Study

Utilizing coping nudges to promote PM adoption appears to be a promising approach. Previous research hints at the fact that the coping appraisal constructs (self-efficacy, response efficacy, response cost) as described by PMT could indeed be a key aspect in the decision of (not) adopting a password manager. Within information security it is common and arguably useful to convey such messages as nudges, therefore I will follow these examples. The core of the present study is therefore to test three different types of coping nudges (self-efficacy, response efficacy, response cost) based on PMT with the aim of increasing PM adoption and adoption motivation. As there is no clear picture about the relative importance of each coping appraisal construct for PM adoption, I explore if the type of nudge impacts adoption and intention to adopt when comparing the three conditions. Few interventions have assessed actual PM adoption behaviour instead of merely measuring behavioural intentions, which denotes a

distinct contribution of the present research. Apart from that, other factors potentially influence behavioural intention and PM adoption as well. To account for them, I will measure initial trust in password managers, perceived barriers to PM adoption, attitude towards cyber security measures, and current password management practices and knowledge. What follows concerning the experimental manipulation and the core of the study is the following:

- I hypothesize that coping nudges will increase behavioural intention to adopt a password manager
- I hypothesize that behavioural intention to adopt a password manager will have a positive effect of password manager adoption after two weeks
- I explore whether there will be a difference in behavioural intention to adopt a password manager between the coping nudge conditions (self-efficacy, response efficacy, response)
- I explore whether there will be differences in password manager adoption between the coping nudge conditions (self-efficacy, response efficacy, response cost)

Methods

Design

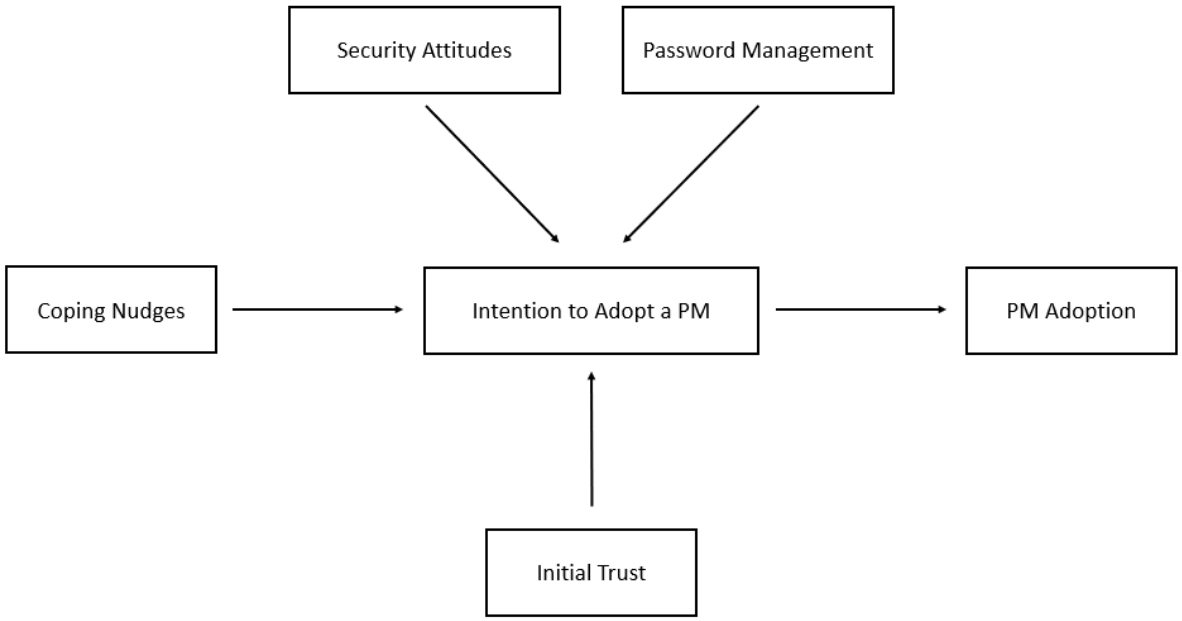
The hypotheses were tested with a longitudinal experimental design. It involved a between-subject factor (coping manipulations) and a within-subject factor (measurements at three different times). The main aim of the present study is to investigate the effect of coping nudges on the behavioural intention to adopt a password manager. The between-subject factor consisted of a coping manipulation that has four conditions: self-efficacy nudge, response efficacy nudge, response cost nudge, and a control group that was not presented with a coping nudge. Participants were randomly assigned to one of the four conditions.

The study entailed within-subject measures that were taken at:

pre-intervention/baseline (Time 1 [T1]), post-intervention (Time 2[T2]), and two-week follow up (Time 3 [T3]). At T1, baseline-measures were taken to prevent bias through the intervention. Baseline measures are basic demographics and topic-specific demographics, behavioural intention to adopt a password manager, and other variables that are expected to affect the intervention effect, i.e., barriers, security attitudes, initial trust, and password management. At T2, participants had received the coping nudge and indicated their intention to adopt a password manager. This way I ensured that any changes in behavioural intention are due to the manipulation. At T3 two weeks after the intervention, participants reported whether they have adopted a password manager. I chose the time interval of two weeks as it gives participants enough time to consider whether they would like to use a password manager and act upon it. For a conceptual representation of the study design see Figure 1.

Figure 1

Conceptual representation of the Study Design



Note. Password management refers to current password management practices and knowledge. Coping nudges are the self-efficacy, response efficacy, and response cost nudges. Barriers for PM adoption are not represented in the figure, as this variable was dropped.

Participants

After excluding non-eligible participants and respondents that did not pass the attention check, 64 participants remained for the interventional study and 22 responses were kept from the follow up survey. For the attention check, participants were asked to select the seventh option on a 7-point Likert scale to show that they are paying attention. The inclusion criteria encompassed being at least 18 years old, and not using a password manager or only for less important accounts. The exclusion of respondents that already use a password manager was chosen in

accordance with the aim of the study, which is motivating the adoption of a password manager. In the interventional study, participants were randomly allocated to the experimental conditions: self-efficacy (n = 14), response efficacy (n = 18), response cost (n = 13), control condition (n = 15). Only 34.4% of respondents participated in the follow up survey, resulting in a small sample size per condition in the follow up: self-efficacy (n = 8), response efficacy (n = 6), response cost (n = 6), control condition (n = 2).

Respondents in the interventional study were on average 24.3 years old (SD = 8.9) with an age ranging from 18 to 60, compared to a mean age of 27.9 years (SD = 13.8) with an age ranging from 19 to 60 in the follow up. In the main survey, 3.1% respondents reported being of Hispanic, Latino, or Spanish origin (n = 2), compared to 4.5% participants in the follow up (n = 1). Furthermore, 92.2 % of participants in the interventional study identified as white (n = 95), 4.7 % as Asian (n = 3), and 8% indicated identifying as another race or ethnicity (n = 5). In the follow up survey, 95.5% reported identifying as white (n = 21), and 9% identified (n = 2) as another race or ethnicity. For a detailed overview of participant's demographic characteristics, see Appendix A.

Materials

Coping Manipulation

The coping manipulation consisted of a coping nudge that was designed to increase behavioural intentions to adopt a password manager by enhancing participants' self-efficacy or response efficacy, or by diminishing perceived response cost (see Appendix B for the coping nudges). All coping nudges entailed basic information about the password manager such as: password managers save passwords for the user, password can be manually entered and stored in the password manager or saved when they are entered on a website, and a suggestion for the

mobile password manager Bitwarden.

I decided to recommend the password manager Bitwarden based on the following considerations. First, I considered the popular password managers (i.e., Dashlane, LastPass, Keeper, and 1Password). However, the usability of these managers is low (Seiler-Hwang et al., 2019). I established three selection criteria to minimize adoption barriers: all functions must be free of charge, availability is given for all operating systems (i.e. Linux, macOS, Windows, Android, iOS), and synchronization of multiple devices is possible. Even though the better-known manager KeePass fulfills these standards, its usability is not satisfactory as determined through a usability test by the researcher. Relevant criteria were simplicity of design, understandability of instructions, and how quick and intuitive the most important functions could be accessed. Bitwarden on the other hand offers these features, whilst having acceptable usability as judged by the researcher. Precisely, the interface is simple and clear, and the main functions (i.e., overview of saved passwords, password generator, activating auto-fill) are quick and easy to spot. Generally, I decided to suggest a mobile version of a password manager since Karole et al. (2011) found that less technically-savvy users prefer a smartphone password manager over an USB- and online password manager, and the sample of the current study is expected to consist mainly of average users who are not necessarily technology-experts.

For the construction of the coping nudges, I adhered to the topics covered by the self-efficacy, response efficacy, and response cost items from Menard et al (2017b), who assessed PMT in the context of PMs. The self-efficacy condition received the information that a browser extension of Bitwarden can be downloaded to PCs to synchronize and use Bitwarden on all devices. Participants of the self-efficacy condition were also informed that password managers have an autofill-password function for websites, and that they are easy and convenient to use. I

chose to provide those pieces of information in accordance with the self-efficacy items of Menard et al. (2017b) regarding password manager use, which cover the topics of convenience, ease of use, and effortlessness. For example, one items states: "Password manager software is convenient to use" (Menard et al., 2017b). This item addresses convenience of PMs, which I adapted to "Password managers are convenient as they have an autofill-password function for websites and a password generator function" for the self-efficacy nudge.

In the response efficacy condition, participants were notified that Bitwarden stores encrypted versions of your passwords to minimize the threat of a cyberattack, password managers are highly secure, offer a secure password generator, and that passwords are protected by a master key. The presented information is based on Menard et al. (2017b)'s response efficacy items concerning the use of password managers. All items revolved around protection. To illustrate, one statement is: "When using password manager software, online accounts are more likely to be protected" (Menard et al., 2017b), which I adapted to "Password managers store and protect your passwords" for the response efficacy nudge.

Participants of the response cost condition were informed that Bitwarden is free of charge, that the user only needs to remember one master key to access all passwords, that Bitwarden has a password generator function, and autofill is activated with one click, making it quick and effortless to set up. Again, the information is centered around Menard et al. (2017b)'s response cost items regarding password manager use. Menard et al. (2017b) required participants to rate how financially costly, burdensome, time consuming, effortful, and worth it they regard password manager use to be. An example item addressing financial costs is: "Using password manager software is financially costly for me" (Menard et al., 2017b). This statement was adapted to "An example of a **free** mobile password manager is Bitwarden" for the response cost

nudge. The control condition received a short notification with basic information: "Password managers store passwords. An example of a password manager is Bitwarden."

Questionnaires

At T1, participants filled out questionnaires concerning barriers for password manager adoption, initial trust in password managers, security attitudes, password management, and participant characteristics. They also reported their behavioural intention to install and effectively use a password manager. At T2, participants again indicated their intention to adopt a password manager. In the follow up survey at T3, participants reported whether they have installed a password manager and used its basic functions.

Participant Characteristics. Participants' demographic and topic-specific characteristics were also assessed. I asked for age, nationality, gender, ethnicity and race, education, employment status, and income. Apart from that, topic-specific questions were covered, consisting of (a) time spent accessing the internet per device, (b) social media use, (c) does the participant have a technical background, (d) has the participants been a victim of cybercrime in the past 12 months, and (e) number of online accounts.

Time spent online. For a study that focuses on password managers for online accounts, the time spent online per device (i.e., smartphone, tablet, and laptop and/or desktop computer) is part of the relevant information about the sample. Participants could choose from five response options to indicate the time they spent online on an average weekday (i.e., not at all, up to 1 hour, 1-3 hours, 3-5 hours, more than 5 hours).

Social media use. Kennison and Chan-Tin (2021) predicted password manager adoption for students through social media use and password manager knowledge with 84.2 percent accuracy. Therefore, I expect that password manager adoption is increased for students who are

heavy social media users. To assess participant's social media use, I asked participants to indicate the time they spend on social media on an average day. Respondents selected from six response options (i.e., less than 30 minutes, between 30 minutes to 1 hours, between 2 hours and 4 hours, between 4 hours and 8 hours, more than 8 hours).

Technical background. Pearman et al. (2019) found out that when password managers involve greater work, users turned to other, generally less secure techniques (e.g., reusing passwords for less important accounts). This was especially true for less technically competent users who wanted to use a password manager that was installed separately. Therefore, I decided to ask participants whether they had technical background. Response options were "Yes" and "No". My expectation is that participants without a technical background (regular users) are less prone to adopt a password manager.

Victim of cybercrime. Participants who have suffered from an account compromise in the past likely want to avoid this in the future and may be more willing to put effort into protecting themselves (Martens et al., 2019). Victims of cybercrime are thus expected to have a predisposition towards password manager adoption and behavioural intention to adoption. For this reason, I asked participants whether they had been a victim of cybercrime in the past 12 months. They could choose between the responses "Yes" and "No".

Number of online accounts. Furthermore, the number of online accounts is part of the participant characteristics as well. Response options were 0-9 accounts, 10-19 accounts, or 20 or more accounts. The assumption is that respondents with a higher number of online accounts are more likely to (intent to) adopt a password manager.

Behavioural intention. To assess password manager adaption intention, I modified one item from Menard et al. (2017b). The original item: "Please indicate the likelihood that you will

install the password manager software described above" (Menard et al., 2017b, p. 1), was adjusted to "Please indicate the likelihood that you will install a password manager" to fit the context of the survey. The item is rated on an 11-point Likert scale ranging from “Extremely unlikely” to “Extremely likely” with a neutral midpoint “Neither likely nor unlikely” as instructed by the authors (Menard et al., 2017a). In addition to that, I self-constructed one scale for behavioural intention of effective PM use to test whether intentions to install a PM translate in intentions to effectively use it. I decided to inspect this relation as previous research indicates a gap between the two (Pearman et al., 2019). For the construction of the four items, I drew on the behaviours that participants must execute to effectively use a password manager. They cover the usage of a password manager and secure password generator, and creation of a master key. An example item is: "I will use a password manager to generate safe passwords for my online accounts". I chose to assess the items on a 5-point Likert scale, ranging from “Strongly disagree” to “Strongly agree” with a neutral midpoint “Neither agree nor disagree”, as this allows for sufficient nuance but does not cause decision fatigue. The self-constructed scale proved good reliability when measured at T1 ($\alpha = .875$), and excellent reliability for the second measurement at T2 ($\alpha = .935$).

Barriers. I included seven items to assess barriers that prevent participants from using a password manager. Since there was no suitable scale available, I developed one myself. Six of the seven items are based on the barriers identified by Pearman et al. (2019) to adopt a password manager and effectively use it. Barriers entail a lack of awareness, security concerns, lack of need, concern about a single point of failure, past negative experiences, and wrong risk assessment. To illustrate, Pearman et al. (2019) labeled a lack of need as “Not Enough to Protect”, detailed by a few examples, e.g., "[Participants] felt that they were able to remember

their passwords without help" (Pearman, et al.,2019), and "[Participants] felt that their accounts were not sufficiently high-value to require extra security like that offered by a password manager" (Pearman et al., 2019). I adjusted the topic with its description to " There is no need for me to use a password manager (e.g., I do not have enough accounts to need a password manager, I can remember my passwords, I use a physical notebook)". On top of that, I added one item concerning usability: "Password managers do not have good usability", as usability of password managers is low and might influence adoption and behavioural intention (Seiler-Hwang et al., 2019). Items were rated on a 5-point Likert scale, ranging from "Strongly disagree to "Strongly agree" with a neutral midpoint" Neither agree nor disagree", as this allows for sufficient nuance but does not cause decision fatigue. As reliability analysis revealed a low Cronbach's alpha ($\alpha = .153$), I tested whether the data is suited for exploratory factor analysis. A Kaiser-Meyer-Olkin's measure of sampling adequacy revealed miserable sampling adequacy at .52. Bartlett's test of sphericity came out non-significant at .45. Both Kaiser-Meyer-Olkin's and Bartlett's test values suggest that the data is not suitable for factor analysis as it cannot be compressed in a meaningful way. Consequently, the scale was dropped from further analysis.

Initial Trust. I adopted five items that measure initial trust in password managers from Farooq et al. (2021). Security concerns, largely concerning the trust in password managers, are likely to have a significant positive impact on adoption intention. Items are derived from on the Initial Trust Model by McKnight et al. (1998) and were modified to fit password managers by Farooq et al. (2021). The scale asked participants to rate the reliability and security of password manager software. The scale showed good reliability ($\alpha = .824$). Items were assessed on a 5-point Likert scale, ranging from "Strongly disagree to "Strongly agree" with a neutral midpoint" Neither agree nor disagree", as instructed by the authors (Farooq et al., 2021).

Security Attitudes. I included a Self-Report Measure of End-User Security Attitudes (SA-6) to assess how participants feel about the use of cyber security measures (Faklaris et al., 2019). A person's general attitude towards these measures may facilities or impede PM adoption (Albayram et al., 2021; Faklaris et al., 2019). The scale includes six items that concern interest, knowledge, and motivation to stay safe online. Participants received the instruction: "Each statement below describes how a person might feel about the use of security measures. Examples of security measures are laptop or tablet passwords, spam email reporting tools, software updates, secure web browsers, fingerprint ID, and anti-virus software." (Faklaris et al., 2019). Items were randomized and rated on a 5-point Likert scale, ranging from "Strongly disagree to "Strongly agree" with a neutral midpoint" Neither agree nor disagree", as instructed by the authors (Faklaris et al., 2019). The scale proved acceptable reliability ($\alpha = .783$).

Password Management. To assess how well participants manage their passwords, I added all nine items about password management from the Human Aspects of Information Security Questionnaire (HAIS-Q), and constructed three items myself (Parsons et al., 2017). If one is not aware of password guidelines, one might falsely believe their current password practices are safe and thus feel they do not need a PM. Consequently, current password management practices and knowledge must be measured. I adjusted the wording of the HAIS-Q items to fit the sample of this study better, which mainly consists of students. To illustrate, in the original study, participants rated how much they agree with the statement "I am allowed to share my work password with colleagues". I adapted it to "I am allowed to share my passwords with friends". HAIS-Q items were assessed on a 7-point Likert scale, ranging from "Strongly disagree to "Strongly agree" with a neutral midpoint" Neither agree nor disagree", as instructed by the authors (Parsons et al., 2017). The three self-constructed items were added to put emphasis on

secure password knowledge. Naturally, individuals who are not aware of the complexity of strong passwords are less likely to feel that they need a password manager. I included these items to test for this effect. An example item is: "It's acceptable to use my birth date as my password". Items were rated on a 7-point Likert scale to be coherent with the previous items from the HAIS-Q. While the scale proved acceptable reliability ($\alpha = .716$), I observed consistently negative inter item correlations of the self-constructed item: "I use words that can be found in a dictionary as my password". After removing the item, reliability increased ($\alpha = .784$).

Behavioural Change. To measure behavioural change, I constructed the following item: "Have you installed a password manager since the first survey two weeks ago? If you already used a password manager, but only for less important accounts, are you using it for important accounts now?" Response options were "Yes" or "No". In addition to that, I decided to test to what extent PM adoption is associated with effective PM use. For that purpose, the four self-constructed items from the behavioural intention scale were altered to describe behaviour instead of intention. For example, this item assessing behavioural intention: "I intend to use a password manager to safely store my passwords", was modified to an item that evaluates behavioural change: "I am using a password manager to safely store my passwords." I chose to assess the items on a 5-point Likert scale, ranging from "Strongly disagree to "Strongly agree" with a neutral midpoint" Neither agree nor disagree", as this allows for sufficient nuance but does not cause decision fatigue. Reliability of the scale could not be assessed due to small sample size ($n = 3$). Lastly, participants in the follow up survey that did not install a PM were asked to indicate a reason, which enables me to understand what prevented participants from using PMs. Participants selected from four response options (I am concerned about the security of password managers, I do not need a password manager, I wanted to look into it but I did not find the time,

Other [i.e., Open text entry]). I chose the response options based on the major barriers for PM adoption (i.e., lack of need, security concerns), and a key obstacle (i.e., lack of time), that is assumed to prevent users with high behavioural intention to act upon their intention (Aurigemma et al., 2017). Lack of awareness was not included as response option as I presumed that the coping nudges would raise awareness of PMs.

Procedure

The surveys were hosted in Qualtrics. Before the start of the study, eligibility was assessed in one question regarding participant's current password manager use (required is no use or use only for less important accounts). If participants were not eligible, the survey automatically ended for them. Eligible respondents received a short overview of the questionnaires, procedure and aim of the study, and gave informed consent (see Appendix C for the written informed consent for the interventional study). In this preview, I withheld the information that the ultimate goal of the study is to motivate password manager adoption, and that adoption will be assessed in the follow up survey. The aim was to prevent any bias participants could experience towards installing a password manager. Following the informed consent, the interventional study began. Participation took approximately 15 minutes.

Participants responded to questionnaires that assessed behavioural intention to adopt a password manager, barriers to password manager use, participant's security attitudes and password management, and initial trust in password manager (see Appendix D for the questionnaires in the interventional study). For all parts of the survey, a response was required to proceed to the next question. Next, participants were randomly assigned to one of the four experimental conditions (self-efficacy nudge, response efficacy nudge, response cost nudge or control condition).

In all conditions, participants were informed that they will be presented with a security notification that should be kept in mind. After receiving the nudge, demographic as well as topic-specific demographic questions were collected. Subsequently, participants reported the likelihood they will install a password manager and use it for core activities, this time with the coping nudge (or no nudge in case of the control group) in mind. Assessing demographics in between these two scales was an intentional choice to obscure the connection between the coping nudges and the second assessment of behavioural intention to adopt a password manager. Lastly, the respondents indicated whether they agree to participate in the follow-up. Those who disagreed to partake in the follow up received a full debrief (see Appendix E for the full debrief). Participants that agreed provided their e-mail address, so they could be invited to the follow up and their results from both surveys may be connected. To ensure that the email address is correct, it had to be entered twice and only if both addresses match the participant may continue. However, since the system is sensitive to upper-and lowercase letter differences as well as spaces, some participants experienced difficulties with the restriction (n = 5), and it was lifted mid-data collection. After that, an incomplete debrief was provided (see Appendix F for the incomplete debrief).

In the follow up survey, participants first received the statement of consent (see Appendix G for the written informed consent for the follow up survey). After agreement, they were asked to enter their e-mail address once again, so that their responses from the interventional study and follow up could be connected. Next, they indicated whether they had installed a PM and if they did, whether they are using it effectively (see Appendix H for the questionnaires in the follow up survey). If participants reported not using a PM, they were asked to indicate the reason. Lastly, participants received a full debrief. Participation in the follow up took circa 5 minutes.

Data Analysis

Main Analyses

The data was analyzed using the statistical software SPSS (version 28). During preliminary analyses, I used a one-way analysis of variance (ANOVA) to test for potential differences between conditions to assess whether randomization to conditions was successful.

Then, the hypotheses and explorations were investigated with different statistical analyses. First, a linear mixed model (LMM) was used to evaluate whether coping nudge conditions increased behavioural intention to adopt a password manager compared to the control group. A mixed effects model is a blended model that allows for analyses on between – and within-subject level. In a second LMM, initial trust, security attitudes, and password management were added to the core model with the aim of controlling for the potential influence of these variables on behavioural intention. For the LMM, the dataset was converted into long format and the measurements of behavioural intention at pre-intervention (i.e., T1) and post-intervention (i.e., T2) were converted into one behavioural intention variable.

Second, a one-way between participant ANOVA was used to assess whether there will be differences in behavioural intention to adopt a password manager depending on coping nudge (self-efficacy, response efficacy, response cost).

Third, I conducted a binary logistic regression to investigate whether behavioural intention to adopt a password manager at post-intervention has a positive effect on password manager adoption after two weeks.

Fourth, I analyzed whether there are differences in password manager adoption at T2 depending on the coping nudge (self-efficacy, response efficacy, response cost) with Pearson's chi square test of independence.

Additional Analyses

I conducted additional analyses to check whether certain variables may influence behavioural intention and to investigate other effects explained below. The assumptions about these relationships are partly derived from literature and partly based on the logic of the present study. First, I used multiple one-way AOVA to examine whether there are significant differences in behavioural intention at pre-intervention (i.e., T1) depending on individual differences in topic-specific demographics (i.e., social media use, number of online accounts, whether participants have a technical background, and whether they have been a victim of cybercrime). Second, multiple one-way ANOVA were implemented to test whether there are significant differences in baseline variables (i.e., initial trust, security attitudes, password management, behavioral intention at T1) for non-users of PMs compared to participants who used a PM for less important accounts at pre-intervention. Lastly, I analyzed frequencies of the reasons that participants reported for not adopting a PM in the follow up survey (i.e., T3), with the aim of understanding the rationale for not using a PM.

Results

Preliminary Analysis

Initially, 149 participants took part in the interventional study. Participants that did not meet the inclusion criteria were automatically excluded (n = 55). Then, I excluded participants that did not pass the attention check (n = 7), and omitted respondents that did not finish the study. A total of 64 participants for the interventional study remained. For the follow up study, all 22 responses were valid and complete, making up a dropout rate of 65,6 %.

Next, I checked for outliers in all scales. One outlier in the scales for password management and initial trust was detected. I paid specific attention to these scores but decided not to exclude the respondents as there was no reason to assume that a data entry error or measurement error was present.

Random Assignment to Conditions

Before the main analyses, I used a one-way ANOVA to investigate whether there are differences between the conditions regarding any baseline measures or topic-specific variables. The conditions were similar in initial trust [$F(3, 60) = 1.56$, $p = .209$], security attitudes [$F(3, 60) = 0.08$, $p = .971$], password management [$F(3, 60) = 1.00$, $p = .398$]. Moreover, the conditions did not significantly differ in social media use [$F(3, 60) = 0.58$, $p = .576$], and whether participants had a technical background [$F(3, 60) = 0.89$, $p = .885$], and whether they had been a victim of cybercrime [$F(3, 60) = 1,62$, $p = .194$]. Thus, random assignment to conditions was successful.

Main Analyses

For an overview of the descriptive statistics of all assessed constructs see Table 1.

Table 1

Descriptive statistics of Behavioural Intention, Initial Trust, Security Attitudes, and Password Management

Variable	*n*	*M*	*SD*	Min	Max
Behavioural intention at T1 [a]	64	5.7	3	1	11
Behavioural intention at T2 [a]	64	5.7	3	1	11
Initial trust [b]	64	3.2	0.6	1	4.6
Security attitudes [b]	64	5.5	0.8	1	4.2
Password management [c]	64	2.6	5.5	2.6	7

Note. Password management refers to current password management practices and knowledge. High scores are indicative of adequate password hygiene, while low scores indicate inadequate password hygiene.

[a] assessed on a 11-point Likert scale

[b] assessed on a 5-point Likert scale

[c] assessed on a 7-point Likert scale

Behavioural Intention

To test my first hypothesis, whether behavioural intention to adopt a password manager increased due to the coping nudges, I used two linear mixed models (LMM). The core model denotes fixed effects of pre/post measurement (i.e., time with the values 1 and 2 for T1 and T2) and condition on the dependent variable behavioural intention, with a fixed effect of the interaction between time and condition. Time was defined as repeated measure and subject was denoted as random effect. Then, I tested for assumptions of normality, homoscedasticity, and

linearity. A histogram of the model's residuals and a kurtosis statistic of -1.19 (*SE* = .46) revealed that the data were not normally distributed. Nevertheless, the assumption of homoscedasticity and linearity was verified with a scatterplot of the predicted values x residuals. Both assumptions were not violated. I proceeded with the analysis of the data with a LMM. The model yielded a significant main effect of condition on behavioural intention [$F(3, 119.81) = 4.81$, $p = .003$]. The main effect of time [$F(1, 119.81) = 0.00$, $p = .994$] and the interaction effect between time and condition [$F(3, 119.81) = 0.21$, $p = .890$] were non-significant. Hence, condition influences behavioural intention, but that effect does not significantly differ for pre/post measurement (i.e., time). In other words, the effect of condition on behavioural intention cannot be attributed to the experimental manipulation. These findings did not confirm my first hypothesis that coping nudges will increase behavioural intention to adopt a password manager compared to the control condition.

In a second LMM, the variables of behavioural Intention, initial trust, security attitudes, and password management were added to the core model as fixed effects covariates. The aim of this analysis was to control for the potential influence of these other variables, to make a more accurate judgement of my first hypothesis. I inspected the assumptions in the same manner as I did for the core model. No assumptions were violated, hence, I proceeded with the LMM. In this model, both main effects of condition and of initial trust were significant. The parameter estimates of fixed effects signify that initial trust is strongly positively related to behavioural intention ($B = 1.51$, $p = <.001$) and the parameter estimate clearly falls into the 95% CI [0.72, 2.30]. As no other significant effects were found, it can be concluded that condition affects behavioural intention, but not as a result of pre/post measurement (i.e., time). These findings thus largely replicate the findings from the first LMM, again not confirming my first hypothesis.

Furthermore, note that compared to the core model, the second model yields a marginally more significant effect of condition with a slightly larger effect size. The tests for the fixed effects are summarized in Table 2.

Table 2

Type III Tests of Fixed Effects for the Dependent Variable Behavioural Intention

Parameter	*Numerator df*	*Denominator df*	*F*	*Sig*
Intercept	1	116.89	1.17	.281
Time	1	116.89	0.00	.994
Condition	3	116.91	5.34	.002
Time * Condition	3	116.89	0.24	.871
Security attitudes	1	116.88	1.98	.163
Initial trust	1	116.88	14.3	<.001
Password management	1	116.88	1.06	.306

Note. Password management refers to current password management knowledge and practice.

While the LMM as a blended model did not indicate that coping nudges affected behavioural intention at T2, a one-way between subject ANOVA was conducted to further examine the relationship between behavioural intention and coping nudge conditions. The aim of this analysis is to investigate my first exploration, whether there were differences between the coping nudge conditions (i.e., self-efficacy, response efficacy, response cost) concerning their behavioural intention at T2. Next, I verified the assumptions of normality, linearity, independence and homogeneity of variances. First, a Shapiro-Wilk test showed that behavioural intention is normally distributed for the response efficacy and response cost condition, but not

for the self-efficacy condition. However, an ANOVA is generally robust to the violations of normality, hence, I progressed with the analyses. Second, I confirmed the absence of outliers using boxplots. Third, due to the randomized design of the present study, the assumption of independence is met. Fourth, the assumption of homogeneity of variances was confirmed by a Levene's test [$F(2, 46) = 1.52$, $p = .229$]. The results of the one-way ANOVA indicated no significant differences between the coping nudge conditions in regard to behavioural intention [$F(2, 60) = 2.482$, $p = .095$].

Behavioural Change

In my second hypothesis, I hypothesized that behavioural intention leads to behavioural change (i.e., password manager adoption) after two weeks. A binary logistic regression was used to examine whether behavioural intention at T2 was associated with the likelihood of behavioural change. The assumption of multicollinearity was met as there is only one independent variable. (tolerance = 1.00). An inspection of standardized residual values revealed that there was no outlier. The predictor variable behavioural intention was tested a priori to verify there was no violation of the assumption of the linearity of the logit ($p = .582$). The outcome variable was behavioural change (i.e., password manager adoption). The model explained between 16.6 % (Cox & Snell R square) and 30.3 % (Nagelkerke R square) of the variance in the dependent variable and correctly classified 86.4 % of cases. However, behavioural intention did not significantly contribute to the model, meaning, behavioural intention did not significantly predict behavioural change [$Exp(B) = .54$, $p = .200$]. These results are not in line with my second hypothesis.

Furthermore, to examine my second exploration, I explored whether there are differences between coping nudge conditions (i.e., self-efficacy, response efficacy, response cost) in respect

to behavioural change (i.e., password manager adoption). A Pearson's Chi Square test of independence was used to test if the frequency of behavioural change is more likely for one coping nudge compared to the others. The outcomes show that behavioural change was achieved to a higher percentage by respondents in the self-efficacy condition (25%) compared to the response efficacy condition (16.67%). Moreover, a higher percentage of participants in the response efficacy condition demonstrated behavioural change compared to the response efficacy condition (0%). However, the Pearson's Chi Square test of independence revealed that behavioural change was not significantly more likely for one condition compared to the others [χ^2 (2, N = 20) = 1.70, p = .429]. However, interpretation of this test may not be meaningful since 50% of the cells have an expected count of less than five, and 0.9 is the minimum expected count.

Additional Analyses

First, I examined whether there are significant differences in behavioural intention at pre-intervention (i.e., T1) depending on individual differences in topic-specific demographics. A one-way ANOVA revealed no significant differences in behavioural intention depending on the social media use [F(5, 58) = 0.26, p = .933], the number of online accounts [F(2, 61) = 4.81, p = .234], whether the participant has a technical background [F(1, 62) = 0.028, p = .868], and whether they have been a victim of cybercrime [F(1, 62) = 0.21, p = .652]. Thus, behavioural intention seems unaffected by variations in topic-specific information.

Second, I tested whether there are significant differences in baseline variables for non-users of PMs compared to participants who used a PM for less important accounts at pre-intervention. A one-way ANOVA indicated no significant differences in initial trust [F(1, 62) = 0.03, p = .871], security attitudes [F(1, 62) = 0.77, p = .383], password management [F(1, 62) =

0.82, $p = .369$], and behavioural intention [$F(1, 62) = 1.42$, $p = .239$] at T1 depending on PM use. Hence, whether participants used a PM before the intervention did not significantly influence baseline measures.

Lastly, I examined why people decided not to use a PM. Half of the participants in the follow up provided an explanation ($n = 11$), from which 45.5% percent reported a lack of need as their main reasoning for not installing a PM ($n = 5$), and another 45.5% said they wanted to look into it, but they did not find the time ($n = 5$) , and 9% were concerned about the security of PMs ($n = 1$).

Discussion

With more and more aspects of our lives taking place online, numerous opportunities arise for cyber criminals to detect security gaps and exploit unprotected systems. In many cases, a weak password is at the core of those vulnerabilities (Gerlitz et al., 2021) However, often users fail to implement strong and unique passwords as they are burdensome to come up with and even harder to remember (Chaudhary et al., 2019). Password managers represent an easy solution to this problem, yet few people are using them (Chaudhary et al., 2019).

Therefore, the present study aimed to raise user's intentions to install a PM and facilitate PM adoption through coping nudges. Furthermore, this study tested whether coping nudges (i.e., self-efficacy, response efficacy, response cost) differ in their ability to increase behavioural intention and facilitate PM adoption. Very few studies have examined the effect of coping nudges on intention to adopt a PM, and merely one investigated their effect on actual adoption behaviour. In addition to that, to the best of my knowledge, this study is the first to measure preexisting behavioural intentions, highlighting the validity and uniqueness of the present study.

The key findings of this research can be summarized as follows. First, contrary to my first hypothesis, the results did not indicate that coping nudges elevated intention to adopt a PM. Second, opposing my second hypothesis, I found that high behavioural intention to adopt a PM did not result in PM adoption two weeks post-intervention. Third, regarding my explorations, I found that no coping nudge was superior to the others in enhancing behavioural intentions or initiating behavioural change.

The findings of this study contribute to previous work in many relevant ways. First, this study largely replicates and validates the findings from Menard et al. (2017a), who tested the effect of different fear appeals on behavioural intention to adopt a PM. In their study, self-

efficacy and response cost nudges did not raise behavioural intention either. Only the response efficacy nudge showed a nearly negligible positive effect on behavioural intention. These, together with the present finding that coping nudges did not raise intentions to adopt a PM, imply that installing a PM may be substantially different from other security behaviour such as using an anti-malware application, for which coping messages have proven to be effective (Aurigemma et al., 2019). In practice, it is often concluded that any intervention is better than no intervention (Hartman, 2009). Only by taking preexisting behavioural intention into account and thus ruling out a potential interference of high baseline intention, it can be concluded with high certainty that this rule of thumb does not apply to the present study.

Unique Factors in Password Manager Adoption

Excessive Effort and Time

Indeed, there may be crucial differences between PM adoption and other security actions that make PM adoption more difficult. First, the present findings may support the conclusion that there is excessive effort associated with setting up a PM. For many users, it takes considerable effort or time to learn how to use a PM and set it up before the tool becomes functional and convenient (Aurigemma et al., 2019). Perhaps the coping nudge could not outweigh the toll of an initial PM arrangement. Indeed, previous research has shown that when password managers require additional effort, users resort to other methods, often less secure (e.g., reusing passwords for lower-value accounts) (Pearman et al., 2019). These findings highlight the user's consistent evaluation of the trade-off between convenience (e.g., required time and effort) and security (Pearman et al., 2019). Further supporting the exceptional role of response cost, nearly half of the participants in the follow up survey who reported a reason for not adopting a PM, indicated that they wanted to look into password managers, but did not find

the time. These outcomes align with previous work, that revealed a lack of time as the most prevalent inhibitor of PM installment (Aurigemma et al., 2017).

The Role of Threat

Second, the finding that a response efficacy nudge did neither encourage PM adoption nor increase behavioural intention, provides further evidence for the presence and importance of threat apathy. Threat apathy describes the idea that threats posed by poor password management are not worth initiating extra action. A response efficacy nudge emphasizes how well a recommended response protects from the threat. However, if one is essentially not concerned with a threat, then a response efficacy nudge becomes irrelevant. People that do not use password management tools often implement weak passwords or reuse passwords as the cognitive burden of creating and remembering strong, unique passwords is too high (Alkaldi & Renaud, 2016). The reason may be that many users do not believe that the threat posed by a weak password requires any protective action, such as the replacement with strong passwords. Indeed, in a survey, 25% of the participants (non-PM users) reported not using a PM due to reasons that can be conceptualized as threat apathy (Aurigemma et al., 2017). Therefore, research in information security may have often yielded a stronger relevance of response efficacy message, as the threat of a weak password is arguably less evident to most users than is the threat of a virus for instance (Huth et al., 2013). On top of that, threat apathy may also unravel why, in the follow up, almost half of the participants that gave a reason for not installing a PM indicated that they do not need a PM, despite overall high password management knowledge in the sample. In other words, it appears as though several participants felt that they did not need a password manager despite being aware of the complexity that is required for secure passwords, thus, supporting the presence of threat apathy.

The Extended Parallel Process Model (EPPM) provides further insight and a theoretical basis for this observed phenomenon. EPPM is a fear appeal theory according to which protection motivation arises as a result of a threat appraisal and an efficacy appraisal (self-efficacy, response efficacy) (Witte, 2009). However, while in PMT coping appraisal and threat appraisal take place simultaneously, according to EPPM the threat appraisal precedes the efficacy appraisal. If no threat is perceived, protection motivation cannot be elicited (Witte, 2009). For the present study this could imply that the coping nudges could not be effective because participants did not perceive a weak password as a threat. These implications could be evidence of a special role that threat appraisal has in PM adoption, that is substantially greater than it was assumed up to this day. In line with this, Ayyagari et al. (2019) incorporated PMT constructs in their model specifically designed to explain the intention to use a PM. The survey data that was collected verified the relevance of threat severity and threat susceptibility as both turned out to be strong determinants of PM use (Ayyagari et al., 2019).

Initial Trust in Password Managers

Third, the adoption of a PM requires considerable trust, given that a data breach – while unlikely – would be fatal. Therefore, usage of this tool may be viewed as risky, which makes it distinct from other security actions (Alkaldi & Renaud, 2022). Importantly, a key finding of the present study is that initial trust in password managers significantly increases the intention to adopt a PM. As such, this study provides strong evidence that initial trust in PMs is critical, and perhaps the primary factor for PM adoption. Its relevance has been recognized by many scholars (Aurigemma et al., 2017; Bahmanziari, 2016; Farooq et al., 2021; Maclean & Ophoff, 2018; Renaud & Zimmermann, 2019). Initial trust conceptualizes the degree to which a technology is reliable, safe, and secure (Farooq et al., 2021). Thus, initial trust might be so powerful in this

context as it covers and touches upon a range of more general security concerns. For instance, many users feel concerned about storing all passwords in the same place (Alkaldi & Renaud, 2016; Fagan et al., 2017; Pearman et al., 2019). Due to the prominence of trust, previous work has sometimes included trust in password managers in models predicting behavioural intention to adopt a PM, proving its effectiveness within different contexts (e.g.., Initial trust model, Unified Theory of Technology Acceptance) (Farooq et al., 2021, Ayyagari et al., 2019; Maclean & Ophoff, 2018). The present results validate these findings and further define the scope of trust for PM adoption. Previous research that tested the limits of the role of trust, found that neither users' trust in general technology (Ayyagari et al., 2019), nor predisposition to trust influence PM adoption (Farooq et al., 2021).

Strengths and Limitations

The present study had multiple strengths. Randomized controlled trials were implemented to test the effect of different coping nudge conditions (i.e., self-efficacy, response efficacy, response cost) on behavioural intention. In my analyses, I confirmed that randomization was successful by establishing that there were no significant differences in baseline measures and topic-specific variables. Using randomized controlled trials prevents selection bias and ensures that any differences in outcome are due to the manipulation. Furthermore, behavioural intention was assessed at pre-intervention and at post-intervention to account for preexisting intention to adopt a PM. Moreover, I did not rely on behavioural intentions alone to assess the effect of the coping nudges, as I included a follow up survey to test whether participants acted upon their intention to install a PM. This is an effective way to address the intention-behaviour gap, which is the failure to follow through on set intentions, and a prevalent issue in research (Faries, 2016). Furthermore, I used a linear mixed model to test the effect of coping nudges on

behavioural intention, and control for other variables that potentially affect behavioural intention (i.e., initial trust in password managers, password management, security attitudes). This analysis enabled me to assess the change in behavioural intention depending on the condition, while accounting for a random factor of participant. As I controlled for other variables, initial trust in password managers could be identified as significant predictor of intention to adopt a PM.

Next, several limitations of the present study need to be discussed. First, the present study may lack a repetition of the coping nudge to unfold its full potential. Other applications of PMT within information security have used periodic fear appeal messages. Boss et al. (2015) for instance successfully encouraged the use of an anti-malware software with repeated fear appeals instead of a single nudge and utilized prompts to continuously remind users to run the program. The element of repetition to escalate the effectiveness of an intervention is well established (Gundu et al., 2019). Furthermore, as users are generally familiar with other major cyber security measures, such interventions may function in itself as a reminder compared to the unfamiliarity with password managers that many users experience (Aurigemma et al., 2019).

Furthermore, the present findings seem to imply that nudging interventions may be less preferred to motivate PM adoption. When comparing this study to Aurigemma et al. (2019), who also used a fear appeal to promote the adoption of a PM, it is somewhat striking that they found a moderate influence of response efficacy and response cost on adoption intention. However, they used a two-minute animated video with plenty of detailed information. A video presentation is arguably more extensive and visually immersive, and thus appears to convey a fear appeal more effectively than the nudge used in the present study. Beyond that, Renaud and Zimmermann (2019) concluded that even a video may not sufficiently address and effectively handle the security concerns users face in regard to PMs, recommending an even more interactive and

personal approach.

Another limitation concerns the design of the study. It cannot be determined whether the coping nudges in fact manipulated coping cognitions (i.e., self-efficacy, response efficacy, response cost), because I did not measure coping constructs. The design of the present study relies on an indirect effect of coping nudges through coping cognitions on behavioral intention. However, the possibility cannot be ruled out that the reason coping nudges did not significantly affect behavioural intention is that coping cognitions were not manipulated.

Moreover, the validity of this study may be threatened due to a small sample size in the interventional study (n = 64) and follow up survey (n = 22). While 64 participants can be deemed sufficient, if they are split between the four conditions, the sample size for each condition is critically small (i.e., between 13 and 18 participants per condition). Thus, the finding that all coping nudges are equally ineffective in increasing behavioural intention to adopt a PM, can be called into question. Regarding the follow up survey, the conclusion that high intention to adopt a password manager does not result in password manager adoption, should be taken with caution. More severely, we should be careful about generalizing the finding that the different coping nudges are equally ineffective in facilitating PM adoption, as it is based on a very small sample (i.e., between 6 and 8 participants per condition).

Lastly, as discussed, there are several seemingly relevant barriers that prevent users from adopting a PM (e.g., lack of need, security concerns, lack of time, high set up cost). Therefore, I constructed a questionnaire to assess barriers and control for them in my analyses. However, the questionnaire demonstrated low reliability, hence, barriers could not be assessed.

Future research

Future research could build on the current findings in several ways. While coping nudges

are a promising approach to facilitate PM adoption and increase behavioural intention to do so, no such facilitation could be observed in the current study. Multiple limitations have been identified, that, if properly handled in future studies, could reveal stronger effects of coping nudges. First, a replication of this intervention is needed that measures coping cognitions at pre- and post-intervention to establish with certainty if coping nudges do not have the power to alter coping constructs, or if coping elements (i.e., self-efficacy, response efficacy, response cost) do not have a sufficient bearing in PM adoption. Second, as previous work shows, the element of repetition may be essential to initiate behavioural change (Gundu et al., 2019). Former interventions within information security used for instance prompts to remind users of the security action that should be performed (Boss et al., 2015). A replication study of this intervention could employ repeated coping nudges to test whether this effectively enhances the use such an easy measure as a nudge. The employment of repeated coping nudges is especially promising if we consider that one of the most prominent reasons that people do not install a PM is lack of immediacy (i.e., planning to install a PM but forgetting about it) (Aurigemma, 2017). In that, a repeated nudge also serves as a reminder to previously set intentions, which in theory further improves the intervention's success.

On a different note, since the present study provides further evidence that trust in PMs is an essential determinant of PM adoption, future studies could aim at nurturing user's trust in PMs. For instance, some users question the security of master keys (Alodhyani, 2020). Indeed, password managers do not enforce common password policies (e.g., inclusion of special characters) for the master key, making them potentially susceptible to hacking attacks (Aloudhyani, 2020). In addition to that, users may fail to establish trust in PMs as PMs rarely provide information on how and where the passwords are stored. Previous work supports the

detrimental effect of this lack of transparency for PM adoption (Alkaldi, 2016; Aloudhyani, 2020). Thus, future studies could build upon these insights by testing whether enforcing password policies for master keys, as well as providing information on how and where passwords are stored, is in fact useful to facilitate PM adoption.

Moreover, the present findings may imply that coping nudges are ineffective as long as users do not perceive a weak password as a threat. Indeed, many users are indifferent to the threat posed by a weak password (i.e., threat apathy) (Aurigemma, 2017). Thus, PM adoption might be better explained by EPPM, as this theory suggests that both threat appraisal and coping appraisal are compulsory to evoke protection motivation (Witte, 2019). Hence, future interventions facilitating PM adoption could benefit from integrating a threat message that emphasizes the risks associated with undesirable password habits, next to a coping message. When designing the threat message, special attention should be given to making the threat of poor password management immediately evident and personally relevant to the user (Burnkrant & Unnava,1989; Johnston, 2015).

Furthermore, in this study, response cost nudges did not increase behavioural intention to adopt a PM. It seems likely that the response cost nudge could not outbalance the effort that is associated with setting up a PM before it becomes usable. Therefore, I advise researchers to build upon the mobile application designed by Alkaldi (2019) that recommends a suitable password manager to the users, in order to relieve the burden of choice (Alkaldi, 2019). In addition, as the usability of common PMs is low (Chaudhary et al., 2019), scholars could focus on implementing an intuitive design and appealing interface to ensure that users perceive the set up and use of PMs as quick and effortless (Carreira et al., 2021).

Implications for practitioners

Based on the findings of the present study, there are some recommendations for practice. In the current study, initial trust significantly affected behavioural intention to adopt a PM. Thus, to successfully encourage PM adoption, advertisements for password managers should focus on emphasizing the trustworthiness of these tools. Based on the initial trust model, initial trust depends to a large extent on structural assurances (Farooq et al., 2021). In a technological context, such assurances are third-party certificates, encryption, and safe procedures (Farooq et al., 2021). For PMs specifically, users are mainly worried about their data and look for guarantees (Farooq et al., 2021). Thus, advertisements of PMs should give information on how the data is stored and processed, as well as provide and highlight guarantees.

Conclusion

In the present research, I set out to understand how different coping nudges influence password manager adoption. Despite the limitations, this study provided clear support that coping nudges do not to facilitate PM adoption or increase intentions to do so. The rationale for implementing coping nudges was that they have been successful at facilitating other cyber security behavior, and they have rarely been tested in this context. The current findings indicate that the adoption of a password manager may be substantially different from other security behavior within information security for which coping messages have proven effective. Particularly, the results demonstrate that password manager adoption requires considerable trust, which often represents a barrier for adoption. That way, the present research underlines that security concerns are essential to overcome first. Based on these conclusions, I recommend that practitioners emphasize the trustworthiness of password managers when advertising for them. To better understand the implications of the present results, future studies could replicate this study with additional pre and post measurements of the relevant coping constructs, as well as test

whether the effectiveness of the coping nudges may be elicited through repetition of the nudge. Overall, the present study contributed to cyber security research and the understanding of what determines or hinders PM adoption, by testing the applicability of coping nudges for PM adoption.

References

Albayram, Y., Liu, J., & Cangonj, S. (2021). Comparing the effectiveness of text-based and video-based delivery in motivating users to adopt a password manager. *European Symposium on Usable Security 2021*. https://doi.org/10.1145/3481357.3481519

Alkaldi, N., & Renaud, K. (2016). Why do people adopt, or reject, smartphone password managers? *Proceedings 1st European Workshop on Usable Security*. https://doi.org/10.14722/eurousec.2016.23011

Alkaldi, N., & Renaud, K. (2018). Encouraging password manager adoption by meeting adopter Self-Determination needs (extended version). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3259563

Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password Managers—It's all about trust and transparency. *Future Internet*, *12*(11), 189. https://doi.org/10.3390/fi12110189

Aurigemma, S., Mattson, T., & Leonard, L. (2017). So much promise, so little use: What is stopping home End-Users from using password manager applications? *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. https://doi.org/10.24251/hicss.2017.490

Aurigemma, S., Mattson, T., & Leonard, L. (2019). Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. *AIS Transactions on Replication Research*, *5*, 1–21. https://doi.org/10.17705/1atrr.00035

Ayyagari, R., Lim, J., & Hoxha, O. (2019). Why (don't) we use password managers? A study on the intention to use password managers. *Contemporary Management Research*, *15*(4),

227–245. https://doi.org/10.7903/cmr.19394

Bahmanziari, T., Pearson, J. M., & Crosby, L. (2003) Is Trust Important in Technology Adoption? A Policy Capturing Approach. *Journal of Computer Information Systems, 43*(4), 46-54. https://doi.org/10.1080/08874417.2003.11647533

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295x.84.2.191

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022–1035. https://doi.org/10.1080/0144929x.2015.1028448

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/misq/2015/39.4.5

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. https://doi.org/10.1080/0735648x.2019.1692426

Burnkrant, R. E., & Unnava, H. R. (1989). Self-Referencing. *Personality and Social Psychology Bulletin*, *15*(4), 628–638. https://doi.org/10.1177/0146167289154015

Burns, A., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Carreira, C., Ferreira, J. F., & Mendes, A. (2021). Towards improving the usability of password managers. *InFORUM*. Retreived from: https://archimendes.com/publication/2021/Inforum/INFORUM2021_UsabilityPMs.pdf

CBS. (2020, December 18). *Welk percentage van nederlanders koopt online? En wat. . . - nederland in cijfers 2020*. Welk percentage van Nederlanders koopt online? En wat. . . - Nederland in cijfers 2020 | CBS. Retrieved May 25, 2022, from

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69–90. https://doi.org/10.1016/j.cosrev.2019.03.002

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, *7*(1). https://doi.org/10.1186/s13673-017-0093-6

Faklaris, C., Dabbish, L., & Hong, J. I., 2019. A Self-Report measure of End-User security attitudes (SA-6). *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019).* https://doi.org/10.13140/RG.2.2.29840.05125/3

Faries M. D. (2016). Why We Don't "Just Do It": Understanding the Intention-Behavior Gap in Lifestyle Medicine. *American journal of lifestyle medicine*, *10*(5), 322–329. https://doi.org/10.1177/1559827616638017

Farooq A. (2019) *In Quest of information security in higher education institutions: Security awareness, concerns and behaviour of students*. [Doctoral Dissertation. University of

Turku] Turku. https://research.utu.fi/converis/mypages/browse/Publication/42654823

Farooq, A., Dubinina, A., Virtanen, S., & Isoaho, J. (2021). Understanding dynamics of initial trust and its antecedents in password managers adoption intention among young adults. *Procedia Computer Science*, *184*, 266–274. https://doi.org/10.1016/j.procs.2021.03.036

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Furnell, S., & Esmael, R. (2017). Evaluating the effect of guidance and feedback upon password compliance. *Computer Fraud & Security*, *2017*(1), 5–10. https://doi.org/10.1016/s1361-3723(17)30005-2

Gerlitz, E., Häring, M., Smith, M. (2021) Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS)* (pp.17-36). ISBN:978-1-939133-25-0

Gundu, T., Flowerday, S., & Renaud, K. (2019). Deliver security awareness training, then repeat:{Deliver; Measure Efficacy}. 2019 conference on information communications technology and society (ICTAS), 1-6. https://doi.org/10.1109/ICTAS.2019.8703523

Hanus, B., & Wu, Y. A. (2015). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Hartman S. E. (2009). Why do ineffective treatments seem helpful? A brief review. *Chiropractic & osteopathy*, *17*, 10. https://doi.org/10.1186/1746-1340-17-10

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Herley, C., Van Oorschot, P. C., & Patrick, A. S. (2009, February). Passwords: If we're so smart, why are we still using them? In *International Conference on Financial Cryptography and Data Security* (pp. 230-237). Springer, Berlin, Heidelberg.

Huth, A., Orlando, M., & Pesante, L. (2013). Password Security, Protection, and Management. Retrieved from https://www.us-cert.gov/security-publications/password-security-protection-and-management.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ics-03-2017-0018

Johnson, J. (2021, April 29). *U.S. consumers and cyber crime - statistics & facts*. Statista. Retrieved May 25, 2022, from https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/#topicHeader__wrapper

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. https://doi.org/10.25300/misq/2015/39.1.06

Johnston, & Warkentin. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Karole, A., Saxena, N., & Christin, N. (2011). A comparative usability evaluation of traditional password managers. *Information Security and Cryptology - ICISC 2010*, 233–251. https://doi.org/10.1007/978-3-642-24209-0_16

Kennison, S. M., & Chan-Tin, D. E. (2021). Predicting the adoption of password managers: A tale of two samples. *TMS Proceedings 2021*. https://doi.org/10.1037/tms0000097

Kudale, A., & Hemalatha, S. (2021). Cloud computing: An analysis of authentication methods over internet. *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, 765–773. https://doi.org/10.1007/978-981-16-0882-7_68

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51*(3), 71–76. https://doi.org/10.1145/1325555.1325569

Leukfeldt, R. (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Eleven International Publishing.

Maclean, R., & Ophoff, J. (2018). Determining key factors that lead to the adoption of password managers. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. https://doi.org/10.1109/iconic.2018.8601223

Martens, M., de Wolf, R., & de Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Menard, P., Bott, G. J., & Crossler, R. E. (2017a). User motivations in protecting information security: Protection motivation theory versus Self-Determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Bott, G. J., & Crossler, R. E. (2017b). Appendix C: Instrument Items. In User motivations in protecting information security: Protection motivation theory versus Self-

Determination theory. *Journal of Management Information*

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in Health-Related behavior: A Meta-Analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems, 42*. https://doi.org/10.17705/1cais.04207

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19)*. 319–338. http://doi.org/10.5555/3361476.3361500

Pedreira, V., Barros, D., & Pinto, P. (2021). A review of attacks, vulnerabilities, and defenses in industry 4.0 with new challenges on data sovereignty ahead. *Sensors*, *21*(15), 5189. https://doi.org/10.3390/s21155189

Renaud, K., & Zimmermann, V. (2019). Encouraging password manager use. *Network Security, 2019*(6), 20. https://doi.org/10.1016/s1353-4858(19)30075-3

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019). “I don’t see why I would ever want to use it.” *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3319535.3354192

Statista. (2021, March 18). *Financial cyber crime losses in the U.S. 2020, by victim state*. Retrieved May 25, 2022, from https://www.statista.com/statistics/234993/us-states-with-the-largest-losses-through-

cybercrime/#:%7E:text=Financial%20cyber%20crime%20losses%20in%20the%20U.S.%202020%2C%20by%20victim%20state&text=California%20reported%20a%20loss%20of,reported%20cyber%20crime%20in%202020

Summers, W., & Bosworth, E. (2004). Password policy: the good, the bad, and the ugly. *Proceedings of the Winter International Symposium on Information and Communication Technologies (ACM 2004)*. 1–6.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness* (Revised&Expanded ed.). Penguin Books.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

Appendix A

Sociodemographic Characteristics of Participants

Sociodemographic Characteristics	Intervention (N = 64)		Follow-up (N = 22)	
	n	%	*n*	%
Gender				
Male	35	39.1	11	50
Female	25	54.7	10	10
Non-binary/ Third gender	2	3.1	1	4.5
Prefer not to say	2	3.1	0	0
Nationality				
German	39	60.9	14	63.6
Dutch	13	20.3	4	18.2
Other	12	18.8	4	18.2
Educational level				
Less than a high school diploma	2	3.1	2	9.1
Highschool degree or equivalent	28	43.8	8	36.4

Bachelor’s degree	29	45.3	10	45.5
Master’s degree	4	6.3	2	9.1
Doctorate	1	1.6	0	0
Employment Status				
Full-time employment	10	15.6	5	22.7
Part-time employment	5	7.8	3	13.6
Self-employment	1	1.6	0	0
Student	48	75	14	63.6
Apprentice	0	0	0	0
Retired	0	0	0	0
Household income				
Below 10k €	31	48.4	11	50
10k € - 50k €	23	35.9	8	36.4
50k € - 100k €	10	15.6	0	0
100k € - 150k €	10	15.6	3	13.6
> 150k €	0	0	0	0
Victim of cybercrime				
Yes	8	12.5	2	9.1
No	56	87.5	20	90.9
Time spent on smartphone [a]				
Not at all	0	0	0	0
Up to 1 hour	0	0	0	0
1-3 hours	19	29.7	3	13.6

3-5 hours	25	39.1	12	54.5
> 5 hours	1	1.6	7	31.8
Time spent on tablet [a]				
Not at all	44	68.8	18	81.8
Up to 1 hour	7	10.9	1	4.5
1-3 hours	10	15.6	2	9.1
3-5 hours	2	3.1	1	4.5
> 5 hours	1	1.6	0	0
Time spent on PC [a]				
Not at all	1	1.6	1	4.5
Up to 1 hour	4	6.3	9	40.9
1-3 hours	17	26.6	3	13.6
3-5 hours	17	26.6	9	40.9
> 5 hours	25	39.1	0	0
Social media use [a]				
Less than 30 minutes	6	9.4	2	9.1
Between 30 minutes to 1 hour	10	15.6	4	18.2
Between 1 hour and 2 hours	19	29.7	5	22.7
Between 2 hours and 4 hours	18	28.1	6	27.3
Between 4 hours and 8 hours	10	15.6	5	27.7
More than 8 hours	1	1.6	0	0
Technical background				
Yes	16	25	4	18.2

No	48	75	18	81.8

[a] on an average day

Appendix B

Experimental Manipulation

Self-Efficacy Condition

Password managers remember passwords for the user. Passwords can be manually entered and stored in the app or saved when they are entered on a website. Password managers are convenient as they have an autofill-password function for websites and a password generator function. An example of a mobile Password manager is Bitwarden, which is easy to use. A browser extension of Bitwarden can be downloaded to PC to synchronize and use Bitwarden on all devices.

Response Efficacy Condition

Password managers store and protect your passwords. Passwords may be saved as they are entered on a website. An example of a mobile password manager is Bitwarden. Bitwarden stores encrypted versions of your passwords to minimize the threat of a cyberattack. Passwords are protected by and only accessible through a master key, making password managers a highly secure method of storing passwords. Password managers also offer a secure password generator.

Response Cost Condition

Password managers store passwords for the user. With one click they safe a password when it is entered on a website, and autofill it the next time. The user solely needs to remember one master key to access the passwords in the app, making password managers quick and effortless to set up. On top of that, a password generator function creates highly secure passwords to increase online safety. An example of a **free** mobile password manager is Bitwarden.

Control Condition

Password managers store passwords. An example of a password manager is Bitwarden.

Appendix C

Informed Consent: Intervention

Informed Consent

Welcome to this study regarding cybercrime and password manager adoption! This research is conducted by Sophie Graf and Iris van Sintemaartensdijk from the Faculty of Behavioural, Management and Social Sciences at the University of Twente. The purpose of this study is to investigate the reasons for (not) adopting a password manager.

Procedure

Participation in this study takes approximately 30 minutes. You will answer multiple questionnaires concerning protection motivation, technological knowledge, trust in password managers, security attitude, experiences with cybercrime, and demographics. Please read all the questions attentively. On top of that, you will be presented with a security notification that you should keep in mind. At the end of the study, you are asked to indicate your e-mail address, so that you can be invited to the follow up study after two weeks. Participation in the follow up study is voluntary, and all data will be treated confidentially.

Potential Risks and Discomforts

There are no obvious physical, legal, or economic risks associated with your participation in this study. This research was reviewed and approved by the BMS Ethics Committee of the University of Twente. For questions or problems regarding ethics of the study, the Secretary of the Ethics Commission of the faculty Behavioural, Management and Social Sciences at University Twente may be contacted through ethicscommittee-bms@utwente.nl.

Potential Benefits

Participation in this study does not grant any benefits.

Confidentiality

Your privacy will be protected to the maximum extent allowable by law. No personally identifiable information will be reported in the final research product. Only trained research staff will have access to your responses.

Right to Withdraw and Questions

Your participation is voluntary. If you participate, you may decide to withdraw from the study at any time. You will not be penalized or lose any benefits to which you otherwise quality if you decide to not to participate or to stop participating. However, the data you provided before your withdrawal will be processed. If you have questions or concerns regarding this research, please contact us.

Contact Information

Sophie Graf

Supervisor: Iris van Sintemaartensdijk

Statement of Consent

By checking the box below, you confirm that you are at least 18 years of age, you have read and understood all the information, give your consent, and that you voluntarily agree to participate in this study.

- I have been sufficiently informed about the study and all my questions are answered to my satisfaction
- I have the right to withdraw from the study at any time

- I have understood that no personally identifiable information will be reported in the research report and confidentiality is ensured

If you do not agree to this, end the study by leaving the website.

[ ] I agree to participate in this study. I agree that the data obtained during the study will be saved.

Appendix D

Questionnaires Intervention

Behavioural Intention: PM Adoption

**Assessed on a 11-point Likert scale; (Extremely unlikely = 1; Extremely likely = 11)*

Please indicate the likelihood that you will install a password manager.

Intention to Effectively Use a PM

**Assessed on a 7-point Likert scale; (Strongly disagree = 1; Strongly agree = 7)*

Please indicate the level to which you agree with the following statements.

1. I plan to install a password manager for security reasons.
2. I intend to use a password manager to safely store my passwords.
3. I am determined to create a safe master key for my password manager that protects all my passwords.
4. I will use a password manager to generate safe password for my online accounts.

Barriers for PM Use

**Assessed on a 5-point Likert scale; (Strongly disagree = 1; Strongly agree = 5)*

Please indicate the extent to which you agree with the following statements

1. I am aware of password managers.
2. There are security issues associated with password mangers.
3. There is no need for me to use a password manager (e.g. I do not have enough accounts to need a password manager, I can remember my passwords, I use a physical notebook).
4. Password managers represent a single a point of failure and I am concerned about that.

5. I have made negative experiences with password managers in the past.
6. I am not concerned, or I do not care about the risks associated with an account compromise (e.g., I am at low risk for an account compromise, an account compromise would not have important negative consequences).
7. Password managers do not have good usability.

Security Attitudes

**Assessed on a 5-point Likert scale; (Strongly disagree = 1; Strongly agree = 5)*

Each statement below describes how a person might feel about the use of security measures. Examples of security measures are laptop or tablet passwords, spam email reporting tools, software updates, secure web browsers, fingerprint ID, and anti-virus software. Please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel right now, not what you have felt in the past or would like to feel. There are no wrong answers.

1. I seek out opportunities to learn about security measures that are relevant to me.
2. I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
3. Generally, I diligently follow a routine for security practices.
4. I often am interested in articles about security threats.
5. I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
6. I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

Password Management

**Assessed on a 7-point Likert scale; (Strongly disagree = 1; Strongly agree = 7)*

Please indicate the extent to which you agree with the following statement.

1. It's acceptable to use my social media passwords on my work or university accounts.
2. I am allowed to share my passwords with friends.
3. A mixture of letters, number and symbols is necessary for passwords.
4. It's safe to use the same password for social media and other work or university accounts.
5. It's a bad idea to share my passwords, even if a friend asks for it.
6. It's safe to have a password with just letters.
7. I use a different password for my social media accounts and work or university accounts.
8. I share my passwords with friends.
9. I use a combination of letters, numbers and symbols in my passwords.
1. Passwords that contain less than eight characters are secure.
2. It's acceptable to use my birth date as my password.
3. I use words that can be found in a dictionary as my password.

Initial Trust

**Assessed on a 5-point Likert scale; (Strongly disagree = 1; Strongly agree = 5)*

Please indicate the extent to which you agree with the following statement.

1. Password manager software always provides accurate service.
2. Password manager software always provides safe services.
3. Password manager software provides reliable services.

4. Password manager software seems reliable.
5. Password manager software seems secure.

Appendix E

Full Debrief

Thank you for participating in this study regarding cybercrime and password manager adoption!

In our highly digitalized world, cybercrime has become a major problem. While the risks for burglary when leaving the door unlocked and the windows open are evident for most people, this does not seem to be the case for online safety. Using weak passwords and re-using passwords are one of the most common and dangerous habits that can easily cause a security breach. However, safe passwords are hard to remember, and the modern user has numerous online accounts. While password managers alleviate this memory burden and have been around for more than a decade, adoption rates are still low. This is why research in this field is needed to investigate the factors that motivate or prevent users from adopting password managers.

Protection Motivation Theory (PMT) is a framework that views protection motivation as a result of a threat appraisal (threat severity, threat susceptibility) and a coping appraisal (self-efficacy, response efficacy, response cost). In other words, for protection motivation to arise one needs to feel sufficiently scared of a threat, but at the same time feel that they are able to exhibit the recommended protective action and believe that it will prevent them from the threat. Interventions that influence one of these five factors are therefore expected to produce a specific protective response. As research has shown that coping messages are more effective than threat messages in motivating a protective action, this study tested different coping messages to motivate the adoption of a password manager. To this end, participants were randomly assigned to one of seven conditions that each received a different security notification.

Two conditions received a security notification that is meant to increase response efficacy. Response efficacy is the belief that a specific behavior will produce the expected outcome. In the context of this study, it is the belief that using a password manager will reduce falling victim to a cyber-attack. Participants in two other conditions were present with a security notification designed to increase self-efficacy. Self-efficacy is the belief about one's capacity to execute a certain behavior. In other words, participants are ought to believe that they can install and use a password manager. Two other conditions entailed a security notification that is expected to decrease the perceived response cost. In PMT, response cost indicates costs such as time, effort, and money that are associated with the recommended response. In this study, the recommended response is using a password manager. Half of these six conditions, so one per self-efficacy-, response efficacy-, and response cost-condition, received a personified message instead of a regular message. These notifications were constructed around one of the three coping constructs but represented by a made-up person.

While coping messages have been little to moderately effective in motivating safe online behavior, more research is needed to improve the success of such messages even further. The approach tested in this study is new in the field of cyber security. It is based on the idea of role modeling and the observation that information is more convincing and effective if it is presented by a person to which one can relate to. The last condition is a control condition that did not receive any security notification. We predict that protection motivation and password manager adoption is increased for participants that received a security notification with a coping message compared to the control condition. We further predict that this effect is stronger for participants that were presented with a personified message compared to a regular message.

If you have questions regarding this study or the follow-up study, please contact the

researcher:

Sophie Graf

Iris van Sintemaartensdijk

Lastly, if you know others that are participating in this study, please do not discuss the details of this study with them until they completed the survey. Prior knowledge can influence participants and invalidate the results.

Thank you again for your participation!

Appendix F

Incomplete Debrief

Thank you for participating in this study regarding cybercrime and password manager adoption!

In our highly digitalized world, cybercrime has become a major problem. While the risks for burglary when leaving the door unlocked and the windows open are evident for most people, this does not seem to be the case for online safety. Using weak passwords and re-using passwords are one of the most common and dangerous habits that can easily cause a security breach. However, safe passwords are hard to remember, and the modern user has numerous online accounts. While password managers alleviate this memory burden and have been around for more than a decade, adoption rates are still low. This is why research in this field is needed to investigate the factors that motivate or prevent users from adopting password managers. However, this is not the only purpose of this study. Some information must be withheld to not bias participants for the follow up survey. A full debrief, including complete information on the purpose of the study and our predictions regarding the results, will be provided to you at the end of the follow-up study.

If you have questions regarding this study or the follow-up study, please contact the researcher:

Sophie Graf

Iris van Sintemaartensdijk

Lastly, if you know others that are participating in this study, please do not discuss the details of this study with them until they completed the survey. Prior knowledge can influence

participants and invalidate the results.

Thank you again for your participation!

Appendix G

Informed Consent: Follow up

We are pleased to welcome you back to the follow up survey on 'Forgot your Password? Motivating the adoption of a password manager'. This research is conducted by Sophie Graf and Iris van Sintemaartensdijk from the Faculty of Behavioural, Management and Social Sciences at the University of Twente. The purpose of this study is to investigate the reasons for (not) adopting a password manager and check in with you two weeks after the initial study.

Procedure

Participation in this study takes approximately 5 minutes. You will answer questionnaires concerning protection motivation and your current password manager use. Please read all the questions attentively. At the beginning of the study, you are asked to indicate your e-mail address, so that we can connect your results from both studies. Participation in the follow up study is voluntary, and all data will be treated confidentially.

Potential Risks and Discomforts

There are no obvious physical, legal, or economic risks associated with your participation in this study. This research was reviewed and approved by the BMS Ethics Committee of the University of Twente. For questions or problems regarding ethics of the study, the Secretary of the Ethics Commission of the faculty Behavioural, Management and Social Sciences at University Twente may be contacted through ethicscommittee-bms@utwente.nl.

Potential Benefits

Participation in this study does not grant any benefits.

Confidentiality

Your privacy will be protected to the maximum extent allowable by law. No personally identifiable information will be reported in the final research product. Only trained research staff will have access to your responses.

Right to Withdraw and Questions

Your participation is voluntary. If you participate, you may decide to withdraw from the study at any time. You will not be penalized or lose any benefits to which you otherwise quality if you decide to not to participate or to stop participating. However, the data you provided before your withdrawal will be processed. If you have questions or concerns regarding this research, please contact us.

Contact Information

Sophie Graf

Supervisor: Iris van Sintemaartensdijk

Statement of Consent

By checking the box below, you confirm that you are at least 18 years of age, you have read and understood all the information, give your consent, and that you voluntarily agree to participate in this study.

- I have been sufficiently informed about the study and all my questions are answered to my satisfaction
- I have the right to withdraw from the study at any time
- I have understood that no personally identifiable information will be reported in the research report and confidentiality is ensured

If you do not agree to this, end the study by leaving the website.

[ ] I agree to participate in this study. I agree that the data obtained during the study will be saved.

Appendix H

Questionnaires Follow up

Behavioural Change: PM Adoption

**Assessed on a yes/no scale*

Have you installed a password manager since the first survey two weeks ago? If you already used a password manager, but only for less important accounts, are you using it for important accounts now?

Behavioural Change: Effective PM use

**Assessed on a 5-point Likert scale; (Strongly disagree = 1; Strongly agree = 5)*

Please indicate the extent to which you agree with the following statement.

1. I have installed a password manager for security reasons.
2. I use a password manager to safely store my passwords.
3. I created a safe master key for my password manager that protects all my passwords.
4. I use a password manager to generate safe passwords for my online accounts.