Protect Your Password so it can Protect You:

Improving Password Strength Through Coping Messages

Joelle Simon

Department of Psychology of Conflict, Risk & Safety

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

Under the supervision of Iris van Sintemaartensdijk and Steven Watson

January 27, 2022

Abstract

Users not adhering to password guidelines marks a persistent drawback in the fight against cyberattacks. Regardless of password composition policies promoting safer passwords choices, many users work around these requirements and still use easy-to-guess passwords. Inspired by Protection Motivation Theory, this experimental study was set up to understand the impact of three coping messages (i.e., self-efficacy, response efficacy, and self-efficacy and response efficacy combined) to improve password composition, increasing password security intentions and subsequent protective behaviour. Specifically, participants were asked to generate passwords during the study, and the resulting password quality was evaluated based on several password characteristics. Participants also reported their behavioural intentions to create strong passwords after the intervention, and I assessed whether the intention translated into behaviour after four weeks. I found that participants who were reminded of the effectiveness of strong passwords (i.e., response efficacy message) created significantly stronger passwords than those in the other coping message conditions and those who did not receive a coping message. Furthermore, the intention to adopt strong passwords was elevated for participants in all coping message conditions compared to those who did not receive a coping message – but significantly more so in the combined condition. However, the intention did not result in protective behaviour after four weeks. Thus, enhancing users sense of the effectiveness of robust passwords can change immediate password choices. However, many users who express an intention to adopt strong passwords fail to do so. I highlight the need for research into interventions that help people translate intentions into behaviour.

Keywords: online safety, password strength, coping messages, self-efficacy, response efficacy, Protection Motivation Theory

Protect Your Password so it can Protect You: Improving Password Strength through Coping Messages

The development of digitalisation continues to accelerate. Likewise is the threat of cybercrime. 13% of Dutch citizens aged 15 and older reported falling victim to cybercrime in 2019 (Centraal Bureau voor de Statistiek [CBS], 2020). International cybercrime statistics yield a similar trend. For example, the German Bundeskriminalamt (BKA) (2020) warned that the amount of cybercrime registered had risen consistently in recent years. The Federal Criminal Police Office administered around 108,000 cybercrime offences in 2020, representing an increase of 7.9 % compared to the cases recorded in 2019 (BKA, 2020). Furthermore, the Telephone Crime Survey for England and Wales showed a 36% increase in computer misuse and fraud offences in the year ending March 2020 compared to the year ending March 2019 (Office for National Statistics [ONS], 2021). Thus, cybersecurity threats mark a concern for individuals and organizations worldwide.

However, the Home Office National Security Strategy identified that cyberattacks are not inevitably sophisticated or unpreventable (Hammond & Gummer, 2016). The success of an attack is often tied to vulnerabilities in cyber defence systems linked to human behaviour (Hammond & Gummer, 2016). The Data Breach Investigations Report by Verizon found that a common cause of security vulnerabilities at companies was the use of weak passwords (Verizon, 2021). The use of weak passwords has also contributed to significant cybersecurity breaches at Target (Plachkinova & Maurer, 2019) and Dropbox (Guha & Kandula, 2012); however, these are just two examples from numerous cases of password breaches in the past years. Consequently, improving users safe password practices has become a priority for organisations and governmental agencies (Ponnusamy et al., 2020). Accordingly, many employers and websites have adopted password composition policies that limit the minimum length and complexity of the passwords.

Despite such preventive measures, password composition policies failed to achieve the goal of stronger passwords (Komanduri et al., 2011; Shay et al., 2016). A primary reason seems to be the increased cognitive load. To reduce the cognitive load, users conduct a security-convenience trade-off where they work around the requirements of password policies by implementing easy-to-guess passwords or reusing passwords (Inglesant & Sasse, 2010; Shay et al., 2016). To prevent users from employing these poor password practices, scholars have attempted to develop methods to encourage better password practices, for example, nudge interventions (Nicholson et al., 2018; Peer et al., 2020; van Bavel et al., 2019). *Nudging* is defined as the systematic development and implementation of indirect messages in creating behavioural change (Thaler & Sunstein, 2008). Nudges are more flexible than password policies because they do not force users to create passwords strictly according to password policies but indirectly prompt people towards improved password habits.

The present study contributes to this research initiative. We drew on Protection Motivation Theory (PMT) (Rogers, 1975) to test the effectiveness of three coping nudges (i.e., self-efficacy, response efficacy, self-efficacy and response efficacy combined) designed to help people create stronger passwords. The motivation to focus on the coping elements of the PMT builds on previous research which showed that coping messages, compared to threat messages, are stronger predictors for intentions to engage in precautionary online behaviour (Jansen & Van Schaik, 2017; LaRose et al., 2005; van Bavel et al., 2019). However, the effectiveness of the individual coping elements in improving cyber security behaviour has not yet been investigated and will therefore form the unique basis of this study. To assess password behaviour, we created an online experiment that measured observed behaviour (i.e., hypothetical password creation), behavioural intention to create stronger passwords after the

study and self-reported behavioural change four weeks after we presented the nudges to the participants.

Password Security Research

To date, almost everyone is connected to various devices and online accounts (e.g., bank, e-mail, dating portals, streaming platforms) that predominantly require text-based passwords as an authentication mechanism to avoid disclosing sensitive data. Thus, users must create passwords for more and more websites. For example, Eddolls (2016) estimated that the average internet user in the UK has over 100 accounts. However, a meaningful way to improve data security through password authentication requires users to develop difficult-to-guess passwords that are unique for each account (Potter, 2010). Nevertheless, since users have so many accounts, it is evident that creating and recalling numerous strong passwords is challenging. Consequently, users alleviate the memory burden by reusing a smaller collection of weak and easy-to-remember passwords (Bakas et al., 2021; Florencio & Herley, 2007; Gaw & Felten, 2006; Grawemeyer & Johnson, 2011; Von Zezschwitz et al., 2013).

This weakness of password authentication has led scholars to recommend other authentication methods (e.g., Biddle et al., 2012). For instance, biometrics can measure and analyse users physical characteristics (e.g., facial recognition, fingerprint, iris recognition) to grant access to their accounts (Di Campi, 2021). Another alternative is two-factor authentication (2FA). A system using 2FA requires users to confirm a one-time passcode that is forwarded via SMS or other forms of communication (Krol et al., 2015). However, although there is a strong aspiration among the academic community, computer experts, and companies to replace passwords with more secure alternatives, text-based passwords are still the dominant authentication mechanism (Quermann et al., 2018).

Since passwords seem to remain the primary authentication mechanism in the next years, cyber security problems still exist and are well-known by cybercriminals. The most common concerns are that users create overly simple and personalised passwords (Grawemeyer & Johnson, 2011) and reuse the passwords for several accounts (Bakas et al., 2021; Gaw & Felten, 2006). Cybercriminals share that knowledge and keep strategising to exploit the incautions behaviour of users to gain unauthorised access to personal information through password attacks (Di Campi, 2021). Password attacks can be differentiated into two categories: capture and guessing attacks. First, using capture attacks, hackers attempt to expose passwords by capturing login credentials when entered by the user (Biddle et al., 2012; Stobert, 2015). For example, malware and phishing are common forms of capture attacks. Malware uses software to capture keystrokes, mouse movements, or screen output, to obtain login credentials (Biddle et al., 2012). Phishing is a type of social engineering used to trick users into entering their passwords at a corrupted website recording input (Biddle et al., 2012). Second, through guessing attacks, hackers try to access accounts by guessing passwords. Guessing attacks include brute-force attacks where hackers methodically submit many passwords or passphrases with the hope to eventually guess correctly (Stobert, 2015); and dictionary attacks, where the hacker uses a dictionary or list of previously leaked passwords to approximate commonalities (Stobert, 2015). Hence, whether a guessing attack is successful almost entirely depends on the strength of the user-chosen passwords.

In prior research, password strength has been assessed based on different password characteristics. For example, Florencio and Herley (2007) conducted a large-scale study and analysed password strength based on uppercase letters, digits, and special characters. They reported that the average user dominantly employed lower-case only passwords and barely used uppercase and special characters. Bakas et al. (2021) reported similar results. They surveyed 254 users regarding their password strength but extended the assessment

characteristics and included common names, famous English words, and repeats. They also found that most participants employed a weak password (i.e., 105 out of 254 participants scored the lowest of four password strength categories). Another study revealed that people often choose personal terms for their passwords (e.g., children's names, birth dates, and phone numbers) (Andrews, 2002). Therefore, there are significant challenges to ensure that users are both aware of their vulnerability to guessing attacks and can reduce these risks by developing passwords consisting of strong characteristics.

Behaviour Change in Password Security

Protection Motivation Theory (PMT; Rogers, 1975; Maddux & Rogers, 1983) is a theoretical framework applied to understand individuals' protective intentions when faced with a potentially threatening event (here, the possibility of a password attack and the misuse of accessed information). It supposes that for protection motivation to be elicited, people conduct to appraisal processes: threat appraisal and coping appraisal. The threat appraisal focusses on the threat itself, and the coping appraisal regards one's perceived ability to take actions against a threat. Most applications of PMT consider the additive effects of these variables on behavioural intentions to take precautionary measures, and behavioural intention is expected to direct protective behaviour.

The threat appraisal combines people's assessment of how harmful the consequences of an anticipated threat are (i.e., threat severity) and how likely one is to be personally affected by the threat (i.e., threat vulnerability). The coping appraisal consists of three constructs: self-efficacy, response efficacy, and response cost. First, self-efficacy describes the level of confidence in carrying out a protective action (Maddux & Rogers, 1983). Second, response efficacy is related to one's perception of whether undertaking a recommended action effectively removes a threat. Finally, response cost focuses on a protective actions' associated costs (e.g., effort, time). Self-efficacy and response efficacy are positively related

to behavioural intentions, whereas response cost is negatively associated (Mayer et al., 2017). Therefore, the coping appraisal may lead to adaptive behaviours, given that the costs of making an adaptive response are not too high.

Floyd et al. (2000) performed a meta-analysis with 65 studies that assessed at least one PMT construct and included intention and/or behaviour as a dependent variable. Twenty-seven studies assessed intention only, 22 behaviour only, and 16 assessed intention and behaviour. They found significant effects of all PMT constructs. However, the effect sizes for the threat appraisal constructs (i.e., perceived severity and vulnerability) were ranging from small to medium, and the effect sizes for the coping appraisal constructs (i.e., perceived response efficacy, self-efficacy, and response costs) varied from medium to large. In addition, self-efficacy yielded the largest effect size. Furthermore, the effect sizes for intentions were greater than for behaviour for both the threat appraisal and the coping appraisal. Milne et al. (2000) largely replicated the findings in another meta-analysis of PMT studies.

A growing body of research has applied the PMT to investigate online protective behaviour. For example, Boerman et al. (2021) found that perceived severity and response efficacy positively affected protection behaviour, while users reported little confidence (i.e., low perceived self-efficacy) in their ability to act protectively. However, other work shows that response efficacy and self-efficacy are the most influential predictor variables for protective cyber behaviour (Boehmer et al., 2015; Jansen & Van Schaik, 2017). However, only a few scholars have applied the PMT to design nudge interventions. Van Bavel et al. (2019) tested whether PMT nudges will affect people's protective behaviour while making an online purchase. Participants received either a threat nudge (i.e., heightened the awareness of the threat), a coping nudge (i.e., heightened the awareness of the appropriate protective responses), or a nudge that combined the threat and coping elements. They reported that participants exposed to the coping message, either in isolation or in combination with the

threat appeal, acted more securely than participants that did not receive a security message. However, van Bavel et al. (2019) merged a self-efficacy- and response efficacy element into the coping nudge. The empirical literature on the effectiveness of coping nudges is still scarce, and little is known about the independent influence of the individual constructs of coping appraisal on protective behaviour.

Thus, the objective of the current study was to investigate the impact of the PMT coping elements. I designed three coping nudges to promote more secure password choices:

- a self-efficacy message provided users with tips on creating strong and memorable passwords and was meant to increase their confidence in creating passwords;
- a response efficacy message reminded users of the effectiveness of strong passwords to reduce the risk of a cyberattack; and
- a self-efficacy and response efficacy combined message contained both the beforementioned elements.

To look at the effectiveness of the coping elements in isolation and combination, I set up an online experiment and tested the feasibility of the coping nudges on immediate password creation abilities, the intention to create strong passwords after the study, and behavioural change after four weeks. I expected that any positive encouragement might play a significant role when users are asked to change their approach to password composition. Hence, my expectations regarding whether one coping element would be more effective than the other were unclear. On the one hand, the hesitancy to employ strong passwords may be rooted in negative feelings or apprehension of one's ability to create and remember secure passwords (i.e., perceived self-efficacy). On the other hand, the absence of a sense that solid passwords will effectively diminish the risk of a cyberattack also reduces the likelihood that users invest

the time and effort to adopt recommended password habits (i.e., perceived response efficacy). However, I think that users perception of their ability to create strong passwords builds the basis for immediate creation behaviour. Therefore, when I tested the effectiveness of the coping nudges on generated password strength during the study, I included an exploratory planned contrast to compare the messages with a self-efficacy element (i.e., self-efficacy and combined) with the response efficacy and control condition.

I tested the following hypotheses:

H_1: The groups exposed to a coping nudge will create stronger passwords than people who do not receive a coping nudge.

H_2: The groups exposed to a coping nudge will show an increased intention to adopt strong passwords than people who do not receive a coping nudge.

H_3: Intentions to adopt strong passwords will positively affect the adoption of strong passwords after four weeks.

Method

Design

I tested the hypotheses using a longitudinal experimental design. The design comprised a between-subject factor (i.e., coping message condition) and some analysis included a within-subject factor (i.e., multiple measurements over time). I examined the effect of the coping messages on three dependent variables:

- immediate password creation behaviour;
- behavioural intentions to adopt strong passwords; and
- self-reported password behaviour four weeks after the intervention.

The between-subject factor was the kind of coping message participants received during the experiment. It consisted of four conditions: self-efficacy message, response efficacy message, self-efficacy, and response efficacy combined message, compared to a control group that did not receive a coping message. The assignment to the coping message conditions was random. However, since the coping message condition was an independent-measures variable, I controlled for potential differences between conditions before the analyses to ensure internal validity.

There were three within-subject measures in the experiment. The measures took place at pre-intervention/baseline (Time 1 [T1]), post-intervention (Time 2 [T2]), and four-week follow up (Time 3 [T3]). However, variables varied in whether they were measured once, or several times during the experiment. A clear report of the time-points per measure is given in the materials section. In general, at T1, participants completed topic-relevant measures (i.e., baseline measures) to control post-intervention effects better. At T2, participants had received the coping message (or no coping message in case of the control condition) and created hypothetical passwords and reported their behavioural intention to adopt stronger passwords. That allowed me to analyse whether user password creation behaviour and behavioural intentions were elevated immediately following the coping messages while controlling for baseline differences. At T3, participants received a short questionnaire four weeks after the intervention, including questions to assess their password behaviour in the past four weeks.

I chose to collect data over time (i.e., longitudinal element of the study) to assess whether the intentions to adopt strong passwords were acted upon. However, I had to decide on a reasonable time interval between the intervention and the follow-up to establish this. With four weeks, I claim to have set a suitable time interval that allowed participants to encounter situations in which they had to create secure passwords, while the effect of the messages had optimally not worn off yet.

Materials

Coping Manipulation

The coping message manipulation consisted of messages displayed above the text fields for password creation. The messages were designed based on the coping constructs of the PMT, and they were supposed to increase participants perceived self-efficacy, response efficacy, or self-efficacy and response efficacy combined (see Appendix A for a copy of the coping messages). In the self-efficacy condition, the message consisted of three tips to enhance the participants' belief about their capabilities to create and remember secure passwords. For example, one tip was to remove the vowels from a phrase (e.g., "My favourite artist is Elvis" becomes "Myfvrtrtstslvs"). In the response efficacy condition, the message aimed to foster the belief that creating secure passwords will lead to more protection against cyberattacks. Therefore, it highlighted that implementing specific password characteristics will cause hackers to need more than 12 years to crack a password. The combined condition merged the two coping messages into a single message. Lastly, the control condition did not receive any coping message apart from a short default statement, which I also showed to the other groups. The statement noted that "A secure password describes a password that is difficult to identify by humans and computer programs, thus, effectively protecting your personal data from unauthorized access".

Baseline Measures

At pre-intervention, I asked participants about their password knowledge, risk-taking, the strength of current passwords, and their motivation to adopt secure passwords (i.e., PMT constructs) and basic demographic and topic-specific questions. On the one hand, that information enabled me to understand users current password behaviour. Nevertheless, on the other hand, that information also helped me detect whether the experimental randomization

was successful, and I could control for individual differences in later statistical analyses. Except if noted, the battery of questions was evaluated on a 7-point Likert scale ranging from "Strongly disagree" (coded as 1) to "Strongly agree" (7), with a neutral midpoint "Neither agree nor disagree" (coded as 3). The items were partly adapted from scholarly literature (Ameen et al., 2020; Burns et al., 2017; Parsons et al., 2017; Tsai et al., 2016; van Bavel et al., 2019) and partly constructed by the researcher. Hence, given that items were adapted to fit the current context of password security and some items were added without previous testing, the reliability was assessed using Cronbach's alpha. I interpreted Cronbach's alpha in line with Gliem and Gliem's (2003) rule of thumb: $\alpha > .9$ – Excellent, $\alpha > .8$ – Good, $\alpha > .7$ – Acceptable, $\alpha > .6$ – Questionable, $\alpha > .5$ – Poor. In case of questionable or poor scale reliability ($\alpha < .7$), I evaluated the factorial validity using principal component analysis, whereby items with low inter-item correlations (< 0.4) were excluded from further analyses.

Secure Password Knowledge. To assess secure password knowledge, participants indicated their level of agreement with ten statements. I adapted four statements from the human aspects of information security questionnaire (HAIS-Q) (Parsons et al., 2017) but focused on secure passwords and sharing them with friends instead of password habits in the work environment. In addition, I slightly changed the sentence structure. To illustrate, Parsons et al. (2017) asked participants to rate the statements: "It's acceptable to use my social media passwords on my work accounts" and "It's a bad idea to share my work passwords, even if a colleague asks for it". I adjusted them to "It's acceptable to use my social media password for other online accounts" and "It's secure to share my password if a friend asks for it". In addition, I added six items to assess participants knowledge regarding a broader range of secure password characteristics. Example items are "A password that contains upper- and lower-case letters and numbers is secure" and "It's secure to use my birth date as a password". However, the scale proved questionable reliability ($\alpha = .64$). Principal

component analysis revealed that the items “A mixture of letters, numbers, and symbols is necessary for a secure password” and “A password that contains upper-and lower-case letters and numbers is secure” had inter-item correlations below 0.4. After removing the two items, the scale passed the acceptable reliability threshold ($\alpha = .72$). After reverse scoring some items, I computed the mean rating of password knowledge.

Risk-Taking. I assessed users propensity to engage in risk behaviours using the domain-specific risk-taking scale (DOSPERT) (van Bavel et al., 2019). I decided to incorporate a measure of general risk-taking to check whether risk-taking propensity might predict participant dropout from the experiment. Risk-taking behaviour is relevant because users inclination to tolerate risk might moderate their acceptance of security interventions. For example, van Bavel et al. (2019) conducted an experiment using nudges to improve security behaviour and found that dropout rates were higher among more risk-averse participants. Therefore, I asked participants to indicate the likelihood that they would engage in 30 activities or behaviours on a 7-point Likert scale from “Extremely unlikely” to “Extremely likely”, with a neutral midpoint “Not sure”. Examples are “Passing off somebody else’s work as your own” and “Riding a motorcycle without a helmet”. The items were averaged to compose a single risk-taking score. The scale proved good reliability in the sample ($\alpha = .85$).

Strength of Current Passwords. To understand participants’ current password habits, I developed ten items that questioned the characteristics of three of participants’ passwords now in use. I specified that they should consider their most important password for a work or study-related, social media, and banking-related account. On the one hand, asking for several passwords across online accounts allowed for a more accurate representation of user password habits than solely asking for one password. On the other hand, I could estimate whether users might be more protective of their organisational information, social presence,

or financial information. The items were constructed in line with Microsoft's recommendation for password management (Hicock, 2016). The recommendation highlighted that a strong password should have a minimum length of 8-characters and mix upper- and lower-case letters, numbers, and special characters. Furthermore, a strong password should avoid single words, or a sequence of words found in a dictionary, and the password should be hard to guess even by those who know one. Thus, users should avoid names and birthdays of themselves, friends, and family. Example items are "My password only contains numbers", "There are several special characters in my passwords (e.g., @#$%^&)", and "My password contains both upper- and lower-case letters". The answers were dichotomised (i.e., yes/ no). I averaged the three password strength scores to produce a single mean strength score (i.e., maximum score of 10).

Protection Motivation. I included items measuring PMT's core predictor variables: threat severity, threat susceptibility, self-efficacy, response efficacy, and response cost. Although various studies have tested the effect of PMT informed nudges on precautionary motivation and self-protective actions (e.g., Platje, 2021; Story, 2021; van Bavel et al., 2019), relatively few scholars have investigated the working mechanisms of the nudges on the cognitive beliefs underlying the PMT. I aimed for a better understanding of whether the current coping messages modified participants coping cognitions (i.e., self-efficacy and response efficacy). Therefore, I administered all PMT-related items at pre-intervention (i.e., T1), post-intervention (i.e., T2) and follow-up (i.e., T3). Hence, I could explore whether the coping messages modified participants coping cognitions immediately following the intervention and whether this effect was stable over at least for weeks.

Threat Severity. Participants rated how harmful a password breach would be in various scenarios on a 7-point Likert scale ranging from "Extremely harmless" to "Extremely devastating". I used three items from Tsai et al. (2016). Moreover, I added three items to

cover a broader range of threats that could accompany a password breach. Example items are: "[A password breach] reveals my personal information to other online criminals" and "[A password breach] reveals my physical addresses". The items were averaged, and the scale proved excellent reliability in the sample at all three points of measurement (α = .92 – T1; α = .94 – T2; α = .94 – T3).

Threat Susceptibility. Three items from Tsai et al. (2016) were adapted and tailored to the current context of password security. Participants rated their agreement with the following statements: "It is extremely likely that my personal accounts will be compromised by a password breach in the future"; "My chances of a password breach are great"; and "There is a good possibility that my personal accounts will be compromised by a password breach". I computed a mean threat susceptibility score. The scale proved good reliability at T1 (α = .89), and excellent reliability at T2 (α = .93), and T3 (α = .93).

Self-Efficacy. I adapted four coping efficacy items from Tsai et al. (2016). The items were suited to the current context by changing "necessary security measures" with "creating secure passwords". An example item is "I have the resources and the knowledge to create secure passwords". Additionally, I added one item to capture the participants' perceived ability to remember secure passwords: "I feel confident to remember secure passwords". The scale showed good reliability at T1(α = .83) and T2 (α = .86) and acceptable reliability at T3 (α = .72).

Response Efficacy. To assess response efficacy, I adapted two items from Tsai et al. (2016) and adjusted the wording to fit the context of password security. These items are "Secure passwords would be useful for preventing my personal accounts to be compromised" and "Secure passwords would increase my performance in protecting myself from cybercrime". I added one item to account for and isolate item-specific measurement errors by having more than two items to measure the construct. The added item is "Secure passwords

would make it harder for online criminals to compromise my personal accounts". The three items were averaged to compose a response efficacy scale (α = .86 – T1; α = .88 – T2; α = .89 – T3).

Response Cost. I adapted two items from Burns et al. (2017) to test the perceived response cost and focused on "implementing secure passwords" instead of "recommended security measures in organizations". The items are "The inconvenience of implementing secure passwords to protect my personal accounts exceeds the potential benefits" and "The negative side effects of employing secure passwords are greater than the advantages". In addition, I adapted two items from Ameen et al. (2020). I alternated the wording to using secure passwords instead of complying with smartphone security policies. One example is "Using secure passwords requires a considerable amount of my time". Lastly, I added one item to capture the response cost for remembering secure passwords: "Remembering secure passwords is too complicated". The items were reversed coded and averaged to produce a response cost scale (α = .77 – T1; α = .82 – T2; α = .81 – T3).

Participant Characteristics. I also included items concerning the participants' demographic- and topic-specific characteristics. For example, I assessed gender, nationality, education, employment status and household income. Furthermore, participants reported the time spent on different devices to use the internet on an average weekday (i.e., tablet, smartphone, laptop or notebook, desktop computer, other devices). They could select from five responses (i.e., not at all, up to one hour, 1-3 hours, 3-5 hours, and more than 5 hours). Additionally, participants answered if they had been a victim of cybercrime before, where they could choose between "Yes", "No", and "I don't know". Participants who had been victims of cybercrime reported what kind of cybercrime they fell victim to using free text entry. I also asked whether participants changed their passwords to be more secure after becoming a cybercrime victim (i.e., by Yes/No choice). Finally, if participants denied that

they had changed their password, they were also asked to elaborate on why using free text entry.

Behavioural Measures

Created Password Strength. After the coping message intervention (i.e., T2) participants received the instruction that "It is time to create secure (but hypothetical) passwords for three online accounts". They created passwords for a professional networking website, new work or student e-mail address, and online banking account. To evaluate the password quality generated by the participants during the study, I used a self-developed python script that scored the passwords based on Microsoft's recommendation for secure password characteristics (Hicock, 2016). See Appendix B for a copy of the python script. I analysed the passwords based on whether they consisted of seven password characteristics:

- more than eight characters;
- upper- and lower-case letters;
- letters and numbers;
- several special characters (i.e., "\"!@#$%^&*()-+?_=,.~<>/\\\'");
- dictionary words (i.e., Dutch, English, German);
- birthdates (i.e., 1950 to 2004); and
- recent dates (i.e., 2010 to 2022).

Participants received one point when a specific element was present. However, dictionary words, birthdates, and recent dates were reversed scored, and participants received one point if the created passwords did not include those elements. Correspondingly, passwords with a strength score of seven proved the highest quality. Note that I tailored the analysis to the samples' characteristics. For instance, the decision to analyse German and

Dutch dictionary words was because most of the sample (80.2%) reported originating from Germany or the Netherlands. Furthermore, participants were aged 17 to 57 years; hence, I only analysed birth years that might capture guessable birthdates, as participants own birthyear or that of a close family member. Unfortunately, I could not analyse passwords to include names since the available online databases held many exceptionally uncommon names (e.g., ioulo, loari, geru) that could mask genuine randomness of letters. Nevertheless, I manually analysed 50 passwords to check for significant amounts of names in the passwords and did not detect any. Hence, I claim that excluding the name analysis did not default the results. I averaged the three created password strength scores to produce a single mean strength score.

Memory of Created Passwords. Additionally, I included a measure of created password memory, both short- and long-term memory. Many of the deficiencies of passwords as an authentication system arise from memory limitations. In other words, password authentication involves a trade-off. On the one hand, passwords that are easy to remember (e.g., using names or single words to be found in a dictionary) are also easily guessed by cybercriminals (Grawemeyer & Johnson, 2011; Von Zezschwitz et al., 2013). On the other hand, if users try to develop robust passwords, it might be more challenging to remember them. Therefore, participants recited their passwords at T2 (i.e., a few minutes after developing the passwords) and at T3 (i.e., after four weeks) using free text entry. Thus, I could analyse the compatibility of the created and recited passwords while distinguishing the passwords' short- and long-term memorability.

Behavioural Intention and Behavioural Change. I developed ten items to measure participants' behavioural intention at T2 (i.e., immediately following the intervention) and behavioural change at T3 (i.e., four weeks after the intervention). Thus, I used the same questionnaire to measure both behavioural intention and behavioural change but alternated

the wording to correspond to intentions at T2 and behaviour at T3. I constructed the items in conjunction with three elements. First, I assessed the participants' behavioural intention and behavioural change by distinguishing the change of current passwords to be stronger and making more secure password choices when creating completely new passwords. Second, I asked for passwords related to the three domains of work or study-, social media-, or banking related passwords. Third, the items are consisted with the scale that measured participants current password strength. Thus, I describe the implementation of specific elements of strong passwords. Examples for the behavioural intention questionnaire are "I plan to update my current work or study related password for security reasons" and "I am determined not to include names (e.g., family, pets, friends, co-worker) when I create a new password for a social media related account". For the assessment of behavioural change, example items are “I included both letters and numbers when I created a new password for a work or study-related account" and "I did not include names (e.g., family, pets, friends, co-worker) when I created a new password for a social media-related account". The items were averaged to produce mean intention and behavioural change scores. The scale proved good reliability at post-intervention ($\alpha = .81$) and at follow-up ($\alpha = .87$).

Procedure

Both parts of the study were hosted in Qualtrics (see Appendix E and F for copy of the all the scales included the interventional study and follow-up, respectively). To begin, participants received a short synopsis of the study and they confirmed that the conditions for taking part in the experiment were understood. Following this, participants responded to the questionnaires assessing secure password knowledge, risk-taking, PMT constructs, and they indicated the strength of their passwords currently in use. Then, they were randomly allocated to one of four coping message conditions in which participants received either:

- a self-efficacy message;
- a response efficacy message;
- a self-efficacy and response efficacy combined; or
- no coping message (i.e., control condition).

In every condition, participants were then informed that it is time to create secure (and hypothetical) passwords for the three online accounts. After filling the text fields for password creation, participants answered all PMT-related items again, and they completed the questionnaire to assess their behavioural intention to employ strong passwords after the intervention. Next, I collected demographic and topic-specific characteristics (i.e., time spent online, previous cybercrime incidents). Note that I decided to assess demographics at this point of the study to increase the time between password creation and asking participants to recite the passwords. Hence, assessing participants created password memory marked the last element of the first part of my study. Afterwards, I only asked participants whether they agree to participate in the follow-up study. Those who did not agree to continue with the follow-up received a full debrief. Participants who agreed were asked to provide their e-mail address and they received a skimmed version of the debrief (see Appendix G for a copy of the full and skimmed debrief).

The link to the follow-up questionnaire was distributed via e-mail four weeks after the intervention. The follow-up questionnaire included all PMT-related items from the intervention questionnaire, and participants reported their secure password behaviour in the past month. Additionally, I asked participants to recall their created passwords and whether they still remember which coping message they had received. The BMS Ethics Committee of the University of Twente granted ethical approval for this experimental study, and I obtained informed consent from the participants before the intervention and follow-up questionnaire

(see Appendix C and D for a copy of the consent agreement for the intervention and follow-up, respectively).

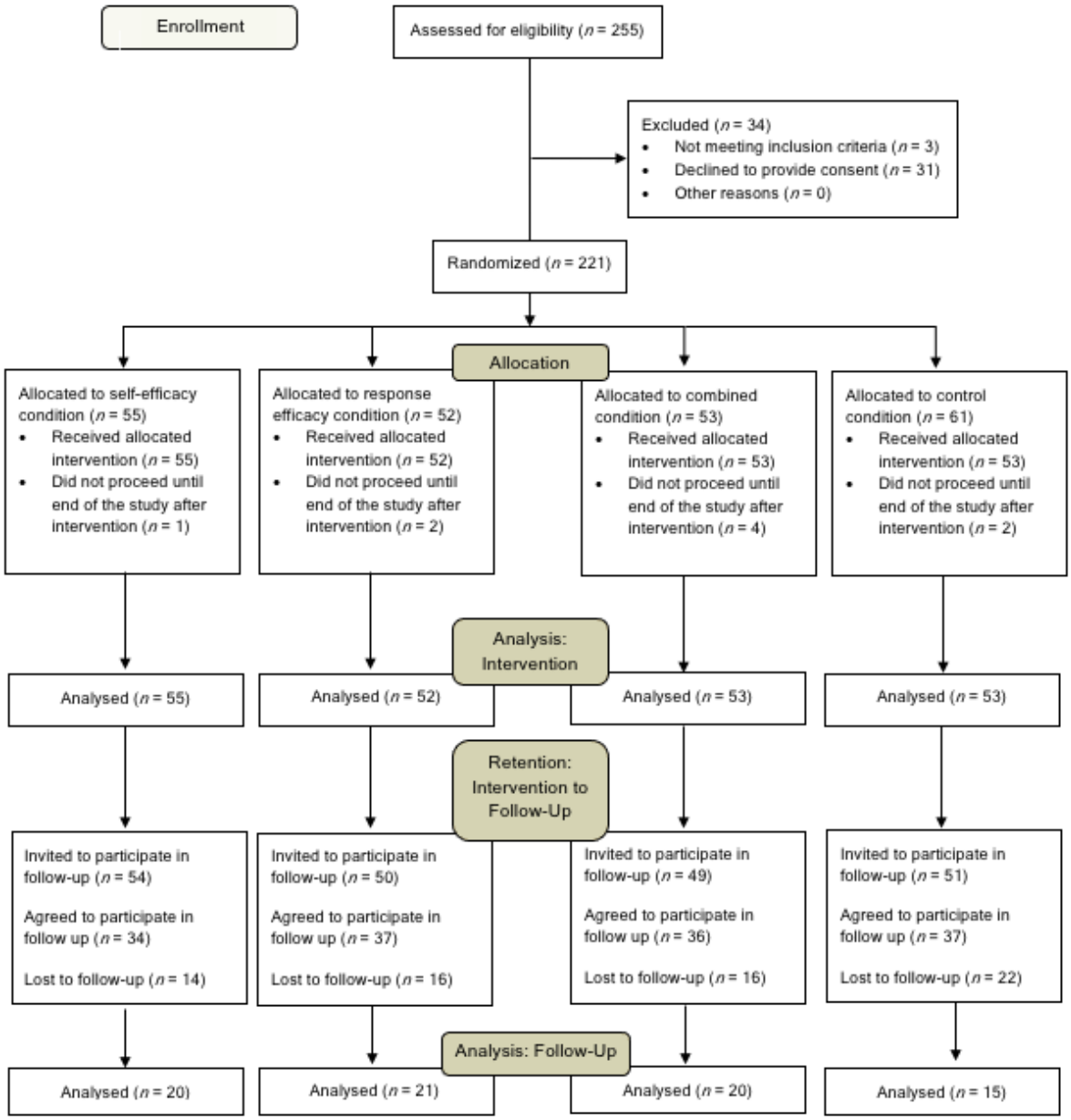
Participants

Initially, 255 people responded to the interventional study and 87 to the follow-up. I anticipated that fewer participants would partake in the follow-up because participants from SONA did not receive additional credits for participation. However, by presenting the study as consisting of two connected parts, I hoped to enhance the response rate at follow-up. Nevertheless, I merited attention to the possible impact of dropouts (i.e., respondents who discontinued the study after the intervention) on the final sample at follow-up.

After scanning the data for incomplete responses (i.e., refusal to provide consent, withdrawal before completing the second questionnaire), I excluded 34 responses from the interventional study. This resulted in a final sample of 221 participants who were randomly assigned to the experimental conditions: self-efficacy (n = 55); response efficacy (n = 52); combined (n = 53); or the control (n = 61). For the follow-up, I applied the same exclusion procedure, resulting in the omission of four participants. In addition, six participants were excluded because they provided an e-mail address that did not appear in the interventional study. Consequently, I was unable to link their responses from the two study parts. Thus, the net response frequency at follow-up was reduced to 77, yielding a retention rate of 34.8%. Hence, most participants did not continue with the follow-up after the intervention. See Figure 1 for a graphical presentation of the participant progress through the study for each experimental condition.

Figure 1

Flowchart for the Progress of Participants per Experimental Condition



The 221 respondents in the interventional part were on average 22.6 (*SD* = 6.25) years old, and most participants reported being from Germany (61.4%) and identifying as female (69%). Participants varied in their education levels, with 42.5% that completed (or are currently completing) a high school degree, 47.8% a bachelor's degree, and 5.8% a master's

degree. The others are divided between PhD, other degrees (e.g., International Baccalaureate Diploma, Propedeus HBO), and 1% of the participants achieved less than a high school diploma. Only 8% of participants have been victims of cybercrime; however, 23.5% reported that they do not know whether they might have been victims. In addition, the sample consisted of frequent internet users, with 39.4% spending 3-5 hours a day using the internet on their smartphone and 21.1% using it more than 5 hours. Table 1 summarizes the participant characteristics for the interventional study and follow-up.

Table 1

Sociodemographic Characteristics of Participants in the Intervention and Follow-up

Sociodemographic Characteristics	Intervention (N = 221)		Follow-up (N = 76)	
	n	%	*n*	%
Gender				
Male	60	29	12	15.8
Female	143	69	62	81.6
Non-binary/ Third gender	2	1	2	2.6
Prefer not to say	2	1	0	0
Nationality				
German	127	61.4	49	64.5
Dutch	39	18.8	10	13.2
Other	35	16.9	15	19.7
Prefer not to say	6	2.9	2	2.6
Educational level				
Less than a high school diploma	2	1	1	1.3
Highschool degree or equivalent	86	42.5	36	47.4

Bachelor's degree	99	47.8	29	38.2
Master's degree	12	5.8	5	6.6
Doctorate	1	.5	1	1.3
Other	7	3.4	4	5.3
Employment Status				
Employed full-time	24	11.6	5	6.6
Employed part-time	15	7.2	1	1.3
Unemployed	2	1	1	1.3
Student	163	78.7	69	90.8
Self-employed	2	1	0	0
Retired	1	.5	0	0
Household income				
Below 10k €	95	45.9	39	51.3
10k € - 50k €	67	32.4	23	30.3
50k € - 100k €	32	15.5	11	14.5
100k € - 150k €	9	4.3	3	3.9
> 150k €	4	1.9	0	0
Victim of cybercrime				
Yes	19	8	7	9.2
No	146	68.5	49	64.5
I don't know	50	23.5	20	26.3
Time spent on smartphone				
Not at all	0	0	0	0
Up to one hour	10	4.7	1	1.3
1-3 hours	74	34.7	28	36.8
3-5 hours	84	39.4	30	39.5

> 5 hours	45	21.1	17	22.4
Time spent on laptop				
Not at all	19	8.9	5	6.6
Up to one hour	15	7	4	5.3
1-3 hours	64	30	20	26.3
3-5 hours	59	27.7	30	39.5
> 5 hours	56	26.3	17	22.4

Note. Age distribution at T1 ranging from 17 to 57 (M = 22.6, *SD* = 6.25); and at T2 ranging from 17 to 47 (M = 21.3, *SD* = 4.55).

Data analysis

I analysed the data using the statistical software SPSS (version 27). Participant dropout and randomisation to coping message conditions were analysed during preliminary analyses. Next, I investigated the research hypothesis using different statistical approaches. First, I used a one-way between-group ANOVA to measure the created password strength difference across the coping message conditions. I obtained the scores for the created passwords by assessing recommended password elements using PyCharm Professional version 2020.2. A planned contrast (self-efficacy, response efficacy, combined vs control) tested the hypothesis that participants in the presence of a coping message will create stronger passwords than those who did not receive a coping message. Additional post-hoc tests were interpreted with the Games-Howell method because the assumption of equal variance had been violated.

Second, I conducted a one-way analysis of covariance (ANCOVA) testing for any significant differences in behavioural intentions between the coping message conditions while controlling for the strength of participants' current passwords. I decided to control participants' current password strength because it seems logical that those who already

employ strong passwords would report a lower intention to implement strong passwords after the intervention. In the case of statistically significant differences between coping message conditions, I followed up with a Bonferroni post-hoc test to determine which specific coping messages differed in terms of their effect on behavioural intentions to adopt strong passwords.

Third, I analysed the congruence between participants behavioural intentions reported immediately following the intervention and behavioural change reported four weeks later. A 4 x 2 mixed-design ANOVA tested for differential changes in the behavioural intentions reported at T2 and behavioural change reported at T3 according to coping message condition. The four coping message conditions were self-efficacy, response efficacy, combined, and control. There were two-time points of measurement: intentions immediately after the intervention and behavioural change after four weeks. The interaction between coping message condition and time assessed the differential change over time. Post-hoc tests were interpreted with a Bonferroni correction.

Lastly, a 4 x 3 (coping message condition x time) mixed design ANOVA was undertaken with coping message condition as a between-participant factor to explore whether the coping messages influenced participants' cognitions of self-efficacy and response efficacy. The within-subject variable was the repeated measurement of the PMT constructs. I assessed coping cognitions three times during the experiment: at pre-intervention (i.e., T1), post-intervention (i.e., T2), and follow-up (i.e., T3). Post-hoc comparisons were corrected via Bonferroni.

Results

Preliminary Analyses

Dropout Analysis

In the following analysis, I examined the retention rate from the interventional study to follow-up as a potential consequence of coping message conditions. Only 34.8% completed both parts of the study. Hence, in contrast to the conditions that received a coping message, the absence of a coping message might have discouraged participants in the control condition from continuing with the follow-up. Indeed, we observed the lowest retention rate in the control (24.6%) and the highest in the response efficacy condition (42.3%). The retention rates in the self-efficacy and the combined condition were 36.4% and 37.7%, respectively. However, an analysis of variance (ANOVA) showed that the difference in retention rates between coping message conditions was statistically non-significant, $F(3, 217) = 1.45$, $p = .228$, $\eta 2 = .02$.

Nevertheless, I tested if participants baseline characteristics were predictive for whether they continued the study at follow-up. Using t-tests, I compared dropouts ($n = 144$) with completers ($n = 77$) regarding risk-taking (i.e., DOSPERT scale) and cognitions of PMT constructs assessed at pre-intervention (i.e., T1). The assumption of the equality of variances was confirmed. See Table 2 for a summary of the results.

Table 2

Results of t-tests comparing Completers and Dropouts on Baseline Variables

Variable	Completers (n = 77)		Dropouts (n = 144)		*df*	*t*	*p*	Cohen's *d*
	M	*SD*	*M*	*SD*				
Risk-taking	3.32	0.69	3.52	0.72	219	2.06	.040	.291

Threat severity	6.04	1.24	5.54	1.34	215	-2.68	.008	-.380
Threat susceptibility	3.38	1.19	3.72	1.35	215	1.87	.063	.256
Self-efficacy	4.66	1.23	4.72	1.29	214	0.32	.753	.045
Response efficacy	6.32	0.78	5.95	1.04	214	-2.69	.008	-.382
Response cost	4.33	1.06	4.24	1.26	214	-0.51	.612	-.072

I found that completers were significantly more risk-averse than dropouts (p = .040). Additionally, completers perceived the threat of a password attack as significantly more severe compared to dropouts (p = .008), and completers also judged secure passwords as significantly more effective than dropouts (p = .008). No other significant differences on baseline variables were found between the two groups. Hence, the results suggest an association between risk-taking, perceived threat severity and response severity and the likelihood that participants completed the entire study.

Random Assignment to Conditions

Before the main analyses, I conducted statistical tests (i.e., ANOVA) to prove that participants in the coping message conditions are similar regarding topic-specific variables, as well as PMT cognitions at T1. The conditions were comparable in password knowledge [$F(3, 217) = 1.81$, p = .146], risk-taking [$F(3, 217) = 0.83$, p = .481], and whether participants had been a victim of cybercrime [$F(3, 212) = 2.01$, p = .114]. Additionally, participants between coping message conditions did not differ in strength of their current passwords [$F(3, 214) = 0.22$, p = .882], and, participants did not differ in perceived threat severity [$F(3, 213) = 0.66$, p = .577], threat susceptibility [$F(3, 213) = 0.11$, p = .957], self-efficacy [$F(3, 212) = 0.13$, p = .940], and response cost [$F(3, 212) = 1.09$, p = .353]. However, I found a significant difference in perceived response efficacy between the coping message conditions [$F(3, 212) = 2.91$, p = .035]. However, a Turkey post hoc test was non-significant for all

paired comparisons. Thus, the random assignment to coping message conditions was successful.

Main Analyses

Created Password Strength

The calculated created password strength (i.e., with a maximum score of seven) differed across coping message conditions, highest in the response efficacy and lowest in the self-efficacy condition (see Table 3 for a summary of means and standard deviations of created password strength). The application of an analysis of covariance (ANCOVA) seemed the most appropriate statistical method to estimate the effect of the coping messages on created password strength while controlling for the strength of passwords participants currently use (i.e., possible confounding variable). However, an application of the model requires that the statistical assumptions are met, which was not the case in our sample. There was no linear correlation between participants created password strength and current strength of passwords. That means that participants who already used strong passwords did not create strong passwords during the study. Hence, I had to drop the variable from the analysis.

Table 3

Means and Standard Deviations of Created Password Strength per Condition

Condition	*n*	*M*	*SD*
Control	60	5.88	1.26
Self-efficacy	55	5.79	0.95
Response efficacy	52	6.36	0.77
Combined	53	5.89	1.01

Consequently, I conducted a one-way between-group ANOVA to determine the difference between the coping message conditions (i.e., self-efficacy, response efficacy, combined) on created password strength. I verified the independence, normality, and homogeneity of variance assumptions, and I checked for outliers. First, the assumption of independence was confirmed because I used a randomized design. Second, the Shapiro-Wilk displayed that the data were normally distributed. Third, Levene's test showed that the variances of the groups were unequal, $F(3, 216) = 0.57$, $p = .002$. However, the ANOVA is usually robust to violations of homogeneity of variances (Howell, 2012). Hence, I continued the analysis but did not assume equal variance when interpreting the planned contrast. In addition, I used Games-Howell for post hoc testing. Lastly, using boxplots, I checked for outliers that were outside of the interquartile range. I excluded four outliers.

Then, I estimated the ANOVA with a planned contrast (i.e., self-efficacy, response efficacy, combined condition vs control) to test the hypothesis that the groups exposed to a coping message would create stronger passwords than the control condition. I also included a second planned contrast in the model (i.e., self-efficacy and combined condition vs response efficacy and control) to explore whether a self-efficacy element might have been beneficial for participants to create stronger passwords. The ANOVA showed a significant main effect of coping message condition on created password strength, $F(3, 212) = 6.28$, $p < .001$, $\eta 2 = .08$. However, the first planned contrast did not confirm my hypothesis and participants who received a coping message did not generally create stronger passwords than the control, $t(78.81) = 1.12$, $p = .267$, $\eta 2 = .30$. Anyhow, the second planned contrast proved significant, $t(176.92) = 2.88$, $p = .004$, $\eta 2 = .37$. Nevertheless, the effect was in the opposite direction than I thought. Participants who received a coping message with a self-efficacy element created significantly weaker passwords than the other coping message condition. Post-hoc tests via Games-Howell clarified that only participants in the response efficacy condition

created stronger passwords compared to the self-efficacy ($p = .001$), combined ($p < .001$) and control condition ($p < .001$). No other significant differences were observed.

Behavioural Intention

A one-way ANCOVA tested for significant differences in behavioural intentions between the coping message conditions while controlling for participants' current password strength (i.e., possible confounding variable). I verified the assumptions testing normality, outliers, linearity, and homogeneity of variance. First, according to the Shapiro-Wilk the data were normally distributed. Second, I excluded three outliers from the analysis because they were outside of the interquartile range using boxplots. Third, looking at matrix scatterplots, it appears that the assumption of linearity between the covariate and behavioural intention was violated for the control and response efficacy condition. Lastly, Levene's test confirmed the assumption of homogeneity of variance, $F(3, 198) = 0.76$, $p = .519$. Table 4 summarises the means and standard deviations of behavioural intention adjusted for participants current password strength.

Table 4

Means and Standard Deviations of Behavioural Intention Adjusted for Participants Current Password Strength per Condition

Condition	*n*	*M*	*SD*
Control	49	4.57	1.08
Self-efficacy	54	4.84	1.02
Response efficacy	49	4.93	0.94
Combined	50	5.12	0.91

The ANCOVA showed that there was a significant main effect of coping message condition after the means had been adjusted for the strength of participants current passwords, $F(3, 197) = 2.84$, $p = .039$, $\eta^2 = .04$. The model also included a planned Helmert contrast (i.e., self-efficacy, response efficacy, combined vs control), which confirmed the hypothesis that participants who received a coping message would report higher intentions to adopt strong passwords than those in the control condition, $p = .012$. However, post hoc comparisons with the Bonferroni correction clarified that only the combined condition reported a significantly higher intention compared to the control, $p = .028$. All other differences were found non-significant: control vs self-efficacy message $p = .876$; and control vs response efficacy $p = .363$.

From Behavioural Intention to Behavioural Change

I hypothesised that participants will have followed up on their behavioural intention with protective passwords behaviour four weeks after the intervention. A 4 x 2 (coping message condition x time) mixed design ANOVA, with condition as between factor and time as within factor (i.e., behavioural intention at T2 and behavioural change at T3) was used to test the hypothesis. Sphericity was assumed. See Table 5 for a summary of the means and standard deviations of behavioural intention at T1 and behavioural change at T3 per coping message condition.

Table 5

Means and Standard Deviations of Self-Reported Intention (T1) and Behavior (T2) per Condition

Measure	Control		Self-efficacy		Response efficacy		Combined		Total	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*

Intention (T1)	4.81	1.01	4.81	1.02	5.17	0.85	5.15	0.87	4.99	0.93
Behaviour (T2)	3.87	1.15	3.69	1.47	3.73	1.19	3.15	1.41	3.59	1.32

There was no main effect of condition, $F(3, 72) = 0.39$, $p = .760$, $\eta 2 = .016$. But the analysis yielded a significant main effect of time, $F(1, 72) = 79.568$, $p < .001$, $\eta 2 = .525$. Hence, where I expected to find no significant difference between the reported behavioural intention at T2 and behavioural change at T2, I found that participants reported significantly less behavioural change then intention regardless of the experimental condition. There was no interaction effect between the coping message conditions and time, $F(3, 72) = 2.25$, $p = .090$, $\eta 2 = .08$.

Additional Analyses

Memorability of Created Passwords

To explore whether participants created passwords they could not remember, participants recited their created passwords at the end of the interventional study (i.e., T2) and the four-week follow-up (i.e., T3). However, the number of participants who recited their passwords substantially decreased between T2 and T3 because of participant dropout (i.e., N = 213 vs N = 76). Since SPSS automatically excludes cases with missing data on the repeated measures variable when conducting a mixed design ANOVA, I did two separate analyses to include all the available data.

First, I averaged the compatibility scores of created and recited passwords at T2. Then, I conducted a one-way ANOVA to determine whether there were statistically significant differences in short-term memorability of the created passwords between coping message conditions. I found that participants across conditions did not significantly differ in their ability to remember their passwords at T2, $F(3, 205) = 2.45$, $p = .065$, $\eta^2 = .03$.

Nevertheless, mean recall accuracy was surprisingly low for all the coping message conditions, with only 37.1% (*SD* = 0.36) recall accuracy in the control, 48% (*SD* = 0.41) in the self-efficacy, 40.6% (*SD* = 0.41) in the response efficacy, and 56.6% (*SD* = 0.38) in the combined coping message condition.

Second, I administered a 4 x 2 (coping message condition x time) mixed-design ANOVA, with coping message condition as between-factor and time as within-factor (i.e., password recall accuracy immediately after the intervention, password recall accuracy after four weeks). Sphericity was assumed. Table 6 summarises the means and standard deviations of recall accuracy for the two measurements.

Table 6

Means and Standard Deviations of the Recall Accuracy of Created Passwords at Intervention and Follow-Up

Time Measure	Control		Self-efficacy		Response efficacy		Combined		Total	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Intervention	0.32	0.36	0.53	0.39	0.41	0.38	0.71	0.3	0.5	0.38
Follow-up	0	0	0.09	0.29	0.08	0.20	0.03	0.12	0.06	0.19

Note. N = 76

There was no significant main effect of coping message condition for recall accuracy, $F(3, 72) = 2.66$, $p = .054$, $\eta^2 = .10$. There was, however, a significant main effect of time, $F(1, 72) = 119.33$, $p < .001$, $\eta^2 = .62$. Turkey pairwise comparisons yielded that participants recalled their passwords significantly better immediately after the intervention than four weeks later ($p < .001$). There was also a significant interaction effect of the coping message

condition and the time of recall assessment, $F(3, 72) = 4.31$, $p = .007$, $\eta^2 = .15$. To explore the nature of the interaction, I looked at tests of simple effects with coping message conditions within each level of time. The analysis showed that the coping message conditions significantly differed in recall accuracy at T2, $F(3, 72) = 3.96$, $p = .011$, $\eta^2 = .14$ but not at T3, $F(3, 72) = 0.88$, $p = .452$, $\eta^2 = .04$. Corrected via Bonferroni, additional post hoc tests specified that at T2, participants in the combined condition recalled their passwords significantly more accurately than the control group ($p = .045$). No other significant differences occurred.

The Effect of Coping Messages on Coping Cognitions

To explore whether the coping messages increased participants cognitions of self-efficacy and response efficacy, I subjected both constructs to a 4 x 3 (coping message condition x time) mixed-design ANOVA, with coping message condition as between and time as within factor (i.e., perception of PMT construct assessed at baseline [T1], post intervention [T2], and at four-week follow-up [T3]). First, I analysed the effect on self-efficacy cognitions. The assumption of sphericity was confirmed, $X^2(2) = 3.734$, $p = .155$. Table 7 summarizes the means and standard deviations for perceptions of self-efficacy per coping message condition and measure over time.

Table 7

Means and Standard Deviations of Self-Efficacy Scores for Condition and Time

Time Measure	Control		Self-efficacy		Response efficacy		Combined		Total	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Baseline	4.84	1.31	4.48	1.25	4.74	1.28	4.52	1.21	4.65	1.24
Post manipulation	5	1.22	4.76	1.22	5.23	1.25	5.21	1.07	5.05	1.18

Follow-up	5.13	0.82	5.04	0.72	5.01	1.05	5.1	1.06	5.07	0.92

There was no main effect of condition on self-efficacy cognitions, $F(3, 71) = 0.24$, $p = .868$. However, I found a significant main effect of time on self-efficacy cognitions, $F(2, 142) = 7.87$, $p < .001$. Pairwise comparisons after Bonferroni confirmed that self-efficacy cognitions were significantly higher at post-manipulation ($p = .001$) and follow-up ($p = .006$) compared to baseline. There was no significant interaction of coping message condition and time, $F(6, 142) = 0.79$, $p = .576$. So, the messages with a self-efficacy element (i.e., self-efficacy and combined condition) did not increase participants' self-efficacy cognitions to implement strong passwords. However, self-efficacy cognitions increased from baseline to post manipulation and follow-up regardless of the coping message participants received.

Second, I analysed the effect of coping messages on response-efficacy cognitions. Mauchly's test of sphericity showed that the assumption of sphericity was not met, $X^2(2) = 20.890$, $p < .001$. Therefore, I interpreted the results of the Greenhouse-Geisser test. A summary of the means and standard deviations is presented in Table 8.

Table 8

Means and Standard Deviations of Response Efficacy Scores for Condition and Time

Time Measure	Control		Self-efficacy		Response efficacy		Combined		Total	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Baseline	6.15	0.88	6.21	1.13	6.51	0.47	6.28	0.59	6.30	0.79
Post manipulation	6.01	1.18	6.03	0.80	6.38	0.58	6.25	0.55	6.18	0.78
Follow-up (T2)	6.51	0.64	6.05	0.63	6.33	0.45	6.07	1.07	6.23	0.76

There was no main effect of condition [$F(3, 71) = 0.89$, $p = .450$] and time [$F(1.59, 112.87) = 0.74$, $p = .452$] on participants perceptions of response efficacy. In addition, there was no interaction of time and condition, $F(4.77, 112.87) = 1.26$, $p = .285$. Hence, the coping messages with a response efficacy element (i.e., response efficacy and combined condition) did not affect participants' cognitions of the construct.

Discussion

Concerns related to user security continue to escalate in relevancy as the diffusion of the Internet accelerates (Eddolls, 2016). In this study, I examined whether short security messages with coping elements:

- increases users immediate ability to create strong passwords;
- increases the behavioural intention to adopt strong passwords; and
- whether the behavioural intention resulted in behavioural change at a four-week follow-up.

This study provides insights into the three subjects. First, I found that, on average, people who received the response efficacy message immediately created stronger passwords than those who received the coping messages with a self-efficacy element (i.e., either in isolation or in combination with a response efficacy element) and those in the control group. Hence, simply reminding participants that strong passwords effectively reduce the threat of a cyberattack can lead user to create stronger passwords without the need to enforce complex passwords policies (Komanduri et al., 2014). In the security domain, several studies have also found support for the influence of response efficacy on security practices (e.g., Marett et al., 2011; Workman et al., 2008). For example, Marett et al. (2011) applied PMT to explain social media security behaviour and found that individuals who believe that removing sensitive information would help protect them from online threats were more likely to agree

not to post sensitive information. In addition, Workman et al. (2008) found that employees were more likely to comply with security policies if they believed the policies were effective. Hence, it seems likely that if users are reminded that recommended password guidelines will prevent password-related threats, they will take protective actions.

Coping messages with a self-efficacy element, on the other hand, did not improve generated password quality compared to the control group. Hence, recommending that strong passwords are easy to create by following password creation tips seems ineffective to improve immediate password choices. This raises an interesting question: Why did the individual response efficacy element promote participants password creation abilities, but there was no such effect if the response efficacy element was combined with a self-efficacy element? I expected that self-efficacy is important in the context of password security behaviour because whether an individual is taking protective action depends on their ability to perform the recommended behaviour (Bandura, 1977). In addition, self-efficacy had been reported to be a key driver of protective security behaviour (e.g., Marett et al., 2011; Siponen et al., 2014; Johnston & Warkentin, 2010).

A potential explanation why the self-efficacy element proved ineffective for immediate password composition might be the nature of the mnemonic tips that I suggested to participants. Ye et al. (2019) looked at four mnemonic techniques, with two comparable to the tips that I provided participants in the self-efficacy and combined condition. First, "keyboard change" recommends choosing a password that is easy to remember and moving one key on the keyboard to the right to create a password of random strings. Second, "sentence substitution" suggests using a random sentence and replacing the words with letters, digits, or symbols. In this study, I recommended leaving out the vowels of a sentence. Ye et al. (2019) found that the passwords created based on these tips were not necessarily strong passwords because participants rarely included uppercase letters and symbols because

they strictly stuck to the tips recommended. Therefore, we should be mindful that the ineffectiveness of a self-efficacy to yield stronger passwords might be due to the password creation tips causing security repercussions. Hence, for example, participants might have missed incorporating numbers and symbols because they concentrated on implementing the tips. A potential solution could be to create and test a self-efficacy message that elevates user's ability to create strong passwords without providing specific mnemonic tips. Future research could test variations of the coping messages to explore which formulations make the coping nudges effective.

Second, the present study found that all coping elements enhanced participants behavioural intentions to adopt strong passwords relative to the control group. However, the behavioural intention scores were only significant for people who received the combined coping message compared with the control condition. These results imply that behavioural intentions can be elevated through messages with individual coping elements. Nevertheless, I have shown that the effect on behavioural intentions is the strongest when a self-efficacy and a response efficacy element are added to a combined message. This implies that intentions to adopt stronger passwords can be raised by making users aware that they can develop and remember strong passwords and simultaneously highlighting the effectiveness of passwords to mitigate the risk of password attacks. This pattern of findings is consistent with previous research. For example, Lee and Larson (2009) found that coping appraisal predicts the adoption intentions of anti-malware software by small- and medium-sized business executives. Van Bavel et al., (2019) also reported that self-efficacy and response efficacy combined were most related to intentions to engage in safe online behaviour.

Third, I found that self-reported behavioural intention did not translate into protective behaviour after four weeks. The results yielded that behavioural change was not predicted by the coping messages; and the self-reported behaviour at follow-up significantly decreased

compared to the behavioural intentions reported during the first part of the study. This marks another contribution to the debate of the intention-behaviour relation (e.g., Sheeran, 2002). By including a follow-up measurement to assess behavioural change (i.e., four weeks after the experimental treatment), I addressed a limitation of a significant body of cybersecurity research that has used intention to be representative of security behaviour (Emery et al., 2014; Hartmann et al., 2014); and only a few studies have assessed the impact of PMT interventions on subsequent behaviour. However, my finding is somewhat disappointing as it suggests that PMT interventions may have a limited impact on behaviour, despite the evidence that points to their ability in altering behavioural intentions.

Thus, there is a clear need for more research on bridging the gap from intention to behaviour. A few scholars have started to explore possible strategies to reduce the difference between self-reported intentions and secure behaviour (e.g., Gollwitzer, 2014; Gundu et al., 2019; Wilkowski & Ferguson, 2016). For example, Gundu et al. (2019) tested a security awareness training promoting organizational security policies. When they first measured behavioural change after the training session, the translation from intention to behaviour was only 50%. Nevertheless, Gundu et al. (2019) found that repeated training reduced this gap. Another tool for enhancing the translation of intention into action is implementation intentions. Implementation intentions include an assessment of opportunities (e.g., situations to implement goal behaviour) and obstacles (e.g., hindering feelings or thoughts that must be countered to continue goal behaviour) (Gollwitzer, 2014). Consequently, if people have identified possible opportunities for action and figured out how to manage obstacles, the likelihood of implementing behaviour increases (Gollwitzer, 2014). A meta-analysis with 94 studies on implementation intentions found a medium-to-large improvement in goal behaviour after forming implementation intentions compared to merely forming behavioural intentions (Gollwitzer & Sheeran, 2006). This has important implications for future research.

First, scholars could repeatedly expose users to the coping messages to test whether repetition effectively decreases the intention-behaviour gap. Second, future research could explore the impact of implementation intentions on behavioural adoption, for example, by replicating the present study with an additional element that asks the user to identify opportunities and obstacles to secure password habits.

However, I should note my findings of the memorability of the created passwords, short-term (i.e., five minutes) and long-term (i.e., four weeks). I suggest being mindful of the trade-off between the strength and the memorability of the created passwords; because upon additional analyses, it became clear that participants poorly recalled their created passwords in both short- and long-term. On average, participants only recalled the passwords with 45% accuracy five minutes after creating them, and after four weeks, mean recall accuracy reduced to only 5%. What we need to recognise is that the password security problem is, in fact, a memory problem. Research has shown that users can only accurately remember five independent passwords (Adams & Sasse, 1999). However, in password practice, users usually face numerous passwords, and it is a real challenge to memorise and correctly connect the stack of passwords to their corresponding accounts (Zviran & Erlich, 2006). Hence, this problem is an information retrieval problem related to long-term memory (Atkinson & Shiffrin, 1968). Password overload forces users to develop techniques to be able to recall multiple passwords. Consequently, users start to use shared passwords for multiple accounts, and such behaviour raises security risks (Adams & Sasse, 1999). To improve password security, I urge technological assistance (e.g., encrypted spreadsheets, or databases that save passwords) to support users to track their passwords.

Interestingly, I found that the coping messages did not increase the targeted coping cognitions. Only relatively few studies that sought to manipulate PMT constructs, have assessed PMT cognitions at separate time points (Milne et al., 2000). However, I measured

the cognitions before the intervention, immediately after participants received the coping messages, and four-weeks after the intervention. Neither self-efficacy-, nor response efficacy cognitions were affected by the corresponding coping messages; but I observed that participants perceived self-efficacy significantly increased from pre-intervention to post-intervention and follow-up regardless of the coping message that they received. Hence, it seems that in terms of motivating people to engage in protective password behaviour, PMT interventions can also produce effects on behavior and behavioural intentions without changing perceptions in the relevant constructs.

Limitations

First, I gathered data via an online survey in which participants created hypothetical passwords. The creation of passwords in this scenario may deviate from how participants would create passwords in everyday life. For example, my analysis revealed that participants could not accurately recall their created passwords in the short-term and long-term. I have already highlighted the memory problem when managing multiple strong passwords. However, it is also possible that in a real-world circumstance in which users create passwords that they would continue to use, they may focus on more memorable passwords as they did in the present study. Participants only received the instruction: “It is time to create secure (but hypothetical) passwords!”. Hence, I did instruct participants that they were supposed to remember their passwords at the point of password creation. Although I purposefully left them in the dark to not bias the results if participants would write down the passwords. Participants might have approached the password creation in the study with less seriousness as if they were to develop passwords in the real world. It might be that in the real-word user would create less strong passwords because they need to remember them. Consequently, the external validity of this research, and the extent to which the findings are generalizable to a real-world scenario, is open to criticism.

A second limitation marks my approach of scoring participants passwords. I took the recommendations for password management from Microsoft (Hicock, 2016) to develop the questionnaire that assessed the strength of participants' current passwords and calculated created password strength. However, even though I captured the complexity of created passwords based on most of the recommended characteristics, I could not assess whether the passwords entailed names due to the noisiness of available online libraries. In addition, I did not look at patterns of password creation that cyber criminals seem to consider when attacking user's passwords. For example, Komanduri et al. (2014) reported that longer passwords do not necessarily provide more protection. When users were asked to develop 16-character passwords, they chose passwords with repeating patterns (i.e., capital letters in the first position, symbols in the last, or numbers in the last two digits). Shen et al. (2016) also found that users mainly use easy-to-reach and frequently used symbols (i.e., "." @!) when symbols are added to passwords. Thus, although users add recommended elements to their passwords, they likely follow patterns and convenience. Therefore, future research could assess the predictability of secure password elements to improve the present study. This could increase the reliability of password strength interpretations.

Lastly, this study offered insights into the effectiveness of coping elements on password security. However, I focused solely on the self-efficacy and response efficacy constructs of the PMT, although the framework also considers response cost as a core construct. Accordingly, secure behaviour incurs an increased response cost (i.e., direct personal cost) in terms of inconvenience, effort, or time (Briggs, Jeske, & Coventry, 2017). Hence, the effectiveness of my coping messages on improving password habits was likely mitigated by a trade-off of participants' perceived cost and inconvenience of developing stronger passwords. However, since this was the same for all conditions (i.e., there was no manipulation of response costs for any condition), the validity of the results was not

influenced. Nevertheless, implementing an independent manipulation of response costs might have given us more information about users cost-trade-off to produce password security effects. Future research could adopt a coping message that aims to decrease the perceived costs associated with secure password habits.

Conclusion

In this study, I set out to understand how three coping messages affected password composition with the additional aim of increasing behavioural intentions and subsequent protective behaviour. I found that participants who were reminded of the effectiveness of strong passwords produced the most robust passwords during the study. Furthermore, participants in all three coping message conditions increased in behavioural intentions compared to those who did not receive a coping message, but significantly more so for users given the combined coping message. However, the behavioural intention did not translate into protective behaviour four weeks after the intervention. My findings have implications for future password creation procedures. I demonstrated that Government guidelines on password composition could be supplemented by a simple nudge (i.e., which most websites have failed to do), explaining to users that passwords are effective to diminish the risk of a password breach. I also demonstrated the need to adopt behavioural measures in addition to mere measures of behavioural intentions. Many people who express an intention to adopt stronger passwords may fail to do so. This suggests the need for further research into interventions that can help people translate intention into action. Repeatedly exposing the user to an invention and implementation intentions might be helpful to decrease that gap. We also must deal with the weaknesses of human memory to accurately recall strong passwords, and I urge more advances towards systems that securely store user passwords.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46. https://doi.org/10.1145/322796.322806

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184. https://doi.org/10.1016/j.chb.2019.106184

Andrews, L. W. (2002). Passwords reveal your personality. *Psychology Today*, *35*(1), 16.

Atkinson, R. C., & Shiffrin, R. M. (1968). Human memory: A proposed system and its control processes. In *Psychology of learning and motivation* (Vol. 2, pp. 89-195). Academic Press. https://doi.org/10.1016/S0079-7421(08)60422-3

Bakas, A., Wagner, A., Johnston, S., Kennison, S., & Chan-Tin, E. (2021). Impact of Personality Types and Matching Messaging on Password Strength. *EAI Endorsed Transactions on Security and Safety*, *8*(28). https://eudl.eu/doi/10.4108/eai.1-6-2021.170012

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

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 1-41. https://doi.org/10.1145/2333112.2333114

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In *Behavior change research and theory*, 115-136. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

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

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953-977. https://doi.org/10.1177%2F0093650218800915

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (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

Bundeskriminalamt [BKA]. (2021). Bundeslagebild Cybercrime 2020. Wiesbaden: BKA. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html

Centraal Bureau voor de Statistiek [CBS]. (2020). Nederland in cijfers. Den Haag: Centraal Bureau voor de Statistiek. https://longreads.cbs.nl/nederland-in-cijfers-2020/welk-percentage-van-nederlanders-koopt-online-en-wat/

Di Campi, A. M. (2021). Password guessing: learn the nature of passwords by studying the human behavior. http://hdl.handle.net/10579/19986

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, *2016*(8), 5-8. https://doi.org/10.1016/s1353-4858(16)30075-7

Emery, S. L., Szczypka, G., Abril, E. P., Kim, Y., & Vera, L. (2014). Are you scared yet?

Evaluating fear appeal messages in tweets about the tips campaign. *Journal of Communication*, *64*(2), 278-295. https://doi.org/10.1111/jcom.12083

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web*, 657-666. https://doi.org/10.1145/1242572.1242661

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

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the second symposium on Usable privacy and security*, 44-55. https://doi.org/10.1145/1143120.1143127

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education*. https://hdl.handle.net/1805/344

Gollwitzer, P. M. (2014). Weakness of the will: Is a quick fix possible?. *Motivation and Emotion*, *38*(3), 305-322. https://doi.org/10.1007/s11031-014-9416-3

Gollwitzer, P. M., & Sheeran, P. (2006). Implementation intentions and goal achievement: A meta-analysis of effects and processes. *Advances in experimental social psychology*, *38*, 69-119. https://doi.org/10.1016/S0065-2601(06)38002-1

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with computers*, *23*(3), 256-267. https://doi.org/10.1016/j.intcom.2011.03.007

Guha, S., & Kandula, S. (2012). Act for affordable data care. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, 103-108. https://doi.org/10.1145/2390231.2390249

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

Hammond, P., & Gummer, B. (2016). National cyber security strategy 2016 to 2021. *HM Government*. https://www.gov.uk/government/uploads/system/uploads/attachment_ data/file/567242/national_cyber_security_strategy_2016.pdf

Hartmann, P., Apaolaza, V., D'souza, C., Barrutia, J. M., & Echebarria, C. (2014). Environmental threat appeals in green advertising: The role of fear arousal and coping efficacy. *International Journal of Advertising*, *33*(4), 741-765. https://doi.org/10.2501/IJA-33-4-741-765

Hicock, R. (2016). Microsoft Password Guidance. https://www.microsoft. com/en-us/research/wpcontent/uploads/2016/06/Microsoft_Password_Guidance-1.pdf.

Howell, D. C. (2012). Statistical methods for psychology. *Cengage Learning*.

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the sigchi conference on human factors in computing systems*, 383-392. https://doi.org/10.1145/1753326.1753384

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566. https://doi.org/10.2307/25750691

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., ... & Egelman, S. (2011). Of passwords and people: measuring the effect of password-composition policies. *Proceedings of the sigchi conference on human factors in computing systems*, 2595-2604. https://doi.org/10.1145/1978942.1979321

Komanduri, S., Shay, R., Cranor, L. F., Herley, C., & Schechter, S. (2014). Telepathwords: Preventing weak passwords by reading users' minds. *23rd {USENIX} Security Symposium, 14*, 591-606. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-komanduri.pdf

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication. *UK Online Banking*.

LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. *The 55th annual conference of the international communication association, 51*(3), 71-76. https://doi.org/10.1145/1325555.1325569

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS*

Transactions on Human-Computer Interaction, 3(3), 170-188. https://aisel.aisnet.org/thci/vol3/iss3/2

Mayer, P., Kunz, A., & Volkamer, M. (2017, August). Reliable behavioural factors in the information security context. *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 1-10. https://doi.org/10.1145/3098954.3098986

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

Nicholson, J., Vlachokyriakos, V., Coventry, L., Briggs, P., & Olivier, P. (2018, July). Simple nudges for better password creation. *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*, 1-12. http://dx.doi.org/10.14236/ewic/HCI2018.46

Office for National Statistics [ONS]. (2021). Crime in England and Wales: Year Ending March 2021. London: ONS. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior*, *109*, 106347. https://doi.org/10.1016/j.chb.2020.106347

Plachkinova, M., & Maurer, C. (2018). Security breach at target. *Journal of Information Systems Education*, *29*(1), 11-20. https://aisel.aisnet.org/jise/vol29/iss1/7

Platje, T. (2021). *Behaviour change in cybersecurity: a mouse-tracking study* (Master's thesis, University of Twente).

Ponnusamy, V., Selvam, L. M. P., & Rafique, K. (2020). Cybersecurity governance on social engineering awareness. *Employing Recent Technologies for Improved Digital Governance*, 210-236. IGI Global. https://doi.org/10.4018/978-1-7998-1851-9.ch011

Potter, B. (2010). Common Sense for Your Network. *IT professional*, *12*(3), 11-13. https://doi.org/10.1109/MITP.2010.86

Quermann, N., Harbach, M., & Dürmuth, M. (2018). The state of user authentication in the wild. *Who are you*. https://wayworkshop.org/2018/papers/way2018-quermann.pdf

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Shay, R., Komanduri, S., Durity, A. L., Huh, P., Mazurek, M. L., Segreti, S. M., ... & Cranor, L. F. (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, *18*(4), 1-34. https://doi.org/10.1145/2891411

Sheeran, P. (2002). Intention—behavior relations: a conceptual and empirical review. *European review of social psychology*, *12*(1), 1-36. https://doi.org/10.1080/14792772143000003

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and personality psychology compass*, *10*(9), 503-518. https://doi.org/10.1111/spc3.12265

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, *61*, 130-141. https://doi.org/10.1016/j.cose.2016.05.007

Shillair, R. (2020). Protection Motivation Theory. *The International Encyclopedia of Media Psychology*, 1-3. https://doi.org/10.1002/9781119011071.iemp0188

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Stobert, E. (2015). *Graphical passwords and practical password management* (Doctoral dissertation, Carleton University). https://doi.org/10.22215/etd/2015-10903

Story, P. (2021). *Design and Evaluation of Security and Privacy Nudges: From Protection Motivation Theory to Implementation Intentions* (Doctoral dissertation, Carnegie Mellon University).

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: improving decisions about health. *Wealth, and Happiness*, *6*, 14-38. https://www.researchgate.net/file.PostFileLoader.html?id=53abe564cf57d7df1e8b45f4&assetKey=AS%3A273548994646025%401442230571326

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

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

Verizon. (2021). Data breach investigations report 2021. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/introduction/

Von Zezschwitz, E., Dunphy, P., & De Luca, A. (2013). Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 261-270. https://doi.org/10.1145/2493190.2493231

Wilkowski, B. M., & Ferguson, E. L. (2016). The steps that can take us miles: Examining the short-term dynamics of long-term daily goal pursuit. *Journal of Experimental Psychology: General*, *145*(4), 516. https://psycnet.apa.org/doi/10.1037/xge0000150

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

Ye, B., Guo, Y., Zhang, L., & Guo, X. (2019). An empirical study of mnemonic password creation tips. *Computers & Security*, *85*, 41-50. https://doi.org/10.1016/j.cose.2019.04.009

Zviran, M., & Erlich, Z. (2006). Identification and authentication: technology and implementation issues. *Communications of the Association for Information Systems*, *17*(1), 4. https://doi.org/10.17705/1CAIS.01704

Appendix A

Experimental Manipulation

Control condition

A secure password describes a password that is difficult to identify by humans and computer programs, thus, effectively protecting your personal data from unauthorized access.

Self-efficacy only condition

A secure password describes a password that is difficult to identify by humans and computer programs, thus, effectively protecting your personal data from unauthorized access.
If you are not sure how to create memorable and secure passwords, try to incorporate the following tricks:
(1) Remove the vowels from a phrase (e.g., “My favourite artist is Elvis” becomes “Myfvrtrtstslvs”)
(2) Shift the keys when typing (e.g., when you type “GoodMorning” but shift one key to the right it becomes “Hppf;ptmomh”)
(3) Double specific characters

Response efficacy only condition

A secure password describes a password that is difficult to identify by humans and computer programs, thus, effectively protecting your personal data from unauthorized access.
By creating highly secure passwords you can easily minimise the likelihood of suffering a cyberattack. If you choose a password that includes mixed numbers, lower and upper case-letters, symbols and more than 8 digits it will take a hacker more than 12 years to crack your password.

Self-efficacy and response efficacy combined condition

A secure password describes a password that is difficult to identify by humans and computer programs, thus, effectively protecting your personal data from unauthorized access.

By creating highly secure passwords you can easily minimise the likelihood of suffering a cyberattack. If you choose a password that includes mixed numbers, lower and upper case-letters, symbols and more than 8 digits it will take a hacker more than 12 years to crack your password.

If you are not sure how to create memorable and secure passwords, try to incorporate the following tricks:

(1) Remove the vowels from a phrase (e.g., “My favourite artist is Elvis” becomes “Myfvrtrtstslvs”)

(2) Shift the keys when typing (e.g., when you type “GoodMorning” but shift one key to the right it becomes “Hppf;ptmomh”)

(3) Double specific characters

Appendix B

Python Script for Analyzing Password Strength

```
import pandas as pd
import numpy as np

pswds = []
excel_data_df = pd.read_excel('data/Passwords.xlsx', sheet_name='Sheet1')
# get column names
headers = excel_data_df.columns.ravel()

# load data from the excel file containing passwords into 3 lists
for i in range(3):
    pswds.append(excel_data_df[headers[i]].tolist())
    print(pswds[i])

scores = np.zeros((3, len(pswds[0])))
special_characters = "\"!@#$%^&*()-+?_=,.~<>/\\\'"

# load dictionaries of words, filter out short words
# english dictionary
enDict = []
with open('data/english.txt') as file:
    while line := file.readline().rstrip():
        if len(line) > 5: enDict.append(line)
# dutch dictionary
nlDict = []
with open('data/dutch.txt') as file:
    while line := file.readline().rstrip():
        if len(line) > 5: nlDict.append(line)

# german dictionary
deDict = []
with open('data/german.txt') as file:
    while line := file.readline().rstrip():
        if len(line) >= 4: deDict.append(line)

# collection of common names and surnames
namesDict = []
with open('data/names.txt') as file:
```

```
    while line := file.readline().rstrip():
        if len(line) >= 4: namesDict.append(line)
with open('data/lastnames.txt') as file:
    while line := file.readline().rstrip():
        if len(line) >= 4: namesDict.append(line)

# date arrays
# year 1950 - 2004
birthDatesDict = np.arange(start=1950, stop=2005)
# year 2010 - 2021
recentDatesDict = np.arange(start=2010, stop=2022)

# lists for separate scores (3 dimensions per list)
passwordLength = np.zeros((3, len(pswds[0])))
numbersAndLetters = np.zeros((3, len(pswds[0])))
upperAndLowerCases = np.zeros((3, len(pswds[0])))
specialCharacters = np.zeros((3, len(pswds[0])))
dictionaryWords = np.zeros((3, len(pswds[0])))
namesOrSurnames = np.zeros((3, len(pswds[0])))
datesOfBirth = np.zeros((3, len(pswds[0])))
recentDates = np.zeros((3, len(pswds[0])))

for j in range(3):
    for i in range(len(pswds[j])):
        scoreCount = 0
        current = str(pswds[j][i])
        # check if longer that 8 characters
        if len(current) > 8: scoreCount += 1; passwordLength[j, i] = 1
        # check if contains numbers and letters
        if not current.isnumeric() and not current.isalpha(): scoreCount +=
1; numbersAndLetters[j, i] = 1
        # check if contains upper and lower case characters
        if any(x.isupper() for x in current) and any(x.islower() for x in
current): scoreCount += 1; upperAndLowerCases[
            j, i] = 1
        # check for special characters
        if any(x in special_characters for x in current): scoreCount += 1;
specialCharacters[j, i] = 1
        # check for dictionary words (dutch, english, german(only most
common words for german))
        # casefold is used to compare strings with case insensitivity
```

```
        if not (any(x.casefold() in current.casefold() for x in enDict)
                or any(y.casefold() in current.casefold() for y in deDict)
                or any(z.casefold() in current.casefold() for z in
nlDict)): scoreCount += 1; dictionaryWords[j, i] = 1
        # check for names
        if not (any(str(x.casefold()) in current.casefold() for x in
namesDict)): scoreCount += 1; namesOrSurnames[j, i] = 1
        # check for dates of birth
        if not (any(str(x) in current for x in birthDatesDict)): scoreCount
+= 1; datesOfBirth[j, i] = 1
        # check for recent dates
        if not (any(str(x) in current for x in recentDatesDict)):
scoreCount += 1; recentDates[j, i] = 1
        # save the total score of the specific password
        scores[j, i] = scoreCount

print(scores[j, i])
output = pd.DataFrame({'passwordLength1': passwordLength[0],
                       'numbersAndLetters1': numbersAndLetters[0],
                       'upperAndLowerCases1': upperAndLowerCases[0],
                       'specialCharacters1': specialCharacters[0],
                       'dictionaryWords1': dictionaryWords[0],
                       'namesOrSurnames1': namesOrSurnames[0],
                       'datesOfBirth1': datesOfBirth[0],
                       'recentDates1': recentDates[0],
                       'passwordLength2': passwordLength[1],
                       'numbersAndLetters2': numbersAndLetters[1],
                       'upperAndLowerCases2': upperAndLowerCases[1],
                       'specialCharacters2': specialCharacters[1],
                       'dictionaryWords2': dictionaryWords[1],
                       'namesOrSurnames2': namesOrSurnames[1],
                       'datesOfBirth2': datesOfBirth[1],
                       'recentDates2': recentDates[1],
                       'passwordLength3': passwordLength[2],
                       'numbersAndLetters3': numbersAndLetters[2],
                       'upperAndLowerCases3': upperAndLowerCases[2],
                       'specialCharacters3': specialCharacters[2],
                       'dictionaryWords3': dictionaryWords[2],
                       'namesOrSurnames3': namesOrSurnames[2],
                       'datesOfBirth3': datesOfBirth[2],
                       'recentDates3': recentDates[2],
```

```
                        'totalScore1': scores[0],
                        'totalScore2': scores[1],
                        'totalScore3': scores[2]})

# create pandas writer for excel
writer = pd.ExcelWriter("scores_output.xlsx", engine='xlsxwriter')

output.to_excel(writer, sheet_name='Sheet1', startrow=1, header=False)

# get the xlsxwriter workbook and worksheet objects.
workbook = writer.book
worksheet = writer.sheets['Sheet1']

# add a header format.
header_format = workbook.add_format({
    'bold': True,
    'text_wrap': True,
    'valign': 'top',
    'fg_color': '#D7E4BC',
    'border': 1})

# write the column headers with the defined format.
for col_num, value in enumerate(output.columns.values):
    worksheet.write(0, col_num + 1, value, header_format)

# close the Pandas Excel writer and output the Excel file.
writer.save()
```

Appendix C

Informed Consent Agreement: Intervention

We are excited to welcome you to take part in this web-based study concerning password security and cybercrime! This research is being conducted by Joelle Simon 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 why it is that sometimes people are inclined to behave in a security-conscious manner regarding their passwords, while others are not?

Procedure

Your participation will take approximately 20 minutes. You will respond to several questionnaires concerning your secure password knowledge, protection motivation, previous incidents of cybercrime, your current password strength, and you will be asked to report your demographics. Please make sure that you read all the questions attentively. In addition, you will be shown a security notification, that you should read and memorize. Next, you will create three hypothetical passwords. Please note, at the end of the study you are also asked to provide your e-mail address. This is so that we can forward a short follow-up questionnaire four weeks after your completion of the current study. Your e-mail address will be treated with full confidentiality, and your participation in the follow-up study is, of course, entirely voluntary.

Potential Risks and Discomforts

There are no obvious physical, legal, or economic risks associated with your participation. This research project has been reviewed and approved by the BMS Ethics Committee. For any problems or questions regarding 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 does not guarantee any benefits for you. Nevertheless, we hope you become more aware of the relevance of password security. Yet, the broader goal of this study is to explore preventive strategies against cybercrime.

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. The questionnaire includes items that are directly related to the passwords you are currently using; however, the questions regard your perception of the password strength and **at no point, you are asked to provide your actual password or any information that could lead to the discovery of that password.**

Right to Withdraw and Questions

Your participation is voluntary. If you decide to participate, you may stop participating at any time. If you decide not to participate or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify. The data you provided before you stopped participating, however, will be processed in this research. If you have questions, concerns, or complaints related to the study please feel free to contact us.

Contact Information

Joelle Simon (J.simon-1@student.utwente.nl)
Iris van Sintemaartensdijk (i.vansintemaartensdijk@utwente.nl)

Statement of Consent

By ticking the "I give my consent" box below, you confirm that you provide your consent, which indicates that you have read and understood all the information, you are at least 16 years of age, and you voluntarily agree that you want to participate in this study.

- I have been given sufficient information about the study.
- My participation is voluntary, and I have the right not to answer any of the questions. If I feel uncomfortable in any way during the study, I have the right to withdraw.
- I have understood that my e-mail address is only collected to forward a follow-up questionnaire. The researcher will not personally identify me in any reports, and my confidentiality as a participant will remain secure.
- I have read and understood the points and statements of this form. I have had all my questions answered to my satisfaction, and I voluntarily agree to participate in this study.

Appendix D

Informed Consent Agreement: Follow-up

Welcome back!

We are happy that you decided to participate in this follow-up survey on the study 'Protect your password so it can protect you: an interventional study'. The follow-up is being conducted by Joelle Simon and Iris van Sintemaartensdijk from the Faculty of Behavioural, Management and Social Sciences at the University of Twente; and the purpose of this survey is to check in with you four weeks after you were involved in the aforementioned interventional study.

Procedure

Your participation will take less than 5 minutes. You will respond to questionnaires that reestimate your protection motivation, and you are asked questions concerning your current password behaviour. Please read all the questions attentively. Note, at the beginning of this survey you will be asked to report your e-mail address again. This is merely so that we can connect your results from both studies.

Potential Risks and Discomforts

There are no obvious physical, legal, or economic risks associated with your participation. This study has also been reviewed and approved by the BMS Ethics Committee. For any problems or questions regarding 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 does not guarantee any beneficial benefits for you. Nevertheless, we hope you become more and more aware of the relevance of password security. Yet, the broader goal of this study is to explore preventive strategies against cybercrime.

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 decide to participate, you may stop participating at any

time. If you decide not to participate or if you stop participating at any time, you will not be penalized or lose any benefits to which you otherwise qualify. The data you provided before you stopped participating, however, will be processed in this research. If you have questions, concerns, or complaints related to the study please feel free to contact us.

Contact Information

Joelle Simon (J.simon-1@student.utwente.nl)
Iris van Sintemaartensdijk (i.vansintemaartensdijk@utwente.nl)

Statement of Consent

By ticking the “I give my consent” box, you confirm that you provide your consent, which indicates that you have read and understood all the information, you are at least 16 years of age, and you voluntarily agree that you want to participate in this study.

- I have been given sufficient information about the study.
- My participation is voluntary, and I have the right not to answer any of the questions. If I feel uncomfortable in any way during the study, I have the right to withdraw.
- I have understood that the researcher will not personally identify me in any reports, and my confidentiality as a participant will remain secure.
- I have read and understood the points and statements of this form. I have had all my questions answered to my satisfaction, and I voluntarily agree to participate in this study.

Appendix E

Questionnaires Intervention

Secure Password Knowledge

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

Please indicate your level of agreement with the following statements.

1. It's acceptable to use my social media password for other online accounts.
2. A mixture of letter, numbers, and symbols is necessary for a secure password.
3. It's secure to share my password if a friend asks for it.
4. A password that contains upper- and lower-case letters and numbers is secure.
5. It's not necessary to use different passwords for my online accounts.
6. It's secure to have a password with just letters.
7. A secure password contains less than eight characters.
8. A password with just numbers is secure.
9. It's secure to use my birth date as a password.
10. A password that consists of words that can be found in a dictionary (of my native language or foreign) is secure.

Risk Taking

** Assessed on a 7-point Likert scale (Extremely unlikely = 1; Extremely likely = 7)*

For each of the following statements, please indicate the likelihood that you would engage in the described activity or behaviour if you were to find yourself in that situation.

1. Admitting that your tastes are different from those of a friend.
2. Going camping in the wilderness.
3. Betting a day's income at a casino.
4. Investing 10% of your annual income in a moderate growth mutual fund.
5. Drinking heavily at a social function.
6. Taking some questionable deductions on your income tax return.
7. Disagreeing with an authority figure on a major issue.
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married man/woman.
10. Passing off somebody else's work as your own.

11. Going down a ski run that is beyond your ability.
12. Investing 5% of your annual income in a very speculative stock.
13. Going white-water rafting at high water in the spring.
14. Betting a day's income on the outcome of a sporting event.
15. Engaging in unprotected sex.
16. Revealing a friend's secret to someone else.
17. Driving a car wearing a seat belt (item reversed in the database).
18. Investing 10% of your annual income in a new business venture.
19. Taking a skydiving class.
20. Riding a motorcycle without a helmet.
21. Choosing a career that you truly enjoy over a more secure one.
22. Speaking your mind about an unpopular issue in a meeting at work.
23. Sunbathing without sunscreen.
24. Bungee jumping off a tall bridge.
25. Piloting a small plane.
26. Walking home alone at night in an unsafe area of town.
27. Moving to a city far away from your extended family.
28. Starting a new career in your mid-thirties.
29. Leaving your young children alone at home while running an errand.
30. Returning a wallet you found that contains $200 (item reversed in the database).

Password Strength

** Assessed using dichotomized answers (Yes/No)*

Please think about your most important password for a

(1) **work or study related account**

(2) **social media account (e.g., Facebook, Instagram, Snapchat, etc.)**

(3) **banking related account**

Read the statements below and indicate if they apply to you.

1. My password contains more than eight characters.
2. My password includes words that can be found in a dictionary (of my native language or foreign).
3. My password contains names (e.g., family, pets, friends, coworker).

4. My password contains a birth date.
5. My password only contains letters.
6. My password only contains numbers.
7. There are several special characters in my passwords (e.g., @#$%^&)
8. My password contains both upper- and lower case-letters.
9. My password contains both letters and numbers.
10. I only remember my password because I have it written down (excluding professional password manager).

Protection Motivation

Threat severity

** Assessed on a 7-point Likert scale (Extremely harmless = 1; Extremely devastating = 7)*

The following are some of the threats to your online safety that a password breach can cause. Please rate how harmful they would be if they happened to you.

How harmful would a password breach be if the information that is accessed…

1. is used to commit crimes against me.
2. reveals my personal information to other online criminals.
3. reveals my social security number or other forms of identification.
4. reveals my credit card information.
5. reveals my physical addresses.
6. could be subject to unauthorized secondary use.

Threat susceptibility

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

Thinking about your online safety based on the strength of your current passwords, please tell us how much you agree with each statement.

1. It is extremely likely that my personal accounts will be compromised by a password breach in the future.
2. My chances of a password breach are great.
3. There is a good possibility that my personal accounts will be compromised by a password breach.

Self-efficacy

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

Please indicate your level of agreement with the following statements.

1. I feel comfortable creating passwords to secure my online accounts.
2. Creating secure passwords is entirely under my control.
3. I have the resources and the knowledge to create secure passwords.
4. Creating secure passwords is easy.
5. I feel confident to remember secure passwords.

Response efficacy

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

Please indicate your level of agreement with the following statements.

1. Secure passwords would be useful for preventing my personal accounts to be compromised.
2. Secure passwords would increase my performance in protecting myself from cybercrime.
3. Secure passwords would make it harder for online criminals to compromise my personal accounts.

Response cost

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

Please indicate how much you agree with the following statements.

1. The inconvenience of implementing secure passwords to protect my personal accounts exceeds the potential benefits.
2. Remembering secure passwords is too complicated.
3. The negative side effects of employing secure passwords are greater than the advantages.
4. Using secure passwords requires a considerable investment of effort.
5. Using secure passwords requires a considerable amount of my time.

Password creation

It is time to create secure (but hypothetical) passwords for three online accounts.

1. Please fill in a password for your professional networking website.
2. Please fill in a password for your new work or student e-mail address.
3. Please fill in a password for your online banking.

Incidents of Cybercrime

Have you been a victim of cybercrime in the past 12 months?

If answered "Yes"

What type oy cybercrime to you fall victim to? Please describe below.

And after becoming of cybercrime, did you change your passwords to be more secure?

If answered "No"

What were the reasons that you did not change your passwords to be more secure? Please fill in below.

Time spent online

Thinking about an average weekday (from when you wake up until you go to sleep), how much time do you spend on each of the following devices to use the internet?

***Tablet* - Smartphone - Laptop or Notebook - Desktop Computer - Other devices**

1. Not at all
2. Up to one hour
3. 1 – 3 hours
4. 3 - 5 hours
5. More than 5 hours

Demographic factors

Please indicate your age:

What gender do you identify as?

1. Male
2. Female

3. Non-binary / third gender
4. Prefer not to say

What is your nationality?

1. Dutch
2. German
3. Other, please specify
4. Prefer not to say

What is your highest degree or level of school you have completed or are currently completing?

1. Less than a high school diploma
2. Highschool degree or equivalent
3. Bachelor's degree (e.g., BA, BS)
4. Master's degree (e.g., MA, MS, Med)
5. Doctorate (e.g., PhD, EdD)
6. Other, please specify

What is your current employment status?

1. Employed full-time (40+ hours per week)
2. Employed part-time (less than 40 hours per week)
3. Unemployed (currently looking for work)
4. Student
5. Retired
6. Self-employed

What is your average household income per year?

1. Below 10k €
2. 10k € - 50k €
3. 50k € - 100k €
4. 100k € - 150k €
5. Over 150k €

Behavioural Intention to Change Personal Passwords

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

Thinking about your personal passwords currently in use or future passwords to be created. Please indicate the level to which you agree with the following statements.

1. I plan to update my current work or study related password for security reasons.
2. I intend to include both letters and numbers when creating a new password for a work or study related account.
3. I will use several special characters when updating or creating a password for a work or study related accounts.
4. I intend to update my social media related password for security reasons.
5. I plan to update my social media related password using a sentence without vowels.
6. I am determined to not include names (e.g., family, pets, friends, coworker) when I create a new password for a social media related account.
7. I intend to update my banking related password for security reasons.
8. I plan to include more than eight characters when updating my current banking related password.
9. I will try to use both upper- and lower case-letters when I create a new password for a banking related account.
10. I intend to create passwords that I can remember without writing them down (excluding professional password manager).

Recall secure password characteristics

Do you remember what constitutes a secure password?

Please list the characteristics of a secure password below.

Memory of created Passwords

Passwords should not only be secure; they also must be rembered! Earlier you were asked to create three hypothetical passwords for different online accounts. Please recite them below.

Note: If you do not remember the passwords, type ‘I don’t remember’.

1. Please recite the password for the professional networking website.

2. Please recite the password for the new work or student e-mail address.

3. Please recite the password for the online banking account.

Appendix F

Complete Survey: Study 2

Memory of Created Passwords

Do you recall that passwords must not only be secure but also have to be remembered?
In the previous study, you were asked to create three hypothetical passwords for different online accounts. Please recite them below.
Note: If you do not remember the passwords, type 'I don't remember'.

1. Please recite the password for the professional networking website.
2. Please recite the password for the new work or student e-mail address.
3. Please recite the password for the online banking account.

Behavioural Change

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

Thinking about your password behaviour in the past 4 weeks.

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

1. I updated my current work or study related password for security reasons.
2. I includeded both letters and numbers when creating a new password for a work or study related account.
3. I used several special characters when I updated or created a password for a work or study related accounts.
4. I updated my social media related password for security reasons.
5. I updated my social media related password using a sentence without vowels.
6. I did not include names (e.g., family, pets, friends, coworker) when I created a new password for a social media related account.
7. I updated my banking related password for security reasons.
8. I included more than eight characters when I updated my current banking related password.
9. I used both upper- and lower case-letters when I created a new password for a banking related account.

10. I created passwords that I can remember without writing them down (excluding professional password manager).

Protection Motivation

Threat severity

** Assessed on a 7-point Likert scale (Extremely harmless = 1; Extremely devastating = 7)*

The following are some of the threats to your online safety that a password breach can cause. Please rate how harmful they would be if they happened to you.

How harmful would a password breach be if the information that is accessed…

1. is used to commit crimes against me.
2. reveals my personal information to other online criminals.
3. reveals my social security number or other forms of identification.
4. reveals my credit card information.
5. reveals my physical addresses.
6. could be subject to unauthorized secondary use.

Threat susceptibility

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

Thinking about your online safety based on the strength of your current passwords, please tell us how much you agree with each statement.

1. It is extremely likely that my personal accounts will be compromised by a password breach in the future.
2. My chances of a password breach are great.
3. There is a good possibility that my personal accounts will be compromised by a password breach.

Self-efficacy

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

Please indicate your level of agreement with the following statements.

1. I feel comfortable creating passwords to secure my online accounts.
2. Creating secure passwords is entirely under my control.
3. I have the resources and the knowledge to create secure passwords.
4. Creating secure passwords is easy.

5. I feel confident to remember secure passwords.

Response efficacy

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

Please indicate your level of agreement with the following statements.

1. Secure passwords would be useful for preventing my personal accounts to be compromised.
2. Secure passwords would increase my performance in protecting myself from cybercrime.
3. Secure passwords would make it harder for online criminals to compromise my personal accounts.

Response cost

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

Please indicate how much you agree with the following statements.

1. The inconvenience of implementing secure passwords to protect my personal accounts exceeds the potential benefits.
2. Remembering secure passwords is too complicated.
3. The negative side effects of employing secure passwords are greater than the advantages.
4. Using secure passwords requires a considerable investment of effort.
5. Using secure passwords requires a considerable amount of my time.

Appendix G

Debriefs

Skimmed Debrief (for participants that continue with study 2)

Thank you for participating in this study concerning password security behaviour!

Cybercrime is an increasing social problem in our digitalised world. While bicycle theft was once the most common crime in the Netherlands, it has been surpassed by cyberattacks in the past two years. One important feature of cybercrime prevention is password security, as it functions as the first line of defence for most computer systems. However, even the most sophisticated security systems are rendered vulnerable if users do not choose their passwords according to current security guidelines. This is why research in this field is highly relevant to investigate how potential victims of cybercrime can be motivated to create secure passwords.

However, there is more to this study that we can not inform you about at this point. Sometimes in research, it is necessary to not provide details of the study until the entire research is completed. If we did, it may affect how you respond to the questions in the follow-up survey, and this would make the results invalid. A full debrief, including information on the purpose of the study, the underlying theoretical framework and our corresponding predictions, will be provided to you at the end of the follow-up study.

If you have any questions regarding this study or the follow-up study, please feel free to contact the researcher.

Joelle Simon (J.simon-1@student.utwente.nl)

Iris van Sintemaartensdijk (I.vansintemaartensdijk@utwente.nl)

As a note, if you know of any friends or acquaintances that are eligible to participate in this study, we ask you to not discuss the procedure of the study with them until after they also have had the opportunity to participate. Prior knowledge of questions asked during the study can invalidate the results.

Thanks again for your participation!

Full Debrief

Thank you for participating in this research project concerning password security behaviour!

Cybercrime is an increasing social problem in our digitalised world. While bicycle theft was once the most common crime in the Netherlands, it has been surpassed by cyberattacks in the past two years. One important feature of cybercrime prevention is password security, as it functions as the first line of defence for most computer systems. However, even the most sophisticated security systems are rendered vulnerable if users do not choose their passwords according to current security guidelines. This is why research in this field is highly relevant to investigate how potential victims of cybercrime can be motivated to create secure passwords.

Protection motivation theory (PMT) provides a framework that explains why people have protection motivation by assessing fear-appeals (severity and vulnerability) and coping-appeals (coping efficacy, response efficacy, and response cost). On that basis, information that is tailored to influence these five factors is expected to motivate people to take specific protective measures. However, studies have shown, that people increased more in secure behaviour when they were presented with a coping message as if they were shown a message meant to induce fear.

Therefore, in this study, we are investigating whether security notifications with coping messages correspond to increased protection motivation and ultimately, better password strength. To do this, you were randomly assigned to read one of four different security notifications.

One of the conditions included a notification expected to increase self efficacy. Self efficacy is the belief about one's capabilities to enact a certain behaviour. For example, a person with high self efficacy regarding their password behaviour has the confidence and necessary knowledge that he or she needs to successfully develop secure passwords.

Participants in another condition got presented with a notification supposed to increase response efficacy, which is the belief that a specific behaviour leads to the expected outcome. This means that a person with high response efficacy regarding their password behaviour believes that secure passwords will be effective in reducing or eliminating the perceived threat of potential cyberattacks.

In another condition, we combined both security messages, and one condition served as a control and did not receive any security message.

We predict that protection motivation and password strength is increased for participants that received a security notification with a coping appraisal, in comparison to the control group.

If you have any questions regarding this study, please feel free to contact the researcher.
Joelle Simon (J.simon-1@student.utwente.nl)
Iris van Sintemaartensdijk (I.vansintemaartensdijk@utwente.nl)

Thanks again for your participation!