The Effects of Message Framing on the Risks and Benefits of Using Strong Passwords

Malin Orywahl (2053039)

Bachelor's Thesis

University of Twente

BMS Faculty

Department of Conflict, Risk & Safety

Supervisors

Steven Watson

Iris van Sintemaartensdijk

March 3, 2022

Abstract

The amount of information an internet user is storing on different websites has been steadily increasing over the past years. This personal data is often only protected by a user created password, which does not necessarily have to adhere to any guidelines, creating the possibility for users to choose weak passwords. This research used the Extended Parallel Processing Model to design messages highlighting the risks and benefits of password use and presenting participants with the basic guidelines to set up a secure password. Further, the study tested whether the effects of warning messages could be enhanced through matching message framing. Thus, assessing whether the type of data stored by a website has an influence on perceived risks, benefits, and affect, and the strength of the password choice. Participants were presented with either a social media platform, online banking, or a website that stores books online, thus each website had a different focus, stored different types of data, and, if hacked, would pose different types of threat to their users (identity, instrumental, or neutral). Each website type had a matching message frame, focusing on a specific type of threat, that was randomly assigned to participants. The results showed that the messages based on the EPPM did influence participants' perception and behaviour, however, no additional value of the matching message frames was found. Further, it was found that initial password choice was entirely motivated by the perceived benefits of creating a strong password rather than concerns about the risks of using a weak password. The results of this research highlight the importance for further research into the long-term effects of simple but repeated warning messages on behavioural change when using the internet.

The Effects of Message Framing on the Risks and Benefits of Using Strong Passwords

Over the last decade the amount of information that people store online has heavily increased. The average internet user has 25 accounts for various websites that require a password to login (Florencio & Herley, 2007; Fordyce et al., 2018). Online platforms are used daily for private matters, ranging from social media to online banking, and work-related tasks which require typing up to eight passwords per day on average (Florencio & Herley, 2007; Fordyce et al., 2018). While users are required to verify themselves through the use of their password or even two-factor-authentication to access their accounts, every year one in twenty-five adults will be affected by a data breach related to fraudulent activities (Roberts et al., 2013). Although there are many different types of cybercrime the most common exploited vulnerability is the chosen password of a user (Weber et al., 2008). When creating a password most internet users have to decide between security of a password and ease of use and, thus, often opting to use one password for multiple websites (Florencio & Herley, 2007; Fordyce et al., 2018; Weber et al., 2008). Research by Florencio and Herley (2007) and Fordyce et al. (2018) has shown that the average internet user has 6.5 passwords, using the same password for 3.9 different accounts. The issue with reusing passwords is that it increases a user's vulnerability, because an attacker, in case of a successful data breach, can access several accounts through one compromised password (Gaw & Felten, 2006).

As cybercrime attacks have been increasing and have become more confrontational and aggressive, especially targeting countries with a well-developed internet infrastructure and online payment systems, most websites have set up basic guidelines to help their users create stronger passwords (Europol, n.d.; Kolb et al. 2014). Users are advised to use at least eight characters, alternating between uppercase and lowercase letters, numbers, and special characters as well as

to choose a unique password for every new account they are setting up (Beno & Poet, 2020; Weber et al., 2008). Password length is directly related to password strength and number of different characters used (Weber et al., 2008). Despite this, most internet users choose to use a short and simple password and prioritise remembering it easily (Weber et al., 2008). Consequently, making it easier for attackers to compromise their accounts through guessing or cracking their password (Weber et al., 2008). Moreover, most hackers are able to try a few hundred passwords before their attacks are noticed, making it possible to hack into an account with a weak password within a few days (Tuesday, 2003). Nevertheless, internet users often create their password around a few common categories, such as names, birthdays, pets, locations, keyboard walks, etc. between which they can alternate resulting in a small set of similar passwords (Wei et al., 2018). Wei et al. (2018) found that the process of setting up a password is perceived as frustrating and unrewarding, thus, making it rare for an internet user to change their password to a more complex one. Furthermore, the research by Wei et al. (2018) has found that the name and semantic theme of a website affects the password choice of a user, for instance, using the word LinkedIn in the user's password for their LinkedIn account. Thus, creating an effortless password for the user as well as making the account more accessible for hackers. Additionally, Ur et al. (2015) found that password choice does differ depending on how much a user cares about the account. While many efforts have been made to encourage people to use stronger passwords, they have not been very successful (Weirich & Sasse, 2001). This research will use a model of persuasion to try and change internet users' behaviour and encourage them to use stronger passwords. Therefore, it is important to focus on how to persuade internet users into creating and using secure passwords as well as finding out which accounts get stronger

passwords. Furthermore, it will first be explored how people make decisions about what passwords to use, including the risk they might perceive when choosing their password.

Perceived Risks

When setting up a new account or changing an old password, internet users are sometimes required to make their password adhere to a few basic guidelines. These guidelines are usually instated to minimise the risk of user accounts being hacked as an internet user might deliberately choose a weak password in favour of remembering it easily as they do not feel very vulnerable to being the target of cybercrime because they perceive the likelihood of getting targeted themselves as rather low. Risk perception can be explained as a subjective judgment which people use to decide how likely they are to be harmed or experience a loss through an activity (Darker, 2013). Risk perception is separated into perceived likelihood and perceived severity which distinguish between how likely an individual perceives the threat is to affect them and how severe the consequences of the threat are. Applied to cybercrime and password security, risk perception focuses on how likely an internet user believes they are to become a victim of an attack and how severe the repercussions of the data breach would be. Weirich and Sasse (2001; 2002) found that users often underestimate their vulnerability to be a victim of cybercrime and, thus, might use a weak password for multiple accounts as they do not perceive themselves as a very likely target. Watson et al. (2017) conducted a study on unlawful file-sharing behaviour and found that perceived risks and likelihood are important predictors for behaviour when using the internet. While Watson et al. (2017) study did not assess participants' behaviour when creating passwords, risk perception is still assumed to play an important role when operating through the internet. If people are aware that there is a risk of having a weak password but perceive the likelihood of being targeted as low, then the risk will be accepted as it is not worth worrying

about. However, an individual's fear of becoming a target of a crime, not exclusively cybercrime, can have a negative effect on their physical and mental wellbeing (Roberts et al., 2013). Hence, an internet user does not necessarily have to be a victim of cybercrime to be affected by it. Roberts et al. (2013) found that often the mere perception of risk can already impact internet users behaviour, meaning that perceived risk can potentially be a motivation for taking protective action. However, perceived risk is not the only determinant of behaviour, people must also perceive benefit from creating a secure password in order to be motivated to create a strong password. Previous research has found that perceived risk is often associated with perceived benefits which, in turn, are often considered to influence each other through the affect heuristic. As well as that perceived benefits can have a direct effect on behaviour and a secondary effect via the affect heuristic.

Affect Heuristic

The affect heuristic explains that individuals are heavily influenced by their current emotions and, thus, rely on how they feel when making a decision (Fordyce et al., 2018; Van Schaik et al., 2020). Previous research often refers to risk as a feeling, meaning that the feeling of risk is a fast and intuitive reaction to danger which is seen as the primary role in motivating behaviour (Slovic et al., 2004). Van Schaik et al. (2020) suggest that affect heuristic plays an important part in how internet users perceive risks and benefits when using the internet. While benefits and risks often have a positive correlation in the world, that is, the greatest risks often come with the greatest rewards, this is often not the case for people’s association with risks and benefits. This means that every activity or technology is not only judged on the basis of what an individual thinks about it but also on their feelings towards the activity/technology (Slovic et al., 2004). Therefore, if an activity is seen as favourable, people are more likely to judge it as having

a low risk and high benefits than an activity that is unfavourable (Slovic et al., 2004). Most research on risk perception also focused on the role of affect, yet other studies have shown that perceived benefits can also have a direct effect on the risks an individual perceives (Slovic et al., 2014). Therefore, it can be argued that benefit and positive affect produce the same outcome. Consequently, providing an individual with information about the benefits of an activity or technology can change their perception of risk (Slovic et al., 2014). For instance, if an individual has to create a new account and type a new password when coming home after a long and stressful day at work, then this could, unconsciously, affect their password choice and password strength (Fordyce et al., 2018). Hence, the benefits of choosing a simple and already used password are high and the risks that are associated with such a password are estimated as low because the individual feels low affect toward making the effort to create a secure password. However, if, throughout the process of setting up their account, they are reminded of the benefits a strong password has, for instance, through a security message, their perception of risk can also change (Slovic et al., 2014). On the contrary, if they perceive benefits of a simple password are low then the risks of an easy password are perceived as higher which would motivate a user to create a stronger password. Thus, affect heuristic can be a crucial factor in online safety as it can be utilised, for example, through a security message, to motivate internet users to not ignore the risks of an often-used password in favour of remembering it. The security message should then emphasise the benefits of a strong password as well as that the message should focus on trying to manipulate the individuals' affect so that it feels like an easy and positive thing to do.

Most research on cybercrime has used the Protection Motivation Theory (PMT) to change participants' internet use through applying it to message framing (Kimpe et al., 2021). The PMT focuses on how an individual reacts when they are confronted with a threat (van Bavel

et al., 2019; Kimpe et al., 2021). Moreover, the theory identifies two processes at the core that influences individuals' motivations for protection, namely threat appraisal and coping appraisal (van Bavel et al., 2019; Kimpe et al., 2021; Norman et al., 2005). Coping appraisal uses self-efficacy and response-efficacy to evaluate an individual's ability to prevent or cope with a risk (Kimpe et al., 2021; Rogers, 1975). Threat appraisal assesses how serious a risk is for an individual, by focusing on the perceived severity and perceived vulnerability of that risk (Kimpe et al., 2021; Rogers, 1975). So, previous research that has used the PMT has mostly only focused on using an individual's risk perception and self-efficacy to change internet usage.

Witte (1992) has adapted and extended the PMT by developing the Extended Parallel Process Model (EPPM). In addition to focusing on the coping response of a person upon encountering a perceived risk/threat, the model takes into account the negative emotional arousal an individual might associate with an activity or technology (Kimpe et al., 2021; Witte, 1992). Hence, the EPPM can explain a person's affect response as affect heuristic is associated with how an individual is affected by their emotions towards a certain activity or technology.

Both, the EPPM and the PMT are often used in risk communication to appeal to an individual's risk perception and coping response. Van Bavel et al. (2019) have shown that providing individuals with a message to create awareness for a security issue has a positive effect on how they behave when using the internet. In their research, participants were presented with different security notifications focusing on either coping, threat appeal, or coping and threat appeal. Johnston and Warkentin (2010) and Mwagwabi et al. (2014) suggest that fear appeal as a persuasive message can have a positive influence on a user's compliance with secure internet behaviour. However, these interventions were mostly of limited effectiveness as long-term effects were often not visible (Chenoweth et al., 2019). So, while these studies included

persuasive messages they were mostly only related to threat and coping appraisal. Therefore, this research will focus on incorporating and highlighting the benefits of a change in behaviour can have for an individual (Chenoweth et al., 2019).

To conclude, individuals that perceive high benefits of repeatedly using simple passwords are likely to underestimate the risks that are associated with reusing passwords. Moreover, people that perceive low risks when using the same simple password for multiple accounts are likely to overestimate the benefits that are associated with reusing the same passwords. In order to change an internet user's behaviour, they should be reminded of the benefits a strong and secure password has, for instance through the use of an intervention message. However, while positively framed messages are expected to be more effective, intervention messages should also be aligned with the specific types of data websites store to assess whether the message increases the efficacy of messages.

Using Message Framing to Increase the Power of Persuasion

People use a multitude of different platforms and accounts for various internet activities. While some websites store barely any personal information, others require users to not only fill in personal data, such as address or bank details, but also keep track of their personal messages or media. So, not every hacked account holds the same level of threat to an internet user and the nature of threat also differs among accounts.

Websites like Instagram, Facebook, and Snapchat store valuable information about a user's identity ranging from private pictures to personal messages. Hence, if an external party gets access to an account that stores this information the user might possibly face the risk of their data being shared, causing significant social embarrassment (Bechmann & Vahlstrup, 2015; Gündüz, 2017). On the contrary, websites that could possibly give hackers access to a user's

substantial assets, like online banking or insurances, are seen as instrumental concerns as a user could possibly, for instance, lose money, etc. (Anderson et al., 2008). To illustrate, if an account of instrumental concern is hacked, the involved user might be requested to pay a ransom in order to get their account back and then, would lose money due to this fraudulent account.

Overall, the purpose of an account affects the type of threat that it imposes on a user in case it gets compromised. Thus, users might perceive different risks and benefits of their password choice based on what type of account they are signing up to. Ur et al. (2015) found that users do distinguish between the importance of an account. This subjective classification can influence their password choice as they might carefully consider their password for accounts that are important to them (Ur et al., 2015). Accounts that could possibly be of instrumental or reputational harm to a user might have a stronger password than accounts that hold no personal data. This knowledge could be used to motivate people to use stronger passwords by affecting how they feel about their security, as they could be persuaded to use a stronger password by matching a security message to the type of information protected by the account. Generally, people differ in the way that they receive messages and how they communicate (Taylor, 2002). Individuals tend to filter messages for those parts that they want to hear, therefore, it is important to have short and clear communication (de Bruijn & Janssen, 2017). Hence, when presenting an individual with a message regarding secure internet use and password creation it is crucial to take this into account and only present them with information that is relevant to them and their situation.

Current Research

This research aims to determine what effect an intervention message has on how a person perceives risk and benefits and, on their affect, as well as on an individual's password choice. Therefore, the following hypotheses are proposed:

Hypothesis 1: Benefits and affect are negatively correlated with risk perception.

Hypothesis 2: Perceived risks, perceived benefits, and affect have a positive effect on password strength.

Hypothesis 3: Messages based on the EPPM increase perceived affect and perceived benefits and reduce risk in comparison to before the message was presented.

Hypothesis 4: When message framing matches the type of data stored by a website, participants are more likely to adopt a stronger password.

Methods

Participants

Participants were recruited through SONA, social networks, social media, and snowball sampling. The only inclusion criteria were that participants had a sufficient understanding of English, a stable internet connection, and they had to be at least 18 years old, leading to a total of 134 participants. The participants' ages ranged from 18 to 67 with a mean of 22.56 (SD = 7.76). Furthermore, 65.7% of participants were female (n=88), 32.8% male (n= 44), two participants (1.5%) preferred not to disclose their gender. Most of the participants were German (52.2%, n=70), with another large group coming from the Netherlands (31.3%, n= 42). Additionally, a large group of participants reported a high school degree as their highest attained education level

(69.4%, n= 93). Further, 85.8% (n = 115) of participants stated that they use the same password for multiple accounts.

Design

The conducted study was a mixed factorial design, with participants randomly allocated to different conditions. The research followed a 3 (Type of data stored by the website: instrumentally sensitive data, identity sensitive data, non-sensitive data) x 3 (Intervention messaging frame: instrumental frame, identity frame, neutral frame) x 2 (Time of measure: before vs. after the intervention message) mixed design. The data type variable and messaging frame variable were between participants variables, and time measurement was a within participants variable.

Data type was operationalised by having participants sign up to a new website which primarily stored data associated with either instrumental concerns (an online bank), identity concerns (social media), or non-sensitive data (a repository for textbooks). Textbooks were chosen as a neutral type of data to reduce the overlap with identity concerns as they usually hold no personal information. The presentation of the different intervention messages were either tailored to the instrumental frame (financial threat), identity frame (reputational threat), or neutral frame (general data threat). Furthermore, this was measured before and after the intervention message was shown.

The dependent variables used in the research are three different scales measuring the perceived risk, perceived benefits, and affect and the strength of the chosen password. All dependent variables are measured before and after the intervention message is presented.

Materials and Measures

Simulated Websites

Each experimental condition had its own simulated online environment to replicate real-world behaviour as closely as possible. Participants were introduced to their website through a video displaying all the features and functions of each website to prime the specific concerns/threats of each website (identity and instrumental) and the low risk of the control website.

Identity Condition Simulated Website - 'Your Canvas'. In the identity group, participants were presented with an online environment that simulated a social media platform called 'Your Canvas'. In a short video of 20 seconds participants saw the features of the website which included storing and sharing personal pictures and videos, chatting with friends, commenting on posts, connecting all around the world with strangers, and creating a personal page. 'Your Canvas' advertised to users that they could create their own page to express themselves and share their content with the world. The website highlighted all the private media and communication that would be collected when creating an account, thus priming that valuable personal information may be at risk if the account was to be compromised and could be of reputational harm to a user. 'Your Canvas', a social media platform, was chosen as a suitable website type as most internet users are generally familiar with its function through websites like Instagram, Facebook, Twitter, or Snapchat.

Instrumental Condition Simulated Website - 'Bank To Go'. Participants were presented with an online environment that was replicating a bank account, thus, presenting the different functions of the websites. The online bank was named 'Bank To Go' and offered users a personal bank account in which they can store all their assets. Apart from money, the online

bank website would also store their personal data and provide the user with an account tailored to their needs. This was simulated through a short video of 15 seconds that participants were provided with to give them an overview of the design, functions, and benefits of setting up an account. Thus, instrumental concerns are highlighted to the participant through handling all their finances online and the mention of accessing the account from everywhere setting it up to be of high risk and repercussions if it was hacked.

Control Condition Simulated Website - 'Bookshelf'. The control condition was presented with a platform for storing books online called 'Bookshelf', this included novels, textbooks, and newspapers and magazines. The short video of 15 seconds that introduced participants to the website highlighted that the account could be easily accessed from everywhere and be used from multiple devices, making it the ideal place to keep their books. However, it also showed to participants that no valuable data would be stored making the website an extremely low risk account as it is not of identity or instrumental concern.

Risk Perception Scale

A risk perception scale was used to measure the participants perceived risks for the website they were asked to create an account for (Identity, instrumental, or control) (See Appendix A). A new scale was created to measure a participant's perceived risk to tailor it directly to this research and the websites participants were asked to create an account for. The scale included nine items that were directly addressing a participant's perceived risk by asking them to reflect on their new account and choosing a password for the website. Further, the items in the scale were divided into risk severity and risk likelihood. For instance, "If someone were able to hack into my account, I would lose valuable personal information" or "I think it is very likely that the account I just created will be targeted by hackers". Participants were asked to

indicate how much they agree with the statements made using a 5-point Likert scale (1= Strongly disagree and 5= Strongly agree). The risk perception scale as a whole had a Cronbach's alpha of .82 (Time 1), 'Item 6' was excluded from the analysis to reach a higher internal consistency for the scale.

Benefit Perception Scale

A perceived benefits scale was created to assess how a participant perceived the benefits for creating a new account (Identity, instrumental, or control) (See Appendix A). Van Schaik et al. (2020), originally developed by Finucane et al. (2000), was used to develop four new items measuring the benefits perceived by a participant for their website by asking them to reflect on the account they just created. With a 5-point Likert scale (1= Not beneficial and 5= Very beneficial) participants were asked to indicate how much they agree with the statements made, for example, "How beneficial is the password you created for reducing the harm you might experience if someone were to get unauthorised access to your account?" or "How beneficial do you think it is choosing a strong password for the website you just signed up to?". 'Item 1' was excluded from the benefit perception scale in order to increase the internal consistency of the scale and reach a Cronbach's alpha of .66.

Affect Scale

A scale measuring a participant's affect towards the website (Identity, instrumental, or control) was created (See Appendix A). Five new items were formulated asking participants to reflect on the previously shown website and indicate how much they agreed with the made statement using a 5-point Likert scale (1= Strongly disagree and 5= Strongly agree). For instance, stating "I felt secure when I set up my account for the website" or "I am satisfied with

my password choice". The affect scale had a Cronbach's alpha of .60, which means that the scale is of questionable internal consistency.

Intervention Message Frame

Multiple intervention messages with the same aim but different content were designed. Each condition, identity, instrumental, and neutral, had its own tailored warning message (See Appendix A). This message focused on the risks of weak passwords, the benefits of setting up a secure password, and simultaneously presented participants with the basic guidelines on how to create a strong password, in short it was a threat, benefit, and coping message. The intervention message was shown to check whether highlighting the benefits of a strong password would affect a participants password choice as well as if it would influence how they perceive the risks, benefits, and affect associated with making a password for a website. Van Bavel et al. (2019) security notifications were used and adapted to the different conditions (Identity, instrumental, and control), displaying the type of threat a participant would experience if their account was compromised. Van Bavel et al. (2019) have shown that simply providing participants with an intervention message increases their overall security behaviour. The messages used in this research were simultaneously targeting risk, affect, and benefits of password choice to motivate a behavioural change. Participants in the identity condition were presented with a message that mentioned that a stronger password would have an increase of protection for their personal data (messages and media) and could prevent them from reputational damage. Participants in the instrumental group received a message that explained that a stronger password could protect them from someone else accessing their finances. Participants in the neutral condition received a warning message reminding them that a stronger password could prevent their personal data being compromised by someone else having access to their account.

To assess whether a message focused on the data stored on the website presented to a participant had a higher effect than a message that was not fitting the website's purpose, the three different messages were randomly allocated between all conditions. Hence, a participant in the identity condition could, for instance, receive an intervention message tailored for instrumental threat recommending them to use a strong password to prevent an external party from having access to their finances and making unauthorised transactions.

Passwords

When creating the new account participants were first asked to choose a password (password1). Later on, they were presented with an intervention message, explaining the benefits of a strong password, which was followed by the option to change their password to a more secure password (password2). Participants were given the option to change their password in order to assess whether the intervention message had an effect on their password choice. While participants had to read the intervention message, they were free to choose if they wanted to create a new password. If a participant chose to keep their old password (password1) it would be automatically filled in as their 'password2' as well, resulting in an identical score. If they chose to change their password, they would have two different password scores (password1 and password2). The safety of their passwords (password1 and password2) was then assessed by using the 'Password Strength Test' of the University of Illinois and Chicago (https://www.uic.edu/apps/strong-password/). The 'Password Strength Test' was chosen as it scores passwords through a variety of different requirements ranging from the use of uppercase and lowercase letters to repetition of characters and then rating the passwords complexity and overall score. Furthermore, the 'Password Strength Test' website has the benefit that it scores passwords without storing any data on the website itself which was a necessary ethical

requirement to protect the participants of this research. The website provides one final score that is easy to interpret and not dependent on a computation that shows how much time is needed to crack the password, like other websites do. Having a score that shows how long it takes to crack a password is problematic as it then does not calculate how secure the password on its own is as well as that every password can be cracked at some point, it might just take more time for a strong password. Thus, the final score provided by the 'Password Strength Test' is calculated through all bonus points a password scored through fulfilling the basic criteria minus the deductions due to missing elements. The result is a score running between a minimum of 0 and a maximum of 100 points. Therefore, a high score is associated with a more secure password which would be harder to crack, which is important as it provides continuous measures which can be used to compare the password strength at two points.

Demographic Questionnaire

The demographic questionnaire included questions about age, gender, nationality, and education as well as questions about the participants' internet use. However, the questions about a participants internet usage were not further used for the research.

Procedure

Before data collection, ethical approval was obtained from the University of Twente Ethical Committee of the BMS Faculty (Request number: 211235). Upon opening the link participants were presented with an introduction to the study and instructions of what was expected of them. Participants were told that their task was to set-up an account for a new online platform and that they had to complete multiple questionnaires. Participants also had to give consent in order to move on with the research study.

As participants were randomly divided among the three website conditions, they were then forwarded to a page that showed them either a short video about a social media called ‘Your Canvas’ (Identity condition), an online bank named ‘Bank To Go’ (Instrumental condition), or a website that stored books named ‘Bookshelf’ (Control condition). Afterwards, they were requested to imagine they were genuinely signing up to use this service and to complete their account. All conditions had a pre-chosen username, so participants only had to choose a password (password1) to finish setting-up the account. This was followed by the first risk- and benefit perception and affect scale. Thus, participants' baseline beliefs about the risks, benefits, and their affect of signing-up to their condition website could be measured. Then participants were randomly presented with an intervention message mentioning the benefits of a secure password focusing on either reputational threat, instrumental threat, or control message only explaining the benefits. To illustrate, participants in the instrumental group received a message that explained the consequences of having a weak password emphasising the loss of personal finances, the identity group was presented with a message that explained the consequences of having a weak password and focused on the reputational harm it might bring, and the neutral group received a warning message that explained the consequences of having a weak password.

After receiving the warning message, participants could choose between keeping their old password, in which case they would have the same total score for ‘password1’ and ‘password2’, or to change their password, meaning that they would have two different password scores for password1’ and ‘password2’. A participant’s password choice was measured twice to check if the intervention message had an effect on the complexity and safety score of their password.

Next participants were asked to fill in the risk- and benefit perception and affect scale again. Participants were asked to complete the scale a second time to check if the warning

message had an impact on their risk perception, benefit perception or affect. Lastly, participants had to fill in a demographic questionnaire. The research study ended with a debriefing in which participants received a more detailed explanation of the aim of the research.

Results

Total Means and SD

On average the mean scores of risk, benefit, affect, and password all increased from the first to the second measure (Table 1).

Table 1

Mean Scores and Standard Deviations of Risk, Benefit, Affect, and Password

	Mean	*SD*
Risk 1	2.98	0.77
Risk 2	3.02	0.78
Benefit 1	3.46	0.89
Benefit 2	3.81	0.90
Affect 1	3.20	0.62
Affect 2	3.43	0.46
Password 1	74.64	28.08
Password 2	84.67	22.86

Correlations between Risk, Benefit, and Affect

A Pearson correlation coefficient was computed to assess the relationships between risk, benefit, and affect and password. Hypothesis one proposes that risk and benefit/affect are negatively correlated, however, only a positive relationship between the two variables affect and benefit ($r(132) = .53$, $p < .001$) was found while no significant relationship with risk was found. Moreover, the correlations were also used to determine whether there are any bivariate

relationships with risk, benefit, and affect and how strong participants' password choice was before the intervention. Correlations were found between benefit and password strength ($r(132) = .35$, $p < .001$) and between affect and password ($r(132) = .31$, $p < .001$). These correlations show that there are positive relationships between perceived benefits and password strength as well as between affect and password strength (Table 2).

Table 2

Correlations between Risk, Benefit, Affect, and Password

		Risk 1	Benefit 1	Affect 1	Password 1
Risk 1	Pearson Correlation	1			
	p				
Benefit 1	Pearson Correlation	.197	1		
	p	.023			
Affect 1	Pearson Correlation	.119	.539*	1	
	p	.173	.000		
Password 1	Pearson Correlation	.065	.357*	.317*	1
	p	.458	.000	.000	

* Correlation is significant at the 0.01 level (2-tailed)
** Correlation is significant at the 0.05 level (2-tailed)

Regression

A multiple linear regression was used to test if a participant's risk, benefit, and affect score (independent variables) had an influence on the strength of participants' password choice (dependent variable) before the intervention. The overall regression was statistically significant, $R^2 = .14$, $F(3, 130) = 7.6$, $p < .001$. However, it was found that risk did not significantly predict the password choice of a participant ($\beta = -.29$, $p = .92$) as well as that affect did not have a

significant effect on the strength of a participants password choice (β = 7.97, p = .06). However, perceived benefit significantly predicted password choice (β = 8.26, p = .008) (Table 3).

Table 3

Regression Table for the Effect of Risk, Benefit, and Affect on Password Strength

Effect	*B*	*SE B*	*p*	Confidence Intervals	
				Lower Bound	Upper Bound
Constant	21.31	14.13	.13	-6.65	49.28
Risk	-0.29	2.97	.92	.6.17	5.59
Benefit	8.26	3.05	.008	2.21	14.30
Affect	7.97	4.34	.06	-0.61	16.56

Testing the Effects of Message Framing

A mixed 3 (Type of data stored by the website: identity sensitive data, instrumentally sensitive data, non-sensitive data) x 3 (Intervention message frame: identity frame, instrumental frame, neutral frame) x 2 (Time of measure: before vs. after the intervention message) ANOVA was conducted for risk, benefit, affect, and password. Thus, the website type and message frame were between participant variables and the time of measure was a within participant variable. Interaction effects between the three factors, website type, message frame, and time, were also tested.

Perceived Risks

No statistically significant main effects for time on perceived risk were observed (F(1, 125) = 0.81, p = .36, η^2 = .007). No effect of message frame or website type on risk was found as well as no interaction effects (Fs < 2.54, ps > .05). However, the between-subjects effects do

show that there was difference between the risk scores among the different website types, $F(2, 125) = 21.08$, $p < .001$, $\eta^2 = .252$. The Gabriel post-hoc test was chosen as, due to the different website types and message frames, the groups for the conditions were rather small and of unequal size. The post-hoc test showed that the instrumental website type had significantly different risk scores than the identity and control website type ($p < .001$). Participants in the instrumental ($M = 3.42$, $SD = 0.70$) website type group had significantly higher risk perception scores than participants that experienced the identity ($M = 2.89$, $SD = 0.59$) or neutral ($M = 2.61$, $SD = 0.78$) website type.

Table 4

Means and Standard Deviations of the Risk Perception Scale

	Condition	Message	*Mean*	*SD*
Risk Score 1	Identity	Identity	2.73	0.65
		Instrumental	3.01	0.56
		Control	2.94	0.55
		Total	2.89	0.59
	Instrumental	Identity	3.23	0.84
		Instrumental	3.38	0.71
		Control	3.63	0.49
		Total	3.42	0.70
	Control	Identity	2.45	0.76
		Instrumental	2.56	0.46
		Control	2.82	1.00
		Total	2.61	0.78
	Total	Identity	2.80	0.81
		Instrumental	2.98	0.67
		Control	3.17	0.81

		Total	2.98	0.77
Risk Score 2	Identity	Identity	2.73	0.78
		Instrumental	3.07	0.71
		Control	3.06	0.51
		Total	2.94	0.69
	Instrumental	Identity	3.46	0.62
		Instrumental	3.49	0.63
		Control	3.55	0.54
		Total	3.50	0.58
	Control	Identity	2.69	0.81
		Instrumental	2.59	0.61
		Control	2.50	0.86
		Total	2.59	0.76
	Total	Identity	2.97	0.81
		Instrumental	3.05	0.73
		Control	3.05	0.80
		Total	3.02	0.78

Perceived Benefit

Statistically significant main effects of time on benefit perception were observed ($F(1, 125) = 18.51$, $p < .001$, $\eta^2 = .129$), meaning that benefits scores increase after the intervention (Before: $M = 3.46$, $SD = 0.89$, After: $M = 3.81$, $SD = 0.90$). No other main or interaction effects were statistically significant ($Fs < 0.92$, $ps > .05$).

Table 5

Means and Standard Deviations of the Perceived Benefits Scale

	Condition	Message	*Mean*	*SD*

Benefit Score 1	Identity	Identity	2.97	0.86
		Instrumental	3.73	0.74
		Control	3.66	0.97
		Total	3.44	0.90
	Instrumental	Identity	3.56	0.93
		Instrumental	3.55	0.84
		Control	3.49	0.88
		Total	3.53	0.86
	Control	Identity	3.39	1.12
		Instrumental	3.37	0.65
		Control	3.47	0.97
		Total	3.41	0.92
	Total	Identity	3.32	0.99
		Instrumental	3.55	0.74
		Control	3.53	0.92
		Total	3.46	0.89
Benefit Score 2	Identity	Identity	3.26	0.97
		Instrumental	3.85	0.63
		Control	3.87	0.74
		Total	3.64	0.83
	Instrumental	Identity	4.33	0.67
		Instrumental	3.64	1.10
		Control	3.98	0.57
		Total	3.99	0.83
	Control	Identity	3.75	0.73
		Instrumental	3.80	0.68

		Control	3.79	1.46
		Total	3.78	1.01
Total		Identity	3.80	0.89
		Instrumental	3.76	0.82
		Control	3.88	1.00
		Total	3.81	0.90

Perceived Affect

A positive, statistically significant, main effect of time on affect was observed ($F(1, 125) = 18.48$, $p < .001$, $\eta^2 = .129$), meaning that affect scores increased after the intervention (Before: $M = 3.20$, $SD = 0.62$, After: $M = 3.43$, $SD = 0.46$). No main effect of website type was found as well as no interaction effects ($Fs < 0.76$, $ps > .05$). However, the message frame also showed an effect $F(2, 125) = 5.47$, $p = .005$, $\eta^2 = .081$. The Gabriel post-hoc test showed that the identity message frame was significantly different from the instrumental ($p = .03$) and the control ($p = .01$) message frame. This was mostly due to low affect scores in the first affect scale and a later increase of affect in the second affect scale. However, the affect scores of the identity group in the second measure were rather similar to the mean scores of the instrumental and control message frame. Thus, it suggests that the deviating affect scores were due to the differences between participants at allocation rather than differences in the efficacy of the message frame. The instrumental and control conditions did not significantly differ from each other ($p = .99$).

Table 6

Means and Standard Deviations of the Affect Scale

	Condition	Message	*Mean*	*SD*
Affect Score 1	Identity	Identity	2.74	0.59

		Instrumental	3.28	0.53
		Control	3.52	0.46
		Total	3.15	0.61
	Instrumental	Identity	2.82	0.52
		Instrumental	3.48	0.39
		Control	3.30	0.45
		Total	3.20	0.52
	Control	Identity	3.07	0.79
		Instrumental	3.32	0.68
		Control	3.33	0.66
		Total	3.24	0.71
	Total	Identity	2.88	0.65
		Instrumental	3.36	0.54
		Control	3.37	0.53
		Total	3.20	0.62
Affect Score 2	Identity	Identity	3.35	0.45
		Instrumental	3.38	0.40
		Control	3.61	0.32
		Total	3.44	0.40
	Instrumental	Identity	3.5	0.37
		Instrumental	3.48	0.36
		Control	3.41	0.48
		Total	3.47	0.40
	Control	Identity	3.36	0.52
		Instrumental	3.40	0.37

		Control	3.40	0.75
		Total	3.38	0.56
Total		Identity	3.42	0.45
		Instrumental	3.42	0.37
		Control	3.45	0.56
		Total	3.43	0.46

Password

A statistically significant positive main effect for time on password strength was observed ($F(1, 125) = 28.95$, $p < .001$, $\eta^2 = .188$), meaning that password strength increased over time (Before: $M = 74.64$, $SD = 28.08$, After: $M = 84.67$, $SD = 22.86$). No main effects for website type or message frame were found nor were interaction effects found ($Fs < 1.84$, $ps > .05$).

Table 7

Means and Standard Deviations of the Password Scores

	Condition	Message	*Mean*	*SD*
Password Score 1	Identity	Identity	64.64	31.62
		Instrumental	74.78	29.25
		Control	77.81	22.01
		Total	72.00	28.19
	Instrumental	Identity	70.81	35.80
		Instrumental	73.86	22.56
		Control	81.17	32.29
		Total	75.43	30.59
	Control	Identity	83.81	24.47

		Instrumental	65.13	25.87
		Control	78.43	24.60
		Total	76.02	26.65
	Total	Identity	73.45	31.31
		Instrumental	71.18	25.72
		Control	79.34	26.72
		Total	74.64	28.08
Password Score 2	Identity	Identity	78.42	29.15
		Instrumental	83.28	27.26
		Control	81.27	20.82
		Total	80.97	25.75
	Instrumental	Identity	87.87	24.85
		Instrumental	88.60	12.25
		Control	92.88	11.08
		Total	89.87	16.99
	Control	Identity	86.68	25.93
		Instrumental	73.33	22.97
		Control	86.75	24.96
		Total	82.44	24.95
	Total	Identity	84.58	26.32
		Instrumental	81.70	22.07
		Control	87.75	19.63
		Total	84.67	22.86

Discussion

Over the past years there has been an increase in use of private accounts which are protected by a password as well as that the numbers of cybercrime targeting weak and repetitive passwords has been rising. This research has been focusing on factors that might have an influence on password strength and the question if tailored warning messages would be able to change a participant's behaviour. No relationship between benefit and affect on risk was found. However, high benefits scores were positively correlated with password strength before the warning message was even presented. Additionally, presenting participants with an intervention message did improve perceived benefits, affect, and password strength, but not perceived risk. However, the instrumental group ('Bank To Go') perceived more risks than participants that had to sign-up to the other websites. Further, the type of message that was presented had no additional effect over the already exhibited basic effect. A possible exception for affect measure was visible, however, this was due to differences in the sample's pre-intervention scores. No other effects were found.

Correlations Between Perceived Risks, Benefits, and Affect

This study looked at the correlations between perceived risks, benefits, and affect. It was hypothesised that benefit and affect are negatively correlated with risk perception. However, only a positive correlation between benefit and affect was found. Additionally, correlations between high benefit scores and password strength were found, as well as high affect scores and password strength. Meaning that participants that tended to have high benefit or affect scores also had high password scores. As has been argued before, positive affect and benefit produce very similar if not even identical outcomes (Slovic et al., 2014). The outcomes of this research also suggest that both constructs are related as well as that they both have similar effects on

password strength. However, the regression showed no relationship between perceived affect and password strength which is contradicting the results of the correlation analysis. Yet, this might be a result of the construct similarities between benefit and affect which are both trying to explain the same things. These similarities can also be seen in the regression analysis that was conducted where the relationship between benefit and password can partially be attributed to the correlation with affect and it suggests that, if it is necessary to choose, perceived benefits might be more impactful than affect.

Contrary to what previous research has suggested, neither benefit nor affect had any correlation with risk. Thus, Slovic et al. (2024) proposition that highlighting the benefits of an activity or technology can change an individual's risk perception could not be confirmed by the results of this research. Notably, this finding contradicts most research and literature about the correlations between risk and benefit and risk and affect. To get clearance on this and explore the results pertaining to the correlation between benefit and risk and affect and risk, further research is needed.

Effect of Perceived Risks, Benefits, and Affect on Password Strength

The results of the regression showed that if a participant perceived high benefits from creating a strong password and signing-up to the website this would have a positive effect on their password choice, making perceived benefits an important predictor for password strength. However, the same effect could not be found for perceived risk or affect. Previous research has often suggested that internet users are motivated by the risks and benefits they perceive of an activity (Watson et al., 2017). However, it has to be carefully considered and differentiated between when people are motivated by benefits and when they are motivated by risks. In this study, participants seemed to have associated creating a strong password with security, thus

security was a motivational factor to create a strong password. Therefore, this research is supporting the notion that perceived benefits are a good predictor for password strength. To extend, when creating a password participants focused primarily on the usefulness of a secure password and not how risky it might be and how they feel about it.

EPPM Messages and Perceived Risks, Benefits, and Affect

Presenting participants with a warning message did increase their perceived benefits and affect scores, but it had no effect on participants' risk perception. Additionally, it was also not relevant what type of message participants were presented with as the mere mention of a warning was enough.

The increase in perceived benefits overtime was due to being presented with an intervention message. The message frames showed participants the risks of choosing a weak password and the benefits of having a strong password in addition to presenting them with the knowledge on what a strong password would look like. Therefore, participants could see that through a simple change, that does not require a lot of effort, they could have a secure password and as passwords are often chosen through convenience, the warning message showed participants effectively that a strong password is beneficial (Weber et al., 2008). Affect scores increased overtime as well. Thus, the intervention message was successful in increasing participants' affect which means that participants were more influenced by their emotions as a reaction over time. This change in perception can be attributed to having participants reminded of the dangers of cybercrime and weak passwords immediately before asking them about their feelings towards the account. Hence, making it a recent memory and current problem which appeals to the affect heuristic (Fordyce et al., 2018; Van Schaik et al., 2020).

Additionally, for the affect scores participants that received the identity message frame

had a considerable increase in their affect scores. However, this was only possible because their scores were very low at the baseline and while there was an increase of their affect scores after the message was presented this did not exceed the affect scores of the instrumental and control group.

Lastly, it is to mention that participants that were asked to sign-up to the website type 'Bank To Go' showed an increase in risk scores after the intervention but this occurred independent of the intervention. After all, this might be due to the importance the account holds for the participant. The 'Bank To Go' website advertised to participants that they would store all their finances and grant them access through their accounts online, making it clear that the account was holding all their assets. Thus, the increased risk scores for the 'Bank To Go' condition are most likely due to the importance of the account as a data breach would be detrimental. Even though the sample is rather young, with an average age of 22 years old, and might not be wealthy or earn their own money through work, they still have their own bank account and are still at risk of being the target of fraud. Thus, banks are generally associated with importance and that might have had an effect on how participants perceived the severity of risk (Sarker et al., 2012). Although most people are familiar with social media platforms, not everyone uses it as extensively as a bank account as well as that it might not hold any real personal value, particularly for the older generations. Therefore, it would be important to regularly highlight how much personal information a platform like Instagram or Facebook stores of their users to raise awareness and increase risk perceptions for other types of threats.

To conclude, hypothesis three, that suggests that messages based on the EPPM increase perceived affect and perceived benefits and reduce risk, can partially be supported.

EPPM Messages and Password Strength

Hypothesis four proposed that having message framing match the type of data stored by a website would make participants more likely to adopt a stronger password. The analysis has shown that password strength on average did increase after the intervention. However, the increase in password strength was not dependent on the type of message framing and the results suggest that it was simply due to being presented with a reminder/warning message. Therefore, the fourth hypothesis that suggested that when message framing matches the type of data stored by a website, participants are more likely to adopt a stronger password cannot be accepted based on the results of this research. The general idea of these findings can be related to previous research that suggests that presenting internet users with a warning message can persuade them to change their password to a stronger one (van Bavel et al., 2019; Ur et al., 2015). However, van Bavel et al. (2019) found that coping messages were the most effective type of message framing, the type of message framing made no difference in this study. In this study, presenting participants with some type of warning message highlighting the importance of creating a strong password seemed to be enough for participants to react and change their behaviour. Therefore, it was redundant to have the message framing match the type of data stored by the website. However, it would have been interesting to see how participants that did not receive any type of warning message would have reacted to the request of choosing another password without any explanation.

Limitations and Future Research

The current study had several limitations which need to be mentioned. First, this research is not longitudinal study and while actual behaviour is recorded only the behavioural change directly after the intervention can be measured. Thus, using the data recording the change in

behaviour immediately after the intervention might work for the purpose of this research no conclusion can be drawn from the results to make predictions about long term behavioural change. Therefore, future research should incorporate a post-intervention measure in which participants are asked after the original research to assess whether the behavioural change is long lasting or not.

The second limitation concerns the password assessment and scoring. The tool, 'Password Strength Test' of the University of Illinois and Chicago, that was used to assess participants' password scores holds different requirements regarding length, number of characters, numbers, etc. While the tool is suitable when looking at basic password set-up it does not take into account whether participants were using names, birthdays, locations, or other common categories. However, these are patterns that hackers are often taking into account when trying to crack passwords. Therefore, future research could focus on including a scoring method for these common categories to increase the reliability of the password scores and account for hackers using these patterns.

Thirdly, the choice of the neutral website has to be further discussed. While 'Bookshelf' was originally designed to be a website that would just store textbooks this was not clearly enough specified. To illustrate, the video that participants were presented with highlighted that the website would store textbooks, novels, magazines, and newspapers. Therefore, participants might have assumed that the website would also store sensitive data such as adult magazines and books which could make the data stored by 'Bookshelf' an identity threat. Therefore, future research, when choosing a neutral type of website, should make sure that the features of the website are actually neutral and hold no private data with identity or instrumental concerns

Lastly, participants were not explicitly asked to remember their created passwords even though it has often been discussed that internet users choose their passwords based on convenience and not on strength. While most participants had rather adequate password scores in the first measure it is uncertain if they would be able to repeat these passwords at a later point. Even though, when participating from home through an online environment, it cannot be guaranteed if participants would use copy and paste, future research should account for this and specifically ask participants to remember their password for a later point in the research.

Even though this study had numerous flaws it also has to be pointed out that the use of the 'Password Strength Test' of the University of Illinois and Chicago was the ideal tool choice to score participants' passwords. The website considered a wide range of factors when scoring the passwords which resulted in a continuous variable that was very suitable and straightforward. Furthermore, as the study was conducted online and was concerned with internet behaviour nearly everyone could participate with little to non-effort.

Conclusion

Taking into account that this research was unsuccessful with proving that a tailored intervention message was needed to elicit perception of risk, benefit, and affect or adopting a stronger password, it could be shown that a general reminder of how to navigate safely through the internet was enough to have an effect on participants perception and lead to behavioural change, at least immediately after the intervention. All in all, this study has shown that supporting internet users with regular reminders on how to safely use the internet and especially how to correctly create a secure password has its effectiveness. These messages can prevent the influx of hacked accounts so that not every twenty fifth adult has to experience at least one compromised account every year (Roberts et al., 2013).

References

Anderson, K., Durbin, E., & Salinger, M. (2008). Identity Theft. *Journal of Economic Perspectives, 22*(2), 171-192. doi: 10.1257/jep.22.2.171

Bechmann, A., & Vahlstrup, P. B. (2015). Studying Facebook and Instagram data: The Digital Footprints software. *First Monday, 20*(12). https://doi.org/10.5210/fm.v20i12.5968

Beno, R., & Poet, R. (2020, November). *Hacking Passwords that Satisfy Common Password Policies* [Conference Session]. 13th International Conference on Security of Information and Networks, New York, NY, USA. https://doi.org/10.1145/3433174.3433616

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology.* https://doi.org/10.1080/0144929X.2021.1905066

Darker, C. (2013). Risk Perception. In M. D. Gellman & J. R. Turner (Eds.), *Encyclopedia of Behavioral Medicine* (2013 ed.). Springer, New York, NY. https://doi.org/10.1007/978-1-4419-1005-9_866

Europol (n.d.). *What is cybercrime?* https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Finucane, M., Alhakami, A., Slovic, P., & Johnson, S. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17. https://doi.org/10.1002/(SICI)1099-0771(200001/03)13:1%3C1::AID-BDM333%3E3.0.CO;2-S

Florencio, D., & Herley, C. (2007, May 8). *A Large-Scale Study of Web Password Habits* [Conference Session]. In Proceedings of the 16th international conference on World Wide Web (WWW '07), New York, NY, USA. https://doi.org/10.1145/1242572.1242661

Fordyce, T., Green, S., & Groß, T. (2018, December 5). *Investigation of the Effect of Fear and Stress on Password Choice* [Conference Session]. In Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, New York, NY, USA. https://doi.org/10.1145/3167996.3168000

Gaw, S., & Felten, E. (2006, July 12). *Password Management Strategies for Online Accounts* [Symposium]. Proceedings of the second symposium on Usable privacy and security, New York, NY, USA. https://doi.org/10.1145/1143120.1143127

Goodall, C., & Reed, P. (2013). Threat and Efficacy Uncertainty in News Coverage About Bed Bugs as Unique Predictors of Information Seeking and Avoidance: An Extension of the EPPM. *Health Communication, 28*(1), 63-71. https://doi.org/10.1080/10410236.2012.689096

Gündüz, U. (2017). The Effect of Social Media on Identity Construction. *Mediterranean Journal of Social Sciences, 8*(5). doi: 10.1515/mjss-2017-0026

Johnston, A., & Warketin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, 34*(3), 549-566. doi: http://dx.doi.org/10.2307/25750691

Kolb, N., Bartsch, S., Volkamer, M., & Vogt, J. (2014). Capturing Attention for Warnings about Insecure Password Fields – Systematic Development of a Passive Security Intervention. *Human Aspects of Information Security, Privacy, and Trust*, 172-182.

Krimsky, S. (2007). Risk communication in the internet age: The rise of disorganized skepticism. *Environmental Hazards, 7*(2),157–164. https://doi.org/10.1016/j.envhaz.2007.05.006

Mwagwabi, F., McGill, T., & Dixon, M. (2014, January 6-9). *Improving Compliance with Password Guidelines: How USer Perceptions of Passwords and Security Threats Affect Compliance with Guidelines* [Conference Session]. 47th Hawaii International Conference on System Science, Waikoloa, HI, USA. doi: 10.1109/HICSS.2014.396

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner, & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models* (pp. 81-126). Open University Press.

Roberts, L., Indermaur, D., & Spiranovic, C. (2013). Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry, Psychology and Law, 20*(3), 315-328. https://doi.org/10.1080/13218719.2012.672275

Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology, 91*(1), 93-114. doi: 10.1080/00223980.1975.9915803

Sarker, S., Bose, T., & Khan, A. (2012). Attitudes of customers towards the financial institutions-A comparison between private commercial banks and nationalized commercial banks in Bangladesh with implications of Fishbein model. *International Journal of Managing Value and Supply Chains, 3*(4). doi: 10.5121/ijmvsc.2012.3402

Slovic, P., Finucane, M., Peter, E., & MacGregor, D. (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk as Analysis, 24*(2), 311-322. https://doi.org/10.1111/j.0272-4332.2004.00433.x

Taylor, P. (2002). A Cylindrical Model of Communication Behavior in Crisis Negotiations. *Human Communication Research, 28*(1), 7-48. https://psycnet.apa.org/doi/10.1111/j.1468-2958.2002.tb00797.x

Tuesday, V. (2003, December 1). *Bad Policy Makes for Weak Passwords.* Computerworld. https://www.computerworld.com/article/2573523/bad-policy-makes-for-weak-passwords.html

Ur, B., Noma, F., Bees, J., Segreti, S., Shay, R., Bauer, L., Christin, N., & Cranor, L. (2015, July 22-24). *"I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab* [Symposium]. Symposium on Usable Privacy and Sexurity, Ottawa, Canada. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ur.pdf

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

Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security, 90*. https://doi.org/10.1016/j.cose.2019.101651

Watson, S. J., Zizzo, D. J., & Fleming, P. (2017). Risk, benefit and moderators of the affect heuristic in a widespread unlawful activity: Evidence from a survey of unlawful file sharing behavior. Risk Analysis, 37, 1146-1156. https://doi.org/10.1111/risa.12689

Weber, J., Guster, D., Safonov, P., & Schmidt, M. (2008). Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective*, *17*(1), 45-54. https://doi.org/10.1080/10658980701824432

Wei, M., Golla, M., Ur, B. (2018, August 12-17). *The Password Doesn't Fall Far: How Service Influences Password Choice* [Symposium]. Who are you?! Adventure in Authentication, Baltimore, MD, USA. https://www.blaseur.com/papers/way2018-wei.pdf

Weirich, D., & Sasse, M. (2001). Persuasive Password Security. http://dx.doi.org/10.1145/634067.634152

Weirich, D., & Sasse, M. (2002). Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. https://doi.org/10.1145/508171.508195

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

Appendix A

Instructions and Informed Consent

You are being invited to participate in a research study named “Online risks and password development”. This study is conducted for a bachelor’s thesis in the Faculty of Behavioural, Management and Social Sciences at the University of Twente.

This research aims to understand internet user’s password development when setting up a new account.
In order to participate you need to be at least 18 years old and be comfortable reading in English.

On the following pages, you will be asked to set-up an account for a new website, so you will have to fill in a password to complete your account. This platform does not exist, and is created just for our research, but we ask that you act as you would if you were genuinely signing up for the website. While we store all data anonymously, to increase your security we strongly recommend you do not use a genuine password that you use for any of your existing online accounts. Afterwards, you will be presented with questionnaires, including a demographic questionnaire, that you need to fill in. The study will take you around 10 minutes to complete.

Your response will only be used for the purpose of this research or follow up research based on this study. Anonymous data (excluding passwords) may be made available to the research community in accordance with the principles of open science. However, all data will be collected and stored anonymously and, thus, cannot be tracked back to you. For extra security, we will remove all submitted passwords from any data that we share with other researchers.

Participation in this research study is completely voluntary and you can be withdrawn at any time until you finish the study. You can do so by closing the tab or window you have used to open the research study. Upon doing so, all your data that has been collected so far will be deleted. As all data is stored anonymously, after you have completed the experiment we can no longer delete your data because we will not be able to identify your responses.

If you have any questions after participating you can contact me, Malin Orywahl, by sending an email to m.f.m.orywahl@student.utwente.nl or you can contact my supervisor, Dr. Steven Watson, by sending an email to s.j.watson@student.utwente.nl.
If you have any questions about your rights as a participant or concerns about the research you can contact the Ethics Committee of the Faculty of Behavioural, Management and Social Sciences at the University of Twente by sending an email to ethicscommittee-bms@utwente.nl.

Thank you for participating!

--- Page Break ---

Please read the information below carefully:

Participation in the Study

- I am at least 18 years old and am comfortable reading in English.
- I have read and understood the information regarding the study.
- I am voluntarily participating in this study, and I am aware that I can choose to withdraw from participating at any time during the study without providing a reason.
- I understand that because data is stored anonymously, I am unable to withdraw my data after I have completed the study.
- I understand that the researchers will store my data on secure servers and will not share the passwords I enter with others, but to ensure there are no risks to taking part in this research, I should NOT use a password that I actually use for any of my online accounts.

Use of Information

- I understand that taking part in the study involves answering questions about my demographics and performing tasks related to setting up an account for a website.
- I understand that all information I provide will be used for a bachelor's thesis, and may form the basis of publications in a peer reviewed journal or at an academic conference.
- I understand that my (anonymised) data will be accessible for at least 10 years due to the data management policy of the BMS faculty at the University of Twente.

Risk- and Benefit Perception

Risk Perception

Reflect on the website that you have just created a password for and indicate how much you agree with the statements made below.

By risk we mean the likelihood and severity of any harm that might come to you personally because you have signed-up to the service. Please assume the service is legitimate and there is no danger at all of the website itself deliberately misusing your data. Rather, we ask that you consider the danger of an external person obtaining unauthorised access to your account by guessing or otherwise working out your password.

Please rate the following statements based on how much you agree with them.

Item (General)
- When creating the new account, I was worried about someone else getting access to that account

Item (Severity)
- If someone were able to hack into my new account, I would lose valuable personal information

Item (Severity)
- If someone were able to hack into my new account, I think something bad would happen

Item (Severity)
- I think it would have severe consequences if someone would hack the account I just created

Item (Likelihood)
- I think it is very likely that the account I just created will be targeted by hackers

Item (Likelihood)
- I think it will be very easy to hack into the account I just created

Item (General)
- The account I just created stores valuable personal information about me

Item (Identity)
- If someone were able to hack into my new account I would be very worried about them using the information in my account to embarrass me

Item (Instrumental)
- If someone were able to hack into my new account, I would be very worried about them using the information in my account to harm me financially

Benefit Perception

Reflect on the website that you have just created a password for to set-up your account and indicate how much benefit you think there is associated with signing up to that website.

By beneficial, we mean an overall evaluation of how useful the service would be in your everyday life. Assume you do not already have an account for any similar websites that perform a similar function.

Item
- Overall, how beneficial would the service be for you?

Item (Password)
- How beneficial is the password you created for reducing the likelihood of someone getting unauthorised access to your account?

Item
- How beneficial is the password you created for reducing the harm you might experience if someone were to get unauthorised access to your account?

Item
- How much benefit do you think you have from choosing a strong password for the website you just signed up to?

Affect Heuristic

Reflect on the website that you have just created a password for to set-up your account and indicate what you felt when signing up to that website by indicating how much you agree with each statement.

Item
- I felt secure when I set up my account for the website

Item
- I felt confident when choosing my password for the website

Item
- I am satisfied with my password choice

Item
- I felt vulnerable when creating an account for the website

Item

- I am happy with the amount of personal information the website is storing about me

Warning Message

Identity

Navigate safely. You can easily minimise the possibility of suffering a cyber-attack if you use a secure password (e.g., by using at least eight characters and combining lower and upper cases, numbers, and symbols). If you don't, your personal data could be compromised, and this could mean someone has access to any personal messages and photos and videos stored on this website which could damage your reputation.

Instrumental

Navigate safely. You can easily minimise the possibility of suffering a cyber-attack if you use a secure password (e.g., by using at least eight characters and combining lower and upper cases, numbers, and symbols). If you don't, your personal data could be compromised, and this could mean someone has access to your personal finances and may withdraw money from your account or make unauthorised transactions.

Neutral

Navigate safely. You can easily minimise the possibility of suffering a cyber-attack if you use a secure password (e.g., by using at least eight characters and combining lower and upper cases, numbers, and symbols). If you don't, your personal data could be compromised, and this could mean someone has access to your account.

Debriefing

Dear participants,

In this study, you were presented with the task to either create an account for a bank, a social media, or a document storing system.

The aim of the research is to find out if internet users differentiate between what passwords they use based on what type of information is protected by that password. For instance, using a password that does not adhere to the common security guidelines (such as a long length and mixing symbols and numbers with letters) for an account that is not frequently used and does not hold any personal information versus websites that contain much more sensitive types of data. Therefore, participants were randomly presented to one of the three different types of websites. Participants were asked to create an account for one of three types of account: an online bank which stores financial data, a new social media website which stores social and personal data, and a website which only stores textbooks and so holds non-sensitive data. The warning message that you received after you completed your first password was also randomly allocated. It either matched the website you saw or it did not (E.g. highlighting the danger of unauthorised access to your personal finances if you signed up to an online bank or highlighting the danger of

unauthorised access to your personal finances if you signed up to a new social media account). Furthermore, you were asked twice to fill out a risk- and benefit perception scale which will be used to assess if the warning message had an effect on your risk- and benefit perception when setting up your fictional account. We are interested in whether people are more likely to use a more secure password depending on the type of data a website stores, and whether a prompt to use a secure password matches the function of a website.

If you have chosen to use a real password of yours please make sure that you change that password immediately!
While we will do all we can to protect your data, no data storage is 100% safe and so it is safest to change any passwords you use that match what you entered into this study.

For further questions, you can contact the researcher Malin Orywahl (m.f.m.orywahl@student.utwente.nl) or the supervisor Dr. Steven Watson (s.watson@utwente.nl).