The Influence of Knowledge and Self-efficacy on the Intention to and Actual Use of Strong Passwords

Hannah Olden

S2157047

University of Twente

1st Supervisor: Dr. Iris van Sintemaartensdijk

2nd Supervisor: Dr. Steven Watson

2022

Abstract

In this digital age, cybersecurity is an important concern for all internet users. According to preceding research in the field of cybersecurity, previous password knowledge and self-efficacy play an important part in whether people intend to and actually behave safely online. In this study, health behaviour models were used to make an inference about the possible interaction effect of self-efficacy and knowledge on the intention to and use of strong passwords. In a two-part online study, 121 participants took part. In the first part, participants were asked about their previous knowledge on passwords, after which they were tasked to construct three passwords themselves. Lastly, their levels of self-efficacy, risk-taking and their behavioural intention are inquired about. The introduction to the task was manipulated using a newspaper article that either stated that it is a very hard (low self-efficacy) or easy task (high self-efficacy). For the control condition, there was only the task without a newspaper article. In the follow-up study, participants were asked about their knowledge, self-efficacy and their security behaviour. While there was no significant influence of the manipulations on participants´ level of self-efficacy, there were also no significant effects of self-efficacy on its own or in combination with knowledge on intention and actual behaviour. Previous knowledge influenced the intention to and actual use of strong passwords. Further, it was found that intention directly increases actual behaviour. This study emphasizes the need for more research into the connection between knowledge and self-efficacy concerning the use of strong passwords.

Keywords: cybersecurity, strong passwords, self-efficacy, knowledge, behavioural intention, behaviour

Introduction

Background

In recent decades, the internet has made a considerable advance in size and the number of users. In 2021, 4.88 billion people used the internet actively worldwide, while this number increases daily by about 600,000 people (*Digital Around the World*, 2021). With this increase in range, undesirable features of the internet also grew. One of the biggest problems arising is cybercrime, which is defined as criminal acts that use "electronic communications networks and information systems" as an instrument (European Commission, n.d.). According to National Cybercrime Initiative (2017), 3-5% of the Netherlands´ population fall victim to online consumer fraud, hacking or malware each year. When comparing this to the numbers of bike thefts or burglaries in the Netherlands, the percentage is closely similar (3-4%). Thus, cybercrime happens just as often or even more often than those rather conventional forms of crime.

This does not show the complete extent of the problem, as there is no concrete estimated number of unreported cases because the likelihood is high that cybercrimes are not being reported by the victim (National Cybercrime Initiative, 2017). As Briggs et al. (2017a) found, people are more likely to report a computer-related problem when they feel like it is beneficial for them to do so. Further, if the problem is framed as technical rather than security-relevant, the problem is also reported more often. It is therefore possible that employees expect that their organization would react faster to technical problems, like software or hardware issues, than to cybersecurity issues (Briggs et al., 2017a). Possibly, this can be expanded to the general population that expects for instance their internet provider´s reaction to be faster for technical issues. This is a great inconvenience in the fight against cybercrime, as the crimes are relevant to cybersecurity, and are not being investigated properly if they are not reported to officials.

Risk factors of falling victim to cybercrime include the use of weak passwords, like 123456. Those passwords are easily compromised by a hacker, which happened to the 23.2 million accounts on different websites worldwide that use this simple number password (National Cyber Security Centre, 2021). Most of the time these passwords consist of only numbers, only small letters or have a capital letter at the beginning and a special character at the end. Further, in the UK Cyber Survey of 2019 (Ipsos MORI, 2019), it was found that 62%

of participants never or rarely use a password manager on their mobile devices, while over 40% save some or all their passwords in their web browser, which is an unsafe practice (Ontech Systems, 2018). The fact that not all people use password managers adds to the problem in such a way that they cannot remember all passwords for their accounts if they create different or complicated ones, which would be the safest option. Instead, people tend to use similar or even the same passwords for multiple accounts, which is a second severe security risk (National Cyber Security Centre, 2021). Accordingly, the human is seen as the weakest link in the chain of cybersecurity (Moustafa et al., 2021).

In order to combat this growing problem, studies have investigated how effective different interventions on cybersecurity as a whole are in making people handle their data more securely. The findings on those interventions differed widely, as some found that the measures are effective, even over a longer period of time, like 2 years, while others found that the interventions are not very effective (Bowen et al., 2011; Caputo et al., 2014; Pattinson et al., 2012). As an example, Bowen et al (2011) found that in all cases, their participants could be trained to be careful when an email looks suspicious and could therefore be an attempt of phishing. Caputo et al. (2014) on the other hand found no difference in susceptibility to phishing, no matter if participants had been trained or not trained in between their trials.

Furthermore, various factors were established to be an influence on the intention to behave in a secure way when using a computing device. The National Cybercrime Initiative (2017) identified motivation as a central factor. Overall, there is a consensus that people must understand the advice that is given to them, while they also need to feel capable and motivated to do as the advice states. This is assumed to change attitudes and intentions, and should, therefore, indirectly lead to more cybersecure behaviour (Bada et al., 2019). A specific technique to prompt people to behave more securely is called nudging and consists of trying to influence people´s behaviour without using commands or restrictions (Thaler & Sunstein, 2008). In the current context, it works best when a simple nudge is combined with information for the recipient (Zimmermann & Renaud, 2021). A simple nudge is here defined as a given stimulus that targets automatic processing and is not necessarily educational.

Different factors were identified that make actually complying with security policies and recommendations more likely. Moustafa et al. (2021) determined that different

personality traits, like impulsivity and lack of thinking about the future, are related to not complying. Sheeran and Webb (2016) further investigated human behaviour concerning cybersecurity. They reviewed multiple meta-analyses on cybersecurity intentions and came to the insight that the intention to behave in more secure ways on computing devices was present, but the actual behaviour did not always follow, which is called the intention-behaviour gap.

According to Mack et al. (2019), the intended goals need to be kept salient in order to bridge the intention-behaviour gap. In their study on the intention-behaviour gap in electricity saving, this was done by means like reminding people of their intentions and asking them about their progress in the pursuit of their intended goals. Possibly, Mack et al.´s (2019) findings can be transferred to the cybersecurity sector as well, in which sending digital reminders or status questionnaires to people about their progress in using strong and differing passwords would be helpful in overcoming the intention-behaviour gap.

Protection Motivation Theory, Self-efficacy and Knowledge

A psychological theory that has been used in the design of nudges is the Protection Motivation Theory (PMT). The PMT gives a framework to understand fear as a motivator for protective behaviours (Rogers & Prentice-Dunn, 1997), and its components have been applied to interventions for cybersecurity behaviours in multiple studies. As specified in the PMT, individuals who make a decision on whether they will take protective action engage in two different appraisals. Firstly, the threat appraisal consists of the individual taking note of the severity of the threat and how vulnerable they are to it. During the coping appraisal, the individual calculates the response costs and judges both their response efficacy and their self-efficacy (Rogers, 1983). Self-efficacy is defined as the person´s appraisal of their own abilities to perform the needed or desired behaviour (Bandura, 1986). In general, how individuals appraise the cybersecurity threat and their self-efficacy to cope can help in understanding the influence on willingness and execution of cybersecurity behaviours (Briggs et al., 2017b). If individuals perceive their vulnerability to the threat as high, as well as their self-efficacy, they show a greater likelihood to act in counter to the threat. This is classified as an adaptive response, according to Rogers (1983), as it aims to combat the threat rather than the emotions that the threat triggered in the individual. A maladaptive response is triggered by intrinsic and extrinsic rewards whereas the person´s beliefs about the severity of

the negative consequences and their vulnerability to those consequences decrease the likelihood of maladaptive responses (Rippetoe & Rogers, 1987). Therefore, effective cybersecurity interventions should deliver a coping message, rather than a fear appeal, as this way, a high perceived vulnerability to the threat and high response- and self-efficacy together trigger an adaptive response (van Bavel et al., 2019).

As seen in the research using the PMT, a crucial variable in the appraisal of a threat is self-efficacy. It also plays an essential role in the decision whether to act against the threat, so an adaptive response, or against the feelings the threat triggered in the individual, a maladaptive response (Rogers, 1983). Therefore, in multiple different fields of application, studies tested the effect of self-efficacy on desired outcome behaviours. Particularly in health behaviour research, it was established that the more self-efficacy concerning health behaviours participants perceived, the healthier their behaviour was in the long term (Rimal, 2000). Furthermore, self-efficacy is an important part of the motivation needed to fulfil the intended behaviours (Faries, 2016). Thus, the more self-efficacious a person is, the more likely it is that they will execute the desired behaviour.

In addition to this, the desired outcome should be slightly challenging but still obtainable in order to motivate the individuals that are addressed by the message. These individuals are then more likely to train their skills in healthy behaviour, as found by Faries (2016). As this has been found in other fields before, the current study examines self-efficacy in connection to cybersecurity. In general, there is a close connection between self-efficacy and the intent to implement the desired behaviour, as well as actually acting on this intention. To elaborate, Mwagwabi et al. (2018) established that high self-efficacy is connected to a higher level of intention to use strong and differing passwords for every account. Additionally, Hameed and Arachchilage (2021) found that self-efficacy is positively correlated to the likelihood of adopting innovations in information system security. This means that increasing self-efficacy for addressed people could lead to better enactment of security measures, which can also be extended to the cybersecurity sector, especially for using different passwords for different accounts and using strong passwords for each account.

A second crucial influence on intention to and actual use of safe passwords is the knowledge people hold about the topic. This includes knowing that a weak password puts you at risk and that you should not use the same password for every account. The more

people know about using and constructing a secure password, the higher their intention is to use them (Kennison & Chan-Tin, 2020). As knowledge and self-efficacy both affect people´s cybersecurity behaviour, it is likely that they interact. This has not yet been explored in the field of cybersecurity, while it has been investigated in the health domain. To illustrate, in a study about the intake of sugar-sweetened beverages, Wang and Chen (2022) found that self-efficacy has a larger influence on their intake than knowledge has. They established a model in which they determined that knowledge, as well as the perceived benefits and barriers to consuming sugar-sweetened beverages, influenced self-efficacy, which in turn influenced consumption. Knowledge also influenced consumption directly, but only marginally, and therefore, not statistically significantly.

Furthermore, other studies had similar results on the interaction between knowledge and self-efficacy. In particular, in a study with patients who suffer from Type 2 Diabetes, the results showed that educating those patients had a positive influence on their self-efficacy to deal properly with their illness (Atak et al., 2008). Moreover, knowledge has barely any influence on behaviour when self-efficacy is not present. In other words, knowledge is important in the process of influencing behaviour, but it does not affect behaviour without self-efficacy. This can be seen in people who want to give up smoking as well as in dietary research. If people feel they do not have the fitting capabilities to perform the desired behaviour, it does not matter if they know a lot about, for instance, the benefits of the behaviour (Rimal, 2000). As the influence of knowledge and self-efficacy was examined separately in the cybersecurity domain, it is surprising that both have not been investigated in connection to each other. Since an impact of the interaction between knowledge and self-efficacy has been found in other areas, like healthy behaviour, it needs to be examined whether this interaction can be applied to protective behaviour in the wider sense, of which cybersecurity is a big part. Therefore, it is necessary to investigate this interaction in connection with the intention to and actual use of strong and differing passwords. By making an inference from health psychology models (Faries, 2016; Rimal, 2000), it is expected that the knowledge about the use of strong and differing passwords only influences the behaviour of internet users when self-efficacy is given. Self-efficacy itself is expected to have an influence on intention and behaviour, regardless of whether knowledge is present.

The current study

As seen in previous research, the knowledge that people have about the topic, and the self-efficacy they perceive regarding the topic at hand are important influences on intentions and behaviour. Both of those variables were often studied separately regarding multiple topics, as well as cybersecurity. There is little research, on the other hand, on both variables in connection with cybersecurity. It is important to research this further, as this way, one can find more ways to encourage cybersecurity behaviour, like through strengthening knowledge and self-efficacy on the use of strong passwords. Moreover, users should be encouraged to secure their data online, as there are many potential problems when certain accounts are easily accessible to scammers or hackers. This is the reason why the first part of the study in this thesis will investigate if prior knowledge and self-efficacy have a combined effect on cybersecurity intentions to use strong and differing passwords. Additionally, in a follow-up study with the same participants, it will be examined whether self-efficacy, prior knowledge and behavioural intention predict actual security behaviour, in this case, the use of secure passwords.

Hypotheses

H_1: Individuals with a high self-efficacy for using strong passwords show a higher intention and execution of using strong and different passwords compared to those with low self-efficacy.

H_2: Individuals with a high self-efficacy for using strong passwords who score higher on knowledge show a higher intention and execution of using strong and different passwords compared to those who scored lower on knowledge.

H_3: Individuals who have a higher intention to use strong and different passwords are more likely to act on this intention and execute the behaviour.

Methods

Design

In the current study, a between-subject design was employed. There was one independent variable, called *self-efficacy*, with three conditions, high and low self-efficacy, as well as a control condition. Further, the variable *knowledge* was expected to have an

interaction effect with *self-efficacy*. The two dependent variables were *behavioural intention* and *security behaviour*. For the second part of this study, *self-efficacy*, *knowledge* and *behavioural intention* were independent variables, while *security behaviour* was the dependent variable.

Participants

In total 225 participants took part in the first part of the study. Out of those, 121 took part in the second study and could successfully be matched to their answers in the first part (female: 89, male: 30, non-binary or other: 2). The study was distributed using SurveyCircle and the Sona Psychology Test Subject Pool, which is a website allowing students at the University of Twente to publish their studies and to take part in other students´ research to gain study credits. Furthermore, participants were asked to take part in the study through postings on Instagram and WhatsApp. Therefore, a convenience and voluntary response sample was used. In the control condition, there were 37 valid participants, while the high and low self-efficacy conditions had 44 and 40 valid participants, respectively (valid: 65.3% German, 16.5% Dutch, 18.2% other nationalities). Participant´s age ranged from 18 to 72, with 52.1% being between 19 and 21 years old (M_{age} = 24; SD_{age} = 9.05). Most participants had the A-levels as their highest completed level of education (54.5%), followed by a Bachelor´s degree (23.1%), secondary school (10.7%), a Master´s degree (8.3%) and vocational training (3.3%).

Materials

Online questionnaires

Knowledge measurement. To measure the previous knowledge that participants have on the topic of strong passwords, a scale was designed that asked what participants know so far about constructing and remembering strong passwords, as well as using different passwords and storing them correctly (see Appendix A). Overall, the questionnaire consisted of eight items measured on a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree) and had a Cronbach´s alpha of .82, which means the scale has acceptable internal reliability. An example item is “The use of upper- and lowercase letters makes a password strong”. This scale was given before and after the task described below, in order to assure that the task did not increase participants´ knowledge. It was given again in the follow-up questionnaire to be controlled for.

Self-efficacy scale. In order to measure how self-efficacious participants feel in either of the conditions, multiple items of the new general self-efficacy scale by Chen et al. (2001) were adapted to fit the current research topic, therefore changing Chen et al.´s (2001) general statements about tasks and performances into statements about using strong passwords. Furthermore, additional scale items were adapted from Amo et al. (2015), whose scale is already oriented towards cybersecurity. The scale in the current study then included eight items which are measured on a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree) and had a Cronbach´s alpha of .87 (see Appendix A). An example of this would be the item "I am able to successfully keep my passwords private". This scale was presented once in each part of the study.

Response efficacy scale. A short three-item questionnaire about response efficacy, which is the person´s belief in whether the recommended action will protect them from the threat, was adapted from Vance et al. (2012). The Cronbach´s alpha was computed at .79. As this scale included less than 10 items, the average inter-item correlation was chosen as a further means of assessing internal consistency. In the current study, the average inter-item correlation reached .4, which is within the ideal range between .15 and .5 (*Average Inter-Item Correlation*, 2018). The questionnaire included items like "If I comply with password security policies, it is unlikely that I will have security problems". This scale was given once in the first part of the study and once in the follow-up study.

Risk-taking DOSPERT scale. In the current study, risk-taking in the domains of financial, ethical, health and safety-related, recreational and social topics was examined as an explorative measure (Blais & Weber, 2006). This was done because Van Bavel et al. (2019) determined that in their experimental groups, those participants that were more risk-seeking tended to finish the study completely, while those that were more averse to risk would more likely drop out of the study. Risk-taking is measured on a 7-point Likert scale from 1 (extremely unlikely) to 7 (extremely likely). In the current study, this scale had a Cronbach´s alpha of .85. To illustrate, one of the items in this scale was "Betting a day's income at a high-stake poker game". This scale was administered once in the first part of the study.

Behavioural intention and actual behaviour scale. In order to measure if participants intend to behave safer regarding their passwords, a security intention scale was adapted from Tsai et al. (2016). In the current study, the scale contains 5 items, instead of the original 8,

regarding the different measures that are explained at the beginning of the study, like changing passwords regularly or constructing strong passwords. Three items were taken out of the scale by Tsai et al. (2016) because they were not about passwords but rather about internet browser settings. The average inter-item correlation of the behavioural intention scale in the current study was .32, which is within the acceptable range. An example item is "I will use passwords that are harder to guess". This scale was given once in the first part of the study and then modified into a self-reported behavioural measure to be administered in the follow-up study. Here, an example item is "I used passwords that are harder to guess".

Task and manipulation

After the knowledge questionnaire, participants were introduced to the task of creating a password for three different types of accounts, namely passwords for an online banking account, a social media account and their health insurance. These choices of accounts were made because participants are likely to have those accounts already. Furthermore, online banking and health insurance passwords are very important to protect. Therefore, it was stated that participants should type out three passwords that they consider strong, and that they should try to remember them for the second part of the study. This was important to tell participants to show them that they will need these passwords again, and to remind them to handle the passwords like they would actual passwords for those accounts. For the control group, it was only stated what the task entailed. For the manipulations of self-efficacy, in either the heightened or lowered self-efficacy condition, the task was introduced by a short newspaper article showing how severe the risk of a data breach is and how vulnerable participants are to it. In this article, the general use of strong and differing passwords was framed either as very easy and not time-consuming at all (low response cost and high self-efficacy) or as difficult and associated with effort (high response cost and low self-efficacy; see Appendix B). For example, in the low self-efficacy condition, the article entailed sentences like "Unfortunately, coming up with multiple one-of-a-kind passwords is an annoying and exhausting process", whereas the high self-efficacy condition was introduced by sentences like "Luckily, coming up with multiple one-of-a-kind passwords is a quick and easy process". After the article, the same task description as for the control group was given.

Procedure

After signing up for the study on Sona Systems or SurveyCircle, participants could take part in the first part of the study. They started the questionnaire, which was constructed using Qualtrics, by choosing either the German or the English version, and then reading an information sheet about the study. After giving their consent to participate, they read the short introduction to the topic of strong passwords and subsequently had to answer demographic questions regarding age, gender, nationality and educational background. Furthermore, they were asked to estimate how many passwords they have to fill in daily. In order to be able to connect the first and the second part of the survey for each participant, they had to construct a code made up of the first two letters of their mother´s name, the last two letters of their father´s name and their house number. Next, participants were presented with the knowledge questionnaire, followed by the task of constructing three strong passwords and remembering them for the follow-up questionnaire. Here, they randomly received either the high self-efficacy, low self-efficacy or control frame of the task. Afterwards, the self-efficacy and response efficacy scales were presented. Lastly, the behavioural intention of participants was measured. Participants were then asked for their email addresses to be notified of the follow-up survey. After approximately 4 weeks, participants were sent an email containing the link to the second survey and a small reminder of what they had done during the first study. In the second survey, as explained above, participants were asked if they had done what they intended to do and they were prompted to write down the passwords they made during the task again. Lastly, participants were shown a debriefing in which the different conditions were explained. Furthermore, they could find information on how to correctly construct and handle their passwords as well, in order to prevent possible misbeliefs that could arise due to the experimental manipulations (see Appendix C).

Data Analysis

The responses to the questionnaire were exported from Qualtrics to IBM SPSS Statistics 26 for analysis. For some exploratory analyses, RStudio (version 2021.09.1+372) was used. Packages needed for these analyses are haven (Wickham, Miller, et al., 2022), dplyr (Wickham, François, et al., 2022) and RecordLinkage (Sariyar & Borg, 2022). To find out whether self-efficacy has a direct influence on the behavioural intention and the self-reported execution of cybersecurity behaviour, a One-Way ANOVA was computed with each

dependent variable respectively. In order to test hypothesis 2 that self-efficacy and knowledge interact to impact intention and behaviour, a Two-Way MANOVA with an interaction effect was run to determine whether knowledge interacts with the influence of the self-efficacy manipulations on behavioural intention and execution. Further, to assess hypothesis 3, a linear regression was run with behavioural intention as an independent variable and execution of cybersecurity behaviour as the dependent variable.

Results

Preliminary analyses

To investigate the impact of the manipulations, a One-Way ANOVA was computed for the dependent variable of self-efficacy. There was no statistically significant difference found between the means of self-efficacy per condition ($F(2,118) = 1.454$, $p = .238$). This means that the experimental manipulations did not have the desired impact on participants´ self-efficacy.

As a preparation for the following analyses, it was examined whether the self-efficacy intervention had impacted the knowledge or response efficacy participants held about using strong passwords, as it is possible that in the manipulation, some information was mentioned that could increase participants' knowledge or response efficacy. According to the Repeated Measures ANOVA with a Greenhouse-Geisser correction, the knowledge variable did not show a statistically significant difference in means between before and after the manipulation by the newspaper articles, as well as the follow-up study, even when taking into account the experimental condition ($F(3.607, 212.837) = 1.861$, $p = .125$). Furthermore, after repeating this analysis for response efficacy, it was found that response efficacy was also not influenced by the self-efficacy interventions ($F(1,120) = 3.394$, $p = .068$).

Descriptive statistics

First, the mean scores of the dependent and independent variables were calculated (see table 1). A visualization of the means for each condition can be found in Appendix D. A Shapiro-Wilk test showed a significant departure from normality for the security behaviour variable, $W(121) = .98$, $p = .032$. The variable is positively skewed with a value of 0.22.

Table 1

Means and Standard Deviations for the Main Variables

Variable	*M*	*SD*
Previous knowledge	4.06	0.45
Self-efficacy	3.76	0.64
Behavioural intention	3.56	0.71
Security behaviour	2.70	1.00

Furthermore, the Pearson correlations between the independent and dependent variables were calculated. It was found that all variables positively correlate. All correlations and respective p-values can be found in table 2.

Table 2

Correlation Table of the Independent and Dependent Variables

		Knowledge	Self-efficacy	Security behaviour	Behavioural intention
Knowledge	*r*	1			
	p				
Self-efficacy	*r*	.452**	1		
	p	.000			
Security behaviour	*r*	.240**	.372**	1	
	p	.008	.000		
Behavioural intention	*r*	.365**	.420**	.569**	1
	p	.000	.000	.000	

**. Correlation is significant at the .01 level (2-tailed)

Hypothesis testing

Influence of Low Versus High Self-efficacy on the Intention to and Actual Use of Strong Passwords

Firstly, the first hypothesis about the influence of the level of self-efficacy on the behavioural intention and actual behaviour of using strong passwords was tested. To do this, a one-way ANOVA was run with the experimental condition as an independent variable and the intention to and actual use of strong passwords as separate dependent variables. Three cases needed to be excluded as they were significant outliers. There was no statistically significant difference between the conditions for behavioural intentions ($F(2,115) = 1.192$, p

= .307) and actual behaviour (F(2,115) = 1,13, p = .327). This means that the level of self-efficacy did not significantly influence behavioural intention and actual behaviour.

Influence of Knowledge and Self-efficacy Combined on the Intention to and Actual Use of Strong Passwords

For hypothesis 2, a two-way MANOVA was conducted to examine the effect of the experimental condition, the previous knowledge and a possible interaction effect of both on the behavioural intention and self-reported behaviour. Therefore, knowledge and the experimental condition were the independent variables, while intention and behaviour were used as dependent variables. There were no significant effects on behavioural intention found for the experimental condition or the interaction effect (F(2,78) = 0.032, p = .968; F(22,78) = 1.127, p = .339), while there was an effect of previous knowledge on behavioural intention (F(18,78) = 2.292, p = .006). For the dependent variable of actual behaviour, the experimental condition or the interaction effect did not have a significant effect (F(2,78) = 0.647, p = .526; F(22,78) = 1.02, p = .339), whereas previous knowledge had a significant influence on the actual behaviour (F(18,78) = 2.22, p = .008). These results mean that previous knowledge has a significant influence on both the intention to and actual use of strong passwords.

Prediction of Actual Use of Strong Passwords by Behavioural Intention

Lastly, to find out whether a higher intention to use strong passwords was followed by higher use of strong passwords a linear regression was executed. The model showed that the intention to use stronger passwords has a significant influence on the actual use of strong passwords (F(1, 119) = 57.014, p < .001, R^2 = .324, $R^2_{adjusted}$ = .318). The regression coefficient (B = 0.81) indicated that with an increase of 1 point in behavioural intention, actual behaviour would increase by 0.81 points. Thus, when intention goes up, actual behaviour increases as well.

Exploratory Analyses

Similarity Between the Passwords in First and Second Study

A comparative analysis was computed in RStudio to examine the amount of overlap between the passwords that participants gave in the first task and those passwords they entered in the follow-up study. This was done to see whether participants had remembered their constructed passwords correctly, or if they were incorrect, to see how similar they were

to those passwords made in the first part of the study. In table 3, the overlap between the first and second time the passwords were entered is given per website and condition ($M_{overlap}$ = .576). In a One-Way ANOVA, it was established that there were no statistically significant differences in means between the conditions. This was true for the overlap scores for the banking passwords ($F(2,100) = 1.003$, $p = .370$), the social media account ($F(2,91) = 0.787$, $p = .458$), and the health insurance passwords ($F(2,94) = 2.578$, $p = .081$). This means that participants´ experimental condition did not have an influence on their ability to recall the passwords correctly.

Table 3

Overlap Between Passwords from the First Study and Follow-up Study

Website	Experimental condition	Overlap
Online Banking	Control condition	.489
	High self-efficacy condition	.568
	Low self-efficacy condition	.622
Social Media Account	Control condition	.523
	High self-efficacy condition	.591
	Low self-efficacy condition	.656
Health Insurance	Control condition	.468
	High self-efficacy condition	.603
	Low self-efficacy condition	.668

Strategies for Remembering Passwords

In addition to the dependent and independent variables, participants were also asked about their strategy concerning how they remembered the passwords for the study as an exploratory measure. In a qualitative analysis, participants´ statements were coded according to the categories seen in table 4. In the frequency table below (Table 4), one can see that most

participants either wrote the passwords down or took a picture of them, as well as trying to keep them in their heads.

Table 4

Frequency Table for Participants´ Strategies to Remember Passwords

Strategy	Frequency	Percent
Kept in the head	36	29.8
Written down or took a picture	35	28.9
Forgotten	15	12.4
Password manager	10	8.3
Association with the website	7	5.8
No strategy	6	5.0
Association with names/dates	4	3.3
Using their standard password or a slight variation of it	3	2.5
Uncategorised	5	4.1
Total	121	100.0

Influence of Risk-Taking on Drop-out Rate

The risk-taking level of participants was determined as an exploratory measure for the drop-out rates between the first and second studies. When comparing the means between the participants who took part in the first part only and those who also did the second part, the t-test showed no difference in the mean score for risk-taking ($t(191) = -0.040$, $p = .968$). This means that there was no significant effect of risk-taking on whether participants dropped out of the study or finished both parts.

Discussion

Over the past years, an ever-growing number of cybersecurity threats arose against which users need to protect themselves. In order to keep their data safe, users need to have strong passwords for their online accounts, as this minimizes the risk of being jeopardised. Inspired by findings from health behaviour research, I investigated the influence of self-efficacy and knowledge on the intention to and actual use of strong passwords, to broaden the understanding of how much people know and how capable they feel to use strong and differing passwords for their online accounts. As health behaviour is a type of protective behaviour as well, it was expected that findings in that area could also be applied to protective cybersecurity behaviour, in this case, the use of strong passwords. This research approach was realised using online questionnaires with a task for participants to construct their own passwords. As for the overall findings, there were no statistically significant effects of self-efficacy on either intention or behaviour, while knowledge had an impact on both intention and behaviour. Furthermore, the interaction between knowledge and self-efficacy did not have a significant effect on the intention to and actual use of strong passwords. This means that the interaction of knowledge and self-efficacy, which was found in the health behaviour domain, did not apply to cybersecurity intentions and behaviour in the current study.

Influence of Self-efficacy on Intention and Behaviour

In previous research, Mwagwabi et al. (2018) found that a higher level of self-efficacy is connected to a higher level of intention, which is why the first hypothesis was that individuals who score higher in cybersecurity self-efficacy show more intention to and actual use of strong passwords than those lower in self-efficacy. Further, Faries (2016) and Hameed and Arachchilage (2021) established that a higher level of self-efficacy means a person is more likely to execute the desired behaviour, in the current study the use of strong passwords. Surprisingly, these expectations were not met, as self-efficacy alone did not influence either the intention to or the actual use of strong passwords. An additional finding from the exploratory analyses was that participants´ level of self-efficacy did not significantly influence their ability to reproduce their self-made passwords correctly in the second study. This means that no matter their belief in their own cybersecurity abilities, participants were only accurately repeating their passwords a little more than half of the time. A possible

reason for this could be that the coping message in the high self-efficacy condition, telling participants that they could definitely behave safely, was expected to be effective in heightening the self-efficacy of participants (van Bavel et al., 2019). I did not find this effect of the experimental manipulations in the current study, making a similar mean self-efficacy over conditions the reason for the statistically non-significant effects of self-efficacy on intention.

Furthermore, if self-efficacy did not differ significantly between conditions, this can explain why there was no difference in behaviour. As established by Rimal (2000), self-efficacy is crucial in a person´s decision whether to work against the threat, in this case, to use strong passwords, or to work against the feelings that cybercrime triggered in the person. Hence, if self-efficacy was not affected by the manipulation, this decision about the course of action could not have significantly different outcomes between the conditions. Overall, it is not unusual that a manipulation targeting self-efficacy does not trigger this trait in participants. As an example, in a study by Weinhardt (2013), a direct effect on self-efficacy could not be established through intervention or training. In the current study, it is possible that the chosen newspaper articles did not elicit a change in self-efficacy, but rather some other trait, like motivation. There are multiple ways to improve self-efficacy which have been found useful in different areas, like health behaviour or learning (Margolis & Mccabe, 2006; Rajati et al., 2014). These strategies include successful performance, vicarious experience and verbal persuasion. However, those approaches are difficult to apply to strong password use for the general population, while it would be possible to use for instance verbal persuasion in a study setting. Participants could be verbally encouraged and told that others can succeed in constructing strong passwords, which should heighten participants´ self-efficacy.

Influence of Interaction between Knowledge and Self-efficacy on Intention and Behaviour

Previous research by Kennison and Chan-Tin (2020) found that those people who know more about making and using safe passwords also show a higher intention to use those passwords. This is consistent with the current findings, where previous knowledge has a significant effect on the intention to use strong passwords. Therefore, through increasing knowledge, it is possible to heighten the intention of the addressed people to use strong and

differing passwords. Additionally, according to Rimal (2000), knowledge has little to no influence on behaviour when the person is not self-efficacious. However, in the current study, I found that previous knowledge on its own does affect the use of strong passwords. It is possible that this effect occurred because the setup of the study reminded participants that they know their passwords should be strong, therefore, leading them to implement this knowledge after being reminded.

Further, when investigating the influence of knowledge and self-efficacy combined on behaviour, the literature suggests an interaction effect rather than moderation or mediation. Contrarily, neither self-efficacy nor an interaction between self-efficacy and knowledge had an impact on the use or intention to use strong passwords in the current study. This was unexpected as according to van Acker et al (2014), those who have more experience and a higher level of self-efficacy would be more likely to intend to and actually use secure passwords. Hence, the direct effect of knowledge alone on intention and behaviour is unexpected in light of the finding that self-efficacy did not have a significant influence alone or in combination with knowledge. It is possible that knowledge about strong passwords has more impact than self-efficacy when trying to predict whether people intend to and actually use strong passwords in their day-to-day life. If this is the case, cybersecurity interventions should focus rather on offering knowledge and making sure the information is understood than on increasing self-efficacy.

Another possible explanation of this finding is that there is no interaction effect because self-efficacy is a mediator variable for the relationship between knowledge and intention, as well as knowledge and behaviour. This would mean that self-efficacy influences the relationship between knowledge and intention or behaviour respectively, rather than interacting with knowledge to influence intention or behaviour. Additionally, there might be some overlap between the definitions of knowledge and self-efficacy regarding the use of strong passwords. In order to be self-efficacious, an individual needs to hold at least basic previous knowledge about strong passwords, as otherwise if they did not know anything about it, they could likely not feel capable to construct safe passwords. As knowledge and self-efficacy are confounding each other, the findings should have shown that the self-efficacy manipulation increased participants´ knowledge, which was not the case in the current study. Therefore, one can speculate that if knowledge would increase through an

intervention, it is possible that both behavioural intention and actual behaviour would increase as well. To increase or keep knowledge about strong passwords on a high level, frequent and regular reminders can be of use. Furthermore, those reminders can also be useful in bridging the intention-behaviour gap, that might occur in some internet users (Mack et al., 2019). To illustrate, interventions to teach about cybersecurity and strong passwords could be held in different organizations as well as schools or universities. This way, it is most likely that internet users come into contact with the topic and get reminded of the negative consequences that unsafe internet behaviour can have.

Prediction of Actual Use of Strong Passwords by Behavioural Intention

The third hypothesis was that those who show a higher intention to use strong passwords will also follow through with this behaviour. This hypothesis could partly be verified because of the finding that in the current study, an increase in behavioural intention came along with an increase in the actual use of strong passwords. Even though there was a strong correlation in the current study between intention and behaviour, it was not a perfect correlation. This means that not in all cases did the intention to use strong passwords lead to the actual use of strong passwords. Oftentimes, in previous research, an intention-behaviour gap was discovered. For instance, through a meta-analysis, Sheeran and Webb (2016) revealed that while the behavioural intention to behave more securely is present, the actual behaviour does not always follow. Although for most participants that intended to behave securely this intention was realised into behaviour, there is still a small intention-behaviour gap in the current study.

As there were no differences between conditions pertaining to the actual use of strong passwords, it is possible that in this study, participants were motivated to behave securely. As stated above, for example, the task description for constructing passwords or the newspaper article participants had to read could have been interpreted as a challenge that they can win, therefore, motivating their intention to use strong or stronger passwords in their day-to-day life (National Cybercrime Initiative, 2017). Additionally, making people think of future consequences of their behaviour can increase the actual use of strong passwords (Moustafa et al., 2021). Possibly, participants were prompted to think of the future when they read the newspaper article which read “In the midst of data breaches and passwords getting leaked, it is now more important than ever to have a unique, strong password for every online account

you own", hinting at the considerable problems that follow the use of weak passwords. Furthermore, it is important to keep in mind that the intention to and actual use of strong passwords also includes remembering the passwords one created in order to be safe. In the current study, it appeared as if many participants did not remember at all, or if they remembered, the passwords from the first and second part did not always overlap. Possibly, this happened because the passwords were hypothetical and participants might make a bigger effort to correctly remember their real passwords, especially for online banking and health insurance.

Strengths, Limitations and Future Recommendations

One of the strong points of this research is that a total of 121 people completed both parts of the study. Furthermore, when compared to other studies in the field of cybersecurity, it is valuable that I measured behaviour as well, instead of only measuring intention. Another strong point is that participants might have learned a lot about their own password use, seeing as they oftentimes couldn't remember the passwords to fill in in the second study. This study has possibly amplified their awareness of their own weaknesses concerning the use of strong passwords, and therefore, possibly encouraged participants to work on these shortcomings.

A limitation of this study is that the self-efficacy manipulations did not change participants´ levels of self-efficacy. It is possible that the manipulations did not trigger self-efficacy, but instead another variable. As mentioned in the results, knowledge was tested for an influence of the experimental conditions, but it did not change. Further, response efficacy also did not change after the task. Therefore, it is unknown which variable could have been triggered by the manipulation. Additionally, the study was held online for both of its parts. In contrast, newspaper articles, like the format in the manipulated conditions are oftentimes read on paper instead of online. Therefore, it is also possible that the manipulation of self-efficacy was not successful because of this. Future studies should be directed at finding sustainable ways to increase self-efficacy to be able to test whether self-efficacy has a significant effect on the use of strong passwords. Overall, it is necessary for future research to investigate more the relationship between knowledge and self-efficacy in the cybersecurity domain.

Secondly, another limitation is that only self-efficacy and response-efficacy were measured as components of the PMT, while response cost was left out. Theoretically, response cost would be high for making strong passwords, as it takes time and effort when

done by hand. In future research, it is important to measure this concept as well to be able to report definitively if PMT is also applicable to the intention to and actual use of strong passwords.

Conclusion

This research aimed to investigate whether prior knowledge and self-efficacy have a combined or individual effect on the intention to and actual use of strong passwords. I demonstrated that there is no interaction between previous knowledge and self-efficacy when considering their influence on intention and behaviour. Furthermore, knowledge has a direct impact on both intention to and actual use of strong passwords, while self-efficacy does not influence either intention or behaviour. I also established that the intention to use strong passwords increases the actual behavioural response. Although self-efficacy and knowledge combined are crucial for changing health behaviour, this effect could not be replicated in changing safe password behaviour. This begs the question if knowledge and self-efficacy are equally important when looking at cybersecurity behaviour. Overall, more research is needed into previous knowledge and self-efficacy in the cybersecurity domain, especially into how they can be used to increase the usage of strong passwords. It is recommended that future research looks further into the relationship between knowledge and self-efficacy and how together, they can influence behavioural intention and actual behaviour.

References

Amo, L. C., Zhuo, M., Wilde, S., Murray, D., Cleary, C., Amo, C., Upadhyaya, S., & Rao, H. S. (2015). *Cybersecurity Engagement and Self-Efficacy Scale*. https://sites.google.com/site/amoceses/home

Atak, N., Gurkan, T., & Kose, K. (2008). The Effect of Education on Knowledge, Self Management Behaviours and Self Efficacy of Patients with Type 2 Diabetes. *The Australian Journal of Advanced Nursing*, *26*(2), 66–74. https://doi.org/10.3316/ielapa.198857737071665

Average Inter-Item Correlation: Definition, Example. (2018). Statistics How To. https://www.statisticshowto.com/average-inter-item-correlation/

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv:1901.02672 [Cs]*. http://arxiv.org/abs/1901.02672

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.

Blais, A.-R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1*(1), 15.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235. https://doi.org/10.1109/THS.2011.6107876

Briggs, P., Jeske, D., & Coventry, L. (2017a). The Design of Messages to Improve Cybersecurity Incident Reporting. In T. Tryfonas (Ed.), *Human Aspects of*

Information Security, Privacy and Trust (pp. 3–13). Springer International Publishing. https://doi.org/10.1007/978-3-319-58460-7_1

Briggs, P., Jeske, D., & Coventry, L. (2017b). Chapter 6—Behavior Change Interventions for Cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behavior Change Research and Theory* (pp. 115–136). Academic Press. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Caputo, D. D., Pfleeger, S., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*. https://doi.org/10.1109/MSP.2013.106

Chen, G., Gully, S. M., & Eden, D. (2001). Validation of a New General Self-Efficacy Scale. *Organizational Research Methods*, *4*(1), 62–83. https://doi.org/10.1177/109442810141004

Digital Around the World. (2021). DataReportal – Global Digital Insights. https://datareportal.com/global-digital-overview

European Commission. (n.d.). *Cybercrime*. Retrieved 15 May 2022, from https://ec.europa.eu/home-affairs/cybercrime_en

Faries, M. D. (2016). Why We Don't "Just Do It". *American Journal of Lifestyle Medicine*, *10*(5), 322–329. https://doi.org/10.1177/1559827616638017

Hameed, M. A., & Arachchilage, N. A. G. (2021). The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Personal and Ubiquitous Computing*, *25*(5), 911–925. https://doi.org/10.1007/s00779-021-01560-1

Ipsos MORI. (2019). *UK Cyber Security Survey 2019*. Ipsos MORI. https://www.ipsos.com/ipsos-mori/en-uk/uk-cyber-security-survey-2019

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, *11*, 3030. https://doi.org/10.3389/fpsyg.2020.546546

Mack, B., Tampe-Mai, K., Kouros, J., Roth, F., Taube, O., & Diesch. (2019). Bridging the electricity saving intention-behavior gap: A German field experiment with a smart meter website. *Energy Research & Social Science*, *53*, 34–46. https://doi.org/10.1016/j.erss.2019.01.024

Margolis, H., & Mccabe, P. (2006). Improving self-efficacy and motivation: What to do, what to say. *Intervention in School and Clinic*, 218–227.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*, 1969. https://doi.org/10.3389/fpsyg.2021.561011

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems*, *42*(1). https://doi.org/10.17705/1CAIS.04207

National Cyber Security Centre. (2021). *Most hacked passwords revealed as UK cyber survey exposes gaps in online security*. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

National Cybercrime Initiative. (2017). *The human factor in cybercrime and cybersecurity: Research agenda* (R. Leukfeldt, Ed.). Eleven International Publishing.

Ontech Systems. (2018). *The Risk of Browser Saved Passwords: It's No Joke*. Ontech Systems. https://ontech.com/browser-saved-passwords/

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*, 18–28. https://doi.org/10.1108/09685221211219173

Rajati, F., Sadeghi, M., Feizi, A., Sharifirad, G., Hasandokht, T., & Mostafavi, F. (2014). Self-efficacy strategies to improve exercise in patients with heart failure: A systematic review. *ARYA Atherosclerosis*, *10*(6), 319–333.

Rimal, R. N. (2000). Closing the Knowledge-Behavior Gap in Health Promotion: The Mediating Role of Self-Efficacy. *Health Communication*, *12*(3), 219–237. https://doi.org/10.1207/S15327027HC1203_01

Rippetoe, P. A., & Rogers, R. W. (1987). *Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat.* https://doi.apa.org/doiLanding?doi=10.1037%2F0022-3514.52.3.596

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation* (J. Cacioppo & R. Petty, Eds.; pp. 153–177).

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). Plenum Press.

Sariyar, M., & Borg, A. (2022). *RecordLinkage: Record Linkage Functions for Linking and Deduplicating Data Sets* (0.4-12.3) [Computer software]. https://CRAN.R-project.org/package=RecordLinkage

Sheeran, P., & Webb, T. L. (2016). The Intention–Behavior Gap. *Social and Personality Psychology Compass*, *10*(9), 503–518.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness* (pp. x, 293). Yale University Press.

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

van Acker, F., Vermeulen, M., Kreijns, K., Lutgerink, J., & van Buuren, H. (2014). The role of knowledge sharing self-efficacy in sharing Open Educational Resources. *Computers in Human Behavior*, *39*, 136–144. https://doi.org/10.1016/j.chb.2014.07.006

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

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Wang, C.-W., & Chen, D.-R. (2022). Associations of sugar-sweetened beverage knowledge, self-efficacy, and perceived benefits and barriers with sugar-sweetened beverage consumption in adolescents: A structural equation modeling approach. *Appetite*, *168*, 105663. https://doi.org/10.1016/j.appet.2021.105663

Weinhardt, J. M. (2013). *Assessing the Influence of a Self-Efficacy Intervention on Students' Motivation and Performance*. 77.

Wickham, H., François, R., Henry, L., & Müller, K. (2022). *dplyr: A Grammar of Data Manipulation* (1.0.9) [Computer software]. https://CRAN.R-project.org/package=dplyr

Wickham, H., Miller, E., & Smith, D. (2022). *haven: Import and Export 'SPSS', 'Stata' and 'SAS' Files* (2.5.0) [Computer software]. https://CRAN.R-project.org/package=haven

Zimmermann, V., & Renaud, K. (2021). The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Transactions on Computer-Human Interaction*, *28*(1), 7:1-7:45. https://doi.org/10.1145/3429888

Appendix A

Knowledge questionnaire

For the following questions, please indicate to which degree you agree to the statements regarding how you deal with passwords.

1. I know how to make a strong password.
2. The use of upper- and lowercase letters makes a password strong.
3. I use or have used a password manager before.
4. I can distinguish a strong password from a weak password.
5. It does not matter where I store my passwords.
6. I think it is important to have different passwords for each account that I own.
7. Using only lowercase letters is enough to construct a strong password.
8. It does not matter how often I change my password.
9. Using numbers is not necessary for a strong password.

Self-efficacy questionnaire

For the following questions, please indicate the degree to which you currently agree to the statements.

1. I am confident in my ability to construct strong passwords.
2. I am certain that I can store my passwords safely.
3. I can use different passwords for each account I have.
4. For all my accounts, I can succeed in finding the option to change my password.
5. I am able to successfully keep my passwords private.
6. I am able to change my passwords regularly.
7. I can think of a solution if I have forgotten my password.
8. Compared to other people, I am quite good at using passwords safely.

Response efficacy questionnaire

For the following questions, please indicate the degree to which you currently agree to the statements.

1. Complying with password security policies reduces the security threat to my own data.

2. If I comply with password security policies, it is unlikely that I will have security problems.
3. Compliance with password security policies would help me reduce security problems with my own data.

Risk-taking questionnaire (DOSPERT Scale)

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. (S)
2. Going camping in the wilderness. (R)
3. Betting a day's income at the horse races. (F/G)
4. Investing 10% of your annual income in a moderate growth diversified fund. (F/I)
5. Drinking heavily at a social function. (H/S)
6. Taking some questionable deductions on your income tax return. (E)
7. Disagreeing with an authority figure on a major issue. (S)
8. Betting a day's income at a high-stake poker game. (F/G)
9. Having an affair with a married man/woman. (E)
10. Passing off somebody else's work as your own. (E)
11. Going down a ski run that is beyond your ability. (R)
12. Investing 5% of your annual income in a very speculative stock. (F/I)
13. Going whitewater rafting at high water in the spring. (R)
14. Betting a day's income on the outcome of a sporting event. (F/G)
15. Engaging in unprotected sex. (H/S)
16. Revealing a friend's secret to someone else. (E)
17. Driving a car without wearing a seat belt. (H/S)
18. Investing 10% of your annual income in a new business venture. (F/I)
19. Taking a skydiving class. (R)
20. Riding a motorcycle without a helmet. (H/S)
21. Choosing a career that you truly enjoy over a more secure one. (S)
22. Speaking your mind about an unpopular issue in a meeting at work. (S)
23. Sunbathing without sunscreen. (H/S)

24. Bungee jumping off a tall bridge. (R)
25. Piloting a small plane. (R)
26. Walking home alone at night in an unsafe area of town. (H/S)
27. Moving to a city far away from your extended family. (S)
28. Starting a new career in your mid-thirties. (S)
29. Leaving your young children alone at home while running an errand. (E)
30. Not returning a wallet you found that contains $200. (E)

Note. E = Ethical, F = Financial, H/S = Health/Safety, R = Recreational, and S = Social.

Intention questionnaire

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect yourself and your data online.

1. I will take security measures to protect my data
2. I will change my passwords so they do not repeat on different accounts to protect myself better online
3. I will change my passwords more often
4. I will use passwords that are harder to guess
5. I will use a password manager to safely store my passwords

Behaviour questionnaire

Thinking back to your past actions, indicate the degree to which you agree or disagree with the following statements regarding if you implemented security measures to protect yourself and your data online.

This applies to the time **since you took part in the last study**!

1. I took security measures to protect my data
2. I changed my passwords so they do not repeat on different accounts to protect myself better online
3. I changed my passwords more often
4. I used passwords that are harder to guess

5. I used a password manager to safely store my passwords

Appendix B

Newspaper Article for the High Self-efficacy Condition

The Daily

Issue 020 April 2021

Password Security

In the midst of data breaches and passwords getting leaked, it is now more important than ever to have a unique, strong password for every online account you own. Luckily, coming up with multiple one-of-a-kind passwords is a quick and easy process. It does not take a lot of time to check for each password if the guidelines for strong, secure passwords are met as this is mostly stated on the websites when creating passwords. And because the human is still the weakest link in the chain when looking at online security, it is empowering to know that you are able to hinder hackers by constructing a robust and secure password. As it is not hard to know how to construct a secure password, you can be sure that you are always well equipped to get new online accounts that keep strangers away from your data.

Newspaper Article for the Low Self-efficacy Condition

The Daily

Issue 020 April 2021

Password Security

In the midst of data breaches and passwords getting leaked, it is now more important than ever to have a unique, strong password for every online account you own. Unfortunately, coming up with multiple one-of-a-kind passwords is an annoying and exhausting process. It can take a lot of time to check for each password if the guidelines for strong, secure passwords are met. Sadly, there is little to no way around this struggle as the human is still the weakest link in the chain when looking at online security. It is your own fault if someone can guess your passwords if you were not able to make it robust enough. Furthermore, every website sets different requirements for your password to be considered strong and secure. Maybe you know the feeling of asking oneself how to know whether your passwords are actually useful in keeping strangers away from their data.

Appendix C

Debriefing of Study 2

Thank you for taking part in this study. Here, I aimed to investigate the influence of password knowledge and password self-efficacy on the intention to and actual use of strong passwords. Self-efficacy is the extent to which you feel like you are able to do certain things, in this case constructing and using strong passwords.
In this study, your self-efficacy for the use of strong passwords was tested and possibly manipulated.

If you did not have to read a short newspaper article before constructing passwords yourself in the first study, you were in the control condition and therefore, not manipulated.

If the newspaper article before the task in the first survey read "*It is not hard to know how to construct a secure password, you can be sure that you are always well equipped to get new online accounts that keep strangers away from your data*", it was aimed at making you believe that the task is very easy and that you can achieve it without much practise or effort. This was then the high efficacy condition.

If the newspaper article read things like "*It is your own fault if someone can guess your passwords if you were not able to make it robust enough*", it was aimed at making you believe that the task is difficult and hard to accomplish. This was then the low efficacy condition.

Now that you know that your self-efficacy was possibly impacted, you should also know that it is not difficult to construct strong passwords and to use different passwords for different accounts and websites. If you feel like you cannot remember all the passwords you have to make, please consider using a safe password manager. This contributes to your cybersecurity and safety and protects your data and you online.

Always try to incorporate most, if not all, of the following characteristics of a strong password:

- At least 8 characters long
- Mixing uppercase and lowercase letters
- Adding numbers
- Including one or more special characters like **#** or **?**

Please never write down your passwords anywhere and make a new, different password for each of the online accounts you possess! This way, most of your data can stay safe even if one of your passwords gets leaked. For more information, take a look at the following website:
https://its.lafayette.edu/policies-draft/strongpasswords/

I would once again like to thank you for taking part in this study.

Appendix D

Bar Chart of the Mean Distributions per Condition