Behaviour change in cybersecurity: a mouse-tracking study

Master Thesis

Tabea Platje

S1987100

M.Sc. Psychology

Psychology of Conflict, Risk and Safety

University of Twente

29-06-2021

Supervisor: I. van Sintemaartensdijk

Second Supervisor: Dr. S.J. Watson

Abstract

This study investigated whether different appeals in nudges influence online security behaviour. Based on the Extended Parallel Process Model (EPPM), a risk message nudged the participants (N = 143) to perform an online security behaviour (changing passwords). The effect of the risk message condition (threat-appeal condition, coping-appeal condition, combined-appeal condition) on participants' fear, anxiety, behavioural intention, coping, confidence in trustworthiness of websites, whether they wanted to drop out, and denial to improve their cybersecurity was examined including risk-taking as interaction factor. Mouse tracking was used to get insights into participants' online behaviour. Results showed that participants' fear was higher for the threat-appeal condition and coping-appeal condition compared to the combined-appeal condition. The risk message condition did not appear to have an effect on anxiety, behavioural intention to change the behaviour, coping scores, the confidence in trustworthiness of websites, and the question of whether the participant wanted to drop out of the study. The risk message condition including risk-taking as interaction factor did not predict the denial to improve their cybersecurity. Due to technical circumstances, the mouse-tracking data could not be statistically analysed. Heatmaps indicated more mouse movement around the button that made it possible to deny improving the cybersecurity in the coping-appeal condition and the combined-appeal condition than in the threat-appeal condition. Future research should focus on the placement of nudges, development of validated scales, and mouse tracking as well as on the influence of external rules and regulations on cybersecurity behaviour.

Behaviour change in cybersecurity

Criminal activities that involve a computer or the internet are on the rise currently and make online security a big topic. Cybercrimes involve any crime that includes the usage of a computer and a network (Moore, 2010). Not only because we are living in a digital age people are more prone to become a victim of cybercrime but also because the Coronavirus pandemic has forced many people to work from home. This still provides more attack surfaces for cybercrime. As cybercrime has many personal and financial costs, we need to change people's behaviour to be able to protect themselves from becoming victims of cybercrime (Abdalla Mabrouk Khiralla, 2020). The human is the weakest part of the cybersecurity chain (Cisco, 2017), and so, behaviour change of victims is important.

As nudges have been used to change people's behaviour successfully and in the long-term in other domains (Farrington & Welsh, 2002), they can be a useful tool in influencing people to behave safely when being online (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). This research will focus on using nudges while the Protection Motivation Theory (PMT) and the Extended Parallel Process Model (EPPM) will stand in focus and will be used in creating the nudges.

Technology and cybercrime

A big factor that, among other things, facilitates crime is technology as it leads to crime being encountered in many domains of an individual's life (Laycock, 2004). The fast-moving world nowadays and the developing technologies track almost anything we do. People seek more technology because it makes things easier and, in their perception, sometimes also more secure through devices like surveillance cameras. However, through technological developments, it becomes easier and also more likely to become a victim of a crime. A new vulnerability is created for individuals and companies to become a victim of a cyber-attack (Lewis, 2002), as technology often is a tool that makes it effortless or even

possible for offenders to commit a crime (Graham, Kutzli, Kulig, & Cullen, 2019). The increasing risk to become a victim makes it essential to protect individuals from cyber risks. Yet, technology is not only a big factor that makes it possible for offenders to commit a crime, but it also gives victims the possibility to protect themselves (Laycock, 2004). They can protect themselves by using, for instance, technologies like cameras that help against burglary (Maiti & Sivanesan, 2012) or password generators that can help to protect themselves against being hacked by offenders in cybercrime (Tsokkis & Stavrou, 2018).

Behaviour change in cybersecurity

It is important to change people's behaviour to make the individuals able to do something against the crime themselves because the human is weak in terms of cybersecurity behaviour. This means that we need to stop victims from being or becoming victims through behaviour change. Behaviour change in victims is still a novel and scarcely researched topic when it comes to using technologies. In other domains like health psychology, technologies have been effectively used for many years. Health psychology uses for instance fitness trackers to help people dieting, working out, or tracking their food (Niess & Woźniak, 2018). Such behaviour change interventions are not yet developed in the domain of crime but since they have proven to be effective, they should be researched in more detail.

A start has been made by van Bavel et al. (2019) with their paper focussing on the Protection Motivation Theory (PMT) on behaviour change in cybercrime. The PMT by Rogers (1975) focuses on behaviour change in individuals when being confronted with a threat message. When an event happens that is perceived as threatening, two cognitive appraisal processes can occur in an individual. These two cognitive processes are the threat appeal process and the coping appeal process.

The threat appraisal consists of the severity and the vulnerability of the circumstances. The severity of the threat and the vulnerability of the individual influence the likelihood to

engage in maladaptive behaviours. Another factor of the threat appraisal process are the rewards that result from the (negative) behaviour. Thus, the combination of the severity and the vulnerability subtracted by the rewards results in the threat experienced/ threat appraisal. In definition, “a threat appeal means the cognitive and emotional process involved in assessing the potentiality and level of threat” (American Psychological Association, n.d.-f).

The coping appraisal consists of response efficacy and self-efficacy, as well as response costs. The response efficacy, which means the belief that the behaviour will be effective to reduce the threat, and the self-efficacy, which is the belief that the person is able to perform the behaviour that can reduce the threat, influence the likelihood of an adaptive response. The physical or psychological costs associated with the recommended coping behaviour are response costs (Witte, 1992). In relation to cybersecurity, these response costs can have weak or negative influences on secure online behaviour (Mayer, Kunz, & Volkamer, 2017). A coping appraisal is “an evaluation of one’s possibilities to cope with the presented threat” (Witte, 1992). When the severity and the vulnerability are high and the rewards are low while the response efficacy and the self-efficacy are high and the response costs are low, this leads to behaviour intention and the individual is likely to engage in protection motivation.

In the above-mentioned study, van Bavel et al. (2019) used the PMT and nudges to research and manipulate people’s behaviour change. In the nudges that were meant to influence the people’s protection motivation, messages were used that contained threat appeals and/ or coping appeals. This was done as it has been found that warning messages or policy campaigns are not always effective because they assume that users make informed or rational decisions (Acquisti, Brandimarte, & Loewenstein, 2015). So, in the study by van Bavel et al. (2019), the nudges either pronounced the severity and the vulnerability of a cyberthreat (threat-appeal message), the response efficacy and the self-efficacy of the user

(coping-appeal message), both (combined-appeal message), or nothing (no appeal message). They studied which appeal message is better to convince the participants to show a safer online behaviour through, for instance, changing their passwords or logging out.

In their study, van Bavel et al. (2019) found that a coping-appeal message alone and a combined-appeal message worked better to induce a behaviour change than the threat-appeal message alone. Also, they recorded that many participants in the threat-appeal condition decided to quit the study but significantly less in the coping-appeal condition or the combined-appeal condition. They proposed an explanation for the differences in behaviour change due to the different appeals in their nudges and the higher dropout rates in the threat-appeal condition. Since threat appeals often lead to defensive responses, fear-appeals alone can be counterproductive when it comes to behaviour change (Ruiter, Kessels, Peters, & Kok, 2014). As users do not know how to deal with the threat because they have no coping appeal and because the threat makes them feel uncomfortable, they might have engaged in risk denial, refused to attend the threat-appeal messages, or engaged in biased information processing (Ruiter et al., 2014).

As the dropout rates in van Bavel et al. (2019) are significantly higher in the threat-appeal condition, it can be assumed that the participants reacted with the defence mechanism denial, since they ignored to engage in protection motivation behaviour to resolve emotional conflict or reduce anxiety by dropping out of the study. According to the American Psychological Association (n.d.-a), defence mechanisms are also called escape mechanisms and “are seen as normal means of coping with everyday problems and external threats, but excessive use of any one, or the use of immature defences, is also considered pathological”. As indicated above, defence mechanisms, such as denial, are an explanation of the findings in van Bavel et al. (2019). This perfectly maps onto the Extended Parallel Process Model (EPPM), which is an extended version of the PMT. Van Bavel et al. (2019) have not taken

the EPPM into account, which also focuses on the cognitive processes that a risk message causes but also includes a defence mechanism as a consequence of too much fear.

More specifically, the EPPM focuses on a critical point which is the balance between the perceived threat and the perceived coping behaviour. This leads either to no response or to the process of danger control or fear control. If the severity and the vulnerability of the threat are perceived as low, the individual will show no response as it does not perceive any threat. The danger control process occurs when an individual perceives the severity and the vulnerability to be high but also feels that the own self-efficacy is high and is convinced to be able to deal with the threat. This means that the individual accepts the threat message and engages in protection motivation. The fear control process occurs when the individual perceives the severity and vulnerability of the threat as high, but the ability to deal with the threat as low. Consequently, the individual engages in fear control instead of danger control. This means that the individual rejects the threat message and responds with a defence mechanism (Zhang & Borden, 2019).

Defence mechanisms are for instance projection, rationalisation, or the above-mentioned denial. A projection is defined by the American Psychological Association (n.d.-c) as “the process by which one attributes one’s own individual positive or negative characteristics, affects, and impulses to another person or group.”. Rationalisation, according to the American Psychological Association (n.d.-d) is “an ego defense in which apparently logical reasons are given to justify unacceptable behaviour that is motivated by unconscious instinctual impulses.”. Denial is defined by the American Psychological Association (n.d.-b) as “a defense mechanism in which unpleasant thoughts, feelings, or events are ignored or excluded from conscious awareness. [..] Denial is an unconscious process that functions to resolve emotional conflict or reduce anxiety.”

Since the study by van Bavel et al. (2019) detected that the dropout rates in the threat-appeal condition were significantly higher than in the coping-appeal condition and in the combined-appeal condition denial of engaging in protection motivation is assumed to be the reason. As in their study, they could not detect the extent to which dropout might be a dependent measure when focussing on behaviour change theory and the use of nudges to improve online security behaviour, research needs to focus on the dropout as a dependent measure and with this on the critical point of the EPPM. This is important to investigate as the study by van Bavel et al. (2019) indicates that people who do not know how to engage in cyber-secure behaviour deny taking action against victimisation and are more likely to become a victim of cybercrime. This can cause several severe personal and financial costs for the individual.

To complete the picture of the EPPM, coping and behavioural intention need to be included. As mentioned above, when an individual feels able to cope with the threat, this leads to behavioural intention, and they will engage in the recommended behaviour. This is the process of danger control. In their study, van Bavel et al. (2019) found that messages that include a coping appeal were the most successful approach and led the participants to engage in the recommended behaviour. Also, Hanus and Wu (2016), who studied the impact of information security awareness on desktop security behaviour using the PMT, found that the coping appeal impacts recommended security behaviour as people know how to cope with the threat.

Risk-taking as influencing factor

Another factor, that needs to be considered when it comes to behaviour change in cybersecurity is risk-taking, as it was found to influence people's cybersecurity behaviour (van Bavel et al., 2019). According to the American Psychological Association (n.d.-e), risk-

taking means “accepting a challenging task that simultaneously involves potential for failure as well as for accomplishment or personal benefit. […]”.

Risk-taking is an important factor to consider as every individual tolerates a risk to a different extent. Several studies have found that cybersecurity behaviour is related to an individual’s general risk-taking (Kennison & Chan-Tin, 2020; McCormac et al., 2017). People higher in risk-taking more often engage in risky cybersecurity behaviours like using non-secure Wi-Fi or not logging out of accounts. Also van Bavel et al. (2019) included risk aversion as an independent factor in their study about cybersecurity. They found that the individuals who dropped out of the study after being exposed to the nudge tended to be more risk-averse, while the individuals that tended to stay were more risk-taking.

The present study

The central question of this research is whether people quit the study more often when being confronted with a threat-appeal message rather than when being confronted with a coping message or a message that contains a threat appeal and a coping appeal. Next to that, other influencing variables of the EPPM and risk-taking will be examined.

In this study, participants will be asked to engage in cybersecurity behaviour. When being asked to perform this behaviour, they will have the opportunity to press a button that shows “skip this question” to skip performing this behaviour. Relating this to the dropout in the study by van Bavel et al. (2019), this is seen as denial to improve their cybersecurity.

Due to the fact that in the study by van Bavel et al. (2019) the dropout rates in the threat-appeal conditions were higher than the dropouts in the coping-appeal condition and in the combined-appeal condition, it is expected that the fear message leads to higher fear appeal and thus also to a higher denial to improve their cybersecurity. Relating this to the EPPM, this would mean that when being confronted with the threat message this leads to a defence mechanism and so to message rejection. Thus, an individual is reacting with fear

control. When being confronted with a coping-appeal message, the outcome is protection motivation, and the individual accepts the message. This means that the individual is engaging in danger control. According to van Bavel et al. (2019), also a combined-appeal message leads to protection motivation which, related to the EPPM, also means that an individual would accept the message and reacts with danger control.

Thus, it is hypothesised that a threat-appeal message leads to higher fear and anxiety than a coping-appeal message or a combined-appeal message. Also, the coping-appeal message and combined-appeal message are expected to lead to higher feelings of being able to cope with the situation and to engage in the recommended behaviour than a threat-appeal message. Next to that, the denial to improve the cybersecurity is assumed to be higher when being confronted with a threat message than when being confronted with a coping-appeal message, and when being confronted with a combined-appeal message. As risk-taking was found to be higher in people that stayed in the study by van Bavel et al. (2019), it is hypothesised that the interaction effect is stronger for the people who are higher in risk-taking.

Method

Design

The design that was used in this study was a between-subjects design with three risk message conditions. These conditions were a threat-appeal condition, a coping-appeal condition, and a combined-appeal condition. The dependent variables in this research were fear, anxiety, behavioural intention, and coping. A moderator was risk-taking and control variables were knowledge, confidence in the trustworthiness of websites, whether the participants have been a victim of cybercrime before, whether they wanted to quit the study at some point, and the denial to improve their cybersecurity.

Participants

The study comprised a total sample of 176 participants. One hundred twenty participants were recruited through a subject pool where they also gained credits for participation and 56 participants were recruited through personal contacts by asking for participation. The selection criteria for the inclusion in this study were being above the age of 16, having sufficient English skills, which was assessed by the participant's decision, and using a device with a mouse or a trackpad. Thirty-three participants were excluded from the analyses as they quit the study.

After excluding, the sample comprised N = 143 participants with a mean age of 31.43 years old with a range from 18 years to 51 years (SD = 3.65). The gender was female for 76.2% of the participants and male for 23.8% of the participants. The country of origin was Germany for 74.1% of the participants, the Netherlands for 21.7% of the participants, and other for 4.2% of the participants. The educational level was College/ University degree for 53.8% of the participants and High school diploma for 46.2% of the participants. The participants were randomly assigned to one of the three risk message conditions (threat-appeal condition, coping-appeal condition, combined-appeal condition). The distribution of the participants was 50 in the threat-appeal condition, 50 in the coping-appeal condition, and 43 in the combined-appeal condition. The study was approved by the Ethics Committee of the Behavioural Management and Sciences Faculty of the University of Twente. Through signing an informed consent, the participants agreed to participate voluntarily.

Materials

Prior knowledge scale. The participants were asked about their knowledge of cybercrime. This was measured using three items that have been used in a study by Misana-ter Huurne, van Houten, Spithoven, Notté, and Leukfeldt (2020). On a 7-point Likert scale from "Strongly disagree" to "Strongly agree", the participants were asked what they know

about the risks of becoming a cyber-victim, how to recognize a cybercrime attempt, and what to do when becoming a cyber-victim (e.g.: "I know how I can recognize an attempt at cybercrime."). Cronbach's Alpha for the prior knowledge scale was .77, which is acceptable (George & Mallery, 2003).

Password creating scenario. The participants were asked to interact with a website by creating a password. Therefore, they had to imagine creating a password for an online banking account. The page showed the instruction: "Please create a password" with a text field below so that they could insert the password (Figure A1, Appendix A).

Domain Specific Risk Taking (DOSPERT) Scale. The general risk-taking of the participants was measured using the 30-item DOSPERT Scale by Blais and Weber (2006). The participants had to indicate on a 7-point Likert scale ranging from "Extremely unlikely" to "Extremely likely" how likely they would engage in the described activity or behaviour if they were to find themselves in that situation (e.g.: "Passing on somebody else's work as your own"). The scale included the subscales Ethical, Financial, Health/ Safety, Recreational, and Social. The Cronbach's alpha was .86 for the risk-taking measures, which is good (George & Mallery, 2003).

Password changing scenario, nudges and "skip this question"-button. For the second part of the password scenario, the participants were instructed to change the password ("Please change your password") they have just created in the text field that was shown below the instruction. Meanwhile, a nudge was shown on the screen. This nudge was located right next to the text field for the password.

Depending on the participants' risk message condition, the nudge contained a threat-appeal message, a coping-appeal message, or a combined-appeal message. These messages have been used in the study by van Bavel et al. (2019). For the threat-appeal condition, the participants got the nudge: "Navigate safely. If you don't, your personal data could be

compromised, or you could introduce a virus onto your computer.", for the coping-appeal condition, the participants got the message: "Navigate safely. You can easily minimise the possibility of suffering a cyber-attack if you use a secure password (e.g., combining lower and upper cases, numbers and symbols).". Participants in the combined-appeal condition got the nudge: "Navigate safely. You can easily minimise the possibility of suffering a cyber-attack if you use a secure password (e.g., combining lower and upper cases, numbers and symbols). If you don't, your personal data could be compromised, or you could introduce a virus onto your computer.".

In addition to the nudges, there was a button that showed the statement "skip this question" which made it possible for the participants to get to the next question in case they denied changing their password. This scenario, including the button, was constructed to detect whether participants react with denial or coping behaviour when being confronted with a request for a password change. The layout of the web pages for the different risk message conditions can be seen in Figure A2 – A4 (Appendix A).

Confidence in trustworthiness of websites. In order to exploratorily check whether the risk message condition had an effect on the confidence in trustworthiness of websites and to check how confident the participants were about their being able to detect cybercrime, screenshots of different websites were shown to them. On some of the screenshots, the original website was shown, and, on some screenshots, characteristics were modified to make them look untrustworthy. Therefore, logos were changed, spelling mistakes were added, and URLs were modified as Abbasi, Zhang, Zimbra, Chen, and Nunamaker (2010) gleaned these as fake website cues. On a 7-point Likert scale from "Not at all" to "Very confident" the participants were asked, "How confident are you that this is a trustworthy website?".

Intention scale. The intention of the participants to change their cyber-security behaviour that is related to the management of their passwords was measured using five self-

created items based on behavioural intention items used by Herath and Rao (2009). On a 7-point Likert scale from “Strongly disagree” to “Strongly agree”, the participants had to indicate the likelihood they would engage in the described activity or behaviour (e.g.: “I intend to change my password for the most important websites”). Computed Cronbach’s alpha for the intention scale was .59, which is poor (George & Mallery, 2003)

Cybernetic Coping Scale (CCS). In order to measure to what extend the participants felt capable to deal with the scenario, the 15-item CCS was used (Guppy et al., 2004). The participants were asked to indicate how they coped with what they have experienced during the password scenario (e.g.: “I tried to just let off steam”) using a 7-point Likert Scale ranging from “Did not do at all” to “Did very much”. Subscales were Change the Situation, Accommodation, Devaluation, Avoidance, and Symptom Reduction which all consist of three items. Overall Cronbach’s alpha was .87, which is good (George & Mallery, 2003).

Fear scale. In order to measure whether the participants experienced fear, four fear items that have been used in a previous study by Nabi and Myrick (2019) were used in this study. The participants were asked to indicate how they feel right now using the emotions fearful, afraid, scared, anxious for the fear assessment (e.g.: “I feel scared”). They had to indicate how they feel on a 7-point Likert scale ranging from “Not at all” to “Completely”. The fear items showed a reliability of .88, which is good (George & Mallery, 2003).

State Trait Anxiety Inventory (STAI-T). To assess the state anxiety the STAI by Spielberger, Gorsuch, Lushene, Vagg, and Jacobs (1983) has been used. The STAI assesses state anxiety (STAI-S) as well as trait anxiety (STAI-T). As only the state anxiety was of interest, the STAI-T has been excluded. This was possible since the reliability of the STAI-S only was found to be good/ excellent (Spielberger et al., 1983). To assess state anxiety, the participants had to indicate how they feel right now using the emotions tense, upset, or

nervous (e.g.: “I feel upset”) on a 7-point Likert scale. The Cronbach’s alpha for the STAI-S was .94 which is considered excellent (George & Mallery, 2003).

Victimisation scale. To conduct some exploratory analysis in order to see whether having been a victim of cybercrime had an effect on behavioural intention, the participants were asked whether they have ever been a victim of cybercrime and if they have been, the question “What type of cybercrime have you been victim of?” followed. The answer possibilities were for instance phishing and hacking.

Demographic questions. After completion of the general study, the participants were asked to answer demographic questions about age, gender, nationality, and education.

Desire to Drop Out. A meta-question was included in order to assess whether the participants wanted to drop out of the study (“Have you been planning to give up at some point during the study?”), which the participants had to answer on a 7-point Likert scale ranging from “Definitely no” to “Definitely yes”. The question was meant to assess whether the participants had the intention to drop out but decided not to do so.

Mouse tracking. To study the behaviour of possible victims of cybercrime, several techniques and technologies can be used. Much research has been using eye-tracking as a method to gather data related to online marketing research or usability testing (Wedel & Pieters, 2008) but also in cybersecurity contexts (Yuan, Li, Rusconi, & Aljaffan, 2017). In studies that are focused on online actions, another method to research behaviour is the usage of mouse tracking. According to Cepeda et al. (2018), the eye movements of an individual are related to their mouse movement, in concern to online behaviours.

In this study, to extend the measure of the usage of the “skip this question”-button, mouse tracking was used to see how the participants hover their mouse over the screen and especially in the area of the “skip this question”-button during the password change. This means that mouse tracking, in this research, is used to detect whether people focus on the

button, as the mouse movement is related to the eye movement. The purpose of this is similar to the “skip this question”-button, as it is supposed to detect whether people want to skip the question due to denying improving their cybersecurity.

Mouse tracking is the best measure available for the purpose of this study as it is a cost-effective and easy method to gather data. Next to that, it is already implemented in a computer which makes an unobtrusive method. As many different behaviours can be extracted from mouse-movement data and due to the fact that it is often used for usability testing or to study user’s behaviour it can be assumed to be a helpful tool in studying cybercrime.

Procedure

First, information about the purpose of the study was shown to the participants and they gave consent to participate in the study. Then, they had to answer the prior knowledge scale, which was seen as a control measurement. After that, the participants engaged in the first part of the password scenario and then they were asked to answer the DOSPERT Scale. The scale had been put in between the tasks of creating a password and changing the password because it could have been confusing for the participants to change a password they have just created.

Next, the participants engaged in the second part of the password scenario in which they were instructed to change the password they have just created while the nudge with the risk message appeared to them. Also, a “skip this question”-button was shown in case they denied changing the password. After engaging in the password scenario, the participants received a question about the change of the password: “What characteristics of your password did you change?” with the answer possibilities length, letters, lower/upper cases, numbers/symbols, and nothing.

Then, the participants had to rate the confidence in trustworthiness of websites. Several screenshots of different trustworthy and untrustworthy websites were shown to the participants, and they had to rate the websites on a Likert scale from 1 (not at all) to 7 (very much) on the question:" How confident are you that this is a trustworthy website?". After that, the participants were asked to answer the intention scale, the CCS, the fear scale, the STAI-S, the victimisation scale, the demographic questions, and the Desire to Drop Out. Finally, the participants were thanked for their participation in this research and debriefed about the different risk message conditions and the mouse tracking.

Results

The data for the study were saved in "Qualtrics". To analyse the data, IBM SPSS Statistics 26 for Windows-PC and R-Studio (version 1.3.1093) with the packages haven (version 2.3.1), tidyverse (version 1.3.0), foreign (version 0.8.80), ggplot2 (version 3.3.2), and lattice (version 0.20.41) were used.

First, unfinished study data were excluded from the analysis. Then, the data was split into two files where one included the data of the participant's responses to the scenario and the questions, and the other file included the data of the mouse tracking. For the responses file, reversed items were recoded. After that, descriptive statistics were computed and Cronbach's alphas.

Preliminary analyses

Preliminary analysis has been conducted to test whether prior knowledge about cyber victimisation differed per risk message condition. Therefore, a GLM was conducted. The independent variables were the risk message conditions, and the dependent variable was knowledge. The mean for the coping-appeal condition was 4.35 (SD = 1.18), for the threat-appeal condition was 3.87 (SD = 1.28), and for the combined-appeal condition was 4.32 (SD

= 1.09). The results of the GLM showed that there was no significant main effect between the risk message conditions for prior knowledge, F (2,143) = 2.42, p = .09, η2 = .03. The results of a post hoc test also did not show a significant difference in means for prior knowledge for any of the risk message conditions. Consequently, the variable knowledge was not added as covariate to the models.

Main analyses

Testing differences in the risk message conditions on the effect of fear, state anxiety, intention, coping, confidence in trustworthiness of websites, Desire to Drop Out. The General Linear Model (GLM) was used to compare how the independent variable risk message condition and the predictor variable risk-taking affected the dependent variables intention, coping, fear, state anxiety, as well as the confidence rating of the websites, and the Desire to Drop Out. The results of the main effects can be seen in Table 1.

Table 1

GLM of differences in risk message condition for dependent variables

Predictor	Df	*F*	η2	*p*
Fear scale	2	4.07	.06	.02
State anxiety	2	2.65	.04	.07
Intention scale	2	1.68	.02	.19
Cybernetic-Coping Scale	2	.62	.01	.56
Desire to Drop Out	2	.58	.01	.56
Confidence in trustworthiness of websites	2	.67	.01	.51

Fear scale. The GLM showed that there was a significant main effect between the risk message conditions for fear, F (2,143) = 4.07, p = .02, η2 = .06. Post hoc analysis was

performed to differentiate between the three risk message conditions. For fear, the post hoc test showed a significant difference between the threat-appeal condition and the combined-appeal condition, F (1, 143) = 7.41, p = .02, η2 = .05, CI[-1.09; -.17], and between the coping-appeal condition and the combined-appeal condition, F (1, 143) = 4.77, p = .05, η2 = .03, CI[.05; .97]. The mean fear for the coping-appeal condition was 2.17 (SD = 1.22) for the threat-appeal condition was 2.29 (SD = 1.19), and for the combined-appeal condition was 1.66 (SD = .88). This means that participants in the threat-appeal condition and in the coping-appeal condition experienced more fear than the participants in the combined-appeal condition.

State anxiety. The GLM did not show a significant main effect between the risk message condition for state anxiety and also post hoc tests did not show differences between the risk message conditions. Thus, there were no significant differences for state anxiety means between the coping-appeal condition, the threat-appeal condition and the combined-appeal condition (Appendix B).

Intention scale, Cybernetic-Coping Scale. The results of the GLM did not show a significant main effect between the risk message conditions for the intention scale and the Cybernetic-Coping Scale and also post hoc analysis did not show differences between risk message conditions. This means that there were no significant differences in the means for the participants' behavioural intention to engage in the recommended behaviour and coping between the coping-appeal condition, threat-appeal condition, and the combined-appeal condition (Appendix B).

Desire to Drop Out. The GLM did not show a significant main effect for the Desire to Drop Out between the risk message conditions. Also, a post hoc analysis did not show any significant differences between the risk message conditions. Thus, the means for the Desire to

Drop Out (Appendix B) were not significantly different. This means that people did not plan to drop out of the study depending on the risk message condition.

Exploratory analysis. Exploratory analysis on the confidence in trustworthiness of websites between the risk message condition was done using the GLM. The results of the GLM did not show significant differences between the risk message conditions for confidence in trustworthiness of websites. Also, a post hoc analysis did not show significant differences between the three risk message conditions. Thus, the means for the confidence in trustworthiness of websites (Appendix B) was not significantly different between the risk message conditions which means that the confidence in trustworthiness of websites was not influenced by being in one of the three risk message conditions. Also, it was checked whether risk-taking had a served as moderator between the risk message condition and all dependent variables. Including risk-taking as interaction in the GLM did not show different significant results.

Victimisation scale. Another exploratory analysis was conducted to detect whether participants who have been a victim of cybercrime scored higher in behavioural intention. Therefore, a GLM was conducted with the victimisation scale as independent variable and the behavioural intention scale as dependent variable. The results of the GLM showed that there was no significant main effect between victimisation and behavioural intention, F (1, 141) = .17, p = .68, $\eta 2$ = .001. This means that having been a victim of cybercrime or not having a victim of cybercrime does not influence the behavioural intention to engage in the recommended behaviour.

Testing the "skip this question"-button usage and the rating of the Desire to Drop Out. To be able to see how many people used the "skip this question"-button, frequency tables were computed. Then, a logistic regression was conducted to analyse whether the risk message condition and the risk-taking score predicted the usage of the "skip

this question"-button. The interaction between the risk message condition and risk-taking was included in the model. The independent variables were the risk message condition, risk-taking as well as the interaction between the risk message condition, and risk-taking. The only categorical predictor was the risk message condition. The risk message conditions were compared using indicator contrasts where the combined-appeal condition was the comparison group. The dependent variable was the button click.

The frequency table showed that in the coping-appeal condition 14 (9.8%) participants used the "skip this question"-button, in the threat-appeal condition 12 (8.4%) participants used the "skip this question"-button, and in the combined-appeal condition, 8 (5.6%) participants used the "skip this question"-button. The results of the logistic regression can be found in Table 2. It was found that the overall model was able to classify 76.2% of participants' clicks/ non-clicks. When only using the constant, this reflected a non-significant increase over prediction (Cox and Snell $R^2 = .01$, X^2 (5) = 1.52, $p = .91$). Also, the independent variables alone did not significantly predict the usage of the "skip this question"-button.

This means that the risk message condition, risk-taking, their interaction did not predict the usage of the "skip this question"-button. Also, the risk message condition did not predict whether a participant clicked the button. So, the participants in the threat-appeal condition did not click the button more often than the participants in the coping-appeal condition or in the combined-appeal condition. This was also confirmed by the results of the GLM for the Desire to Drop Out, as there were no significant differences for planning to drop out of the study between the risk message conditions. Participants' risk-taking also did not predict the usage of the skip button. This means that participants who clicked the "skip this question"-button did not score lower on risk-taking than the participants who did not click the "skip this question"-button.

To conclude, the usage of the "skip this question"-button was not predicted by the risk message condition or risk-taking. Also, no interaction effect was found between risk message condition and risk-taking and including knowledge as covariate also showed no significant association.

Table 2

Logistic regression of predictors of clicking the "skip this question"-button

Predictor	Beta	OR	Lower CI	Upper CI	Wald	*p*
Constant	-2.36	.10			1.48	.22
Risk message condition					.25	.89
Risk message condition (coping)	.82	2.28	.02	292.82	.11	.74
Risk message condition (threat)	1.22	3.37	.03	421.14	.24	.62
risk-taking	.26	1.30	.44	3.87	.22	.64
Risk message condition*risk-taking					.15	.93
Risk message condition (coping) by risk-taking	-.09	.91	.23	3.59	.02	.89
Risk message condition (threat) by risk-taking	-.27	.77	.19	3.10	.14	.70

Mouse tracking analysis. Using R-Studio with the packages haven, tidyverse, foreign, ggplot2, and lattice the mouse movement of the participants in the different risk message conditions was analysed, to see whether the mouse of the participants in the threat-appeal condition stayed longer in the area of the "skip this question"-button than the mouse of the participants in the coping-appeal condition and the combined-appeal condition. Therefore, the mouse-tracking data has been separated by the commas as it was a long text

string, and it was put into long format. Each row represented the participant number, the risk message condition of the participant, the index of the single mouse-movement data, the x-coordinates, and the y-coordinates to be able to analyse the data. As the mouse position of the participants was recorded every ten milliseconds, the difference between the rows was the set number of ten milliseconds. Then, the data was cleaned by excluding 20 cases in which the mouse tracking did not work, or participants did not use a mouse or a trackpad.

Unfortunately, issues in the analysis of the mouse-tracking data arose. Because the participants used their own devices, which were all different from each other, the scales of the virtual x-coordinates and y-coordinates were different for every participant. Thus, the exact location of the "skip this question"-button varied per participant which made it impossible to locate an area of interest but the approximate location of the "skip this question"-button was in the lower left of the website. Consequently, it was also not possible to analyse the mouse-tracking data as it was planned. However, heatmaps per risk message condition were created that show an indication of the distribution of the mouse-movement data. The heatmaps were used to see how much the participants were tempted to move their mouse towards the lower left corner of the screen rather than moving the mouse from the top to read instructions and do the task and then going to the next page ("→"). It was expected that the participants in the threat-appeal condition more often use the "skip this question"-button and deny improving their cybersecurity than the participants in the coping-appeal condition and in the combined-appeal condition. Thus, it was also expected that the heatmaps would show more activation around the lower left corner for the threat-appeal condition than for the other two risk message conditions.

To resemble the mouse coordinates in a graph, the y-values of the mouse tracking were transformed to negative values because the y-coordinates of the virtual coordinates were vice versa to the y-coordinates of the heatmaps. As the scales for the risk message conditions

were different, the scales were transformed so that each heatmap showed the same range on the x-axis and the y-axis. The x-axis ranges from 0 to 700 while the y-axis ranges from 0 to 1000. The darker the spots, the more the participants hovered their mouse in that area.

The heatmap with the mouse movement coordinates for the coping-appeal condition can be seen in Figure 1. The heatmap shows that the mouse movement of the participants is spread very much across the screen. The heatmap shows more dark spots in the area from 250 to 755 on the y-axis and from 200 to 255 on the x-axis. This means that the participants moved their mouse into that area more often. Some mouse movement can be seen in the lower left corner of the heatmap where the “skip this question”-button was located. The heatmap with the mouse movement data for the threat-appeal condition can be seen in Figure 2. This heatmap shows a slight negative linear line across the movement. The darker spots are spread almost across the whole y-axis but mostly stayed in the area between 250 and 350 on the x-axis. No mouse movement in the left lower corner can be seen, which was the area of the “skip this question”-button. The heatmap with the mouse movement for the combined-appeal condition can be seen in Figure 3. The mouse movement of the participants in this risk message condition is also spread like a negative line across the screen. Most of the dark spots are located from 275 to 550 on the y-axis and from 200 to 350 on the x-axis. In this heatmap, there was some mouse movement in the left lower corner of the screen.

It was expected that there would be more mouse movement in the left lower corner of the heatmaps for the threat-appeal condition than for the coping-appeal condition because the “skip this question”-button was located in that area. Comparing the heatmaps, in the threat-appeal condition there is less mouse movement in the left lower corner than in the coping-appeal condition and in the combined-appeal condition. This means that participants in the coping-appeal condition and in the combined-appeal condition hovered their mouse more

often in the area of the “skip this question”-button than the participants in the threat-appeal condition.

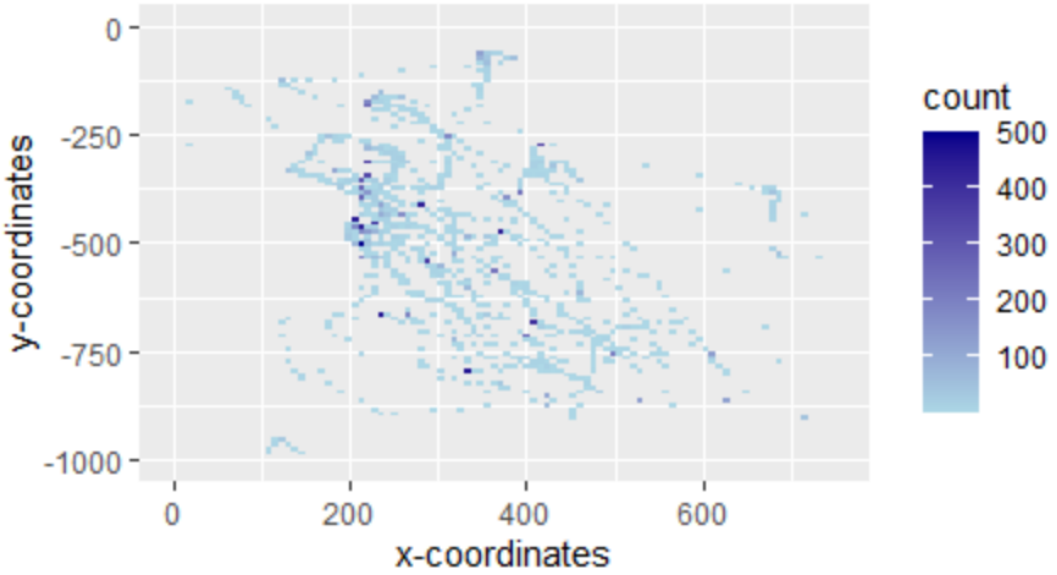

Figure 1. Heatmap for the mouse-movement in the coping-appeal condition.

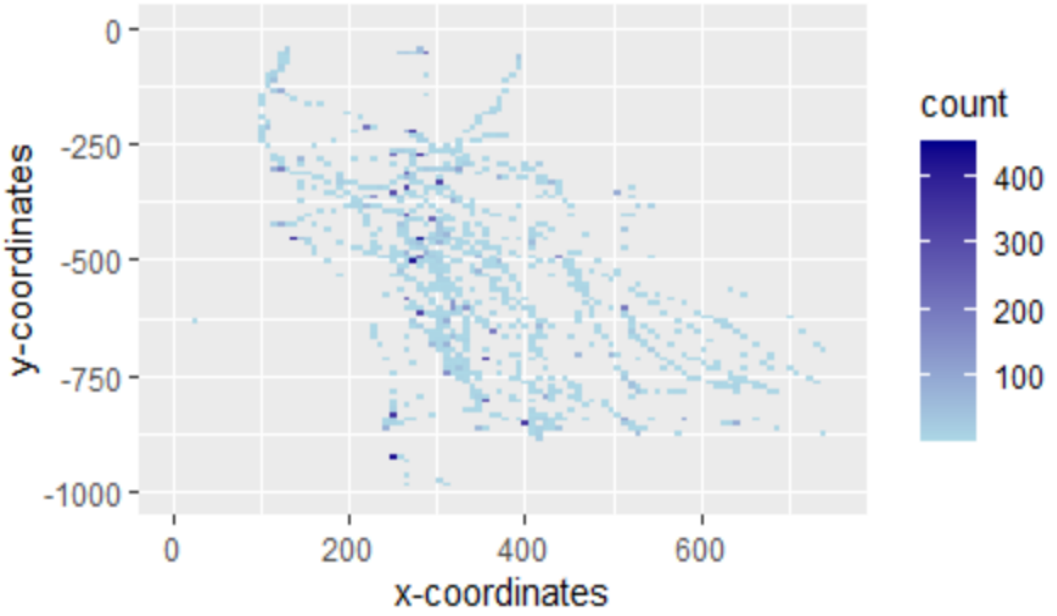

Figure 2. Heatmap for the mouse-movement in the threat-appeal condition.

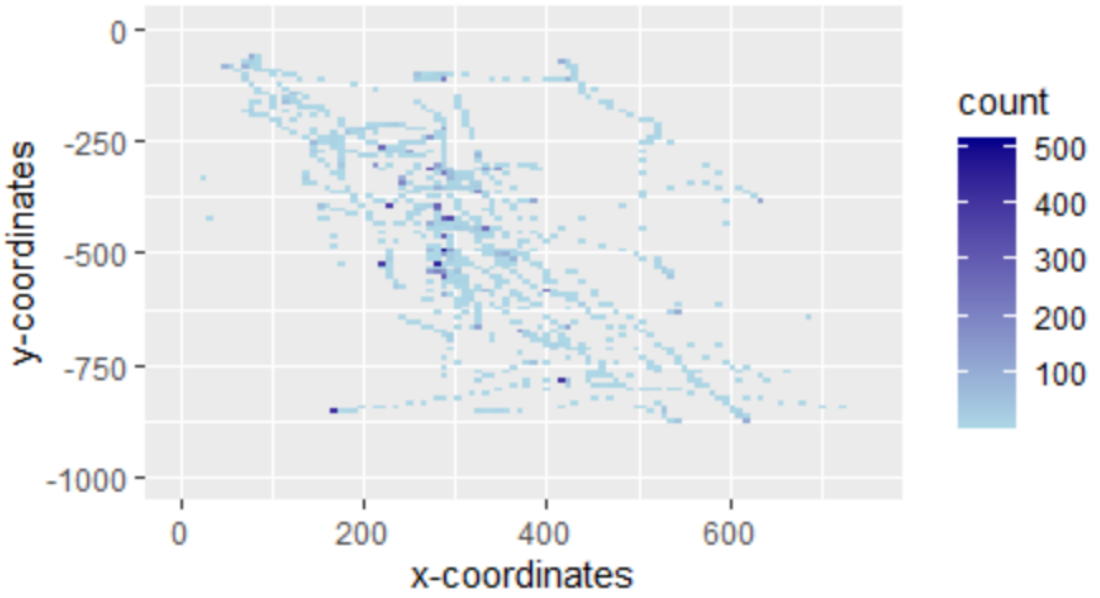

Figure 3. Heatmap for the mouse-movement in the combined-appeal condition.

Discussion

This study aimed to examine the effect of three different appeal messages in relation to cybersecurity behaviour based on the EPPM. More specifically, the link between a coping-appeal message, a threat-appeal message, or a combined-appeal message, as well as individual risk-taking and confidence in trustworthiness of websites, behavioural intention, coping, fear, state anxiety, denial to improve the cybersecurity, and planning to drop out of the study was examined. It was found that fear is higher in the coping-appeal condition and the threat-appeal condition compared to the combined appeal condition. No differences were found for the predictor variable risk-taking and the dependent variables state anxiety, behavioural intention, coping, the desire to drop out of the study, the confidence in trustworthiness of websites and the denial to improve their cybersecurity. The risk message condition, as well as risk-taking, did not predict the denial to improve their cybersecurity of the participants. Further, risk-taking did not moderate the effect between the risk message conditions and the dependent variables and prior knowledge about cybercrime did not have a significant effect on the outcomes.

Understanding the effect of appeals

The current study showed that people in the coping-appeal condition and in the threat-appeal condition scored higher on fear than the participants in the combined-appeal condition. Thus, the combined appeal seems to lower the fear in the participants compared to the coping-appeal condition and the threat-appeal condition. So, the coping-appeal or the threat-appeal alone did not lower the fear in the participants. This is contrary to what van Bavel et al. (2019) stressed. They found that a combined-appeal message but also a coping-appeal message alone are successful when telling people how to cope with a threat. As the nudges in the study by van Bavel et al. (2019) were shown in a pop-up message after the participants entered the e-environment while the nudges in this study were placed next to the password change instruction, the time and the placement of the nudges seem to play a role in the effectiveness of the appeals. Studies in other domains have found that the placement of nudges (Gainsbury, Aro, Ball, Tobar, & Russell, 2015) affects the effectiveness of nudges. Messages that appeared in the middle of a screen compared to messages in the edges of the screen were recalled more easily. A systematic review of nudge theories and strategies found that also the delivery mode has an effect on the influence of nudges (Kwan et al., 2020). Thus, the different placement of the nudges in this study versus the study by van Bavel et al. (2019) might be a factor for the differing results.

Further, the participants in the threat-appeal condition did not score higher on state anxiety than the participants in the coping-appeal condition and combined-appeal condition. This is not in line with the hypothesis, as it was expected that the participants in the threat-appeal condition score higher on state anxiety than the participants in the coping-appeal condition and in the combined-appeal condition. The threat appeal alone was expected to lead to more anxiety than the coping appeal alone and the combined appeal as there was no information given to the participant on how to deal with the threat.

Additionally, this study found that the confrontation with a coping appeal or a combined appeal did not lead to higher scores in feeling able to cope with a threat and in the intention to engage in the recommended behaviour to lower the threat than being confronted with a threat appeal. As a coping appeal has the function to approach the self-efficacy and the response-efficacy of a person, the participants who were confronted with a coping appeal were expected to feel more able to cope with the threat and engage in protection motivation (Witte, 1992). This can also be seen in the article by van Bavel et al. (2019), as the coping-appeal and the combined-appeal were more effective in relation to the participants' coping than the threat-appeal. This study's finding can be explained by the response costs, which are the physical or psychological costs of engaging in coping behaviour. According to Mayer et al. (2017), response costs can have weak and strong negative influences on cybersecurity behaviour. Because the physical or the psychological costs that are associated with engaging in online security behaviour might have been too high for this scenario, the participants did not have enough response efficacy or self-efficacy to outweigh the response costs. Consequently, they did not feel able to cope with the threat and engage in the recommended behaviour.

Next to that, this study found that there is no difference in the denial to improve their cybersecurity either for being confronted with a coping appeal, a threat appeal, or a combined appeal nor for scoring high on risk-taking versus scoring low on risk-taking. It was assumed that being confronted with a threat appeal or scoring low on risk-taking versus being confronted with a coping appeal, a combined appeal, or scoring high on risk-taking would lead to a higher denial to improve the cybersecurity. In previous studies, participants who were confronted with only a threat appeal were more likely to drop out than participants confronted with only a coping appeal or a combined appeal. This might have been due to risk-denial, which occurs when an individual perceives the severity and the vulnerability of

the threat to be high, but the ability to cope with the threat as low. Thus, a risk-denial helps to control the fear. Also, it was found that people who scored lower on risk-taking were more likely to drop out of the study and people higher in risk-taking tended to stay (van Bavel et al., 2019). This study's finding that neither the risk message condition nor the risk-taking score predicts the denial to improve the cybersecurity is also confirmed by the non-significant findings related to the Desire to Drop Out that was asked at the end of the study. Because it was expected that the participants in the threat-appeal condition would be more likely to deny improving their cybersecurity than the participants in the coping-appeal condition and in the combined appeal condition, the results of the Desire to Drop Out should have emphasized this as well. So, since the scores of the Desire to Drop Out also did not show differences in the risk message condition, this confirms that the risk message condition did not predict whether the participants wanted to drop out of the study. An explanation for these findings is related to the environment of the participants. As around 120 of the participants were university students who were recruited through a subject pool and gained credits for their participation, it is likely that they did not want to risk not gaining the credit through denying improving their cybersecurity. This could have been a factor for many of the participants to stay in the study. Relating this to an everyday situation that requires cybersecurity behaviour, this would imply that people, however, their online security may be threatened, still stick to the rules and the regulations of the environment. Thus, although there is a threat to the people's cybersecurity, the people might pay more attention to external influences and omit to pay attention to their cybersecurity. An example could be that people skip changing a password or logging out because they have time pressure.

Experimental measures including the effect of the different risk message conditions and the risk-taking on the confidence in rating the trustworthiness of websites did not show any effects. This means that the risk message condition and the risk-taking did not influence

the confidence of the participants that the websites are either trustworthy or untrustworthy. So, neither the threat-appeal condition, the coping-appeal condition, the combined-appeal condition nor scoring either high or low on risk-taking has an influence on the confidence of a participant that a certain website is trustworthy or not. Also, exploratory analysis found that there is no difference in engaging in recommended behaviour between people who have been a victim of cybercrime and people who have not been a victim of cybercrime.

Due to technical circumstances, it was not possible to conduct statistical analyses for the mouse-tracking data. The participants took part in this study using their own devices, which led to different scales of the x-coordinates and the y-coordinates for every participant. This means that also the coordinates of the “skip this question”-button differed per participant. These variations in the scales made it impossible to statistically compare the data between risk message conditions. Yet, heatmaps were created to get an indication of how and where the participants hovered their mouse and to see whether there were differences between risk message conditions. This data is interpreted with the necessary caution that these are not exact calculations. As the “skip this question”-button was located in the left lower corner of the screen, attention is paid to this area. Unexpectedly, the heatmaps show that participants in the coping-appeal condition and in the combined-appeal condition hovered more in the left lower corner than the participants in the threat-appeal condition. Interpreting this with caution, it could mean that the participants in the coping-appeal condition and in the combined-appeal condition focused more attention on the “skip this question”-button. Although the logistic regression did not show significant differences between the risk message conditions and as the heatmaps just show an indication of the people’s mouse movement, this should be further investigated as the mouse tracking is able to provide information about the people’s cybersecurity behaviour.

Strengths and Limitations

There are some potential limitations concerning the results of this study. The study was done during the COVID-19 pandemic and thus it was conducted online. This was done to guarantee the safety of the participants and to ensure that recruiting enough participants during this time was possible.

The first limitation is that the data analysis of the mouse-tracking data, as this raised problems. Because every participant was participating in the study using a different device, the scales of the virtual x-coordinates and the y-coordinates were different for every participant. As this means that also the virtual coordinates of the "skip this question"-button were different for every participant, the mouse-tracking data could not be used for statistical analysis to see whether participants in one risk message condition hovered more in the area of the button than participants in another risk message condition. Thus, conducting the study online raised a problem in analysing the mouse-tracking data.

Although this study has limitations through being conducted online, it also benefits from being arranged in an online environment. Through this method, it was possible to observe the people's behaviour when being in their everyday environment in which much of the online behaviour is normally performed. So, the study was not a laboratory study which for the participants means that they were not influenced by the circumstances and the environment of the lab. Another strength of this study was the mouse tracking itself. Mouse tracking is a very useful tool in observing people's online behaviour, as it is cheap and easy to implement. Next to that, it is unobtrusive which is a big benefit as it does not distort the results of the study (Cepeda et al., 2018)

Another limitation that applies to this study concerns the scales that have been used to assess the participants' knowledge about cybercrime, participants' intention to engage in secure online behaviour, and the fear scale. This means, that non-validated have been used,

which makes the results less concrete. Since some of the non-validated scales have successfully been used in other research as well or were based on used scales (Herath & Rao, 2009; Misana-ter Huurne et al., 2020; Nabi & Myrick, 2019), they almost certainly measure what they intend to measure.

Implications and future research

Despite the limitations, the results suggest several theoretical and practical implications. Theoretically, these results confirm that threat appeals alone are not useful when aiming to change people's behaviour (Ruiter et al., 2014). Also, coping appeals alone seem to be not as effective regarding people's behaviour change as expected because coping-appeal messages alone do not reduce peoples' fear, while combined-appeal messages were able to do so.

Alternative explanations imply that there might be other factors that influence the ability to cope with the recommended behaviour, like the placement of the nudges and their delivery mode. In practice, this means that attention should be paid to the usage of the appeals. The best way is to use combined-appeal messages as this was found to be an effective way to reduce the fear that people might feel regarding the threat.

Since there were no differences found in the denial to improve their cybersecurity between the risk message conditions and between high and low risk-taking scorers, another implication is that people are influenced by the external environment and its rules. As the participants possibly did improve their cybersecurity because of the credits they would gain when successfully completing the study, this at a higher level implies that people still stick to the rules and the regulations of the external environment, although their online security may be threatened. Since in this study, the cybersecurity of the participants was not actually threatened this needs to be investigated. It has been found that users are likely to define the threat as unlikely or irrelevant because they do not have the time to respond (Bulgurcu,

Cavusoglu, & Benbasat, 2010). This signifies that external influences play a role in peoples' responses to cyberthreat.

Future research on this topic needs to focus on maintaining the strength of this research while improving the limitations. In order to really assess the mouse tracking of the participants, a lab study needs to be conducted to avoid the problem of participants having different screens resulting in issues to statistically analyse the mouse movement data. As this was the reason this study could not statistically analyse the mouse tracking data and thus could not conclude concrete results of the mouse tracking, this needs to be investigated in future studies. So, either mouse tracking needs to be used again, or eye-tracking should be implemented to assess people's online security behaviour.

Alternatively, the original online study needs to be repeated while making sure that the resolution of every participant's device is the same. The latter method should be strongly considered as it is important to study people's cybersecurity behaviour while they are in their everyday environment where they are not disturbed by the circumstances and the environment of the unfamiliar lab. As the results of the heatmaps show an indication for more hovering in the area of the "skip this question"-button for the coping-appeal condition and the threat-appeal condition than for the combined-appeal condition, this needs to be investigated in more detail and with statistical analysis. When this study is being repeated, the participants should participate voluntarily in means of not being rewarded for participation as this could influence their behaviour.

Additionally, it needs to be investigated whether the temporal and spatial placement of nudges plays a role in the effectiveness of the nudges. Previous studies found that differences in the placement of nudges have an influence on their effectiveness (Gainsbury et al., 2015; Kwan et al., 2020). As differences in dependent measures were found across cybersecurity studies using nudges to influence people's behaviour, it is of reasonable

importance to investigate the most effective placement of nudges in the cybersecurity context.

Next to that, scales that focus on the research of cybercrime should be developed and validated. Cybercrime needs to be reduced by behaviour change in people, as people need to protect themselves against cybercrime. This is essential as human behaviour is seen as the weakest link in a cybersecurity chain (Cisco, 2017). Thus, to reduce the successful cyberattacks, it is important to do further research on the topic of behaviour change in the cybersecurity context, as most of the fateful cybersecurity mistakes happen due to people's misbehaviour. Therefore, validated scales that are developed only for this purpose are necessary. Different results were found across several studies regarding the participants' emotions and their cybersecurity behaviour (van Bavel et al., 2019). This might be a consequence of the usage of non-validated scales, but also it needs to be investigated whether the placement of the nudges including the different appeals plays a role in this. It might be that people are more influenced by the nudges when being nudged at the beginning of a scenario or when entering an e-environment, as it was done in the study by van Bavel et al. (2019) but it might also be the case that nudges that are being presented at the moment the recommended behaviour needs to be performed are more effective, as it was done in this study. As there is no concrete literature about where nudges should be placed in the context of cybersecurity behaviour, this needs to be investigated.

Conclusion

This study aimed to show the relation between three different appeal messages (coping-appeal, threat-appeal, combined-appeal) as well as risk-taking and their effect on people's cybersecurity behaviour in an e-environment based on the EPPM. The present research supports some of the previous findings on behaviour change in cybersecurity. It was found that being confronted with a threat-appeal message and a coping-appeal message alone

led to a higher fear compared to the combined-appeal message. So, this study suggests that only a combined-appeal message is able to lower fear in people. No differences were found in the participant's anxiety between the risk message conditions. Coping and behavioural intention were not found to differ between risk message conditions, as the response costs to engage in the behaviour seemed to be too high. There were no differences found between risk message conditions in relation to denial to improve their cybersecurity and consequently there was also no interaction effect including risk-taking. Because the placement and the delivery mode of the nudges seem to influence their effectiveness, this needs to be further investigated. Also, the development of validated scales needs to stand in focus of future research. Since mouse-tracking data can give valuable insight into people's behaviour in their normal environment, this needs to be further investigated, as well as the influence of external rules and regulations on people's cybersecurity behaviour.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly, 34*(3), 435-461. doi:10.2307/25750686

Abdalla Mabrouk Khiralla, F. (2020). Statistics of Cybercrime from 2016 to the First Half of 2020. *International Journal of Computer Science and Network*, 9(5). doi: 10.13140/RG.2.2.30131.66088

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. doi:10.1126/science.aaa1465

American Psychological Association. (n.d.-a). Defense meachanism. *In APA dictionary of psychology.* Retrieved May 5, 2021, from https://dictionary.apa.org/defense-mechanism

American Psychological Association. (n.d.-b). Denial. *In APA dictionary of psychology.* Retrieved May 5, 2021, from https://dictionary.apa.org/denial

American Psychological Association. (n.d.-c). Projection. *In APA dictionary of psychology.* Retrieved May 5, 2021, from https://dictionary.apa.org/projection

American Psychological Association. (n.d.-d). Rationalization. *In APA dictionary of psychology.* Retrieved May 5, 2021, from https://dictionary.apa.org/rationalization

American Psychological Association. (n.d.-e). Risk taking. *In APA dictionary of psychology.* Retrieved June 1, 2021, from https://dictionary.apa.org/risk-taking

American Psychological Association. (n.d.-f). Threat appraisal. *In APA dictionary of psychology.* Retrieved May 5, 2021, from https://dictionary.apa.org/threat-appraisal

Blais, A.-R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision making, 1*(1), 33-47. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1301089

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Cepeda, C., Rodrigues, J., Dias, M. C., Oliveira, D., Rindlisbacher, D., Cheetham, M., & Gamboa, H. (2018). Mouse Tracking Measures and Movement Patterns with Application for Online Surveys. In A. Holzinger, P. Kieseberg, A. Tjoa, E. Weippl (Eds.), *Machine Learning and Knowledge Extraction* (pp. 28-42). doi: https://doi.org/10.1007/978-3-319-99740-7_3

Cisco. (2017). Annual Cybersecurity Report. Retrieved from https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html

Farrington, D. P., & Welsh, B. C. (2002). Improved street lighting and crime prevention. *Justice Quarterly, 19*(2), 313-342. doi:10.1080/07418820200095261

Gainsbury, S., Aro, D., Ball, D., Tobar, C., & Russell, A. (2015). Determining optimal placement for pop-up messages: evaluation of a live trial of dynamic warning messages for electronic gaming machines. *International Gambling Studies, 15*(1), 141-158. doi:10.1080/14459795.2014.1000358

George, D., & Mallery, P. (2003). *SPSS for Windows step-by-step: A simple guide and reference, 11.0 update* (4th ed.). Boston: Allyn & Bacon.

Graham, A., Kutzli, H., Kulig, T. C., & Cullen, F. T. (2019). Invasion of the Drones: A New Frontier for Victimization. *Deviant Behavior, 42*(3), 1-18. doi:10.1080/01639625.2019.1678973

Guppy, A., Edwards, J. A., Brough, P., Peters-Bean, K. M., Sale, C., & Short, E. (2004). The psychometric properties of the short version of the Cybernetic Coping Scale: A multigroup confirmatory factor analysis across four samples. *Journal of Occupational*

and Organizational Psychology, 77(1), 39-62. doi:https://doi.org/10.1348/096317904322915900

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management, 33*(1), 2-16. doi:10.1080/10580530.2015.1117842

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:https://doi.org/10.1016/j.dss.2009.02.005

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*(546546). doi:10.3389/fpsyg.2020.546546

Kwan, Y. H., Cheng, T. Y., Yoon, S., Ho, L. Y. C., Huang, C. W., Chew, E. H., . . . Low, L. L. (2020). A systematic review of nudge theories and strategies used to influence adult health behaviour and outcome in diabetes management. *Diabetes & Metabolism, 46*(6), 450-460. doi:https://doi.org/10.1016/j.diabet.2020.04.002

Laycock, G. (2004). New Challenges for Law Enforcement. *European Journal on Criminal Policy and Research, 10*(1), 39-53. doi:10.1023/B:CRIM.0000037560.81599.ed

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats.* Washington, DC: Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

Maiti, A., & Sivanesan, S. (2012, April 25-27). *Cloud controlled intrusion detection and burglary prevention stratagems in home automation systems* [Paper presentation]. 2nd Baltic Congress on Future Internet Communications, Vilnius, Lithuania. doi:10.1109/BCFIC.2012.6218000.

Mayer, P., Kunz, A., & Volkamer, M. (2017, August 29 -September 1). *Reliable Behavioural Factors in the Information Security Context* [Paper presentation]. Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 9. doi:https://doi.org/10.1145/3098954.3098986

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69,* 151-156. doi:https://doi.org/10.1016/j.chb.2016.11.065

Misana-ter Huurne, E., van Houten, Y., Spithoven, R., Notté, R. J., & Leukfeldt, E. R. (2020). *Cyberweerbaarheid. Risicibewustzijn en zelfbeschermend gedrag random cybercrime onder jongeren en mkb'ers*. Deventer/Den Haag: Saxion Hogeschool, De Haagse Hoogeschool.

Moore, R. (2010). *Cybercrime: Investigating high-technology computer crime*. Routledge: Elsevier.

Nabi, R. L., & Myrick, J. G. (2019). Uplifting Fear Appeals: Considering the Role of Hope in Fear-Based Persuasive Messages. *Health Communication, 34*(4), 463-474. doi:10.1080/10410236.2017.1422847

Niess, J., & Woźniak, P. W. (2018, April 21-26). *Supporting Meaningful Personal Fitness: the Tracker Goal Evolution Model* [Paper presentation]. CHI Conference on Human Factors in Computing Systems, Montreal QC, Canada. doi: https://doi.org/10.1145/3173574.3173745

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology, 49*(2), 63-70. doi:https://doi.org/10.1002/ijop.12042

Spielberger, C. D., Gorsuch, R. L., Lushene, R., Vagg, P. R., & Jacobs, G. A. (1983). *Manual for the State-Trait Anxiety Inventory*. Palo Alto, CA: Consulting Psychologists Press.

Tsokkis, P., & Stavrou, E. (2018, 19-21 June). *A password generator tool to increase users' awareness on bad password construction strategies* [Paper presentation]. International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy. doi: https://doi.org/10.1109/ISNCC.2018.8531061

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. doi:https://doi.org/10.1016/j.ijhcs.2018.11.003

Wedel, M., & Pieters, R. (2008). A review of eye-tracking research in marketing. In N.K. Malhotra (Ed.) *Review of marketing research (pp. 123-147)*. Bingley: Emerald Group Publishing Limited

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

Yuan, H., Li, S., Rusconi, P., & Aljaffan, N. (2017, July 9-14). *When Eye-Tracking Meets Cognitive Modeling: Applications to Cyber Security Systems* [Poster presentation]. International Conference on Human Aspects of Information Security, Privacy and Trust, Cham. doi: https://doi.org/10.1007/978-3-319-58460-7_17

Zhang, X. A., & Borden, J. (2019). How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research, 23*(10), 1336-1352. doi:10.1080/13669877.2019.1646315

Appendix A

Password scenario

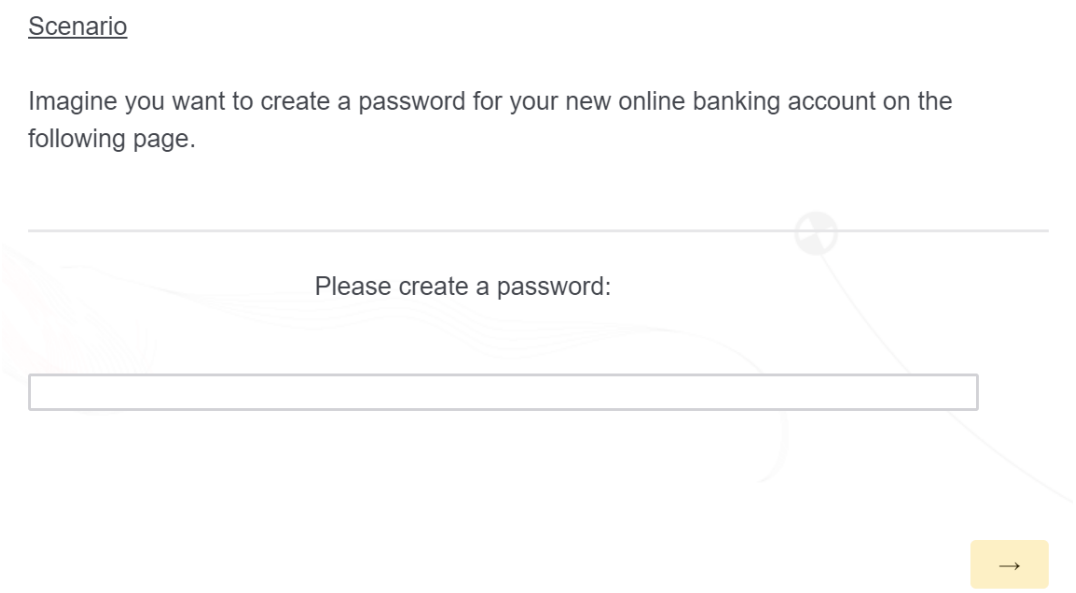

Figure A1. Password creating scenario.

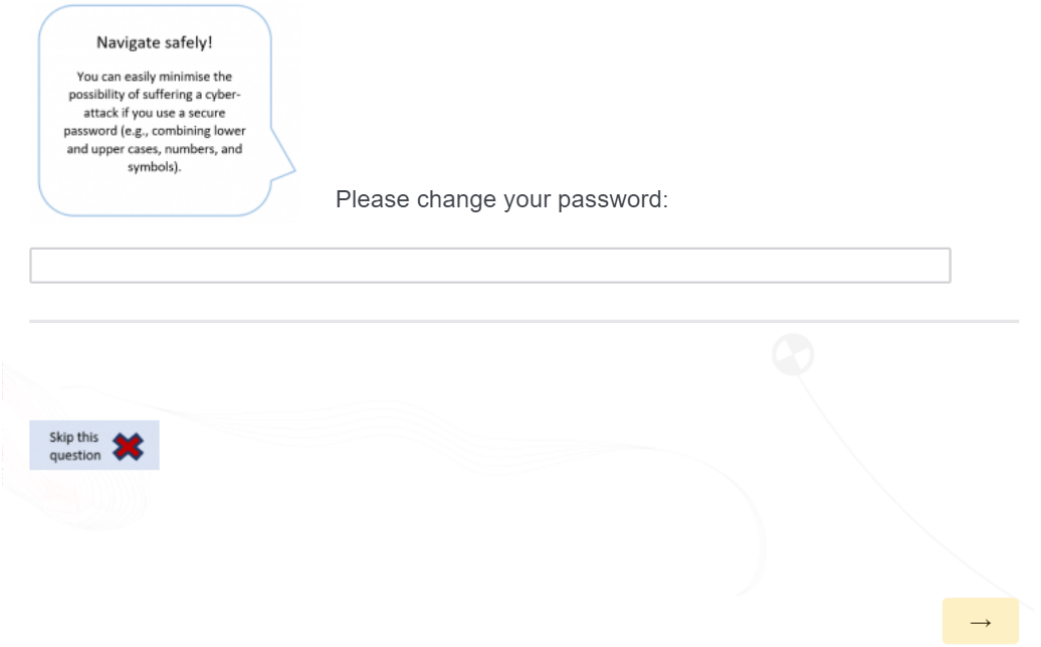

Figure A2. Password changing scenario – coping-appeal condition.

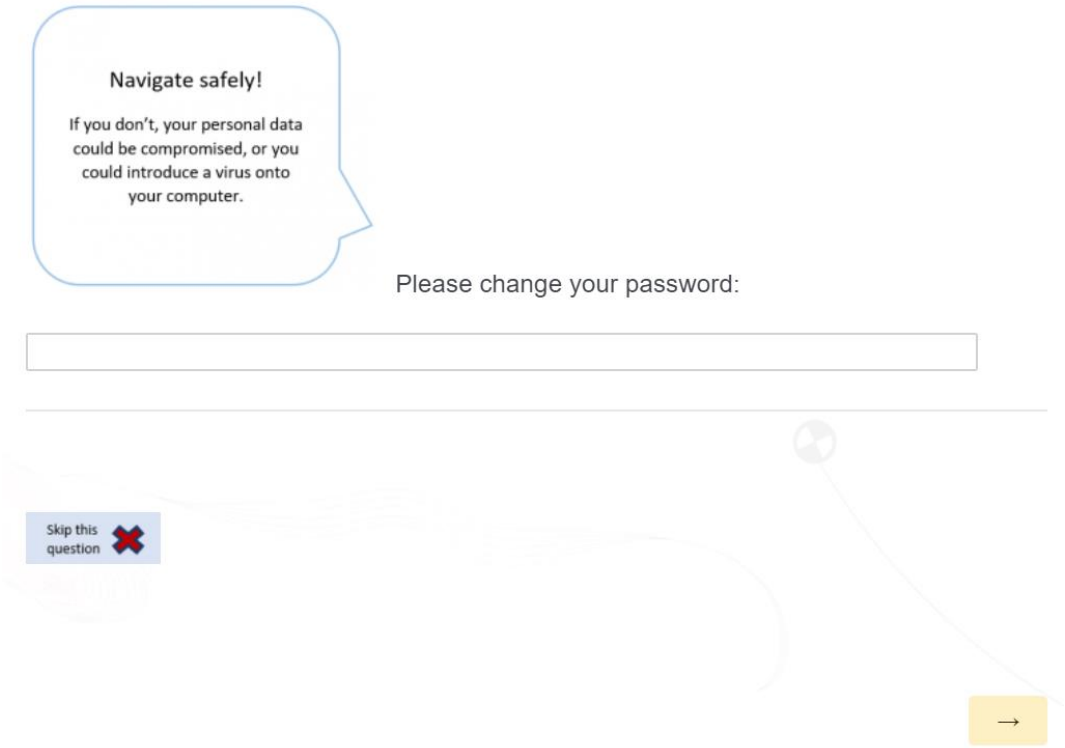

Figure A3. Password changing scenario – threat-appeal condition.

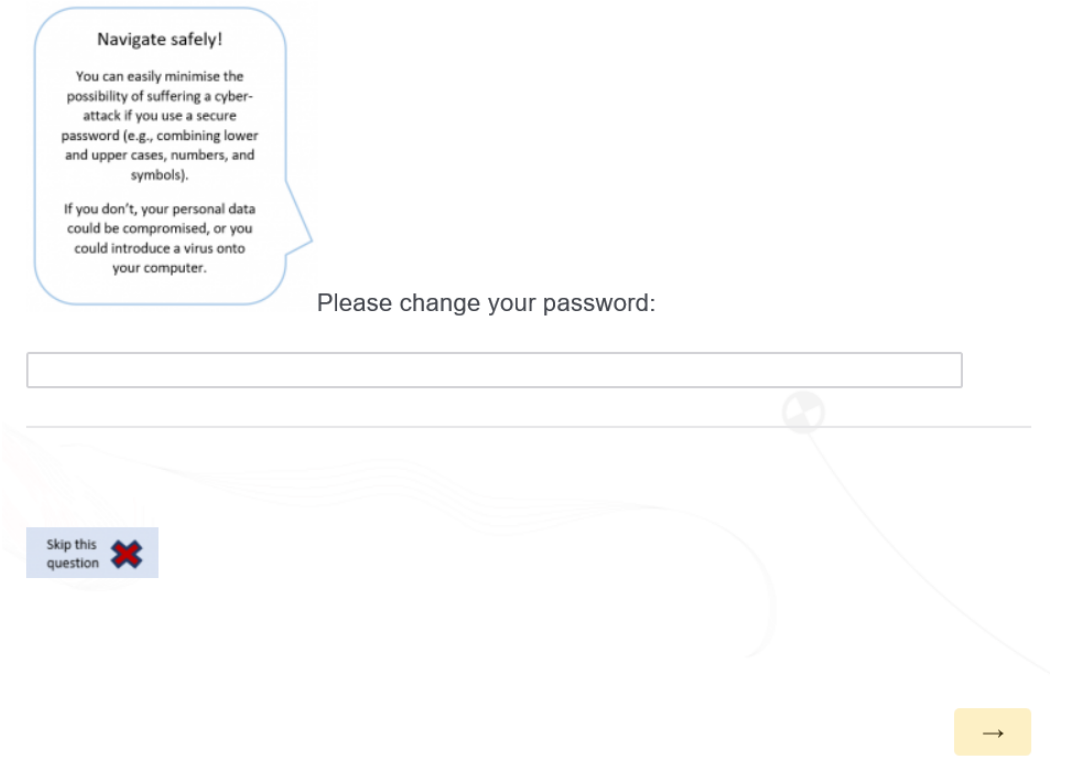

Figure A4. Password changing scenario – combined-appeal condition

Appendix B

Means and standard deviations in risk message conditions

Table B1.

Means and standard deviations of risk message condition per dependent variable

Dependent variables	Coping-appeal message		Threat-appeal message		Combined-appeal message	
	M	*SD*	*M*	*SD*	*M*	*SD*
Fear scale	2.17	1.22	2.29	1.19	1.66	.88
State anxiety	2.93	1.11	3.04	1.08	2.56	.93
Intention scale	4.56	.72	4.77	1.16	4.92	.88
CCS	3.18	.87	3.39	1.10	3.29	.88
Desire to Drop Out	2.64	1.86	2.82	1.78	2.42	1.75
Confidence in trustworthiness of websites	4.56	.59	4.56	.57	4.44	.50

Note. 7-point Likert scale for all dependent variables.