Bachelor Thesis Rosalien Braakman

The effect of cybersecurity messages and personality on cybersecurity behavior.

Rosalien Braakman
S2179393

June 28th, 2021

University of Twente
BMS Faculty
Department of Psychology

Supervisor: I. van Sintemaartensdijk

Abstract

Cybercrime is a rapidly growing problem. An increasing dependence on the Internet has created more and more risks and vulnerabilities and made it easier for criminals to make their moves in the online world. The first goal of this study is to investigate the effect of cybersecurity messages on the cybersecurity behavior and the intentions towards these behaviors. The second goal of this study is to investigate the potential effect of personality traits on cybersecurity behavior. An online survey was distributed through social media and through the University of Twente Sona website. The results suggest that personality traits do not have a significant effect on the cybersecurity behavior of the participants. The results also indicated that the expected positive effect of the combined message on the threat and coping appraisal was not found. Thus, no significant differences were found between the combined message compared to the individual threat and coping messages. Limitations and future research of this research are extensively discussed.

Introduction

Today, the world we live in is driven more and more by digital technology including social networks and online transactions. Although the launch of the Internet and other new communication technologies started only a couple of decades ago. It is impossible to imagine a world without the possibilities that the Internet gives us (Näsi, Oksanen, Keipi, & Räsänen, 2015). While rapid growth in the possibilities that the Internet and computer technology has given the world and the social and economic growth that it provoked, an increasing dependence on the Internet has provided a growing number of risks as well as vulnerabilities and opened up new possibilities for criminals to see opportunities for their criminal activities online. (Interpol, 2017).

Cybercrime is one of the most rapidly growing types of crime and refers to any crime that involves computers and technological networks. This includes fraud with credit cards, including online credit card fraud, online identity fraud, phishing, and the distribution of for example child pornography, threatening messages and online racist messages on social media (Bossler & Holt, 2010; Oksanen & Keipi, 2013).

Cybercrime is becoming an urgent and serious problem in today's society, and it is expected that the number of cybercrime victims will increase rapidly in the future (Jardine, 2020). In order to prevent the violation of privacy caused by cybercrime, we need to understand what drives this problem. Therefore, it is important to gain knowledge about the different factors that can lead to an increased or decreased probability of becoming a cybercrime victim.

Most of the previous literature concerning the improvement of online security is focused on improving the technology rather than looking at human factors. However, lacking technology that makes people vulnerable to cybersecurity problems is only one factor that has an impact on cybercrime. Next to technology problems, human behavior also has an impact on online security. Stanton et al. (2004) were one of the first that acknowledged the importance of the human factor behind security. Ögütçü, Testik and Chouseinoglou (2015) found that people tend to have low levels of awareness towards threats and their level of information security is low.

Since human behavior plays such a large role in effective cybersecurity, it is important to understand which factors drive online security behavior. Then again, it is also important to state that many researchers state that it is unreasonable to simply cite ‘human error’ as a

major factor without first understanding users are simply faced with overly complex security systems, unusable cybersecurity policies and a complex range of other job demands than mean that they lack the knowledge, the time and the support to be able to deal with cyber threats (Kraemer et al., 2009).

In the current study, more insight will be gained in the potential effect of the content of a cybersecurity message on the cybersecurity behavior of users. Also, the possible influence of knowledge of cybercrime on the effect between nudges and cybersecurity behavior will be studied. Next to that, the potential effect of personality traits on cybersecurity behavior will be studied. The outcomes of this study can help to gain better insight in these potential relationships. In the next paragraphs, cybercrime will be examined shortly. Thereafter, the protection motivation theory and the extended parallel process model will be considered. Finally, the possible link between personality and cybersecurity behavior will be examined.

The growing problem of cybercrime

Cybercrime is a growing problem in today's society. The growth of digital technology has provided the world with innovation and a rapid economic growth. However, it also causes the rapidly increasing threat of cybercrime, which is one of the fastest growing threats in today's society (Cisco, 2017). With all the new technologies in place, cyber threats are likely to increase in the future (Jardine, 2020). Cybercrime does not have a uniform definition. Chandra & Snowe (2020) defined cybercrime as an act that uses computer technology to commit a crime. Another definition of cybercrime is that cybercrime is any crime involving computers or computer networks including fraud with credit cards, including online credit card fraud, online identity fraud, phishing and the distribution of for example child pornography, threatening messages and online racist messages on social media (Bossler & Holt, 2010; Oksanen & Keipi, 2013).

The perception of cybersecurity behaviors

As mentioned above, with the rise of online networks, human vulnerabilities have escalated as information posted online can be used to identify potential. For many years, researchers and security professionals have reported that the 'weakest link' in any security chain is human behavior. However, online security warnings in the design of security messages are not optimally used. Simple policy campaigns or warning messages, intended to increase their awareness of the risks involved are not always effective, as they implicitly rely on users making very informed or rational decisions Also, users find it relatively easy to

dismiss the threat as irrelevant or unlikely, or they fail to act, simply because they have neither the time nor the skills to respond (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019).

The Protection Motivation Theory states that when facing a threatening event, a person makes two estimations of the threat. The first is focused on the threat itself, the threat appraisal. In their threat appraisal, people will consider how negative the consequences of the threat are, the perceived severity. Secondly, the likelihood that the threat will affect them directly is considered, the perceived vulnerability (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019).

The second estimation is on the persons' capability to act against that threat, the coping appraisal. This affects their intention to take action and results in adaptive or maladaptive behaviors regarding the threat. In their coping appraisal, people will assess whether undertaking a commended course of action will remove the threat (response efficacy) and also their level of confidence in being able to carry that action out (self-efficacy). This appraisal may lead to adaptive behaviors, providing that the costs of making an adaptive response (response costs) are not too high (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019).

A problem is that the PMT is not able to explain why fear appeals work in one situation but not in another situation. The PMT does not take into consideration that in addition to cognitive responses of a threat there are also emotional responses to fear. On the contrary, The Extended Parallel Process Model builds on the previously mentioned protection motivation theory but in addition to that, the EPPM tries to clarify why a fear appeal works sometimes and fails other times (Popava, 2012).

According to the EPPM, the assessment of a fear appeal comprises two appraisals of the message, which result in one of three outcomes. When individuals encounter a threat, they first evaluate the threat (Witte & Allen, 2000). If the threat is perceived as non-relevant or not threatening enough, then there is no motivation to process the message further, and people just deny and ignore the fear appeal.

In contrast, when a threat is displayed as and believed to be serious and relevant, the person is likely to become afraid. This feeling encourages them to take some sort of action that will reduce the feeling of fear (Witte & Allen, 2000) (Masuch, Hengstler, Schulze, & Trang, 2021). If the individual believes that he is encountering a severe threat, he will be more motivated to start the second appraisal. The second appraisal is an assessment of the

self- and response-efficacy of the recommended response. When both self- and response-efficacy are high enough. The person tends to be motivated to consider ways to remove the risk. Alternatively, when there is low response efficacy and/or low self-efficacy, people tend to be driven more to control their fear by denying the fear (Masuch, Hengstler, Schulze, & Trang, 2021).

As mentioned above, the PMT does not distinguish between the effectiveness of the different messages. Instead, the EPPM states that a functioning fear appeal contains both a threat and a coping message. In the current study, it will be investigated if the EPPM outperforms the PMT.

The messages that will be used in this study are three messages designed by Van Bavel et al., (2019). These messages can be described as: A coping message told users that it is easy to reduce the chances of cybersecurity problems; A fear appeal that warns internet users that not behaving secure online could leave them vulnerable to cybersecurity problems; and a threat and coping message containing both elements described above.

Personality and cybersecurity behavior

There are various factors that can have an effect on cybersecurity behavior. Next to technology problems, human behavior also has an impact on online security. Stanton et al. (2004) were one of the first that acknowledged the importance of the human factor behind security. Nearly one-quarter of all cybersecurity failures are due to human error (Waldrop, 2016).
Ögütçü, Testik and Chouseinoglou (2015) found that people tend to have low levels of awareness towards threats and their level of information security is low. One of these factors is personality. Previous research showed that personality may be a strong predictor of behavior (Shropshire et al., 2015).

Personality traits are characteristics that are internal to a person that seem to be quite stable across the grown-up life of the individual (Matt & Peckelsen, 2016). In extension of previous personality models, Lee and Ashton (2007) designed a new six-dimensional model to measure personality, named the HEXACO model. This model is suitable in this study

because the model contains the personality trait Honesty-Humility which is often not included in other personality models.

Conscientiousness is defined as “the propensity to follow social norms for impulse control, to be goal directed, to plan, and to be able to delay gratification.” (Roberts, Jackson, Fayard, Edmonds, & Meints, 2009). Thus, Conscientious individuals tend to be organized and are known for their self-control. Self-control is also a factor that is linked to cybercrime victimization. Individuals with high self-control do not make impulsive decisions, like sharing their personal information online, which decreases their chance of becoming a victim of cybercrime (Chua & Chua, 2017; Bossler & Holt, 2010). The personality trait conscientiousness has demonstrated a positive relationship with better cybersecurity behavior (Hadlington & Murphy, 2018).

People who are high in agreeableness are often described as people who have a social oriented attitudes toward others. In addition, agreeable persons seem to be higher in self-control as well. Traits that are often seen in more agreeable people is that people who are high in agreeableness have the tendency to increase correct judgement over whether information should be trusted. The high self-control in combination with good judgment decreases the chance of being victimized by cybercrime (Cho, Cam, & Oltramari, 2016).

On the other hand, people high in the trait Honesty-Humility tend to be sincere, fair and modest. Honest individuals also tend to be more likely to believe in the honesty of other people and they often have difficulty with seeing danger in situations. Therefore, individuals that are high in the Honesty-Humility trait have a higher chance of becoming a victim of cybercrime due to their high expectation of the honesty of other people (Baiocco et al., 2017).

For people who score high in Openness to Experience, people who score high on Openness to Experience tend to have lots of imagination and are open to exploring new experiences (Albladi & Weir, 2017.) Chua and Chua (2017) mentioned that Openness to experience is positively related to the use of social networks without first investigating the reliability of these networks, which could increase the chance of being victimized online.

The six cybersecurity behaviors that are chosen to use in this study in order to measure the online security score of the participants are: using a VPN connection; creating a strong password; changing passwords after six months; installing updates directly; using different passwords for different accounts; logging out after using a site. All these behaviors are

cybersecurity behaviors that have a significant impact on the chance of being victimized by cybercrime (Wijayanto & Prabowo, 2020).

H1: People who score high on Conscientiousness or Agreeableness behave more securely online in comparison to people who score low on these traits.

H2: People who score high on Openness to Experience or Honesty-Humility behave less securely online in comparison to people who score low on these traits.

H3: After a combined threat and coping message, participants have a higher fear- and coping appraisal in comparison to a threat message and copping message individually.

Method

Participants

Of the original dataset consisting of 138 participants, 21 participants were deleted from the dataset due to incomplete responses. There were 117 participants between the ages of 18 and 77 ($M = 29.68$ $SD = 13.12$). The dataset consisted of 50 males and 66 females. One participant preferred not to answer this question. Participants in this study had different nationalities (Dutch: $n = 77$; German: n = 29; Other nationality: n = 11). Finally, participants' current and highest level of education was asked (Highschool: n = 22; Bachelor's degree: n = 69; Master's degree: n = 26). Participants were recruited by distributing the online questionnaire on social media and on the SONA website of the University of Twente. Participation was voluntary.

Measures

Personality

Personality was measured by using the HEXACO-60 scale by Lee and Ashton (2007). In which a five-point Likert Scale (1= strongly agree, 5 = strongly disagree) was used for answering these questions. This 60-item version is a shortened version of the HEXACO Personality Inventory-Revised.

The openness subscale consists of 10 items. One example item is: *I'm interested in learning about the history and politics of other countries.* The mean and standard deviation

were (*M* = 2.75, *SD* = 0.61) The subscale had an acceptable reliability (α = .78).

The honesty-humility subscale consists of 10 items. One example is: *I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed.* The mean and standard deviation were (*M* = 2.83 , *SD* = 0.55). Subscale had an acceptable reliability. (α = .71).

The emotionality subscale consists of 10 items. One example item is*: I would feel afraid if I had to travel in bad weather conditions.* The mean and standard deviation were (*M* = 2.80, *SD* = 0.65). The subscale had a good reliability (α = .80).

The extraversion subscale consists of 10 items. One example item is*: I feel reasonably satisfied with myself overall.* The mean and standard deviation were (*M* = 2.78, *SD* = 0.67). The subscale had a good reliability (α = .84).

The agreeableness subscale consists of 10 items. One example item is*: I rarely hold a grudge, even against people who have badly wronged me.* The mean and standard deviation were (*M* = 2.93, *SD* = 0.67). The subscale had a good reliability (α = .84).

The conscientiousness subscale consists of 10 items. One example item is*: I plan ahead and organize things, to avoid scrambling at the last minute.* The mean and standard deviation were (*M* = 2.59, *SD* = 0.67). The subscale had a good reliability (α = .84).
The participants were asked to rate to what extent they agreed with the 60 statements on a 1 (strongly agree) to 5 (strongly disagree) scale.

Knowledge

Knowledge of cybercrime was measured to investigate a possible relationship between prior knowledge of cybercrime and cybersecurity behavior. Participants were asked to rate their knowledge of cybercrime. The item that was used is *"How do you rate your knowledge about cybercrime?"*. The participants were asked to rate to what extent they agreed with this statement on a scale ranging from 1 (very bad) to 7 (very good). A high score on this scale meant that the participant perceived his knowledge of cybercrime as good.

Perceived severity

Perceived severity is a part of the threat appraisal that is included in the Protection Motivation Theory and Extended Parallel Process Model and was measured by using the 2-item scale by Woon, Tan, & Row (2005). One example item is *"Not <performing security behavior> would be a serious problem for me."* The 2 items were asked for the following security behaviors: using a VPN connection; creating a strong password; changing passwords after six months; installing updates directly; using different passwords for different accounts; logging out after

using a site. The participants were asked to rate to what extent they agreed with these statements on a 1 (strongly disagree) to 7 (strongly agree) scale. The mean and standard deviation were (M = 4.06, SD = 0.85). The scale had a good reliability (α = .88). The perceived severity score was created by averaging the score of these 2 items. A high score on this scale meant that participants' level of perceived severity of a specific behavior was high.

Perceived vulnerability

Perceived vulnerability is a part of the threat appraisal that is included in the Protection Motivation Theory and Extended Parallel Process Model and and was measured by using a 2-item scale by Herath and Rao (2009). One example item is *"I could be subjected to an information security threat if I will not <perform security behavior>*. The 2 items were asked for all 6 security behaviors. The participants were asked to rate to what extent they agreed with these statements on a 1 (strongly disagree) to 7 (strongly agree) scale. The mean and standard deviation were (M = 4.48, SD = 0.88). The scale had an excellent reliability (α = .90). The perceived vulnerability score was created by averaging the score of these 2 items. A high score on this scale meant that participants' level of perceived vulnerability of a specific behavior was high. .

Response efficacy

Response-efficacy is a part of the coping appraisal and was measured by using a 3-item scale by Woon, Tan, & Row (2005). One example item is: *"If I comply with <performing behavior>, my mobile device related security problems will be scarce",* The 3 items were asked for all 6 security behaviors. That means that the scale consists of 18 items. The participants were asked to rate to what extent they agreed with these statements on a 1 (strongly disagree) to 7 (strongly agree) scale. The mean and standard deviation were (M = 4.941, SD = 0.73). The scale had a good reliability (α = .91). The response efficacy score was created by averaging the score of these 3 items. A high score on this scale meant that participants' level of response efficacy of a specific behavior was high.

Self-efficacy

Self-efficacy is a part of the coping appraisal was measured by using a 3-item scale by Woon, Tan, & Row (2005). These items were: *"I would feel comfortable to <perform behavior> on my own."* The 3 items were asked for all 6 security behaviors. That means that the scale consists of 18 items. The participants were asked to rate to what extent they agreed

with these statements on a 1 (strongly disagree) to 7 (strongly agree) scale. The mean and standard deviation were (M = 4.480, SD = 0.778). The scale had excellent reliability (α = .92). The self-efficacy score was created by averaging the score of these 3 items. A high score on this scale meant that participants' level of self-efficacy of a specific behavior was high.

Intention to comply with behavior

The intention to behavior scale was used to measure the intention of the participants to comply with the security behaviors after they finished the scenario. Intention was measured by one item of Piquero & Piquero (2006). The security behaviors that were measured are: Using a VPN connection, creating a safe password, changing passwords in time, logging out, using different passwords, updating software directly, using a password manager. This item was: *"After completing this study, I intend to comply with <performing security behavior>."* This item was asked for all 7 security behaviors. The participants were asked to rate to what extent they agreed with these statements on a 1 (strongly disagree) to 7 (strongly agree) scale. A high score on this item meant that participants' intention to a certain behavior was high.

Procedure

Participants were presented with a digital survey, sent to them via a weblink, accessible through PC, mobile phones and tablets. The survey was created using Qualtrics.

Participants were presented with a digital survey, sent to them via a weblink. The survey was created by using the program Qualtrics. At the beginning of the survey, participants were informed about the structure of the study and filled in the informed consent.

The first questions of the survey were questions about the age, gender, nationality, and education level of the participants. After these demographic questions, participants had to fill the HEXACO 60-item questionnaire followed up with a question about their knowledge of cybercrime. Next, participants were evenly and randomly divided into three groups: one group was presented with a coping message, the second group was presented with a threat message, and the third group was presented with a combination of the threat and coping message.

The coping message was: “you can easily minimize the possibility of suffering a cyber-attack if you choose safe connections, remember to log out and use secure passwords”. The threat message was: “Navigate safely. If you don’t, your personal data could be compromised, or you could introduce a virus on your device”. The combined threat and coping message was the following: “Navigate safely. You can easily minimize the possibility of suffering a cyber-attack if you choose safe connections, remember to log out and use secure passwords. If you don’t, your personal data could be compromised, or you could introduce a virus onto your computer”.

After being presented with one of the three messages, participants were asked seven questions about the cybersecurity behavior of the participants. These questions were about using a VPN connection, accepting cookies, creating a safe password, changing passwords, updating applications, using different passwords, and logging out.

Thereafter, for each cybersecurity behavior, questions measuring perceived severity, perceived vulnerability, response efficacy, self-efficacy, and intention of behavior were asked. At the end of the survey, the participants were debriefed and thanked for their participation.

Results

Preliminary analysis

A preliminary analysis was used to explore possible correlations between the different variables that were investigated in this research. Most findings are to be expected, such as the correlation between intention towards behavior and knowledge. The correlation also points out that higher cybercrime knowledge is associated with a higher intention to perform cybersecurity behavior.

Table 1

Bivariate Correlation-Matrix

		1	2	3	4	5	6	7	8	9
1. age	Pearson correlation	1	.071	-.181	.092	.175	**.257****	.217*	.224*	**.255****
	p	-	.447	.051	.322	.059	.005	.019	.015	.006
2. Intention	Pearson correlation		1	**.285****	.045	-.170	-.096	.047	-.077	**-.245****
	p		-	.002	.632	.209	.303	.617	.411	.008
3. Knowledge	Pearson correlation			1	.068	.143	-.110	-.014	.050	*-.185**
	p			-	.464	.125	.239	.880	.593	.046

4. Honesty	Pearson correlation	1	.139	*.196**	**-.280****	.167	*.192**
	p	-	.136	.034	.002	.072	.038
5. Openness	Pearson correlation		1	.100	*.229**	.164	.046
	p		-	.281	.013	.077	.620
6. Conscientiousness	Pearson correlation			1	-.079	**.377****	.170
	p			-	.397	.000	.066
7. extraversion	Pearson correlation				1	-.118	-.156
	p				-	.207	.092
8. emotionality	Pearson correlation					1	.034
	p					-	.713
9. agreeableness	Pearson correlation	.					1
	p						-

Italics $p < .05$.
Bold $p < .01$.

Hypotheses testing

For hypothesis 1: People who score high on Conscientiousness or Agreeableness behave more securely online. A Poisson regression was conducted to compare online security score in people high in Conscientiousness or Agreeableness and people low in Conscientiousness or Agreeableness. In the regression, one online security score was made by adding up the right decisions on the six security behaviors (using a VPN connection; creating a strong password; changing passwords after six months; installing updates directly; using different passwords for different accounts; logging out after using a site). The Poisson regression revealed that Conscientiousness $\chi 2 = .283$ (1, N = 117) = -.047, $p < .595$ and Agreeableness $\chi 2 = 1.525$. (1, N = 117) = -.101, $p < .217$ had no significant effect on any security behavior . Based on these findings, the hypothesis was rejected.

For hypothesis 2: People who score high on Openness to Experience or Honesty-Humility behave less securely online. The same Poisson regression was used to compare online security score in people high in Openness to Experience or Honesty-Humility or people low in Openness to Experience or Honesty-Humility. The Poisson regression revealed that Openness to Experience $\chi 2 = .231$ (1, N = 117) = -.046, $p < .631$ and Honesty-Humility $\chi 2 = .428$ (1, N = 117) = .071, $p < .513$ had no significant effect on any security behavior as on the total security score of the participants .Based on these findings, the hypothesis was rejected.

For hypothesis 3: People with the combined threat and coping message have a higher threat and coping appraisal in comparison to people who received a threat message or a coping message. A one-way ANOVA was conducted to test this possible effect. A significant effect was found for response efficacy (F (2.114) = 4.851; p = .010). The following means and standard deviations were found for the different messages in which after the coping message participants response efficacy was the highest (M = 5.21, SD = .68), followed by the combined message (M = 4.91, SD = .76), and after the threat message the mean response efficacy was the lowest (M = 4.71, SD = .68). The post-hoc-Tukey-test shows a significant difference between the coping and the threat message (p = .007). However, no significant effect was found between the threat and combined message (p = .448) and the coping message and combined message (p = .150).

For Self-efficacy the following means and standard deviations were found for the different messages. The following means and standard deviations were found for the different messages in which after the coping message participants self-efficacy was the highest (M = 5.67, SD = .80) followed by the combined message (M = 5.53, SD = .74) and after the threat message the mean self-efficacy was the lowest (M = 5.27, SD = .76). However, no significant differences in these mean scores were found (F (2.114) = 2.831; p = .0.063).

For perceived severity, the following means and standard deviations were found for the different messages. The following means and standard deviations were found for the different messages in which after the coping message participants perceived severity was the highest (M = 4.18, SD = .99) followed by the combined message (M = 4.16, SD = .80) and after the threat message the mean perceived severity was the lowest (M = 3.84, SD = .73). The means were in the expected direction. However, no significant differences in these mean scores were found (F (2.114) = 1.916; p = .0.152).

For perceived vulnerability, the following means and standard deviations were found for the different messages. The following means and standard deviations were found for the different messages in which after the combined message participants perceived vulnerability was the highest (M = 4.66, SD = .87) followed by the coping message (M = 4.55, SD = .94) and after the threat message the mean perceived vulnerability was the lowest (M = 4.25, SD = .78). The means were in the expected direction. However, no significant differences in these mean scores were found (F (2.114) = 2.379; p = .097).

Explorative analysis

An additional analysis was done to investigate the potential effect of the different messages on the total security score. A one-way ANOVA was conducted to test this possible effect. The following means and standard deviations were found for the different messages in which after the combined message participants total security score was the highest (M = 3.44, SD = 1.31) followed by the coping message (M = 2.94 SD = 1.72) and after the threat message the mean security score was the lowest (M = 2.52, SD = .1.41) A significant difference between the three messages was found. (F (2.114) = 3.689; p = .028). The post-hoc-Tukey-test shows a significant difference between the combined message and the threat message (p = .021). However, no significant effect was found between the threat and coping message (p = .426) and the coping message and combined message (p = .325).

A second additional analysis was performed to investigate the potential effect of the different messages on the intention towards behavior. Another one-way ANOVA was conducted to test this possible effect. The following means and standard deviations were found for the different messages in which after the combined message participants intention towards behavior was the highest (M = 4.91, SD = .97) followed by the coping message (M = 4.72, SD = .98) and after the threat message the intention towards behavior was the lowest (M = 4.31, SD = .87). A significant difference between the three messages was found (F (2.114) = 4.245; p = .017). The post-hoc-Tukey-test shows a significant difference between the combined message and the threat message (p = .014). However, no significant effect was found between the threat and coping message (p = .137) and the coping message and combined message (p = .640). These results mean that after receiving the combined message, participants performed more behaviors in a secure way in comparison to participants who received the threat message.

Discussion

The current study had the goal to investigate the potential relation between personality and cybersecurity behavior. In previous research, the personality traits conscientiousness and agreeableness had demonstrated a positive relationship with better cybersecurity behavior (Hadlington & Murphy, 2018). On the other hand, people high in the traits Honesty-Humility and people high in the trait Openness to Experience were more likely to behave less secure online (Baiocco et al., 2017; Van Gelder and De Vries, 2012).

However, findings of the current research indicate that personality did not significantly affect cyber security behavior. Therefore, the hypothesis was that people with the combined threat and coping message have a higher threat and coping appraisal in comparison to people who received a threat message or a coping message. However, findings indicate that the combined message did not outperform the threat message and coping message, A significant effect was found for response efficacy: response efficacy was higher when a coping message was present rather than a threat message, but no difference between coping or combined message. In the exploratory analysis investigating the effect of the three different messages on intention towards behavior, a significant difference between the combined message and the threat message. In which the combined message had a positive effect on participants' intention towards behavior. Another significant difference was found while looking at the effect of the messages and security behavior score. A significant difference was found between the means of the security score after receiving the combined message compared to the means of the security score after receiving the threat message.

Interpretation of Findings

There was no significant effect of any of the personality traits on the cybersecurity behaviors. This indicates that participants' personality did not influence participants' security behavior. This was against the expectations based on the literature. It is possible that the behaviors that were used in the current study were not suitable to add up as one security score. Other studies clustered security scores in behaviors that are connected to each other. Wijayanto and Prabowo (2020) grouped their cybersecurity behavior into Behavior of Using Password, Behavior of Information Access; Behavior of Device and Internet Usage; Behavior of social media and Behavior of Using Smartphone Devices. The security behaviors used in our study are also measured in the study of Wijayanto & Prawobo (2020) but are not following each other in a thoughtful way.

The third hypothesis, people with the combined threat and coping message have a higher threat and coping appraisal in comparison to people who received a threat message or a coping message, was also rejected. There was no significant difference in the mean scores on the self-efficacy, response-efficacy, perceived-vulnerability and perceived-severity scales when comparing the mean score of the combined message to the mean scores of the individual threat and coping messages. Nevertheless, there was one significant difference

found in a different direction than expected. A significant difference in the mean score of the response efficacy scale was found between the coping and the threat message. This indicates that receiving a coping message instead of a threat message provides more belief in the effectiveness of implementing the cybersecurity behaviors. (Martens, De Wolf, De Mares, 2019). Thus, receiving a coping message ensures more belief in the effectiveness of the measures that can be taken.

An additional analysis was done to investigate the potential effect of the different messages on the total security score. A significant difference was found in a way that the mean security score after receiving the combined message was significantly higher in comparison to the security score after receiving the threat message. The security behaviors that create the security score are: using a VPN connection; creating a strong password; changing passwords after six months; installing updates directly; using different passwords for different accounts; logging out after using a site. Therefore, this finding can be interpreted in a way that after receiving the combined message, participants performed more behaviors in a secure way in comparison to participants who received the threat message.

A second additional analysis was performed to investigate the potential effect of the different messages on the intention towards behavior. The effect that was found was that after receiving the combined message, participants scored higher on the intention to behavior scale compared to participants who received the threat message. This corresponds with the Protection Motivation Theory literature which stated that the components of the coping appraisal had a larger effect on intentions of behavior in comparison to the elements of the threat appraisal (Van Bavel et al., 2019).

Limitations

The first, and most important limitation that needs to be considered in the current research is that it is arguable if the current study measured actual behavior instead of intention towards behavior. This study tried a research method that was not used before in this area of cybercrime research. This method already comes closer to measuring actual behavior by giving participants a scenario in which they had to put themselves into the scenario and they choose what they would have done in the situation. However, in future research it would be interesting to measure actual behavior in a lab study instead of through a questionnaire.

One of the limitations of the used questionnaire was that the survey was only available in the English language. However, none of the participants was a native English speaker. Even though one criteria to participate in this study was to understand and read the English language, it cannot be ensured that participants fully can fully understand and process the whole questionnaire. This might be the reason that a lot of participants did not end the survey. Secondly, it is questionable if participants could fully focus till the end of the survey. That is why it would be better to give participants the choice to fill out the questionnaire in German or Dutch. Another limitation of the questionnaire itself is that the questionnaire took approximately 20 minutes to complete. This is a long questionnaire to fully focus on till the end. Some participants needed to be excluded due to irregular responses. Research showed that motivation lowers when questionnaires are too long, respondents are then likely to look for easier ways to respond to the questions, for example not reading as careful as before (Scott et al., 2011).

A third limitation is that it was not considered if people already have previous experience with cybercrime. This could influence the way they think about cybercrime, behave on the internet and their threat and coping appraisal. In previous research, previous victimization of phishing was found to prevent a person from becoming a victim again (Workman 2007). In the next study it would be better to take this previous experience into account.

Future Research

Despite the fact that there were only a few significant effects found in the current research, there was a trend in the mean scores. Participants that were subjected to either the combined message or the individual coping message had a higher security score in comparison to participants that were subjected to the threat message. Taking these outcomes into consideration, future research should try to investigate the effectiveness of different formulated combined messages and individual coping messages coping and combined coping and threat messages on cybersecurity behaviors. Differences in the length of the message, structure of the message, and even font, and font size can be considered to optimize the security messages (Anderson, Vance, Eargle, & Jenkins, 2017).

Secondly, there might be differences in the need for information that are needed to optimally inform different groups about the risks of cybercrime. Different age groups could differ in their needs for information on this topic. When groups that differ in age are

compared, there are differences in remembering and evaluating information. Elderly adults are found to perform more poorly when facing new information in comparison to the general adult population and the same difficulties are also found in young adults (John & Cole, 1996)

Conclusion

All in all, the current study offered some interesting insights. In today's society it is important to be able to behave securely online. However, it is not fully the responsibility of the internet users to know what the best way is to protect themselves in the more and more complicated online world full of potential harms. The current research showed that no significant effect of personality on cybersecurity behavior. On the other hand, cybersecurity messages did significantly influence both cybersecurity behavior and also the intention towards behavior. That is why future research should focus on optimizing the impact of the message on different groups.

References

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227-236. DOI: https://doi.org/10.1016/j.jcrimjus.2010.03.001

Helweg‐Larsen, K., Schütt, N., & Larsen, H. B. (2012). Predictors and protective factors for adolescent Internet victimization: Results from a 2008 nationwide Danish youth survey. *Acta paediatrica*, *101*(5), 533-539. DOI: https://doi.org/10.1111/j.1651-2227.2011.02587.x

Jardine, E. (2020). Taking the Growth of the Internet Seriously When Measuring Cybersecurity. *Researching Internet Governance: Methods, Frameworks, Futures*. Retrieved from: JardineTakingtheGrowthoftheInternetSeriouslyWhenMeasuringCybersecurity.pdf

John, D. R., & Cole, C. A. (1986). Age differences in information processing: Understanding deficits in young and elderly consumers. *Journal of consumer research*, *13*(3), 297-315. DOI: https://doi.org/10.1086/209070

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387-402. DOI: https://doi.org/10.1057/ejis.2008.29

Kewenig, W. (2017). Interpol. *Legal Magazine*. Retrieved from: Summary_CYBER_Strategy_2017_01_EN LR.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying routine ativity theory to cybercrime. A theoretical and emperical analysis. *Deviant Behavior*. https://doi.org/10.1080/01639625.2015.1012409

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

Masuch, K., Hengstler, S., Schulze, L., & Trang, S. (2021, January). The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware. In *Proceedings of the 54th HawaiiInternational Conference on System Sciences* (p. 6691). Retrieved from: Microsoft Word - HICSS-54 Submission 2667 Final Manuscript.docx (hawaii.edu)

Matt, C., & Peckelsen, P. (2016, January). Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4832-4841). DOI:10.1109/HICSS.2016.599

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210. https://doi.org/10.1080/14043858.2015.1046640

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309. DOI: https://doi.org/10.1080/17450128.2012.752119

Popova, L. (2012). The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, *39*(4), 455-473. DOI: 10.1177/1090198111418108

Piquero, N. L., & Piquero, A. R. (2006). Control balance and exploitative corporate crime. Criminology, 44(2), 397-430. https://doi.org/10.1111/j.1745-9125.2006.00053.x

Rogers, R. W. (1975). "A protection motivation theory of the fear appeals and attitude change". *Journal of Psychology.* 91 (1): 93-114. doi:10.1080/00223980.1975.9915803

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019, May 23). Personality as a Predictor of Cybersecurity Behavior. Psychology of Popular Media Culture. Advance online publication. doi: http://dx.doi.org/10.1037/ppm000024

Stanton, N. A., Hedge, A., Brookhuis, K., Salas, E., & Hendrick, H. W. (Eds.). (2004). Handbook of human factors and ergonomics methods. CRC press. Retrieved from: https://books.google.nl/books?hl=nl&lr=&id=RApSggShPc8C&oi=fnd&pg=PP1&dq=stantnon+et+al+2004&ots=xeZmwaNWhA&sig=I_NFHW2Pjxz-61NjHnAy5M3YUnk&redir_esc=y#v=onepage&q=stantnon%20et%20al%202004&f=false

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

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412. DOI: 10.1089/cyber.2017.0028

Voors, M., Turley, T., Kontoleon, A., Bulte, E., & List, J. A. (2012). Exploring whether behavior in context-free experiments is predictive of behavior in the field: Evidence from lab and field experiments in rural Sierra Leone. Economics Letters, 114(3), 308-311. https://doi.org/10.1016/j.econlet.2011.10.016

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, *27*(5), 591-615. DOI: https://doi.org/10.1177/109019810002700506

Woon, Tan, & Low, A protection motivation theory approach to homewireless security, International Conference on Information Systems (ICIS)2005, pp. 367–380. Retrieved from: https://aisel.aisnet.org/icis2005/31

Workman M (2007) Gaining access with social engineering: an empirical study of the threat. Inf Syst Secur 16(6):315–331. https://doi.org/10.1080/ 10658980701788165

Appendix A

Cybercrime and personality

Dear participant, thank you for participating in this research. The aim of this research is to find out more about the link between personality variables and the individuals' threat appraisal and coping appraisal of cybercrime. During this study, you will get questions about yourself. Next, you will get a scenario in which you have to interact with a website. Thereafter, you will get some questions about cyber security behavior. This study will take about 20 minutes to complete.
If you are a student at the University of Twente, you will receive SONA points for finishing your participation.

Informed consentI herebly declare that I have been clearly informed about the nature and methods of the study by the researcher. I fully agree to participate in this research. At every moment of this study, I have the right to to withdraw from this research without having to give any reason. I can stop the research at any time. I have been informed that after finishing the research, all information will be anonymized and my identity that my identity will be untraceable. My personal data will not be accessed by third parties.
If I want to get more information about the outcome of the research, I can contact the researchers Rosalien Braakman (r.braakman-1@student.utwente.nl), and Iris van Sintemaartensdijk (i.vansintemaartensdijk@utwente.nl). For complains about this research please contact the Secretary of ethics committee of faculty of behavioral science of the University of Twente, Dr. L.J.M. Kamphuis-Blikman (l.j.m.blikman@utwente.nl).

- ○ I agree to participate in this study
- ○ I do not agree to participate in this study

Skip To: End of Survey If Dear participant, thank you for participating in this research. The aim of this research is to... = I do not agree to participate in this study

End of Block: Consent

Start of Block: Demographics

What is your age?

_____

What is your gender?

- ○ Male
- ○ Female
- ○ Different
- ○ Prefer not to say

What is your nationality?

- ○ Dutch
- ○ German
- ○ Different, namely _____

What is your current level of education?
If you are not a student, please pick the highest level of education that you have completed.

- ○ Primary school
- ○ High school
- ○ Bachelor's degree
- ○ Master's degree
- ○ Other: _____

This part of the survey is focused on your personality, please take your time to consider each statement.
Please read each statement and decide to what extend you agree or disagree with that statement.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I would be quite bored by a visit to an art gallery.	○	○	○	○	○

I plan ahead and organize things, to avoid scrambling at the last minute.	○	○	○	○	○
I rarely hold a grudge, even against people who have badly wronged me.	○	○	○	○	○
I feel reasonably satisfied with myself overall.	○	○	○	○	○
I would feel afraid if I had to travel in bad weather conditions.	○	○	○	○	○
I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed.	○	○	○	○	○
I'm interested in learning about the history and politics of other countries.	○	○	○	○	○
I often push myself very hard when trying to achieve a goal.	○	○	○	○	○
People sometimes tell me that I am too critical of others.	○	○	○	○	○
I rarely express my opinions in group meetings.	○	○	○	○	○
I sometimes can't help worrying about little things.	○	○	○	○	○
If I knew that I could never get caught, I would be willing to steal a million dollars.	○	○	○	○	○
I would enjoy creating a work of art, such as a	○	○	○	○	○

novel, a song, or a painting.					
When working on something, I don't pay much attention to small details.	○	○	○	○	○
People sometimes tell me that I'm too stubborn.	○	○	○	○	○
I prefer jobs that involve active social interaction to those that involve working alone.	○	○	○	○	○
When I suffer from a painful experience, I need someone to make me feel comfortable.	○	○	○	○	○
Having a lot of money is not especially important to me.	○	○	○	○	○
I think that paying attention to radical ideas is a waste of time.	○	○	○	○	○
I make decisions based on the feeling of the moment rather than on careful thought.	○	○	○	○	○
People think of me as someone who has a quick temper.	○	○	○	○	○
On most days, I feel cheerful and optimistic.	○	○	○	○	○
I feel like crying when I see other people crying.	○	○	○	○	○
I think that I am entitled to more respect than the average person is.	○	○	○	○	○

If I had the opportunity, I would like to attend a classical music concert.	○	○	○	○	○
When working, I sometimes have difficulties due to being disorganized.	○	○	○	○	○
My attitude toward people who have treated me badly is “forgive and forget”.	○	○	○	○	○
I feel that I am an unpopular person.	○	○	○	○	○
When it comes to physical danger, I am very fearful.	○	○	○	○	○
If I want something from someone, I will laugh at that person's worst jokes.	○	○	○	○	○
I’ve never really enjoyed looking through an encyclopedia.	○	○	○	○	○
I do only the minimum amount of work needed to get by.	○				
I tend to be lenient in judging other people.	○	○	○	○	○
In social situations, I’m usually the one who makes the first move.	○	○	○	○	○
I worry a lot less than most people do.	○	○	○	○	○
I would never accept a bribe,	○	○	○	○	○

even if it were very large.					
People have often told me that I have a good imagination.	○	○	○	○	○
I always try to be accurate in my work, even at the expense of time.	○	○	○	○	○
I am usually quite flexible in my opinions when people disagree with me.	○	○	○	○	○
The first thing that I always do in a new place is to make friends.	○	○	○	○	○
I can handle difficult situations without needing emotional support from anyone else.	○	○	○	○	○
I would get a lot of pleasure from owning expensive luxury goods.	○	○	○	○	○
I like people who have unconventional views.	○	○	○	○	○
I make a lot of mistakes because I don't think before I act.	○	○	○	○	○
Most people tend to get angry more quickly than I do.	○	○	○	○	○
Most people are more upbeat and dynamic than I generally am.	○	○	○	○	○
I feel strong emotions when someone close	○	○	○	○	○

to me is going away for a long time.					
I want people to know that I am an important person of high status.	○	○	○	○	○
I don't think of myself as the artistic or creative type.	○	○	○	○	○
People often call me a perfectionist.	○	○	○	○	○
Even when people make a lot of mistakes, I rarely say anything negative.	○	○	○	○	○
I sometimes feel that I am a worthless person.	○	○	○	○	○
Even in an emergency I wouldn't feel like panicking.	○	○	○	○	○
I wouldn't pretend to like someone just to get that person to do favors for me.	○	○	○	○	○
I find it boring to discuss philosophy.	○	○	○	○	○
I prefer to do whatever comes to mind, rather than stick to a plan.	○	○	○	○	○
When people tell me that I'm wrong, my first reaction is to argue with them.	○	○	○	○	○
When I'm in a group of people, I'm often the one who speaks on behalf of the group.	○	○	○	○	○

I remain unemotional even in situations where most people get very sentimental.	○	○	○	○	○
I'd be tempted to use counterfeit money, if I were sure I could get away with it.	○	○	○	○	○

How would you rate...

	very bad	moderately bad	somewhat bad	neither good nor bad	somewhat good	moderately good	very good
your knowledge about cybercrime	○	○	○	○	○	○	○

Scenario: Imagine that you are navigating to an online banking website to make an account to be able to transfer money to a friend and you receive this notification.

Scenario: Imagine that you are navigating to an online banking website to make an account to be able to transfer money to a friend and you receive this notification.

Scenario: Imagine that you are navigating to an online banking website to make an account to be able to transfer money to a friend and you receive this notification.

Scenario: When you open your internet browser, you get the question if you want to connect to a VPN connection.

Do you want to use a VPN connection?

- ○ Yes
- ○ No

Scenario:
You need to create a password for your account on this website.
Please create a password:***DO NOT USE YOUR OWN PASSWORDS.***
Please pretend to be in a daily life situation and make a serious password.

_____

How long after making your account do you want to change your password for this website?

I want to change my password after...

- ○ 0 - 6 months
- ○ 7 - 12 months
- ○ 13 - 18 months
- ○ 19 - 24 months
- ○ Longer than 24 months

Scenario:
You get a notification that you need to update the application that you use.

Do you want to install the update directly?

- ○ Yes
- ○ No

Scenario:*You want to send an email to your friend. You need to create a new account on this website. Create a password for this website.*
Please pretend to be in a daily life situation and make a serious password.

_____

Scenario: After you sent the email to your friend you are done.

When you leave your mailbox, do you want to log out?

- ○ Yes
- ○ No

This part of the survey is focused on how you perceive cybercrime and how capable you feel protecting yourself against cybercrime by performing different behaviors.
How do you feel about using VPN connection?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable using a VPN connection on my own.	○	○	○	○	○	○	○
If I wanted to, I could easily use VPN connection on my own.	○	○	○	○	○	○	○
I would be able to make use of a VPN	○	○	○	○	○	○	○

connection even if there was no one around to help me.							
Complying with the use of a VPN connection reduces the security threat to my personal information .	○	○	○	○	○	○	○
If I comply with using a VPN connection, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with using a VPN connection would help to reduce security problems with my own personal data.	○	○	○	○	○	○	○
Not using a VPN connection would be a serious problem for me.	○	○	○	○	○	○	○
If I will not use a VPN connection, there would be serious information security problems for me.	○	○	○	○	○	○	○

I could be subjected to an information security threat, if I will not use a VPN connection.	○	○	○	○	○	○	○
An information security problem could occur if I will not use a VPN connection.	○	○	○	○	○	○	○

How would you feel about using a strong password?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable using a strong password on my own.	○	○	○	○	○	○	○
If I wanted to, I could easily use a strong password on my own.	○	○	○	○	○	○	○
I would be able to make use of a strong password even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with the use of a strong password reduces the security threat to my personal information .	○	○	○	○	○	○	○

If I comply with using a strong password, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with using strong password connection would help to reduce security problems with my own personal data.	○	○	○	○	○	○	○
Not using a strong password would be a serious problem for me.	○	○	○	○	○	○	○
If I will not use a strong password, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not use a strong password.	○	○	○	○	○	○	○
An information security problem could occur if I will not	○	○	○	○	○	○	○

use a strong password.							

How do you feel about logging out?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable to log out on my own.	○	○	○	○	○	○	○
If I wanted to, I could easily log out on my own.	○	○	○	○	○	○	○
I would be able to log out even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with logging out reduces the security threat to my personal information .	○	○	○	○	○	○	○
If I comply with logging out, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with logging out would help to reduce security problems with my own personal data.	○	○	○	○	○	○	○
Not logging out would be a serious	○	○	○	○	○	○	○

problem for me.							
If I will not log out, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not log out.	○	○	○	○	○	○	○
An information security problem could occur if I will not log out	○	○	○	○	○	○	○

How do you feel about using different passwords?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable using different passwords on my own	○	○	○	○	○	○	○
If I wanted to, I could easily use different passwords on my own.	○	○	○	○	○	○	○
I would be able to use different passwords even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with using different	○	○	○	○	○	○	○

passwords reduces the security threat to my personal information .							
If I comply with using different passwords, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with using different passwords would help to reduce security problems with my own personal data.	○	○	○	○	○	○	○
Not using different passwords would be a serious problem for me.	○	○	○	○	○	○	○
If I will not use different passwords, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not use different passwords.	○	○	○	○	○	○	○

An information security problem could occur if I will not use different passwords.	○	○	○	○	○	○	○

How do you feel about directly updating your software?	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable to directly execute updates on my own.	○	○	○	○	○	○	○
If I wanted to, I could easily execute updates directly on my own.	○	○	○	○	○	○	○
I would be able to directly execute updates, even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with directly executing updates reduces the security threat to my personal information.	○	○	○	○	○	○	○
If I comply with directly executing updates, my mobile device related security	○	○	○	○	○	○	○

problems will be scarce.							
Compliance with directly executing updated would help to reduce security problems with my own personal data.	○	○	○	○	○	○	○
Not directly executing updates would be a serious problem for me.	○	○	○	○	○	○	○
If I will not directly execute updates, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not directly execute updates.	○	○	○	○	○	○	○
An information security problem could occur if I will not directly execute updates.	○	○	○	○	○	○	○

How do you feel about using a password manager?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable using a password manager on my own.	○	○	○	○	○	○	○
If i wanted to, I could easily use a password manager on my own.	○	○	○	○	○	○	○
I would be able to make use of a password manager even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with the use of a password manager reduces the security threat to my personal information.	○	○	○	○	○	○	○
If i comply with using a password manager, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with using a password	○	○	○	○	○	○	○

manager would help to reduce security problems with my own personal data.							
Not using a password manager would be a serious problem for me.	○	○	○	○	○	○	○
If I will not use a password manager, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not use a password manager.	○	○	○	○	○	○	○
An information security problem could occur if I will not use a password manager.	○	○	○	○	○	○	○

How do you feel about changing your password?

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I would feel comfortable to change my passwords every six months my own.	○	○	○	○	○	○	○

If I wanted to, I could easily change my passwords every six months on my own.	○	○	○	○	○	○	○
I would be able to change my passwords every six months even if there was no one around to help me.	○	○	○	○	○	○	○
Complying with changing my passwords every six months reduces the security threat to my personal information.	○	○	○	○	○	○	○
If I comply with changing my passwords every six months, my mobile device related security problems will be scarce.	○	○	○	○	○	○	○
Compliance with changing my passwords every six months would help to reduce security	○	○	○	○	○	○	○

problems with my own personal data.							
Not changing my passwords every six months would be a serious problem for me.	○	○	○	○	○	○	○
If I will not change my passwords every six months, there would be serious information security problems for me.	○	○	○	○	○	○	○
I could be subjected to an information security threat, if I will not change my passwords every six months.	○	○	○	○	○	○	○
An information security problem could occur if I will not change my passwords every six months.	○	○	○	○	○	○	○

After completing this study, I intend to…

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
Use a VPN connection	○	○	○	○	○	○	○

Use strong passwords	○	○	○	○	○	○	○
Log out after using a site	○	○	○	○	○	○	○
Use a different password for different websites.	○	○	○	○	○	○	○
Instal updates directly.	○	○	○	○	○	○	○
Use a password manager.	○	○	○	○	○	○	○
Change my passwords every six months	○	○	○	○	○	○	○

Thank you for participating in this research!

The aim of this study is to discover the influence of different notifications on participants perception of cybercrime and their cybersecurity behavior.
This study also aims at detecting a potential link between different personality traits and cybersecurity behavior.

In this study you have been put in one of three conditions. The three conditions contained either a coping-appeal, a threat-appeal, or a combined-appeal. These notifications were supposed to have an influence on your cybersecurity behavior and on your cybercrime perception.
Expected was that participants in the combined-appeal group would have a better cybercrime perception and cybersecurity behavior compared to the other two conditions.

If you have questions or remarks about the study, please send an email to:
r.braakman-1@student.utwente.nl