University of Twente
BSc. Psychology
Bachelor Thesis – Conflict, Risk and Safety
Faculty of Behavioural, Management and Social Sciences
Assistent Dr. Iris van Sintemaartensdijk
Dr. Peter W. de Vries

Risk perception towards Cybercrime among Students in the Netherlands.

The effect of multiple factors on Risk Perception.

Finished: 21.01.2021

Samantha van Seijen

S1974122

COVID-19 Disclaimer

This study was executed during the COVID-19 pandemic, which lead to adjustments for planning the data collection method. The study design had to be conducted remotely, to comply with social distancing measures, which is why personal contact between the researchers and the participants was not possible.

Contents

Abstract

The internet has an integral part of daily life and its increasing more every day. Although the internet has brought many benefits, it has also brought many risks with it. It has given criminals new opportunities to commit crimes. These crimes are called cybercrime, in which the internet is used for facilitating traditional crimes or for crimes that cannot exist without the internet. Individuals who use the internet frequently are most at risk of becoming a victim of cybercrime, but mostly do not know the risks associated with the internet. This phenomenon is called risk perception, which has many factors that could influence the risk perception of individuals.

The main goal of this study was to see whether there was an association between multiple factors and risk perception of students in the Netherlands. This was tested through an online survey that was distributed through Social Media and Sona Systems. The factors studied were demographics, personality, previous experience and vulnerability. In total 63 students participated in the online study. Results indicated that there was a significant association between the personality trait Conscientiousness and risk perception. However, no significant associations were found for the other factors.

The results suggest that there is an association between the personality trait Conscientiousness and risk perception. On this basis, the personality trait Conscientiousness should be taken into account when trying to adjust the risk perception of students in the Netherlands.

Introduction

The internet has become an integral part of everyday life in society and is becoming more important by the day. However, the internet has brought also a multitude of potential risks for people using the internet. According to Holt and Bossler (2016), the internet has changed all aspects of human life, which includes the way people communicate, shop, bank, entertain themselves and obtain the news. In the Netherlands, the majority of the population has access to the internet (96% of households in 2019) and uses the internet every day. In 2019, 87.4 per cent of the Dutch population was active on social media, almost 12 million people shopped online and 84 per cent used online banking (CBS, 2020). According to CBS (2020), the Netherlands was at the top of the European ranking for internet access at home in 2019. Although there are many benefits, the internet also created potential opportunities for criminals to commit diverse forms of crime.

These forms of crime are also called cybercrime. According to Furnell (2002, 21) cybercrime can only occur because 'the perpetrator uses special knowledge of cyberspace'. There are many definitions of cybercrime, however there still no academic and clear definition of cybercrime. Cybercrime is often called as 'computer crime', 'electronic crime', 'hi-tech crime', 'computer-related crime', 'technology-enabled crime', 'cyberspace crime', or 'e-crime'. Therefore, Grabosky (2007) labeled three forms of cybercrime. The first form is when the computer is operated as the instrument of crime when committing crimes, in which conventional crimes can be committed through the use of digital technology. The second form is when the computer is incidental to the crime, where digital technology may have an indirect role in ordinary criminal activity. And, the third form is when the computer itself is the target of crime, in which there will be damage or interference done to information systems. Although this division of cybercrime is imperfect, it is still effective in the understanding of cybercrime. Gordon and Ford (2006) also made a classification of cybercrime. They divided cybercrime

into Type I and Type II crimes on a continuous scale. Type I offenses are crimes which are in nature more technical while Type II offenses depend on human contact instead of technology. The authors also state that *'there are likely to be very few events which are purely Type I or Type II; these types represent either end of a continuum'* (Gordon & Ford, 2006, p.16). However, due to developments in robotics and in artificial intelligence (AI), one could argue that through these developments a Type III could rise, which would be an offense that is committed by instruments capable of self-learning instead of human beings. (Sarre, Yiu-Chung Lau & Chang, 2018).

Whilst Grabosky focused on the computer in his classification of cybercrime, Gordon and Ford focused technology and human nature in their classification of cybercrime. McGuire and Dowling (2013) developed a practical classification tool, in which parts of the classification from Grabosky, Gordon and Ford can be found. McGuire and Dowling classify cybercrime into 'cyber-dependent' crime and 'cyber-enabled' crime. Cyber-dependent crimes are offenses that cannot exist without cyber technology. According to CPS (2019), cyber-dependent crimes can be divided into two main categories: *'illicit intrusions into computer networks, such as hacking; and the disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.'* (CPS, 2019). Cyber-enabled crimes are traditional crimes which are facilitated through using computers. The range of cyber-enabled crimes is endless and these crimes have always been considered as criminal activities, however through the use of the computer these crimes have become much easier to pursue. According to Holt and Bosseler (2014), the difference between cyber-dependent and cyber- crime is that for cyber-dependent crime cyber technology not only is used for enabling crime but that cyber technology also the target is of the crime.

Although there is not much data available, the limited amount of data available shows that in the Netherlands cybercrime is becoming an urgent and serious social problem. According

to the CBS (2019), five per cent of the Dutch population who uses the internet became a victim of one or more cybercrimes in 2018 and the costs of these cybercrimes were estimated around 10 billion euros.

Because cybercrime is becoming an urgent and serious problem in the Netherlands, one can expect that the number of cybercrime victims will increase in the future. Therefore, it is important to gain the knowledge about the different factors that can lead to an increased or decreased likelihood of becoming a cybercrime victim. There are multiple factors related to a increased or decreased likelihood of becoming a victim such as, self-control and personality. According to the general theory of crime from Gottfredson and Hirshi (1990), individuals who have lower self-control are more risk-taking, shortsighted, impulsive, insensitive to other individuals and seek more easy and immediate gratification. These individuals will therefore be more likely be involved with criminal behaviour. Schreck (1999) argues that the general theory of crime can also be used to predict criminal victimization, because absence of preventive behaviour as a result of risk-taking and shortsightedness can make an individual more vulnerable to be victimized. According to Holtfreter, Reisig and Pratt (2008), low self-control is explicitly a risk factor for cybercrime because a degree of cooperation from the victim is needed for the criminal to be successful. It has been shown that an individual has an increased risk of becoming a victim of some types of cybercrime when having lower levels of self-control (van Wilsem, 2011; Ngo & Paternoster, 2011; Bossler & Holt, 2010). Also, Jones, Miller and Lynam (2011) argues that the personality traits agreeableness, emotional stability and conscientiousness from the Big Five personality traits apprehend many elements of self-control as it is identified in the general theory of crime from Gottfredson and Hirschi. It has also been empirically shown by Van Gelder and De Vries (2012) that there is an overlap between agreeableness and conscientiousness and self-control. Research has also shown that individuals

who scored higher to openness to experience, had higher odds of becoming a victim of cyber-dependent crimes, but not of cyber-enabled crimes (Van De Weijer & Leukfeldt, 2017).

Moreover, individuals who use the internet frequently are most at risk of becoming a victim of cybercrime, but are less likely aware of the different risks that are associated with the internet and digital technology (Hargittai & Hinnant, 2008; Friemel, 2016; Riek, Böhme & Moore, 2016).This is also called risk perception and it is an important factor in studying cybercrime victimization. According to Misana-ter Huurne, van Houten, Spithoven, Notté and Leukfeldt (2020), individuals that do not perceive a high risk, will not carry out preventive measures and will therefore be at risk of becoming victims of cybercrime. Also, according to the 'optimistic bias' theory (Weinstein, 1989) or the 'third-person perception' theory (Sun, Pan & Shen, 2008), individuals tend to assess risks in a self-centered way in which individuals tend to underestimate their susceptibility for risks, while overestimating the susceptibility of others. Research has shown that optimistic bias also occurs when assessing online risks (Rhee et al., 2005). According to Misana-ter Huurne et al. (2020), it is important to view optimistic bias as a part of risk perception, because it can cause behaviour that is unsafe, which is caused by an unrealistic personal risk perception. Furthermore, research has shown that previous experience with crime can lead to an increased level of risk perception in individuals (Visser, Scholte & Scheepers, 2013).

According to Bidgoli, Knijnenburg and Grossklags (2016), there is a group of people who are more susceptible and have a heightened risk to cybercrime: undergraduate students. They are more at risk because they have a heightened engagement with technology, social independence and recently discovered financial independence (Bidgoli et al, 2016). It was also found that these individuals profoundly rely on the media and people that they know for information about cybersecurity and cybercrime (Bidgoli et al, 2016). Since undergraduate students are profoundly at risk of cybercrime victimization, it is useful to study this group of

individuals to prevent crime. Therefore, this study will focus on students in the Netherlands from different education levels. Also, it has been shown that risk perception, self-control and personality are important factors regarding victimization of cybercrime. Therefore, the research question is this research will be 'What is the risk perception of students in the Netherlands towards cybercrime?'. This research question will be divided into six sub-questions. The first sub-question is 'is there a difference in risk perception regarding age?', for which the hypothesis is that there is a difference in risk perception regarding age. The second sub-question is 'is there a difference in risk perception regarding education levels?', for which the hypothesis is that there is a difference in risk perception regarding education levels. The third sub-question is 'is there a difference in risk perception between males and females?', for which the hypothesis is that there is a difference between males and females. The fourth sub-question is 'is there a relation between risk perception and personality?', for which the hypothesis is that there is a relation between risk perception and personality. The fifth sub-question is 'does previous experience with cybercrime have an effect on risk perception?', for which the hypothesis is that previous experience with cybercrime has an effect on risk perception. The last sub-question is 'is there a relation between vulnerability and risk perception?', for which the hypothesis is that there is a relation between vulnerability and risk perception.

Methods

Design

A correlational design was conducted in the study in which the independent variable was called 'Students'. This variable had three levels, namely 'University', 'University of Applied Sciences' and 'Intermediate Vocational Education'. The dependent variables that were related to the independent variable were 'Personality', 'Experience', 'Vulnerability', 'Risk Perception', 'Knowledge' and 'Subjective Norms and Motivation to Comply'.

Participants

The research was based on a convenience sample in which 79 individuals participated. These participants were partly reached through an online platform for University students called SONA. The participants were, also, partly reached through social media, such as Facebook, Instagram and WhatsApp by distributing an anonymous link leading to the questionnaire. Table 1 (see appendix B) shows the demographic descriptive statistics of the participants in this research. As seen in the table, participants in this study had different nationalities (Dutch: n = 28; German: n = 28; Other nationality: n = 7; Unknown: n = 16) and their age ranged between 18 to 45 years (M=21.27; SD=4.15). Furthermore, 15 participants were male, 45 participants were female and 3 participants categorized themselves as other. In addition, there were profoundly more female participants (n = 45) in this study compared to participants that identified as men (n = 15) or other (n = 3). Furthermore, there were more participants with university as their current level of education (n = 44) compared to the participants with university of applied sciences (n = 13) and intermediate vocational education (n = 6) as their current level of education. For both groups ‘male’ and ‘female’, the majority of the participants have university as their current level of education. However, in the group ‘other’, there were more participants with university of applied sciences as their current level of education.

To form the final dataset before analysis, participants that did not meet the inclusion criteria were filtered out, meaning that the participants had to be 18 years of age or older. Furthermore, if the participants showed unusual or extreme outliers, they would be marked as outliers and excluded from the final dataset. These different steps ensure that the results were not distorted and that only responses that were valid were included. 79 individuals participated in the study. However, the responses of 15 participants were not fully filled in. Only the agreement to the consent form was recorded from these participants. In addition, one participant did not agree with the consent form, but still filled out the questionnaire. This participant and

the data belonging to this participants were excluded. A total of sixteen participants were excluded. Therefore, the final dataset was reduced to 63 participants.

All individuals that participated in this study were given an informed consent form, which had to be signed in order to participate. In addition, it was made clear to the participants that they could withdraw at any time from the study. An ethical approval was granted for this study by the BMS Ethics Committee of the University of Twente.

Materials

An online questionnaire was used in this study, after participants filled in the consent form. The questionnaire consisted out of 30 question which consisted of multiple scales. The first four questions were demographic questions, which were age, nationality, gender and education level. These questions were followed by the scale 'personality'.

Hexaco-60 questionnaire

The HEXACO-60 was used to measure personality and consists of 60 questions, in which a five-point Likert Scale was used for answering these questions. (See Appendix A). This is a shortened version of the HEXACO Personality Inventory-Revised (Ashton & Lee, 2008; Lee & Ashton, 2004, 2006). The Cronbach's α for this scale ranged between .73 to .80, which indicates that the variable measured showed good reliability. According to Ashton and Lee (2009), this inventory should be used when the administration time is limited. They also stated that '*Correlations of the HEXACO–60 scales with measures of the Big Five factors were consistent with theoretical expectations, and convergent correlations between self-reports and observer reports on the HEXACO–60 scales were high, averaging above .50.'* (Ashton & Lee, 2009).

Cyberweerbaarheid questionnaire

The second scale was taken from Misana-ter Huurne et al. (2020), which is about previous experience with cybercrime. This scale was used to measure whether previous experience with cybercrime has an effect on risk perception. This scale consisted of three questions. The first question is *'Did you become a victim of cybercrime yourself in the last 12 months?'*, in which the participants were able to answer *'yes'*, *'no'* or *'I do not know'*. When answering yes to this question, two questions followed: *'When answered yes, what impact did this have for you personally?'* and *'When answered yes, did becoming a victim of cybercrime made you change your behaviour?'*. For the last question, two answers were possible: *'When yes, how?'* And *'When no, why not?'* (See Appendix A).

The third scale was also adopted from Misana-ter Huurne et al. (2020), which is about measuring personal risk perception and general risk perception of individuals. This scale consisted of three questions, in which a six-point Likert Scale was used for answering two questions and a five-point Likert Scale for one question. The first question was *'How big do you estimate your chances of becoming a victim of ... yourself in the next 12 months?'*, which was divided into becoming a victim of cybercrime and becoming a victim of phishing and had a Cronbach's α of .83. This indicates that the variable measured showed good reliability. The participants were given 6 options to choose from: *'no chance'*, *'very small chance'*, *'small chance'*, *'neutral'*, *'big chance'* and *'very big chance'*. Another question was *'How big do you estimate the chance that an average resident of the Netherlands will fall victim to ... in the next twelve months?'*, which was, also, divided into fall victim to cybercrime and fall victim to phishing. This question had a Cronbach's α of .91, which indicates that the variable measured showed good reliability. Participants were also able to choose *'no chance'* till *'very big chance'* in this question. The last question in this scale was the statement *'If I become a victim of ..., then it does serious damage to me.'*, this question was divided into become a victim of

cybercrime and become a victim of phishing and had a Cronbach's α of .86, which indicates that the variable measured showed good reliability. Participants were able to choose between five options: *'completely disagree'*, *'disagree'*, *'neutral'*, *'agree'* and *'completely agree'* (See Appendix A).

The fourth scale 'self-efficacy' was also adopted from Misana-ter Huurne et al. (2020) and consisted out of four statements, in which a five-point Likert Scale was used for answering. The Cronbach's α of this scale was .83, which indicates that the variable measured showed good reliability. The four statements were: *'I know how to protect myself from cybercrime'*; *'I know what risks I run of becoming a victim of cybercrime'*; *'I know how I can recognize (an attempt at) cybercrime'*; and *'I know what to do when I become a victim of cybercrime'*. The five options for answering these statements were: *'not at all'*, *'a little'*, *'somewhat'*, *'largely'* and *'completely'* (See Appendix A) This scale was used to study the self-efficacy of the students participating.

The fifth scale 'behavioural effectiveness' from Misana-ter Huurne et al. (2020) consisted of two statements, in which a five-point Likert Scale was used for answering. The two statements were: *'I think that I protect myself sufficiently against cybercrime'* and *'The measures I have taken ensure that I have less chance of becoming a victim of cybercrime'*. These questions had a strong correlation (r=.67). The five options for answering were: *'completely disagree'*, *'disagree'*, *'neutral'*, *'agree'* and *'completely agree'* (See Appendix A).

The sixth scale 'subjective norms & motivation to comply' also from Misana-ter Huurne et al. (2020) consisted of four statements, in which a five-point Likert Scale was used for answering. The four statements were: *'People in my area believe it is important that I protect myself against cybercrime'*; *'People in my area expect that I protect myself against cybercrime'*; *'I tend to protect myself because other do too'*; and *'I tend to protect myself because people around me expect that'*. The Cronbach's α for this scale is .78, which indicates

that the variable measured showed good reliability. For answering these statements, five options were given, in which the participants were able to answer from *'completely disagree'* till *'completely agree'* (See Appendix A). This scale was used to measure the social influence of the participants.

The seventh scale '(intentions for) self-protective behaviour was also adopted from Misana-ter Huurne et al. (2020). This scale consisted of three questions. This scale was used for gathering information from the students. The first question in this scale was *'Do you intend to take additional preparatory or self-protective measures against cybercrime in the future?'*, in which participants were able to answer *'definitely not'*, *'probably not'*, *'probably yes'* and *'definitely yes'*. This question was followed by an open question asking participants *'If so, what additional preparatory or self-protective measures do you intend to take against cybercrime? If not, why not?'*. The third question consisted of 24 statements (See Appendix A), in which the options for answering were *'completely disagree'* till *'completely agree'*. This scale was used for gathering information from the participants.

The eighth scale 'need for information' was also adopted from Misana-ter Huurne et al. (2020), which consisted of four questions. This scale was used to study whether students had a need for information about cybercrime. The first question was *'Do you need more information about the risks of cybercrime and how to protect yourself against it?'*, in which participants were able to answer *'yes'*, *'no'* and *'I do not know'*. If participants answered yes to this question, two open questions followed, which were *'What information do you need?'* and *'How and from whom would you like to get this information?'*. The last question *'Do you intend to search for this information yourself?'* also followed, when participants answered yes to the first question, in which the participants were able to answer *'yes'*, *'no'* and *'I do not know'* (See Appendix A).

The nineth scale 'vulnerability' was also adopted from Misana-ter Huurne et al. (2020), which consisted of six statements: *'I quickly react anxiously to situations'*; *'Other people are*

more likely to be victims of cybercrime than me'; *'I would rather not think about the likelihood of becoming a victim of cybercrime myself'*; *'I am personally responsible for preventing cybercrime victimization'*; *'I usually assume the worst'*; and *'There is no point in worrying about cybercrime, if perpetrators want to victimize you, they will succeed anyway'.* The Cronbach's α was .73, which indicates that the variable measured showed good reliability. This scale was used to measure the vulnerability of the participants. Participants were able to answer these statements using a five-point Likert Scale, in which they were able to answer 'completely disagree' till 'completely agree' (See Appendix A).

The last scale 'online activity' was also taken from Misana-ter Huurne et al. (2020), which consisted of two questions. The first question *'How long do you use the internet per day for private purposes?'* was an open question, in which participants had to answer in hours. The second question was *'What are you online for?'*, in which participants had to cross the different options that were given (See Appendix A) This scale was used for gathering information from the participants.

Procedure

The experiment started with the informed consent form informing them about the content of the study, the voluntariness of participation and that it was possible to withdraw from the experiment at any time. In addition, the consent form also ensured that all data from the participants would be treated with confidentiality. The first questions of the questionnaire contained demographic questions (age, gender, nationality, education level). These questions were followed by questions about personality, in which the participants had to choose to what extent they agreed with the statements. After these questions, participants were asked whether they had already been a victim of cybercrime. When answering yes to the question, they were asked what happened, what impact it had and if they changed their online behaviour. These questions were followed by questions about personal risk perception and general risk

perception, in which the participants had to estimate their chances of becoming a victim of cybercrime and the chances of an average resident of the Netherlands of becoming a victim. After these questions, participants were asked to fill out questions about self-efficacy, behavioural effectiveness, subjective norms and motivation to comply to these norms, in which they had to answer to what extent they agreed with statements. These questions were followed by questions about (intentions for) self-protective behaviour. The participants were asked whether they intend to take self-protective measures against cybercrime with explaining why they intend to do it or why not. After this question, different options for countering the risk of possible victimization of cybercrime were given. Participants were asked to fill out to what extent they were already using these options. This question was followed by questions about the need for information about the risks of cybercrime and how to protect yourself against it. After this question, participants had to fill out a question measuring vulnerability in which participants had to answer to what extent they agreed with the statements. This question was followed by the last question of the questionnaire, which was about the participants their online activity. After the final question, participants were thanked and fully debriefed. The experiment took approximately 15-20 minutes to complete.

Results

Risk perception

Table 2 (see appendix B) shows the descriptive statistics of the personal risk perception of the participants. It shows that the mean of the estimate of becoming a victim of cybercrime yourself (M=2.84; SD=0.88) is the same as the estimate of becoming a victim of phishing yourself (M=2.84; SD=1.181). However, there is a higher standard deviation in the group of the estimate of becoming a victim of phishing. This indicates that the data points of the estimate of

becoming a victim of phishing are spread out, and that the data points of the estimate of becoming a victim of cybercrime are more close to the mean.

Furthermore, table 2 shows the descriptive statistics of the general risk perception of participants. It shows that the estimate of an average resident of the Netherlands becoming a victim of cybercrime (*M*=4.13; *SD*=0.92) has a slightly lower mean compared to the estimate of an average resident of the Netherlands becoming victim of phishing (*M*=4.17; *SD*=0.99). It, also, shows that participants have higher means in the general risk perception (*M*=4.13; *M*=4.17) compared to personal risk perception (*M*=2.84; *M*=2.84), which indicates that the participants estimate their own chances of becoming a victim of cybercrime lower than the chances of an average Dutch resident.

Demographics and Risk perception

To analyze if there is an association between demographics and risk perception, one-way ANOVA was used. Table 3 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant association between the age of participants and risk perception. It shows that for the estimate chances of becoming a victim of cybercrime ($p = 0.62$) or phishing ($p = 0.49$) there is no significant difference between the different ages. It, also, shows that for the effect cybercrime ($p = 0.17$) or phishing ($p = 0.23$) would have on the participants there is no significant association with age.

Table 4 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference ($p < .05$) between the gender of participants and risk perception. It shows that there are no significant differences between the gender of participants and risk perception.

Table 5 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference between the level of education of participants and risk

perception. It shows that there are no significant differences between the gender of participants and risk perception.

Personality

The descriptive statistics of personality show that the female participants have a higher mean in Honesty-Humility (*M*=3.57; *SD*=0.60), Emotionality (*M*=3.70; *SD*=0.64), Conscientiousness (*M*=3.65; *SD*=0.59), and Openness to Experience (*M*=3.69; *SD*=0.55) than the male participants. However, male participants have a higher mean in Extraversion (*M*=3.57; *SD*=0.46), and Agreeableness (*M*=3.01; *SD*=0.66)

Personality and Risk perception

Table 6 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference ($p < .05$) between the six personality domains and the variable 'Estimate chances becoming a victim of cybercrime'. It shows that there is no significant relation between all six personality domains and the variable 'Estimate chances becoming a victim of cybercrime'.

Table 7 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference ($p < .05$) between the six personality domains and the variable 'Estimate chances becoming a victim of phishing'. It shows that there are no significant differences between all six personality domains and the variable 'Estimate chances becoming a victim of phishing'.

Table 8 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference between the six personality domains and the variable 'Effect of Cybercrime. The variable 'Effect of Cybercrime' means the effect of becoming a victim of cybercrime will have on the participants. It shows that there is a significant difference between the variable 'Effect of Cybercrime' and the personality domain Conscientiousness

(p = 0.03). The effect size between Conscientiousness and 'Effect of Cybercrime' is small (η_p^2 = 0.16). There were no significant differences found between the other five personality domains and the variable 'Effect of Cybercrime'.

Table 9 shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference ($p < .05$) between the six personality domains and the variable 'Effect of Phishing. The variable 'Effect of Phishing' means the effect of becoming a victim of phishing will have on the participants. It shows that there is a significant difference between the variable 'Effect of Phishing' and the personality domain Conscientiousness (p = 0.01). The effect size between Conscientiousness and 'Effect of Phishing' is small (η_p^2= 0.22). There were no significant differences found between the other five personality domains and the variable Effect of Phishing.

Previous Experience and Risk perception

The descriptive statistics of the risk perception of participants that have previous experience with cybercrime shows that the estimate chances of becoming a victim of cybercrime (*M*=2.67; *SD*=0.58) and phishing (*M*=2.67; *SD*=0.58) have the same mean. Furthermore, the effect of cybercrime (*M*=4.33; *SD*=0.58) has a higher mean than the effect of phishing (*M*=4.00; *SD*=0.00).

The descriptive statistics of the risk perception of participants who do not have previous experience with cybercrime shows that the means of the estimate chances becoming a victim of cybercrime (*M*=2.84; *SD*=0.90) and phishing (*M*=2.82; *SD*=1.23) of participants with no previous experience is higher than the means of the estimate chances becoming a victim of cybercrime (*M*=2.67; *SD*=0.58) and phishing (*M*=2.67; *SD*=0.58) of participants with previous experience. However, the means of the effect of cybercrime (*M*=3.60; *SD*= 0.92) and phishing (*M*=3.56; *SD*=1.00) of participants who do not have previous experience with cybercrime are

lower than the means of the effect of cybercrime (*M*=4.33; *SD*=0.58) and phishing (*M*=4.00; *SD*=0.00) of participants with previous experience.

Table 10 (see appendix B) shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference between personal risk perception and participants who have previous experience with cybercrime. It shows that there are no significant differences between all four parts of personal risk perception and previous experience.

Vulnerability and Risk Perception

Table 11 shows the one-way ANOVA statistics in which it is possible to see if there is a significant difference between personal risk perception and the level of vulnerability of participants. It shows that there are no significant differences between all four parts of personal risk perception and the level of vulnerability of participants.

Discussion

This research focused on the risk perception of students in the Netherlands towards cybercrime. The internet is becoming a more integral part in society its daily life every day. However, this also brings a multitude of risks with it. Therefore, it is important to study how individuals estimate their chances of becoming a victim of cybercrime. In addition, it is important to map the different factors that can influence the risk perception of individuals.

The results showed that there is a significant relation between the personality domain Conscientiousness and the effect cybercrime or phishing will have on the participants. Further, no significant relations were found between personality or previous experience or vulnerability or demographics and risk perception.

Personal and General risk perception

To answer the research question of what the risk perception of students in the Netherlands is towards cybercrime, mean scores of the personal risk perception were compared to the mean scores of the general risk perception. Participants had a lower personal risk perception compared to general risk perception. This means that the participants estimated their own chances of becoming a victim of cybercrime lower than the average Dutch resident. This effect can be explained through the 'optimistic bias' theory (Weinstein, 1989) or the 'third-person perception' theory (Sun, Pan & Shen, 2008), as both theories explain that individuals tend to assess risks in a self-centered way in which they underestimate their susceptibility for risks while overestimating the susceptibility of other individuals. This could lead to students underestimating the risks of becoming a victim of cybercrime, which in turn could lead to a higher risk of becoming a victim of cybercrime.

Personality and Risk Perception

Moreover, this research also focused on the different factors that could influence the risk perception of individuals, such as personality. For measuring personality of participants, the HEXACO-60 was used, in which personality has been divided into six domains: Honesty-Humility, Emotionality, Extraversion, Agreeableness, Conscientiousness and Openness to Experience . The results showed that there were no significant associations between all six personality domains and personal or general risk perception. This indicates that personality does not influence the personal or general risk perception of students. However, a significant association was found between the effect of cybercrime or phishing and the personality domain conscientiousness. The personality trait conscientiousness is associated with participants' estimate of the effect cybercrime or phishing will have on them. According to Lee and Ashton (2004), individuals who score high on conscientiousness tend to check carefully for mistakes and consider their options carefully and they tend to be cautious. This can explain the relation

between conscientiousness and the effect of cybercrime or phishing. As these individuals are careful and tend to be cautious it can be expected that cybercrime or phishing will have a greater effect on them. Although a small effect was found, it is a reasonable effect size due to not having a large sample size.

Demographics and Risk Perception

Furthermore, there were no significant relations found between demographic features (gender, age, level of education) of participants and risk perception. This means there is no association between gender, age or level of education and risk perception. However, previous research has shown that there was a relation between gender and risk perception. According to Misana-ter Huurne et al. (2020), males tend to estimate their chances of becoming a victim of cybercrime lower than females.

There was also no relation found between the demographic features of the participants and their estimate of what the effect will be when they would become a victim of cybercrime. However, according to Misana-ter Huurne et al. (2020), there is a relation between demographic features of participants and the effect cybercrime will have on themselves. This study showed that females tend to estimate the effect of becoming a victim of cybercrime higher than males. It also showed that individuals with a higher level of education tend to estimate the effect of becoming a victim of cybercrime higher than individuals with a lower level of education. This effect was not found in this study and could be explained by the low participation of individuals with the lower level of education. Since there was a low participation in this group it could have led to biased results.

Previous Experience and Risk Perception

Furthermore, previous experience with cybercrime was studied to see whether there was a difference in risk perception when having previous experience compared to no previous

experience. The results showed that the mean scores of participants who had previous experience were lower than the mean scores of participants with no previous experience with cybercrime. These participants with previous experience estimated their chances of becoming a victim of cybercrime or phishing lower compared to the other participants. It could be that the participants who had previous experience with cybercrime do not expect it to happen again, due to measures taken or other thoughts. However, the results showed that there is no significant association between previous experience with cybercrime and risk perception.

Strengths and limitations

Due to the outbreak of Covid-19, it was not possible to visit different education institutions for collecting participants from all three levels of education. As a result, there were fewer participants in the group intermediate vocational education and university of applied science than expected. This could have limited the degree to which we can be certain of the results.

Another limitation was that the survey was completely English and that there was no Dutch version. Participants needed to have a sufficient knowledge of English to fulfil the survey. It can be expected that the understanding of English is lower in the group intermediate vocational education, as it is the lowest level of education possible for students. This could be why the dropout rate was higher than expected and especially in the group intermediate vocational education, since the survey requires a good understanding of English.

While this approach in the study could have led to decreased opportunities to partake in this study and could have led to a higher dropout rate, there are strengths as well. Participants were able to partake in this study online while staying at home, which reduced the effort and time needed to participate in this research.

Another strength of this study is that multiple factors that could influence the risk perception of students was researched, instead of one factor. Through researching multiple factors, effort and time were reduced in this study.

Recommendations

Based on the results in this study, future research should focus on the relation between personality and risk perception, and more specifically on the relation between conscientiousness and risk perception, since a significant association was found in this study. Through researching this relation, it could be possible to reduce cybercrime victimization among students in the future. Additionally, a larger sample size or different groups would be interesting.

Conclusion

This study was aimed at examining the risk perception of students and the different factors that could influence risk perception. Although there were not many associations found between factors that could influence risk perception and risk perception, it was found that there is a significant association between the personality trait Conscientiousness and the effect cybercrime or phishing will have on individuals. Therefore, the personality trait Conscientiousness should be taken into account when trying to adjust the risk perception of students in the Netherlands.

References

Ashton, M. C., & Lee, K. (2008). The prediction of Honesty-Humility-related criteria by the HEXACO and Five-Factor models of personality. *Journal of Research in Personality, 42*(5), 1216–1228. doi: 10.1016/j.jrp.2008.03.006

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When Cybercrimes Strike Undergraduates. ECrime Researchers Summit, ECrime, 42-51. doi: 10.1109/ECRIME.2016.7487948

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: 10.1016/j.jcrimjus.2010.03.001

CBS. (2020). *IT, kennis en economie.* The Hague: Statistics Netherlands.

CBS. (2019). *Leerlingen, deelnemers en studenten; onderwijssoort, vanaf 1900.* Retrieved from https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37220/table?ts=1580807485329

CPS. (2019). Cybercrime – prosecution guidance. Retrieved from https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Friemel, T. N. (2016). 'The Digital Divide Has Grown Old: Determinants of a Digital Divide among Seniors'. *New Media & Society, 18*(2), 313-331. doi: 10.1177/1461444814538648

Furnell, S. 2002. *Cyber Crime: Vandalizing the Information Society*. London: Addison Wesley.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of*

Computer Virology, 2(1), 13–20. doi: 10.1007/s11416-006-0015-z

Gottfredson MR, Hirschi T. (1990). *A general theory of crime.* Stanford University Press

Grabosky, P. (2007). *Electronic crime*. New Jersey. Prentice Hall.

Hargittai, E. & Hinnant, A. (2008). Digital Inequality Differences in Young Adults' Use of the Internet'. *Communication Research 35*(5), 602–621. doi: 10.1177/0093650208321782

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189–220. doi: 10.1111/j.1745-9125.2008.00101.x

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. doi: 10.1080/01639625.2013.822209

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series.* New York: Routledge.

Lee, K., & Ashton, M. C. (2004). Psychometric properties of the HEXACO personality inventory. *Multivariate Behavioral Research, 39*(2), 329–358. doi: 10.1207/s15327906mbr3902_8

Lee, K., & Ashton, M. C. (2006). Further assessment of the HEXACO Personality Inventory: Two new facet scales and an observer report form. *Psychological Assessment, 18*(2), 182–191. doi: 10.1037/1040-3590.18.2.182

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence: Summary of key findings and implications*. Home Office Research Report 75. London: Home Office, October.

Misana-ter Huurne, E., Y. van Houten, R. Spithoven, R.J. Notté & E.R. Leukfeldt (2020)

Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercrime onder jongeren en mkb'ers. Deventer/Den Haag: Saxion Hogeschool, De Haagse Hogeschool.

Ngo, F.T., & Paternoster, R. (2011). cybercrime victimization: an examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Rhee, Hyeun-Suk; Ryu, Young; and Kim, Cheong-Tag, "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security" (2005). *ICIS 2005 Proceedings*. Paper 32.

Riek, M., Böhme, R., & Moore, T. (2016). 'Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance'. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261–273. doi: 10.1109/TDSC.2015.2410795

Sarre, R., Yiu-Chung Lau, L., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice and Research, 19(*6), 515-518. doi: 10.1080/15614263.2018.1507888

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*(3), 633–654. doi: 10.1080/07418829900094291

Sun, Y., Pan, Z., & Shen, L. (2008). Understanding the Third-Person Perception: Evidence From a Meta-Analysis. *Journal of Communication, 58*(2), 280–300. doi: 10.1111/j.1460-2466.2008.00385.x

Van Der Weijer, S. G. A., & 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

Van Gelder, J. L., & De Vries, R. E. (2012). Traits and states: integrating personality and affect into a model of criminal decision making. *Criminology, 50*(3), 637–671. doi: 10.1111/j.1745-9125.2012.00276.x

Van Wilsem, J. A. (2011). ‘‘Bought It, but Never Got It.’’ Assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2), 168–178. doi: 10.1093/esr/jcr053

Visser, M., Scholte, M., & Scheepers, P. (2013). Fear of crime and feelings of unsafety in European countries: Macro and micro explanations in cross-national perspective. *Sociological Quarterly, 54*(2), 278–301. doi: 10.1111/tsq.12020

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science, 246*(4935), 1232-3. doi: 10.1126/science.2686031

Appendix A

Consent form

Dear respondent,

Thank you for participating in this study which is part of my bachelor thesis at the University of Twente. This study is about the risk perception of students in the Netherlands towards cybercrime. You will be given questions about cybercrime, risk perception, personality and vulnerability. It will take you about 10 minutes to complete this survey. Please answer the questions honestly; there are no right or wrong answers. You are free to stop the survey at any point of time. Only completed surveys can be used for this research. Your data will be used anonymously and only for the purpose of this study.

If you have any questions, feel free to contact me:

Samantha van Seijen: s.t.vanseijen@student.utwente.nl

Thank you in advance.

I read and understood the previous information and agree that my data will be used anonymously for scientific purposes only. I am 18 or older and I agree to take part in this study on a voluntary basis. I am aware that I can stop the study at any point of time. I want to continue with the study.

- Yes
- No

Questionnaire

1. Please indicate your age:

2. What gender do you identify as?

- Male
- Female
- Other

3. What is your nationality?

- Dutch
- German
- Other

4. Which degree of education are you studying at the moment?

- University (WO)
- University of Applied Sciences (HBO)
- Intermediate Vocational Education (MBO)

5. On the following pages, you will find a series of statements about you. Please read each statement and decide how much you agree or disagree with that statement. Please answer every statement, even if you are not completely sure of your response. (answered through a five-point Likert Scale: Strongly disagree, Disagree, Neutral, Agree, Strongly agree) (HEXACO-60)

1. I would be quite bored by a visit to an art gallery.
2. I plan ahead and organize things, to avoid scrambling at the last minute.
3. I rarely hold a grudge, even against people who have badly wronged me.
4. I feel reasonably satisfied with myself overall.
5. I would feel afraid if I had to travel in bad weather conditions.
6. I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed.

7. I'm interested in learning about the history and politics of other countries.
8. I often push myself very hard when trying to achieve a goal.
9. People sometimes tell me that I am too critical of others.
10. I rarely express my opinions in group meetings.
11. I sometimes can't help worrying about little things.
12. If I knew that I could never get caught, I would be willing to steal a million dollars.
13. I would enjoy creating a work of art, such as a novel, a song, or a painting.
14. When working on something, I don't pay much attention to small details.
15. People sometimes tell me that I'm too stubborn.
16. I prefer jobs that involve active social interaction to those that involve working alone.
17. When I suffer from a painful experience, I need someone to make me feel comfortable.
18. Having a lot of money is not especially important to me.
19. I think that paying attention to radical ideas is a waste of time.
20. I make decisions based on the feeling of the moment rather than on careful thought.
21. People think of me as someone who has a quick temper.
22. On most days, I feel cheerful and optimistic.
23. I feel like crying when I see other people crying.
24. I think that I am entitled to more respect than the average person is.
25. If I had the opportunity, I would like to attend a classical music concert.
26. When working, I sometimes have difficulties due to being disorganized.
27. My attitude toward people who have treated me badly is “forgive and forget.”
28. I feel that I am an unpopular person.
29. When it comes to physical danger, I am very fearful.
30. If I want something from someone, I will laugh at that person's worst jokes.
31. I've never really enjoyed looking through an encyclopedia.

32. I do only the minimum amount of work needed to get by.

33. I tend to be lenient in judging other people.

34. In social situations, I'm usually the one who makes the first move.

35. I worry a lot less than most people do.

36. I would never accept a bribe, even if it were very large.

37. People have often told me that I have a good imagination.

38. I always try to be accurate in my work, even at the expense of time.

39. I am usually quite flexible in my opinions when people disagree with me.

40. The first thing that I always do in a new place is to make friends.

41. I can handle difficult situations without needing emotional support from anyone else.

42. I would get a lot of pleasure from owning expensive luxury goods.

43. I like people who have unconventional views.

44. I make a lot of mistakes because I don't think before I act.

45. Most people tend to get angry more quickly than I do.

46. Most people are more upbeat and dynamic than I generally am.

47. I feel strong emotions when someone close to me is going away for a long time.

48. I want people to know that I am an important person of high status.

49. I don't think of myself as the artistic or creative type.

50. People often call me a perfectionist.

51. Even when people make a lot of mistakes, I rarely say anything negative.

52. I sometimes feel that I am a worthless person.

53. Even in an emergency I wouldn't feel like panicking.

54. I wouldn't pretend to like someone just to get that person to do favors for me.

55. I find it boring to discuss philosophy.

56. I prefer to do whatever comes to mind, rather than stick to a plan.

57. When people tell me that I'm wrong, my first reaction is to argue with them.

58. When I'm in a group of people, I'm often the one who speaks on behalf of the group.

59. I remain unemotional even in situations where most people get very sentimental.

60. I'd be tempted to use counterfeit money, if I were sure I could get away with it.

6. Did you become a victim of cybercrime yourself in the last 12 months?

- Yes
- No
- I don’t know

7. When answered yes, what impact did this have for you personally?

8. When answered yes, did becoming a victim of cybercrime made you change your online behaviour?

- When yes, how
- When no, why not

9. How big do you estimate your chances of becoming a victim of cybercrime yourself in the next 12 months?

- No chance, very small chance, small chance, neutral, big chance, very big chance

10. How big do you estimate your chances of becoming a victim of phishing yourself in the next 12 months?

- No chance, very small chance, small chance, neutral, big chance, very big chance

11. How big do you estimate your chances of becoming a victim of ransomware yourself in the next 12 months?

- No chance, very small chance, small chance, neutral, big chance, very big chance

12. How big do you estimate the chance that an average resident of the Netherlands will fall victim to cybercrime in the next twelve months?

- No chance, very small chance, small chance, neutral, big chance very big chance

13. How big do you estimate the chance that an average resident of the Netherlands will fall victim to phishing in the next twelve months?

- No chance, very small chance, small chance, neutral, big chance, very big chance

14. How big do you estimate the chance that an average resident of the Netherlands will fall victim to ransomware in the next twelve months?

- No chance, very small chance, small chance, neutral, big chance, very big chance

15. To what extent do you agree with the following statement? If i become a victim of …, then it does serious damage to me

- Cybercriminality: completely disagree, disagree, neutral, agree, completely agree
- Phishing: completely disagree, disagree, neutral, agree, completely agree

16. To what extent do you agree with the following statements? I know …

- How to protect myself from cybercrime: not at all, a little, somewhat, largely, completely
- What risks I run of becoming a victim of cybercrime: not at all, a little, somewhat, largely, completely
- How I can recognize (an attempt at) cybercrime: not at all, a little, somewhat, largely, completely
- What to do when I become a victim of cybercrime: not at all, a little, somewhat, largely, completely, no answer

17. To what extent do you agree with the following statements about your own protection against cybercrime?

- I think that I protect myself sufficiently against cybercrime: completely disagree, disagree, neutral, agree, completely agree
- The measures I have taken ensure that I have less chance of becoming a victim of cybercrime: completely disagree, disagree, neutral, agree, completely agree

18. To what extent do you agree with the following statements? People in my area …

- Believe it is important that I protect myself against cybercrime: completely disagree, disagree, neutral, agree, completely agree
- Expect that I protect myself against cybercrime: completely disagree, disagree, neutral, agree completely agree

I tend to protect myself because …

- Others do too: completely disagree, disagree, neutral, agree, completely agree
- People around me expect that: completely disagree, disagree, neutral, agree, completely agree

19. Do you intend to take additional preparatory or self-protective measures against cybercrime in the future?

- Definitely not, probably not, probably, definitely, no answer

20. If so, what additional preparatory or self-protective measures do you intend to take against cybercrime? If not, why not?

Below are a number of options for countering the risks or possible victimization of cybercrime. Please tick below what you are currently doing to protect yourself. (answered with a five-point Likert scale: completely disagree, disagree, neutral, agree, completely agree)

1. I install updates as soon as they are available.
2. I check whether the sender of an email is trustworthy.
3. When paying online I pay attention to the presence of the lock in the browser.
4. I use strong passwords with multiple numbers and characters.
5. I do not download movies, music and/or games illegally.
6. I do not have my profile sites (like facebook, instagram) public.
7. I check the privacy settings of my devices, apps or social media.
8. I am using a virus scanner.
9. I am using a firewall.
10. I use a VPN connection (Virtual Private Network).
11. I do not give my login details to strangers.
12. I delete emails that I do not trust immediately.
13. I am using double verification on my accounts.
14. I use a lock code or password on all my devices.
15. I use the same password for different applications.
16. I back up my valuable files.
17. I avoid using public wifi.
18. I avoid unsafe websites.
19. I am careful about opening attachments.
20. I look at the file type before opening attachments.
21. I am careful about clicking on links.
22. I lock my devices when i am not using them.
23. I encrypt files with a password or other security.
24. I am using a browser extension such as an adblocker.
25. Otherwise, namely

21. Do you need more information about the risks of cybercrime and how to protect yourself against it?

- Yes
- No

22. When yes, what information do you need?

23. When yes, how and from whom would you like to get this information?

24. When yes, do you intend to search for this information yourself?

- Yes
- No

25. To what extent do you agree with the following statements? (answered with a five-point Likert scale: completely disagree, disagree, neutral, agree, completely agree)

1. I quickly react anxiously to situations.
2. Other people are more likely to be victims of cybercrime than me.
3. I would rather not think about the likelihood of becoming a victim of cybercrime myself.
4. I am personally responsible for preventing cybercrime victimization.
5. I usually assume the worst.
6. There is no point in worrying about cybercrime, if perpetrators want to victimize you, they will succeed anyway.

26. How often do you use the internet for private purposes? Please choose 1 answer:

1. Less than once a month
2. At least once a month, but not weekly
3. At least once a week, but not daily
4. Daily

5. Multiple times a day
6. At least every hour (during the hours that I am awake)
7. I am (almost) continuously online (during the hours that I am awake
8. I do not know

27. What are you online for? (note: multiple answers are possible)

- Work, study, shopping, banking, relaxation, social contacts, no answer
- Otherwise, namely

Appendix B

Table 1

Demographics of the participants in the study (N=63)

		Female (n=45) n (71.4%)	Male (n=15) n (23.8%)	Other (n=3) n (4.8	Total (N=63) N (100%)
Age (mean, SD)		20.96 (3.14)	22.40 (6.56)	20.33 (1.53)	21.27 (4.15)
Nationality	Dutch	16 (35.6%)	11 (73.3%)	1 (33.3%)	28 (44.4%)
	German	23 (51.1%)	4 (26.7%)	1 (33.3%)	28 (44.4%)
	Other	6 (13.3%)	0 (0.0%)	1 (33.3%)	7 (11.1%)
Current level of education	University	37 (82.2%)	6 (40%)	1 (33.3%)	44 (69.8%)
	University of Applied Sciences	6 (13.3%)	5 (33.3%)	2 (66.7%)	13 (20.6%)
	Intermediate Vocational Education	2 (4.4%)	4 (26.7%)	0 (0.0%)	6 (9.5%)

Table 2

Descriptive statistics of risk perception (N=63)

	Minimum	Maximum	Mean	Std. Deviation
Estimate chances becoming a victim of cybercrime	1	4	2.84	0.88
Estimate chances becoming a victim of phishing	1	6	2.84	1.18
Effect of cybercrime	1	5	3.62	0.92
Effect of phishing	1	5	3.57	0.98
Estimate chances average Dutch resident becoming a victim of cybercrime	2	6	4.13	0.92
Estimate chances average Dutch resident becoming a victim of phishing	2	6	4.17	0.99

Table 3

*One-way ANOVA statistics age*risk perception*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Estimate chances becoming a victim of cybercrime	Between Groups	5.79	9	0.64	0.80	0.62	0.12
	Within Groups	42.62	53	0.80			
	Total	48.41	62				
Estimate chances becoming a victim of phishing	Between Groups	12.04	9	1.34	0.95	0.49	0.12
	Within Groups	74.47	53	1.40			
	Total	86.41	62				
Effect of cybercrime	Between Groups	10.80	9	1.20	1.51	0.17	0.20
	Within Groups	42.06	53	0.79			
	Total	52.86	62				
Effect of phishing	Between Groups	11.19	9	1.24	1.37	0.23	0.19
	Within Groups	48.24	53	0.91			
	Total	59.43	62				

Note. There is a significance difference when $p < 0.05$.

Table 4

*One-way ANOVA statistics gender*risk perception*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Estimate chances becoming a victim of cybercrime	Between Groups	3.04	2	1.52	2.01	0.14	0.06
	Within Groups	45.38	60	0.76			
	Total	48.41	62				
Estimate chances becoming a victim of phishing	Between Groups	2.10	2	1.05	0.75	0.48	0.02
	Within Groups	84.31	60	1.41			
	Total	86.41	62				
Effect of cybercrime	Between Groups	1.26	2	0.63	0.73	0.49	0.02
	Within Groups	51.60	60	0.86			
	Total	52.86	62				
Effect of phishing	Between Groups	1.03	2	0.51	0.53	0.59	0.02
	Within Groups	58.40	60	0.97			
	Total	59.43	62				

Note. There is a significance difference when $p < 0.05$.

Table 5

*One-way ANOVA statistics level of education*risk perception*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Estimate chances becoming a victim of cybercrime	Between Groups	1.93	2	0.96	1.24	0.30	0.04
	Within Groups	46.49	60	0.78			
	Total	48.41	62				
Estimate chances becoming a victim of phishing	Between Groups	2.44	2	1.22	0.87	0.42	0.03
	Within Groups	83.97	60	1.40			
	Total	86.41	62				
Effect of cybercrime	Between Groups	0.58	2	0.29	0.33	0.72	0.01
	Within Groups	52.28	60	0.87			
	Total	52.86	62				
Effect of phishing	Between Groups	0.54	2	0.27	0.28	0.76	0.01
	Within Groups	58.89	60	0.98			
	Total	59.43	62				

Note. There is a significance difference when $p < 0.05$.

Table 6

*One-way ANOVA statistics personality*Estimate chances of becoming a victim of cybercrime*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Honesty-Humility	Between Groups	0.86	3	0.29	0.61	0.61	0.03
	Within Groups	27.63	59	0.47			
	Total	28.49	62				
Emotionality	Between Groups	1.70	3	0.57	1.20	0.32	0.06
	Within Groups	27.77	59	0.47			
	Total	29.47	62				
Extraversion	Between Groups	0.92	3	0.31	0.92	0.44	0.05
	Within Groups	19.64	59	0.33			
	Total	20.56	62				
Agreeableness	Between Groups	1.09	3	0.36	0.97	0.41	0.05
	Within Groups	21.93	59	0.37			
	Total	23.02	62				
Conscientiousness	Between Groups	0.15	3	0.50	0.14	0.94	0.01

	Within Groups	21.31	59	0.36			
	Total	21.46	62				
Openness to Experience	Between Groups	0.85	3	0.28	0.82	0.49	0.04
	Within Groups	20.42	59	0.35			
	Total	21.27	62				

Table 7

*One-way ANOVA statistics personality*Estimate chances of becoming a victim of phishing*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Honesty-Humility	Between Groups	2.32	5	0.46	1.01	0.42	0.08
	Within Groups	26.17	57	0.46			
	Total	28.49	62				
Emotionality	Between Groups	2.42	5	0.48	1.02	0.41	0.08
	Within Groups	27.05	57	0.48			
	Total	29.47	62				
Extraversion	Between Groups	2.16	5	0.43	1.34	0.26	0.11

	Within Groups	18.40	57	0.32			
	Total	20.56	62				
Agreeableness	Between Groups	0.48	5	0.10	0.25	0.94	0.02
	Within Groups	22.53	57	0.40			
	Total	23.02	62				
Conscientiousness	Between Groups	0.60	5	0.12	0.33	0.90	0.03
	Within Groups	20.86	57	0.37			
	Total	21.46	62				
Openness to Experience	Between Groups	2.74	5	0.55	1.68	0.15	0.13
	Within Groups	18.53	57	0.33			
	Total	21.27	62				

Table 8

*One-way ANOVA statistics personality*Effect of cybercrime*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Honesty-Humility	Between Groups	3.53	4	0.88	2.05	0.10	0.12
	Within Groups	24.96	58	0.43			
	Total	28.49	62				
Emotionality	Between Groups	1.64	4	0.41	0.85	0.50	0.06
	Within Groups	27.83	58	0.48			
	Total	29.47	62				
Extraversion	Between Groups	1.16	4	0.29	0.87	0.49	0.06
	Within Groups	19.40	58	0.33			
	Total	20.56	62				
Agreeableness	Between Groups	1.72	4	0.43	1.172	0.33	0.08
	Within Groups	21.29	58	0.37			
	Total	23.02	62				
Conscientiousness	Between Groups	3.49	4	0.87	2.82	0.03	0.16

	Within Groups	17.97	58	0.31			
	Total	21.46	62				
Openness to Experience	Between Groups	0.85	4	0.21	0.60	0.66	0.04
	Within Groups	20.42	58	0.35			
	Total	21.27	62				

Table 9

*One-way ANOVA statistics personality*Effect of phishing*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Honesty-Humility	Between Groups	2.77	4	0.69	1.56	0.20	0.10
	Within Groups	25.71	58	0.44			
	Total	28.49	62				
Emotionality	Between Groups	2.50	4	0.63	1.34	0.27	0.09
	Within Groups	26.97	58	0.47			
	Total	29.47	62				

Extraversion	Between Groups	2.51	4	0.63	2.02	0.10	0.12
	Within Groups	18.05	58	0.31			
	Total	20.56	62				
Agreeableness	Between Groups	2.34	4	0.59	1.64	0.18	0.10
	Within Groups	20.68	58	0.36			
	Total	23.02	62				
Conscientiousness	Between Groups	4.62	4	1.16	3.98	0.01	0.22
	Within Groups	16.84	58	0.29			
	Total	21.46	62				
Openness to Experience	Between Groups	0.70	4	0.18	0.49	0.74	0.03
	Within Groups	20.57	58	0.36			
	Total	21.27	62				

Table 10

*One-way ANOVA statistics previous experience*risk perception*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Estimate chances becoming a victim of cybercrime	Between Groups	0.09	1	0.09	0.11	0.74	0.00
	Within Groups	46.25	58	0.80			
	Total	46.33	59				
Estimate chances becoming a victim of phishing	Between Groups	0.07	1	0.07	0.49	0.83	0.00
	Within Groups	84.91	58	1.46			
	Total	84.98	59				
Effect of cybercrime	Between Groups	1.55	1	1.55	1.86	0.18	0.03
	Within Groups	48.39	58	0.83			
	Total	49.93	59				
Effect of phishing	Between Groups	0.55	1	0.55	0.57	0.45	0.01
	Within Groups	56.04	58	0.97			
	Total	56.58	59				

Table 11

*One-way ANOVA statistics vulnerability*risk perception*

		Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Estimate chances becoming a victim of cybercrime	Between Groups	8.32	12	0.69	0.87	0.59	0.17
	Within Groups	42.62	50	0.80			
	Total	48.41	62				
Estimate chances becoming a victim of phishing	Between Groups	8.84	12	0.74	0.48	0.92	0.10
	Within Groups	77.57	50	1.55			
	Total	86.41	62				
Effect of cybercrime	Between Groups	11.92	12	0.99	1.21	0.30	0.23
	Within Groups	40.94	50	0.82			
	Total	52.86	62				
Effect of phishing	Between Groups	18.66	12	1.56	1.91	0.06	0.31
	Within Groups	40.77	50	0.82			
	Total	59.43	62				