The big five personality structure as a predictor for victimization in the context of cyber-crime

Name: Bernd Göttker

Student ID: 2152622

Supervisor: Iris van Sintemaartensdijk

2nd Supervisor: Steven Watson

Date: 07.07.21

Abstract

This study investigates the relationship between the big five personality domains and the implementation of online security behaviours. Online security behaviours are preventive measures an individual can carry out in their day-to-day computer usage, such as strong and varying passwords or the use of an anti-malware program. The behaviours related to cyber-crime prevention are divided into three variables with the first one being a complete measure of online security behaviours, the second one being a measure related to cyber dependent crime and the third to cyber enabled crime. Additionally, the technological proficiency of respondents is assessed and investigated for an effect on online security behaviour. This was researched through an online survey. The personality construct of conscientiousness was found to be linked to the implementation of online security behaviour and technological proficiency had a negative effect on the implementation of all three cyber-crime prevention measures.

1.Introduction

In today's society, the internet has become a central part of daily life. It is a convenient tool that eases several aspects of human life. Nowadays, the internet can be utilized to transfer money, establish social contacts, buy a lot of different goods at online shops or as a source of entertainment. Due to the Covid-19 restrictions all over the world, internet usage has increased immensely. Compared to the internet usage of pre-lockdown times, there was an increase in usage of 40% and up to 100% by internet services (De et. al, 2020). Despite the internet's benefits, the negative side effects associated with internet use should still be considered.

In particular, the anonymous structure of the internet, can facilitate individuals to perform criminal acts (Sudzina & Pavlicek, 2020). A crime performed by the aid of IT technology is referred to as cyber-crime (Leukfeldt, 2017). Since the spectrum of possible cyber offenses is diverse and can range from cyber-terrorism to cyber harassment, a small introduction into prevalent offenses is given (Sudzina & Pavlicek, 2020). Hereby, it is also important to mention that only cyber offenses which have consequences on an individual level are investigated in this study.

First, the offense of identity theft, the act when a criminal is using the identity of another person to gain benefits without their permission. Afterall, the victim is left with financial damage (Sudzina & Pavlicek, 2020). The offense of hacking describes the act of unlawfully gaining access to a technological device. This is often done through the usage of spoofing mails where the attachment of said spoofing mail contains malware that is able to identify passwords and can breach through other security barriers (Tsakalidis & Vergidis, 2017). Lastly, the offense of phishing is performed by a criminal acting like a trustful entity with the main goal of acquiring sensitive data of their victims. Mostly, this is achieved through phishing e-mails in which the victims are asked to enter their data on a counterfeit website. The perpetrator is then able to use for their benefits for example acquiring the login data of an online banking account (Al Halaseh & Alqatawna, 2016). In 2015 it was reported that 5.1% of Dutch citizens had been a victim of hacking, 3.5% victim of online consumer fraud and 0.6% victim of identity theft (van de Weijer & Leukfeldt, 2017). In addition, it is believed that one single malware namely "Cryptowall 3.0" caused a monetary damage of 325 million US dollars in the year 2015 (Sarre et. al, 2018).

A classification of cyber-crime

As noted, the spectrum of cyber-crime offenses remains diverse. Therefore, a system to classify the different kinds of cyber offenses is advantageous, since it contributes to a better understanding of the issue and could help combating it. Generally, cybercrime offenses can be distinguished into two categories. The first category is cyber dependent crime which depends on the usage of IT technology both by perpetrator and victim for the execution of the crime (Leukfeldt, 2017). Basically, cyber dependent crime would be non-existent without the invention of IT technology. Examples of cyber dependent crimes are hacking, infecting technology with malware such as trojan viruses or computer worms. The second category is named cyber enabled crime which is traditional crime executed and facilitated by the assistance of IT technology. This category of cyber-crime offenses is diverse since a lot of traditional crime can be facilitated by the use of IT technology. Examples for cyber offenses that fall into this category are online fraud, identity theft and grooming (Sudzina & Pavlicek, 2020; Hernández et al., 2021). However, there are certain crimes that can fall in both of the two categories, so the line to distinguish if a crime is cyber enabled or cyber dependent remains to some extent flexible (Leukfeldt, 2017).

Facilitating factors of victimization

Apart from a classification scheme for cyber offenses, identifying factors that could facilitate the chance of cyber crime victimization would strongly help in tackling the issue of cyber criminality. For the victimization of traditional crime, the factors that facilitate being a victim are already researched extensively. These factors are low self-control, substance abuse, routine activities, or a risky lifestyle and socio demographic factors like living in a poor neighborhood (Weulen Kranenbarg et al., 2019). A person with low self-control is more likely to engage in risky routine activities that make them more prone to victimization (Reisig & Golladay, 2019). Consequently, low self-control could be seen as a mediating factor for taking part in risky activities on a regular basis and thus being at a higher chance of victimization. Since cybercrime is executed in a different environment than traditional crime these risk factors may differ. However, comparing the factors facilitating victimization of cyber-crime which are low self-control and a risky online routine behaviour with the above-mentioned factors for the victimization of traditional crime it becomes apparent that low self-control and risky routine behaviour may be striking factors for victimization in general (Weulen Kranenbarg et al., 2019). In the context of cyber-crime, low self-control is associated with risky routine behaviours such as watching pornography and pirating media, thus increasing the likelihood of malware infection (Ilievski, 2016).

Other factors that are exclusive in facilitating cyber-crime victimization are first of all, technological proficiency since people with a higher technological proficiency are less likely to be the victim of a cyber-crime since technological proficiency helps to identify certain cyber-risks and even the detection of a computer virus occurs more likely under these circumstances (Weulen Kranenbarg et al., 2019). Therefore, a lower technological proficiency could be associated with a higher chance of victimization. Another important finding linked to technological proficiency is the IT self-efficacy a person has. The construct of IT self-efficacy describes the perception a person has on their ability to confidently apply a broad range of skills related to IT technology (Cheng et al., 2020). Hence, IT self-efficacy can be described as the perceived technological proficiency of a person. Having a low IT self-efficacy is related to more easily being the victim of a phishing scam and visiting counterfeit websites where malware could be distributed which could stem from a lack of IT skills (Cheng et al., 2020). In contrast, people high in IT self-efficacy could be at an even higher risk of victimization, since they spent more time online and also due to an overestimation of their IT-skills (Cheng et al., 2020).

Another important factor is age, because it was found that the younger a person is the more likely they are to be victimized by cyber-crime (Leukfeldt & Yar, 2016). Additionally, it was investigated that higher educated people are more likely to be victimized by cyber-crime (Leukfeldt & Yar, 2016). As these factors all contribute to victimization there are also prevention measures for falling victim to cyber-crime. To use the world wide web on a secure basis, different online security behaviours can be implemented. These online security behaviours are for example strong and varying passwords for different accounts or the usage of cyber security software in order to prevent malware attacks.

Personality as a predictor for victimization

One predictor for the execution of online security behaviour is thought to be personality (Shropshire et al., 2015). This assumption can be argued on the basis that personality can contribute to the understanding of differences in the behaviour of individuals (Pervin & John, 1999). When it comes to online security behaviours it is argued that intentions and actual security behaviour may differ from each other (Shropshire et al., 2015). So, the intention may be that one wants to implement a strong password or use cyber security software to prevent being an easy target for cyber criminals, however the actual behaviour does not involve these types of actions. The reason for this discordance between intention and behaviour can be explained by laziness, ignorance, lack of motivation and accidental oversight (Rhee et al., 2009).

In personality research, the big five trait taxonomy provides a structure where personality gets divided into five main domains with each of them comprising different facets. These traits and facets were derived from the analysis of terms people use to characterize themselves and other people (Pervin & John, 1999). The first main domain, extraversion describes people who are sociable, outgoing, talkative, and adventurous. People obtaining a lower degree of extraversion are more likely to be shy, withdrawn and silent (Pervin & John, 1999). Therefore, it can be assumed that extraversion could negatively influence the implementation of online security behaviours related to cyber enabled crime. When taking into account the sociable nature of people scoring high in extraversion, they could be more prone to victimization because of risky routine behaviour for example meeting with a stranger known from a social media plattform. Next, the domain of agreeableness describes an altruistic nature, trust, compliance and sympathy, and a low degree of agreeableness is associated with cold, unfriendly and cruel behaviour (Pervin & John, 1999). This personality trait could contribute to victimization of cyber dependent crimes. A person scoring high in agreeableness could be more prone to phishing or malware infections, due to high levels of trust and compliance. A person obtaining a high degree of conscientiousness is organized, not impulsive, efficient and has high levels of self-control. Low conscientiousness is connected to being forgetful, irresponsible and disordered (Pervin & John, 1999). As conscientiousness is related to self-control and self-control is an important factor in cyber-crime victimization it is assumed that conscientiousness positively influences the implementation of online security behaviours in general. The next trait, neuroticism is related to being shy, moody, tense and not self-confident. A low score in neuroticism is linked to stable, calm and unemotional behaviour (Pervin & John, 1999). Lastly, the trait of openness is connected to curiosity, wide interest and a good imagination. Scoring low in openness is related to being simple, with narrow interests (Pervin & John, 1999).

Current research suggests that the personality constructs of the big five personality test, agreeableness and conscientiousness are strongly correlated with better application of online security behaviour (Hadlington & Murphy, 2018). As of right now there is no consensus in the scientific community whether all five personality constructs of the big five personality test are related to online security behaviour (Shappie et al., 2019). This research tries to investigate the role of personality in the process of cyber-crime victimization. Here the likeliness of falling victim to a cyber-crime will be assessed through a questionnaire that measures if respondents implement certain protective measures that can prevent cybercrime victimization. Another important aspect of this study is the division in protective measures that relate to cyber enabled and cyber dependent crime and a focus on the perceived technological proficiency of respondents. Additionally, this study focuses on higher educated young people aged 18 to 25 years since these are important factors that facilitate cyber-crime victimization.

Research question and Hypothesis

RQ: Is there a relationship between personality traits and the implementation of online security behaviour?

H1: The higher the perceived technological proficiency of respondents the more likely they are to adopt online security behaviours

H2: The big five personality facet of conscientiousness will positively influence the implementation of online security behaviour

H3: The big five personality facet of extraversion will negatively influence the implementation of online security behaviour when only assessing behaviours related to cyber enabled crime

H4: The big five personality facet of agreeableness will negatively influence online security behaviour when only assessing behaviours related to cyber dependent crime

2. Methods

2.1 Design

The research design used in this study is a correlational survey design. The independent variable in this research is the personality of the respondents as measured by the big five-2 inventory and "technological proficiency". Namely, five different personality constructs are measured which are "Extraversion", "Openness", "Agreeableness", "Neuroticisms", and "Conscientiousness". The dependent variables are the three online security behaviour variables which are "Online security behaviour complete", "Online security behaviour dependent" and "Online security behaviour enabled" as measured by the online security behaviour questionnaire.

2.2 Participants

The respondents recruited for this study were higher educated people, namely students who are 18 to 25 years old. To recruit respondents for this research two different methods were used. First, people had the possibility to take part in this study via "SONA" a platform where students are able to take part in studies provided by the "University of Twente" or they were personally asked by the researcher to take part in the study which can be described as convenience sampling. In total 135 people participated in this study, however only 81 responses could be used for further analysis, because 54 respondents either did not fill out the online security behaviour questionnaire or were older than 25 years old. Of these 81 respondents 37 were male, 42 were female and two choose the third/non-binary option. Most respondents of this study were German with 68 respondents, 9 people are from the Netherlands, one from Bolivia, one from Bulgaria, one from Zimbabwe and one from Kosovo. The age group of respondents ranged from 18 to 25 years (M=21,49, SD=2,05). Lastly, four respondents indicated to be lower-class, 64 respondents indicated to be middle-class and 13 to be from the upper-class.

2.3 Materials

Demographic questionnaire

The demographic questionnaire is used to indicate the demographics of the respondents which were age, nationality, gender and the socioeconomic background of their families. The socioeconomic family background was segmented into low-, middle-, and upper-class. Additionally, this questionnaire measured time spend on average on the internet per week and former victimization of cyber-crime. In total this questionnaire has 6 items (Appendix A).

Perceived technological proficiency questionnaire

The perceived technological proficiency of respondents was assessed by four items where participants had to rate their general understanding and capabilities in handling technology on a 5-point Likert-scale with responses ranging from “disagree strongly” to “agree strongly” (Appendix B). The perceived technological proficiency questionnaire was constructed by the researcher and is based on the researchers understanding of what could measure technological proficiency when taking into account day-to-day computer usage. One example for a question displayed in this questionnaire is “Do you often experience difficulties when it comes to day-to-day computer usage?”. The Cronbach’s alpha for this scale was .59.

Bif-2 inventory

Next is the big five-2 inventory, which is an updated version of the bif inventory, used to assess the different main personality domains of respondents (Soto & John, 2017). The five independent variables, “Extraversion”, “Agreeableness”, “Conscientiousness”, “Neuroticism” and “Openness” will be measured by using this personality test. The big five-2 inventory has 60 items with 12 items measuring each main domain and respondents have to rate the extent to which they agree to a set of different statements on a 5-point Likert-scale with possible answers ranging from “disagree strongly” to “agree strongly”. The Cronbach’s alpha of the big five-2 inventory main domains for this study are, Extraversion (α=.83), Agreeableness (α=.69), Conscientiousness (α=.81), Neuroticism (α=.85), Openness (α=.72). An example for the different statements would be “I am someone who tends to be disorganized”, “I am someone who keeps things neat and tidy” or “I am someone who assumes the best about people”.

Online security behaviour questionnaire

The last material used for this study is the online security behaviour questionnaire. This questionnaire has 24 questions and respondents were asked to indicate if they follow different online security behaviours on a 5-point Likert-scale with possible answers ranging from “disagree strongly” to “agree strongly” (Appendix C). The online security behaviours were constructed based on similar measures of online security behaviours like “SeBIS” and the previous knowledge about online security of the researcher (Egelman& Peer, 2015). If a respondent implements adequate online security behaviours is constructed by three different scales.

The first scale consists of behaviours that either prevent or enabled the infection with a computer virus. Likewise, behaviours like the usage of antivirus software or downloading media or software from untrustworthy websites. Examples for the type of questions asked in this category are “I download email attachments from unknown sources” or “I download movies, music or any kind of software from untrustworthy websites”.

The second scale dealt with password safety and consequently only included behaviour that would either strengthen or weaken the password safety of the user. Example questions for this category are “My passwords are consisting of at least a lowercase letter, uppercase letter, a number and a special character” and “My passwords are based on personal information (e.g name, age, family-members)”.

The last scale deals with behaviours that would either prevent or enable being victimized by a cyber enabled crime. An example for this type of behaviour is “I reveal information online about my daily activities (e.g Instagram/Snapchat story)”, here when information about daily activities is revealed a criminal could utilize this information to get access to a house when being sure that nobody is at home. Another example is “I would reveal personal information to a stranger on the internet (e.g address, name, phone number)”, here this information could be utilized by a criminal for identity theft.

When calculating the mean scores of all three scales together, the variable measuring the complete online security behaviour construct, namely “Online security behaviour complete” is computed. This variable consists of 24 items (α=.72). The next variable “Online security behaviour dependent” is constructed by computing the mean of the virus infection scale and the password security scale. This variable consists of 16 items (α=.73) Lastly, the variable "Online security behaviour enabled" is constructed by computing the mean of the password security category and the cyber enabled crime category. This variable consists of 17 items (α=.63). The password security category is used for both dependent and enabled online security behaviour because it can be argued that it is related to both cyber enabled and cyber dependent online security behaviour. On the one hand an unsafe password could be used to gain access to social media accounts thus enable identity theft. On the other hand, an unsafe password could be utilized by cyber criminals to gain access to a system and hacking it in the process making it to a behaviour that could enable cyber dependent criminality.

2.4 Procedure

Respondents where either sent the link to the questionnaire on Qualtrics via "Whatsapp" or received the link via "SONA". When starting the questionnaire respondents first had to read the informed consent and after clicking on "Yes I consent" they could start with filling out the different questionnaires. First the demographic questionnaire was done, then the bif-2 inventory and after that the online security behaviour questionnaire. On average respondents filled out the questionnaire in 20 minutes.

2.5 Data analysis

In the following section the way the data will be analyzed to answer the research question and hypotheses will be elaborated. First, the data will be analyzed using the data analysis tool "SPSS-26". The first step will be to scan the data to search for possible reasons that could justify exclusion from the analysis. Every response outside the age-range will be excluded from further analysis since the target group were 18- to 25-year-olds. Furthermore, every response was excluded from analysis if the respondent did not fill out the survey completely. In this case from original 135 responses, 54 were excluded since they did not meet these criteria. All in all, 81 respondents completed the survey to a satisfying degree, although some survey items were not filled out by some respondents, however this was still justifiable since these were counted as missing values that did not intervene in the data analysis.

After rearranging the dataset and constructing all necessary variables for analysis, descriptive statistics were performed to get a general idea of how the data set is structured.
Then the data was checked for normal distribution to see if the data could be analyzed by using parametric tests.

After checking for normality and reliability the data could be analyzed to see if the hypothesis could either be rejected or accepted which was then utilized to answer the research question. For this cause a multivariate general linear model was used. The reason to use this model is that it allows to analyze multiple dependent and independent variables at once which was useful for the purpose of answering the hypothesis. In this model the dependent variables being “Online security behaviour complete”, “Online security behaviour dependent”, “Online security behaviour enabled” and independent variables being “Technological proficiency(log)”, “Extraversion”, “Agreeableness”, “Conscientiousness”, “Neuroticism” and “Openness”. This method has the advantage that it can be directly observed if any independent variable which is not part of one of the hypotheses, has an effect on one of the three dependent online security behaviour variables.

3. Results

3.1 Descriptive statistics

Table 1:

Descriptive Statistics

Variable	M	SD
Online security behaviour complete	3.43	.45
Online security behaviour dependent	3.44	.55
Online security behaviour enabled	3.36	.47
Extraversion	3.39	.64
Agreeableness	3.69	.53
Conscientiousness	3.46	.62
Neuroticism	2.83	.69
Openness	3.81	.53
Technological proficiency (log)	.77	.28

For every variable except “technological proficiency”, normality can be assumed. Every variable except “technological proficiency” had a p-value above 0.005 after applying the Shapiro-

Wilk test. To counteract the non-normality of “technological proficiency” a log transformation was performed and for the subsequent analysis the log variable of “technological proficiency” was used.

3.2 Multivariate general linear model

A general linear model was applied to test for hypothesis 1 to 4 with dependent variables being “Online security behaviour complete”, “Online security behaviour dependent”, “Online security behaviour enabled” and independent variables being “Technological proficiency(log)”, “Extraversion”, “Agreeableness”, “Conscientiousness”, “Neuroticism” and “Openness”. The only variables which provided statistically significant effects were “Technological proficiency(log)” and “Conscientiousness” (see Table 2).

Table 2:

Results of the multivariate general linear model

Dependent Variable	Independent Variable	b	t	SE	p
Online security behaviour complete	Intercept	3.542	5.923	.598	<.001
	Extraversion	-.109	-1.382	.079	.171
	Agreeableness	-.057	-.596	.095	.553
	Conscientiousness	.203	2.544	.080	.013*
	Neuroticism	.024	.305	.078	.761
	Openness	.055	.586	.095	.560
	Technological Proficiency (log)	-.651	-3.581	.182	.001*
Online security	Intercept	3.988	5.509	.724	<0.01

behaviour dependent					
	Extraversion	-.106	-1.113	.095	.270
	Agreeableness	-.013	-.113	.115	.910
	Conscientiousness	.102	1.059	.096	.293
	Neuroticism	.089	.942	.095	.350
	Openness	-.023	-.198	.115	.844
	Technological Proficiency (log)	-.971	-4.417	.220	<0.01*
Online security behaviour enabled	Intercept	3.391	5.217	.650	<0.01
	Extraversion	-.107	-1.248	.086	.216
	Agreeableness	-.091	-.882	.104	.380
	Conscientiousness	.201	2.325	.087	.023*
	Neuroticism	-.027	-.315	.085	.754
	Openness	.106	1.034	.103	.305
	Technological proficiency (log)	-.456	-2.309	.197	.024*

Hypothesis 1

First it was tested if a higher score in technological proficiency was associated to a higher likeliness of adopting online security behaviours. We find F(1,74)=12.820, p =0.01, ηp 2 =.148. Thus, there is a negative relationship between technological proficiency and adopting online security behaviours (B=-.651, T=-3.581, SE=.182, p=.001). Therefore, hypothesis 1 is rejected.

Hypothesis 2

It was tested if conscientiousness was associated to adopting online security behaviours. We find F(1,74)=6.472, p =.013, ηp 2 =.080. Thus, there is a relationship between conscientiousness and adopting online security behaviours (B=.203, T=2.544, SE=.080, p=.013.). Therefore, hypothesis 2 is accepted

Hypothesis 3

It was tested if extraversion was associated to a higher likeliness of adopting online security behaviours related to cyber enabled crime. We find F(1,74)=1.557, p =.216, ηp 2 =.021. Thus, there is no relationship between extraversion and adopting online security behaviours related to cyber enabled crime (B=-.107, T=-1.2481, SE=.086, p=.216). Therefore, hypothesis 3 is rejected.

Hypothesis 4

It was tested if agreeableness was associated to adopting online security behaviours related to cyber dependent crime. We find F(1,74)=.013, p =.910, ηp 2 =. 000. Thus, there is no relationship between agreeableness and adopting online security behaviours related to cyber dependent crime (B=-.013, T=-.113, SE=.115, p=.910). Therefore, hypothesis 4 is rejected.

4. Discussion

The results of this research found support for an effect of personality and the implementation of online security behaviours. However, only one big five personality facet is considered as statistically significant. The personality facet in question is conscientiousness, which positively predicted the likeliness for performing online security behaviours when taking the complete and enabled measure. Another interesting finding is that technological proficiency negatively influenced the likeliness for the implementation of online security behaviours be it dependent, enabled or the complete measure of online security behaviours. The other facets of the big five inventory, extraversion, agreeableness, openness, and neuroticism could not be linked to the implementation of such behaviours.

Conscientiousness and the relationship between online security

As noted, prior conscientiousness was found to positively influence the application of online security behaviours which is in line with the second hypothesis. When considering the qualities of conscientiousness which are caution, self-control, being planful and responsible, these findings are not surprising (Pervin & John, 1999). A person high in conscientiousness would therefore be more likely to regularly update their anti-malware program and would stay away from unsafe behaviours such as downloading media and software from untrustworthy websites due to their responsible acting.

Furthermore, this finding aligns with current research on the relation of personality and cyber-crime victimization. Hadlington and Murphy (2018) already found that conscientiousness correlates positively to better online security behaviour implementation. Additionally, a low score in conscientiousness had been found to correlate with a greater risk of cyber-crime victimization (van de Weijer & Leukfeldt, 2017). The research of Russel et. al (2017) found a similar effect. In their research a high score in conscientiousness is related to a higher likeliness to perform secure online security behaviours.

Additionally, since conscientiousness is linked to the ability to self-control, the research of Holt, Wilsen, Weijer and Leukfeldt (2018) showed that there is a connection between low self-control and a higher risk of cyber-crime victimization. This relationship was also found by Bossler & Holt (2010) where low levels of self-control were connected to a higher chance of losing a password to third parties and a greater risk of file corruption meaning the risk that someone else deletes, adds or changes computer files. The likeliness of falling victim to hacking and online harassment is also connected to lower levels of self-control (Reyns et. al, 2019). Since conscientiousness regulates the level of self-control a person has, it can be speculated that self-control is the reason for conscientiousness being the only personality facet related to the implementation of online security behaviours.

Extraversion and cyber enabled victimization

The personality facet of extraversion was thought to negatively influence the likeliness of online security behaviour implementation when assessing behaviours related to cyber enabled crime. It was assumed that due to the sociable, outgoing and adventurous nature of people scoring high in extraversion, they would be more prone to not perform cyber enabled security behaviours (Pervin & John, 1999). For example, they would be more likely to build up an online persona on social media and could risk identity theft. However, this hypothesis was rejected, which is not in line with current research. A high score of extraversion can be linked to a higher likeliness of falling victim to grooming, the act where an adult actively seduces and later sexually abuses a minor, by the use of social media (Hernández et al., 2021).
The assumption that extroverted people are more prone to social media use can be linked to the "rich-get-rich" hypothesis by Cheng, Wang, Sigerson & Chau (2019) which postulates that ex-

troverted people use the internet and social media actively to acquire more social contacts.

However, the results showed that this is not the case. A high score in extraversion was found to relate to a risky use of social media (Wang, 2019). But a relationship between extraversion and password safety could not be established (Gratian et. al, 2018) Maybe extraversion is in fact related to a higher chance of being victimized by some cyber-crime offense, however as the results showed not to the measure of online security behaviours related to cyber enabled crime. A reason for this is the diverse nature of cyber enabled crime, so yes there has been found a relationship between some cyber offenses but in conclusion this study found no proof for extraversion being related to cyber enabled crime victimization in general.

Agreeableness and cyber dependent victimization

Since the personality trait of agreeableness is related to trust, altruism, compliance and sympathy it was assumed that this trait could negatively influence the likeliness for performing online security behaviours related to cyber dependent crime (Pervin & John, 1999). A person exhibiting this trait to a great extent was thought to more easily reveal his passwords to others, would visits websites that seem untrustworthy and interact with mails from an unknown addressor, increasing the chance of a malware infection or losing his passwords to third parties. Afterall, this Hypothesis could not be confirmed as well. Research on the relation between cyber dependent crime victimization and agreeableness is not fully evolved right now. There have only been found an association between agreeableness and good online security behaviour, however in relation to cyber dependent crime no prior research could be found (Hadlington & Murphy, 2018). All in all, it might be that agreeableness has an impact on online security behaviours related to some cyber dependent crimes, however it simply could not be proven that it has an impact on cyber dependent crime victimization.

Technological proficiency and risky online security behaviours

It was assumed that technological proficiency would positively influence the implementation of online security behaviours. However, the exact opposite is the case. For all dimensions of online security behaviour, perceived technological proficiency was found to negatively influence the likeliness of their implementation. When looking at the existing body of research, two explanations for this occurrence can be found. First of all, people who exhibit a high technological proficiency are more likely to be the victim of cyber-crime (Cheng et al.,2020) The reason for this could be explained by taking the overconfidence hypotheses into account. The overconfidence hypothesis postulates that people who perceive themselves as technological proficient are more likely to be victimized by cyber-crime due to their increased exposure to

IT-technology and their overconfidence in their ability to prevent victimization (Cheng et al., 2020).

The second explanation for the found effect is connected to the usage of anti-malware programs. A lot of systems already come with a pre-installed anti-malware program such as Microsoft defender and here a problematic effect can be observed. In the research by Ngo & Paternoster (2011) it was found that there is a correlation between having an anti-malware system installed and obtaining a computer virus, therefore it was concluded that an anti-malware system gives the user a false sense of security (Ngo & Paternoster, 2011). The false sense of security that an anti-malware program provides could lead people to more risky online behaviour and thus a negative influence of perceived technological proficiency can be explained

4.1 Limitations

For this study several limitations can be pointed out. First, the online security behaviour questionnaire and the technological proficiency questionnaire were self-constructed. This includes typical issues like a low Cronbach´s alpha for the technological proficiency questionnaire.

Additionally, not the whole range of protective online security behaviours were included in the online security behaviour questionnaire which is due to the fact that not every protective behaviour is assessable through the usage of a survey. These are for example protective measures against cyber bullying or sexual harassment and child pornography. First of all, these are sensitive topics and asking people about these could evoke traumata. Additionally, protective measures related to these offenses are difficult to construct because there are a lot of underlying factors that contribute to victimization. Here it would be more applicable to see if victimization took place and based on the mere fact of victimization, searching for correlating factors among victims. Therefore, it can be argued that implementing all existing cyber criminality offenses would go beyond the scope of this thesis.

It certainly is a major strength of this study to divide security behaviours in enabled and dependent because a lot of research in the area of personality and online security uses only one measure for online security. This single measure for online security can be considered as problematic since cyber-crime offenses are diverse and each offense is related to different security behaviours, therefore grouping them based on a classification of cyber-crime makes more sense.

Lastly, the online security behaviour questionnaire, certainly was constructed from the perspective of a windows and computer user. Other operating systems such as “Linux” or “MacOs” might have different factors that could influence online security behaviours, however these remain unknown since no information regarding those systems have been obtained by the researcher prior to conducting the research. The same can be concluded for mobile phone usage but some behaviours remain universal for both operating systems and mobile phone usage for example the whole range of questions related to password safety.

4.3 Future Research

A first step in future research would be to develop a measure including the whole scope of protective measures against the broad range of existing cyber criminality. When using such an approach the diverse nature of cyber-crime offenses and their related security behaviours can be more confidently investigated. Another promising branch of research could go into the direction of investigating if a difference of operating systems has an effect on the implementation of cyber security behaviour. There could exist a difference between people who obtain a system with windows installed and people with a system that uses “Linux” or “MacOs”. There has been no literature found that investigates the relationship between operating systems and cyber security. Therefore, this issue needs more attention in future research. Additionally, a focus on cyber security behaviour in relation to mobile phone use and personality traits of users would be an interesting topic for investigation since a lot of internet traffic today is handled using a mobile phone. A completely new branch of security behaviours could be investigated here, for example using screen lock, updating mobile application, connecting to free/unsecured Wi-Fi networks or disable GPS when it is not needed (Shah & Agarwal, 2020).

Lastly, more research needs to be conducted into the relation of technological proficiency and cyber-crime victimization to see if the overconfidence hypothesis can be replicated under different situations (Cheng et. al, 2020). Since people high in technological proficiency are at higher risk to be victimized by cyber-crime due to their greater exposure to IT technology they can be considered as an important at-risk group (Cheng et. al, 2020). If the overconfidence is proven to be true by using a better measure of technological proficiency it could direct an important discussion for cyber security in the at-risk group of highly technological proficient persons that were prior to be found to need be at risk that much. In respect to that the usage of anti-malware systems and a false sense of security this might bring to users’ needs to be investigated further (Ngo & Paternoster, 2011).

4.4 Conclusion

The purpose of the research was to investigate if the personality of an individual has an effect on the implementation of cyber security behaviour. As already speculated and shown by previous research, the personality trait of conscientiousness was found to positively predict the implementation of security behaviours to a great deal. This can be linked to a better ability to self-control by individuals with a high score in conscientiousness. Another variable that was assumed to positively predict the implementation of security behaviours was the perceived technological proficiency of respondents. Perceived technological proficiency negatively predicted the implementation of cyber security behaviours in all aspects being dependent, enabled or the complete measure of security behaviours. Here the overconfidence hypothesis could deliver an explanation for this occurrence. There should be a greater focus on cyber security even when people think that they obtain a lot of knowledge on this topic. Especially, when considering that every day new methods and malware programs are developed in order to perform criminal activities. In conclusion, only conscientiousness can be linked to implementation of online security behaviour. All other personality facets could not be linked to the implementation of online security behaviours be it either related to dependent or enabled cyber-crime. When taking into account the increase in cyber-crime offenses over the last decade, finding factors that relate to victimization is an important research field that could guide the construction of interventions to tackle this issue so the internet will be a more secure space in the future.

Reference List

Al Halaseh, R., & Alqatawna, J. F. (2016). Analyzing cybercrimes strategies: The case of phishing attack. In *2016 Cybersecurity and Cyberforensics Conference,* 82-88. doi: 10.1109/CCC.2016.25

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

Cheng, C., Wang, H.-y., Sigerson, L., & Chau, C.-l. (2019). Do the socially rich get richer? A nuanced perspective on social network site use and online social capital accrual. *Psychological Bulletin, 145*(7), 734-764. doi:10.1037/bul0000198

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, 108. doi:10.1016/j.chb.2020.106311

De, R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171. doi:10.1016/j.ijinfomgt.2020.102171

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems,* 2873-2882. doi:10.1145/2702123.2702249

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security*, *73*, 345-358. doi: 10.1016/j.cose.2017.11.015

Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. *Cyberpsychology, Behavior, and Social Networking,* 21(3), 168–172. doi:10.1089/cyber.2017.0524

Hernández, M. P., Schoeps, K., Maganto, C., & Montoya-Castilla, I. (2021). The risk of sexual-erotic online behavior in adolescents–Which personality factors predict sexting and grooming victimization?. *Computers in human behavior*, 114. doi:10.1016/j.chb.2020.106569

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2018). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, 38(2), 187-206. doi: 10.1177/0894439318805067

Ilievski, A. (2016). An explanation of the cybercrime victimisation: Self-control and lifestile/routine activity theory. *Innovative Issues and Approaches in Social Sciences,*9(1). doi:10.12959/issn.1855-0541.IIASS-2016-no1-art02

Leukfeldt, E. R. (2017). Research agenda the human factor in cybercrime and cybersecurity. Eleven international publishing.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263-280. doi: 10.1080/01639625.2015.1012409

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1).

Pervin, L. A., & John, O. P. (1999). Handbook of personality: Theory and research (2nd ed.). Guilford Press.

Reisig, M. D., & Golladay, K. A. (2019). Violent victimization and low self-control: The mediating effect of risky lifestyles. *Violence and victims*, 34(1), 157-174. doi: 10.1891/0886-6708.VV-D-18-00013

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization?. *American Journal of Criminal Justice*, 44(1), 63-82. doi:10.1007/s12103-018-9447-5

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security,* 28(8), 816–826. doi:10.1016/j.cose.2009.05.008

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology*,1(3-4),163-174. doi:10.1080/23742917.2017.1345271

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

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security,* 28(2), 293–318. doi:10.1108/ics-04-2019-0041

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media Culture*. doi:10.1037/ppm0000247

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security,* 49, 177–191. doi:10.1016/j.cose.2015.01.002

Soto, C. J., & John, O. P. (2017). The next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. *Journal of Personality and Social Psychology,* 113, *117*-143. doi: 10.1037/pspp0000096

Sudzina, F., & Pavlicek, A. (2020). Virtual Offenses: Role of Demographic Factors and Personality Traits. *Information*, 11(4), 188. doi:10.3390/info11040188

Tsakalidis, G., & Vergidis, K. (2017). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. IEEE Transactions on Systems*, Man, and Cybernetics: Systems, 1–20.* doi:10.1109/tsmc.2017.2700495

Van de Weijer, & 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

Wang, D. (2019). A study of the relationship between narcissism, extraversion, body-esteem, social comparison orientation and selfie-editing behavior on social networking sites. *Personality and Individual Differences*, *146*, 127-129. doi:10.1016/j.paid.2019.04.012

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, 40(1), 40-55. doi:10.1080/01639625.2017.1411030

Appendices

Appendix A

Demographic questionnaire

Demographic questionnaire

Q1 How old are you?

____

Q2 What is your gender?

○ Male (1)

○ Female (2)

○ Non-binary / third gender (3)

○ Prefer not to say (4)

Q3 What is your nationality?

○ German (1)

○ Dutch (2)

○ Other (3) ____

Q4 What is the economic background of your family?

○ low-class (1)

○ middle-class (2)

○ upper-class (3)

Q5 How much time do you spent on average in the internet (in one week) ?

____

Q6 Have you ever been the victim of a cyber-crime?

○ yes (1)

○ no (2)

Appendix B

Technological proficiency questionnaire

Q1 Do you feel capable to solve your own IT-related problems?

○ Definitely yes (1)

○ Probably yes (2)

○ Might or might not (3)

○ Probably not (4)

○ Definitely not (5)

Q2Do you use a technological device to complete different taks for example online shopping, 25ransferring money etc.

○ Definitely yes (1)

○ Probably yes (2)

○ Might or might not (3)

○ Probably not (4)

○ Definitely not (5)

Q3 Do you often seek help by others when confronted with IT-related problems?

○ Definitely yes (1)

○ Probably yes (2)

○ Might or might not (3)

○ Probably not (4)

○ Definitely not (5)

Q4 Do you often experience difficulties when it comes to day-to-day computer usage?

○ Definitely yes (1)

○ Probably yes (2)

○ Might or might not (3)

○ Probably not (4)

○ Definitely not (5)

Appendix C

Online security behaviour questionnaire

	Disagree strongly (1)	Disagree a little (2)	Neutral; no opinion (3)	Agree a little (4)	Agree strongly (5)
(malware) I download email attachments from unknown sources (1)	○	○	○	○	○
I use an anti-malware programm (e.g Microsoft defender, Norton etc.) (2)	○	○	○	○	○
I regularly scan my device for possible malware-infections (3)	○	○	○	○	○
I update my anti-malware programm as soon as new updates are available (4)	○	○	○	○	○
I download movies, music or any kind of software from untrustworthy websites (5)	○	○	○	○	○
I am familiar with signs that indicate a possible malware-infection (6)	○	○	○	○	○
I click on hyperlinks from unknown sources (e.g hyperlink in an email or sent in social media (7)	○	○	○	○	○

(password safety)	○	○	○	○	○
I share my passwords with other people (8)					
I use the same password or variations of the same password for multiple accounts/websites (9)	○	○	○	○	○
My passwords are consisting of at least a lowercase letter, uppercase letter, a number and a special character (10)	○	○	○	○	○
My passwords are longer than 8 characters (11)	○	○	○	○	○
I use the "remember my password" option (12)	○	○	○	○	○
I write down my passwords (e.g on a piece of paper (13)	○	○	○	○	○
My passwords are based on personal information (e.g name, age, family-members) (14)	○	○	○	○	○
I change my passwords on a regular basis (e.g every 6 months) (15)	○	○	○	○	○

I use the two factor authentication when possible (16)	○	○	○	○	○
(cyber enabled behaviours) I would reveal personal information to a stranger on the internet (e.g address, name, phone number) (17)	○	○	○	○	○
I would establish an online relationship with a stranger (18)	○	○	○	○	○
I would meet a person I only know from social media or a dating website if their account is not verified (19)	○	○	○	○	○
If I would meet a person I only know from social media or a dating website I would establish safety measures like telling another trustful person where we meet or meet at a neutral place like a restaurant (20)	○	○	○	○	○
I reveal information online about my daily activities (e.g Instagram/Snapchat story) (21)	○	○	○	○	○
I present expensive things to an online audience (e.g Instagram/Snapchat story) (22)	○	○	○	○	○

I would lend money to one of my online friends (23)	○	○	○	○	○
I have a social media account where I display personal information like my name, place of residence or a picture of myself (24)	○	○	○	○	○