Determining secure digital behavior of individuals using HEXACO personality traits.

MSc Thesis Behavioral economics, Erasmus School of Economics

Author: Bas van Winsen

Student nr.: 412367

Supervisor: Sophie van der Zee

Date of submission 27-4-2020

Abstract

In an era where technologies play a much more important role, cybercrime becomes a much greater threat to the world. Previous literature suggests that many cyber criminals exploit users rather than technology to successfully attack. Therefore, in this paper we will look at the victims themselves and in particular, their personality traits. This paper focusses on the effect personality traits have on the online behavior of individuals. Specifically, a survey is used to analyze the relation between the 24-item HEXACO personality trait questionnaire by De Vries (2013) and the safe digital behavior using the Security Behavior Intentions Scale (SeBIS) by Egelman and Peer (2015). The HEXACO model consist of the following factors: Honesty-Humility (H), Emotionality (E), Extraversion (X), Agreeableness (A), Conscientiousness (C), and Openness to Experience (O). This way we can identify to which personality trait an individual scores highest and what their Security Score is. The Security Score is a measure of how secure someone behaves online. In total 153 participants completed the survey. The results show that people who score high on the traits Conscientiousness and Agreeableness behave more securely online and are therefore less likely to become a victim of cybercrime. This research also tested whether there was an effect of age and education on the online behavior. No significant results have been found for an effect of these control variables on the online behavior. In this research, we managed to find two traits that could be considered as predictors of secure online behavior and cybercrime victimization.

Contents

Introduction

Information and communication technologies have become very important in the current world we live in. Globally, we now have 4.54 billion active internet users (Hosting Facts, 2020.) Also, computer and laptop usage are increasing every year by 1.5% (Gartner, 2019). The usage of the internet could be very positive for the development of humans, as an increase in technology can create business productivity. However, communication technologies are developing at a fast pace, so it is important to protect yourself from any threats and crimes that could be the result of this development. On a global level, the total cost of cybercrime has increased to 45 billion dollars and the average number of security breaches in the last year rose by 11 percent, from 130 to 145 (Violino, 2019). Ismail (2019) investigated cybercrime with the yearly number of cyberattacks in the world. Ismail found that here is an increase in ransomware attacks of 11% per year. There is also an increase of 56% in web app attacks in comparison to last year. Micro (2014) reported that cybercrime operated more across borders than any other type of crime. Because cybercrime operates across borders and violates people's privacy, cybercrime can be seen as a global problem. Privacy and security are two important values in life, so violations through cybercrime should be prevented in the future.

In order to prevent the violation of privacy caused by cybercrime, we need to understand what drives this problem. Most of the previous literature concerning the improvement of Information Security is focused on improving the technology rather than looking at human factors. Stanton et al. (2004) were one of the first that acknowledged the importance of the human factor behind security. Trcek et al. (2007) claimed that humans are the most important factor in preventing cyberattacks and managing online behavior and security. According to Öğütçü, Testik and Chouseinoglou (2015) people tend to have low levels of awareness towards threats and their level of information security tends to be low. Large companies can invest in a strong technical defense, but the individuals themselves tend to be the weakest link and can therefore be a critical error in the defense of companies (Abawajy, 2014). Recently, according to a research by Mak (2017), human errors are the leading cause of data and security breaches, as they are responsible for 52 % of such incidents. It seems rather difficult to determine the magnitude of the responsibility of humans, as another research by Spadafora (2019) claims that humans are responsible for 90% of data and security breaches in 2019. Since human behavior plays such a large role in effective cybersecurity, it is important to understand which factors drive secure online behavior.

Previous research has demonstrated that several factors can influence online behavior. According to Keszthelyi (2013), it is of vital importance to select a good password in times where we as individuals have to deal with cybercrime. Password management is therefore a factor that can influence online behavior. But other things as social media use, internet use and email use are also factors that influence the security of online behavior (Parsons et al., 2017.) A study by Bubas et al. (2008) also pointed out certain factors that drive online behavior. Disbelief of humans that privacy violations and security threats would represent possible problems was the most concerning factor in their research.

As there are several factors that lead to an improvement of the security of online behavior, there are also several experimental studies that suggest that certain personality types are associated with a higher chance of cybercrime victimization. Halevi, Lewis, and Memon (2013) investigated the relationship between human personalities and their online security by using a phishing experiment. In their research, they showed that when using a prize phishing email, people with certain personality traits were more likely to click on the phishing email. Specifically, people who scored high on Openness to Experience were more susceptible to phishing attacks (Haveli et al., 2013.) Van de Weijer and Leukfeldt (2017) investigated the relation between the personality traits and cybercrime victimization. They examined whether certain personalities could affect (cyber)crime victimization. They also analyzed if certain types of victimization differ on these personality traits compared to non-victims. The results of their research indicated that individuals who score highest on Openness to Experience have higher odds of becoming a victim of cybercrimes. Previous research therefore suggests that personality traits seem related to cybercrime victimization.

Personality may influence the tendency to display certain behaviors, which in turn influence the chance of victimization. Different online behaviors can lead to victimhood, so in order to prevent people from being victimized, it is important to know which insecure behaviors to target for improvement. Until now, not much research has been done between the relationship of personality traits and online behavior. An interesting scope therefore is to look whether certain personalities differ in their risky online behavior, which can help prevent incoming cyberattacks. More specifically, **to what extent do personality traits of an individual influence online behavior?**

Furthermore, this research will potentially give more insights in the relationship between personality traits and online behavior. When individuals behave risky or insecure, they

are more likely to be a victim of cybercrime (Ngo & Paternoster, 2011). A survey will be used to analyze the relation between personality traits and behavior of individuals online. To do so, we combine the 24-item HEXACO personality test made by De Vries (2013) and the Security Behavior Intentions Scale (SeBIS) questionnaire by Egelman and Peer (2015). The HEXACO model consist of the following factors: Honesty-Humility (H), Emotionality (E), Extraversion (X), Agreeableness (A), Conscientiousness (C), and Openness to Experience (O). The HEXACO personality test will reveal a score for each personality trait per individual. The SeBIS questionnaire is a questionnaire where a Security Score is generated to test secure online behavior. The total score is built upon scores for four different subscales, each related to a different security topic. By administering the two scales to a group of participants, we can compare a person's personality trait with their security score on the four subscales. Based on these insights, we can determine which personality trait displays secure online behavior and therefore puts people at risk or not.

Literature Review

Cyberattacks and threats are daily problems in the current environment we live in (Infosec Newsflash, 2020). With all the new technologies in place, these threats are likely to increase in the future. This statement is strengthened by research from Paganini (2020), who argued that the total costs of cybercrimes have increased by 13% in a year (2018 to 2019). It is therefore important for an organization to secure their information and have a good defense mechanism against cyberattacks. The goal of such an organization is to heighten the importance of information system security and spread awareness to the employees about the possible negative effects (Hansche, 2001). Some of these negative effects can be reputation damage, loss of customers and reduction in profits. To tackle such negative effects, it is necessary to improve information security. However, if individuals' use of technology is not optimal and the awareness toward threats is low, significant information security risk is present (Ögütçü et al., 2015). Organizations recognize that employees are the weakest link in the security of an organization and carry therefore the highest risk (Bulgurcy, Cavusoglu, & Benbasat, 2010). Many employees are simply not aware of their actions that cause company risk as consequence (Kritzinger & Smith, 2008). But not only companies have to deal with cybersecurity, it is also important for the government and individuals themselves to have the most secure structure in their organizations or households. Security breaches in the federal government of the United States (U.S.) can leak sensitive citizen data and violates the U.S. law (Bradbury, 2019). To put this in perspective, the largest government data breach to date was in 2015 and leaked information of 191 million individuals, caused by a human error (Lord, 2018). Security awareness is therefore important for privacy and violation of matters. According to Siponen (2000) the term' 'information security awareness''(ISA) is referred to as a level of awareness where users in an organization are aware of their security mission. Many organizations have established programs to raise the information security awareness, so their employees are aware of the security risks, protecting them from potential risk for both the company and themselves (Kruger & Kearney, 2006). The goal of a security awareness program is to highlight the possible negative effects of a security breach and the importance of information systems security.

Many could argue that these cyber threats can be fixed by focusing on the technical side of security. Zhang, Reithel and Li (2009) investigated the possible impact of technical protection on security behaviors. They stated that human errors continue to be the major problem in the field of organizational information security. Also, they found that there is a

negative direct effect between high technical protection and behavioral intentions. This indicates that the higher the technical protection an organization has, the less an individual is willing to comply with the security policies. Ng, Kankanhalli and Xu (2009) studied the relationship between training employees and their behavior. The researchers used the Health Belief model to study computer security behavior and concluded that ISA programs and trainings do not have the desired effectiveness that organizations wanted to achieve. ‘’Employees’ attitude, beliefs and habits have significant impact on intention to comply with an organizations security policy’’ (Pahnila, Siponen & Mahmood, 2007). Therefore, a technical solution is not always the key to prevent cyber threats.

Most of the previous literature concerning the improvement of ISA security has focused on improving the technology rather than looking at the human factors. Stanton et al. (2004) were one of the first that acknowledged the importance of the human factor behind security. Their results suggested that job satisfaction, organization type, job role, and commitment are significant key security behaviors of end users. More recently, Trček et al. (2007) supported this by explaining that during recent years technology alone cannot provide an adequate security of information systems. According to the authors, the main and most important factor behind ensuring information security is humans. In their research they invented a model to treat the information system security by combining technology, human factors and organization characteristics. Sasse, Brostoff and Weirich (2001) stated that simply blaming individuals will not lead to more effective behavior. Their research suggests that developers should take human behavior into account when developing software and hardware. They concluded that existing knowledge and techniques can be used to prevent cyber threats and to improve security.

Behavioral factors and online security

There are several behaviors important for information security. More specifically, these behaviors are password generation and use, social media use, and mobile device usage. According to Keszthelyi (2013), it is critically important to select a good password in times where we as individuals have to deal with cybercrime. Previous research analyzing password strength revealed that most passwords have seven or less characters, end with a numerical character, and can be easily guessed (Bensmann, 2009). Stanton, Stam, Mastrangelo and Jolton (2005) conducted a survey on password-related behavior. In their research they showed that end users that have low technical knowledge tend to share passwords more often and re-use weakly created passwords. With training, awareness, monitoring, and motivation this problem

could be solved. But on the other hand, they showed that if you increase awareness and give them password-training, the likelihood of using the same password for different purposes increases. They use the same password because they think with training, a really strong password is created, and they will use that same password for every purpose. Inglesant and Sasse (2010) identified two main problems in password usage: password mechanisms and organizational factors. These problems erupt due to a lack of communication between the security departments and users, as users do not understand the security issues that can affect the company. Password management is therefore a strong tool to reduce risk of cyberattacks and increase online safety.

Social media usage is also a tool to measure the security of online behavior. Acquisti and Gross (2006) analyzed the security awareness and behavior on social media. In their research they looked at behavioral differences between communities of Facebook members and non-members and they tried to find motivations for the online risky behavior of members. For example, they looked at the visibility of profiles on Facebook and checked with the participants if they were aware that their profile was visible to the public. A significant majority was not aware of the problem that their profile was visible to the public. This group trusts their own ability to manage their privacy settings and control the information they provide to external members of Facebook. A research by Acquisti, Brandimarte and Loewenstein (2015) strengthened this by saying that people are often unaware of the information they are sharing on social media and how to safely utilize it. Gulenko (2013) did similar research on security awareness on Facebook. He argued that most people blindly accept friend requests, granting unknown people access to profile details. This illustrates that most users online are not aware of the potential risk that social media brings to their security online and rely on their own ability to control the risk.

Having high ISA is important for a company to reduce risk of cyberattacks, but how do you measure awareness of information security? The number of studies concerning individuals' awareness and reflection of this awareness on the users' behavior is limited (Ögütçü, Testik & Chouseinoglou, 2015). Mylonas, Kastania and Gritzalis (2013) provided a survey analysis about the security awareness of smartphone users. Their findings suggest that smartphone users believe that downloading applications is risk-free. Their results indicate as well that smartphone users tend to use the same device for both business and personal purposes. This may increase the impact of unauthorized access to stored data. Ponemon (2012) provided a survey indicating that mobile devices can indeed be very risky. He stated that mobile devices have become a

major security threat for 73% of his respondents. Mylonas et al. (2013) suggested the users see smartphones as just telephones and not as mobile devices. To conclude their research, users tend not to be aware of the security applications on their phone and are not using them optimally. This applies not only to phones where users are not aware of the potential threats, this also applies to computers. A research by Arachchilage and Love (2014) shed light on this topic. They stated that due to a lack of knowledge, users have a higher chance of being victimized by phishing attacks.

Measuring ISA

Measuring ISA can be done in different ways. Galba, Solic and Lukic (2015) developed a validated measurement instrument named Information Security and Privacy Self-Assessment Tool (ISPSA). The ISPSA is used to raise awareness on privacy and information issues on the Internet, as privacy and overall information security are significantly affected by the users' awareness, knowledge, and their online behavior. Their questionnaire asks respondents about their potentially risky behavior and their knowledge and awareness on privacy and information issues on the Internet. This can eventually measure the awareness of users. Their work may be important to explain certain aspects of ISA, but they explain by saying that ISPSA does not measure ISA fully. Galba et al. (2015) only measured the ISA partly with their ISPSA tool. The other scales that measure ISA are HAIS-Q (Human Aspects of Information Security Awareness Questionnaire) by Parsons et al. (2014), SeBIS by Egelman and Peer (2015), and four scales to measure the security awareness levels are developed by Ögütçü et al. (2015).

Ögütçü et al. (2015) used four scales to measure ISA which include Risky Behavior Scale, Conservative Behavior Scale, Exposure to Offence Scale, and Risk Perception Scale. For every scale 15 to 20 questions are asked to the respondent where a security score is formulated. For each question 1-5 points could be awarded, depending on their answer. A higher score indicates more secure online behavior and more awareness towards technology threats. Ögütçü et al. (2015) were trying to figure out what individuals think and how they behave, what their awareness levels were and the amount of knowledge they had. The results in their paper suggest that the more participants perceive a threat, the more protective they will behave. Also, a higher education level indicates more information security awareness. Egelman and Peer (2015) developed the SeBIS, which is a 24-item scale to measure information security behavior. This questionnaire also has four subscales that measures attitudes towards choosing passwords,

device securement, proactive awareness and staying up to date. They used Likert Scale questions to measure the ISA, similar to Ögütçü et al. (2015).

Parsons et al. (2014) used a questionnaire with 63-items named the HAIS-Q. The HAIS-Q is a 63-item measure that assesses seven focus areas. These focus areas are Password management, Email use, Social media use, Mobile devices, Information handling and Incident reporting (Parsons et al., 2017). Furthermore, the purpose of this study was to identify whether there was a positive relationship between policy and procedures and self-reported behavior when using a work-related computer and to construct a valid instrument that measures ISA. Results suggest that participants' behavior towards policy and procedures can be measured by the HAIS-Q. In a further study by Parsons et al. (2017) the validity of the HAIS-Q was tested as well. They concluded that the HAIS-Q can predict behavior in a phishing experiment and all the focus areas are internally consistent. A phishing experiment is an experiment that can determine whether for example an employee clicks on a malicious link or reports this activity, which helps to explain behavior and security awareness. In response to the findings by Parsons et al. (2014), McCormac et al. (2016) evaluated the HAIS-Q by looking at the reliability and the internal consistency. They concluded in their research that the HAIS-Q is a reliable and consistent instrument to measure ISA. For our research we are using the 24-item SeBIS questionnaire, as this is a relatively small questionnaire that suits best with our survey.

Measuring personality traits

Human factors play a major role in the security of an organization (Trček et al., 2007). It can therefore be interesting to look at personality traits of human beings, as these traits drive behavior of individuals. Not much research has been done on the relationship between cybercrime victimization and personality traits. One of the first authors that acknowledged the relationship between personality traits and victimization were Gottfredson & Hirshi (1990), as they wrote a book about the general theory of crime. According to them, individuals with lower self-control are more risk taking, shortsighted, insensitive to others, impulsive, and seek more immediate gratification. They are therefore more likely to be involved in a crime. Self-control can be seen as a personality trait as it is described as the individual's ability to manage and monitor their emotions and behaviors. The relation between self-control and crime victimization was also analyzed by Holtfreter, Reising and Pratt (2008). Their findings suggest that low self-control significantly increases the likelihood of being a victim of fraud and in general, males have a higher risk of being a target of fraud. Self-control can therefore be seen

as a powerful predictor of victimization. Although self-control is not a personality trait that is used in this paper, it is however one of the first comparisons made between the personality traits and victimization.

There are two models that measure personality. The first model is the Big Five personality trait model, which include the traits Openness to Experience, Conscientiousness, Extraversion, Agreeableness and Neuroticism. In extension of the Big Five personality traits, Lee and Ashton (2007) developed a new six-dimensional framework for personality structure, named the HEXACO model. This model is a viable alternative to the BF model. According to Lee and Ashton (2007), the HEXACO model is a better model than the BF model, as Honesty-Humility is better accommodated in the HEXACO model. Lee and Ashton (2007) argued that due to the inclusion of the Honesty-Humility trait factor, the HEXACO model outperformed the BF model in predicting several variables of practical importance (e.g. sexual harassment and violence). Honesty-Humility refers to individual differences to use others for personal gain and includes self-enhancing and immoral behaviors. Another research by De Vries et al. (2009) supported the claim that the HEXACO model outperforms the BF model in explaining personality traits. They state when adding the Honesty-Humility trait, it captures the BF outliers such as integrity and egotism. In our research, the personality traits of the HEXACO model will be used as they tend to have more explanatory power.

Van Gelder and De Vries (2012) also analyzed the HEXACO model of Lee and Ashton (2007). They tested whether the HEXACO traits have more explanatory power than the BF model by using a criminal decision-making model that integrated individual differences. The authors concluded that it has a broader personality space and captures both the BF and Self-Control dimensions. The authors also pointed out the advantage of Honesty-Humility, as it turned out to be the strongest personality to correlate with victimization. Regarding the personality trait Emotionality, the authors found an indirect negative significant correlation between Emotionality and victimization. Wilcox et al. (2014) studied the relationship between personality traits and victimization, similar to Van Gelder and De Vries (2012). With a 4-year panel study including over 2200 adolescents, they found a negative correlation between criminal victimization and the traits Agreeableness and Conscientiousness. This suggests that individuals that score high on the traits Agreeableness and Conscientiousness tend to have a lower chance of being victimized.

Personality traits and cybervictimization

Previously mentioned studies examined the effect of personality traits on crime victimization and crime decision making. This research investigates the relationship between HEXACO personality traits and online behavior. It is therefore important to understand what the main characteristics are of these personality traits and how their relationship is with cybersecurity. According to Albladi and Weir (2017), people who score high on Conscientiousness tend to be organized and are known for their self-control. They also are likely to take control and protect their personal information online (Chua & Chua, 2017). We therefore expect a positive indirect effect of Conscientiousness and cybercrime victimization, as people who exhibit Conscientiousness are more likely to protect their personal information online. As for Agreeableness, people who score high on this trait tend to trust others, are kind, and like to help other people (Albladi & Weir, 2017). Also, Agreeable people have the tendency to increase correct judgement over whether information should be trusted, which decreases the chance of being victimized (Cho, Cam, & Oltramari, 2016). A high score on Emotionality displays an increased fear to dangers and have anxiety towards life's stresses. They also rely on emotional support from others and feel empathy and sentimental attachments with others (Lee & Ashton, 2007.) Emotionality can be seen as an important predictor towards cybervictimization, as people with a high score on Emotionality are more prone to anxiety and fear, which results in a less likely chance to be a victim of cybercrime (Ashton et al., 2014).

Previously mentioned traits have a positive effect on online behavior and have therefore a less likely chance for people to be victimized by cybercrime. Extraversion, Openness to Experience and Honesty-Humility are expected to have a negative effect on online behavior. People who score high on Extraversion are usually seen as sociable and attention-seekers (Lee & Ashton, 2007), and they tend to have high motivation to engage in social networks (Albladi & Weir, 2017). A positive impact between the user's willingness to comply to phishing request and Extraversion is also found (Alseadoon, Othman & Chan, 2015). For the Openness to Experience trait, people who score high on this trait tend to have lots of imagination and fantasy to explore the new experiences (Albladi & Weir, 2017.) In a study by Chua and Chua (2017), they found that Openness to experience is positively related to use of social network, which could increase the chance of being victimized online. People with high Honesty-Humility tend to be sincere, fair, and unassuming (Baiocco et al., 2017) In another research by Van Gelder

and De Vries (2012) they found that people who score high on Honesty-Humility are more likely to violate rules, which results into a more likely chance to become victimized.

There have been several studies that shed light on the impact that personality traits have on online behavior. Peluchette et al. (2015) examined the relationship between the victims' personality and risky social online behavior. Their research is showing that the more and more risky people behave online, the higher chance you will get of becoming a victim of cybercrime. According to the authors, the posts you post on Facebook, the number of friends you have online, and the content of your friends are all predictors of victimization. They also looked at the effect of the Big Five personality traits and cyberbullying victimization. A higher score on Extroversion, Conscientiousness, and Openness to Experience were significant predictors of being victimized by cyberbullied. Kokkinos et al. (2013) did similar research on the effect of personality on cyberbullying. Their multiple regression analyses indicated that boys are more likely to participate in cyberbullying. They also found that when scoring higher on Openness to Experience and Conscientiousness results into a more likely involvement in cyberbullying.

Cyberbullying is a very specific type of cybercrime, which is usually not related to the negative financial consequences of cybercrime. However, it is interesting to see the relationship between the Big Five personality traits and cybercrime victimization. Leaking and sharing sensitive information on social media can result into negative financial consequences of cybercrime (Sandle, 2019). Halevi, Lewis and Memon (2013) investigated the relationship between the BF personality traits and Facebook privacy settings. In their research they found that people that score high on the traits Openness to Experience and Extraversion tend post more information on Facebook and have a less strict privacy, which could lead to more cyberattacks and violation of the privacy. Halevi et al. (2013) also investigated the Big Five traits and their online vulnerability to phishing attacks. The authors found that people who score high on the Neuroticism trait were more likely to be exposed to phishing vulnerability.

What remains unknown however is the relationship between the HEXACO personality traits and cybercrime victimization. Our research will fill that gap and expand the factors used to analyze online behavior. Van de Weijer and Leukfeldt (2017) studied the relationship between the personality traits and (cyber)crime victimization. This is the first research that associated the link between the Big Five traits and cybercrime victims. Results show that people who score high on Agreeableness, Conscientiousness, and Emotional Stability tend to have a

lower chance to become victimized by cybercrime. Regarding the findings of Van de Weijer and Leukfeldt (2017) and the main characteristics of the personality traits, we conducted the following hypothesis:

H1: People who score high on Conscientiousness, Agreeableness, and Emotionality behave more securely online

In the paper of Van de Weijer and Leukfeldt (2017) they also stated that people that score high on Openness to Experience and Extraversion are more likely to be victimized by cybercrime. Regarding this finding and the main characteristics of the traits, we conducted the following hypothesis:

H2: People who score high on Openness to Experience, Extraversion, and Honesty-Humility behave less securely online

The relation between our control variables will also be analyzed. Ögütçü et al. (2015) found that students in the age category 18-30 have a higher risk to be victimized by cyberattacks. This is likely due to the usage of social media and internet. The authors state that younger people use social media and internet more than older people, which could increase their chance of being victimized. Therefore, the following hypothesis is conducted:

H3: Older people behave more securely than younger people.

Ögütçü et al. (2015) also found that the higher someone's education level is, the higher their information security awareness is. A higher level of education reduces the level of risk of being victimized. Therefore, the following hypothesis is conducted:

H4: A higher degree of education increases the security of online behavior

Methodology

The research in this paper is reviewed and approved by the ethics committee of the Erasmus School of Economics, with the corresponding ethics code: 2019/10/24-66842svz. This research will test the relationship between the HEXACO personalities and the behavior of individuals online. For this research, an online Qualtrics survey is administered. This survey includes both the SeBIS questionnaire (Egelman & Peer, 2015) and the 24-item Brief HEXACO questionnaire (De Vries, 2013), along with demographic questions about gender, age, and education.

Participants

We used a G-Power analysis[1] to calculate the optimal sample size for this research. We used a medium effect size of 0.15, and a significance level of 5%. The output generated by the G-Power analyses gave us an optimal sample size of 129. The participants in this research filled in a survey online in Qualtrics[2]. The survey was available in both English and Dutch, and was available for everyone older than 18. The survey was completely anonymous, but participants had to provide some demographics like age, gender, and education level. To attract as many participants as possible, a reward was given randomly to a lucky participant. The participants had the option to leave their email address if they wanted to, and with a randomizer a participant was randomly drawn and received twenty euros. Three participants were removed as they did not meet the age criteria or did not fill in the survey completely as was required. The survey that was conducted had in total 153 participants (*M* Age =30.19 years, Range 18-74, Males = 80), which was more than what than the 129 participants we needed. More than 50% of the participants was younger than 25 years. This indicates that the age distribution is not a normal distribution, but more skewed to the left. This is due to an overrepresentation of students. Education, the final variable, was a ranked categorical variable where 1 equals only finishing

[1] A G-power is a tool to compute statistical power analyses for many different t-tests. It can also be used to compute effect sizes and efficient sample sizes (Faul, Erdfelder, Lang, & Bunchner, 2007)
[2] Qualtrics is a only survey tool that allows one to build surveys, distribute surveys and analyze responses.

elementary school and 7 equals a participant that achieved a master's degree. The descriptive statistics are found in table 1.

VARIABLES	N	mean	sd	min	max
Honesty-Humility	153	14.77	3.054	6	20
Emotional	153	10.83	3.105	4	17
Extravert	153	14.70	1.919	8	19
Agreeableness	153	12.42	2.427	6	19
Conscientiousness	153	13.82	2.832	8	20
Openness To Experience	153	13.38	2.708	7	19
SecurityScore	153	73.73	11.02	43	96
Device Securement	153	20.10	4.424	6	29
Password Generation	153	19.86	3.179	12	26
Proactive Awareness	153	16.24	3.335	6	25
Updating	153	14.45	3.926	5	24
Age	153	30.19	14.27	18	74
Sex	153	1.464	0.501	1	2
Education	153	4.112	1.488	1	7

Table 1: Descriptive statistics.

Design

For this research, an online survey is conducted. The type of online survey is a questionnaire where a list of statements is distributed. The survey consists of two questionnaires that contain closed-ended statements in the form of a scale. Because we expect a low dropout rate, the demographics are asked at the end to prevent response biases. Our independent variables in the regression are 6 personality traits and demographic variables. The dependent variables in our research are the Security Score and the subscales. Because each participant is tested under all conditions, we use a within-subjects analysis. Within-subject experiments make it possible to use statistical procedures, which suits best with our research. The survey questions are randomized for each participant. Also, the order in which personality test statements and statements about the online behavior is ranked is randomized, so participants could either start with statements about their online behavior or start with the personality test.

Materials

The first part of the survey consists of the HEXACO personalities. The HEXACO measures how participants score across six different personality traits. HEXACO is used instead of the Big-Five Personalities as literature suggests that HEXACO gives a more thorough view of personalities than the Big-Five Personalities (Lee & Ashton, 2007). In the survey the participants are made aware that filling in the survey correctly is very important for this research. This is because in the beginning of the survey they are being informed that it is highly appreciated if they try to fill in the survey as correct as possible. De Vries (2013) developed a 24-item Brief HEXACO questionnaire to identify the HEXACO traits of individuals. This brief questionnaire will be used in our research as well. The questionnaire has 24 statements and has 4 specific statements per personality trait. For each statement, a person can either agree or disagree with the statements on a 1-5 Likert scale. The questions are framed in a way that in order to score maximum points for a specific personality trait, you have to disagree with two questions and agree with the other two questions. This is in line with the research of De Vries (2013), who also did this order to avoid that people will agree with everything. To simplify this, for every question that you have to disagree with in order to score highest on the given Personality trait, an ''R'' is played behind that question. This can be found in the Appendix, but the ''R" is not shown for the participant as that will lead to biases. With this method, the score per personality trait per participant is revealed. To calculate the score per personality trait per participant, we use the same scoring table as De Vries (2013) used. As mentioned before, there are four statements per personality trait in the questionnaire. For example, the personality trait Honesty-Humility has four questions that contains content about the characteristics of this personality trait (Sincerity, Fairness, Greed avoidance and Modesty.) (Dis)Agreeing with these statements yields the highest score as 5→1, 4→2, 3→3, 2→4 and 1→5. This, however, depends on whether the statement is reversely asked.

In the second part of the survey the security of online behavior is tested by using statements about their online behavior. For this research we use the SeBIS questionnaire made by Egelman and Peer (2015) to test the security online of individuals. The behavior of individuals online is tested in four subcategories which include: Device management, Password Generation, Proactive Awareness, and Updating. Not all categories have the same number of questions in the survey, as for instance 7 statements involve the category Proactive awareness, and only 5 questions are asked about the category Updating. The statements in the survey have

a 1-5 Likert scale, where 1 is Never and 5 is Always. In this questionnaire there are again some questions reversely asked to overcome biases. This way we formulated a minimum risk score (indicating a high security score) and a maximum risk score (indicating a low security score). In total there are 24 statements so the best security score someone can have is 120, while the lowest score is 24, which indicates the worst security score. This way the security score can be drawn from every participant and this can easily be linked with the personality traits. This method is the same for every subcategory where again a maximum and minimum risk score is formulated. The full questionnaire can be found in the Appendix.

In the last part the participants are being asked to fill in their gender, age, and highest degree of education. Age is a continuous variable as participants, while education is a categorical variable which ranges from having only an elementary school diploma and having obtained a master's degree on the university. This data is used to see if there is a relationship between these demographics and the behavior of individuals online. In our research these demographics are only used as control variables and do not cover the main research question.

Proposed analysis

In order to test the effect of the personality traits on the Security Score, multiple regressions have been made to analyze the different coefficient per personality trait. The regressions display whether the coefficient has a negative or positive effect on the Security Score per personality trait. Also, for every subcategory that formulates the Security Score a regression has been made. In total 5 regressions have been made to analyze the effect of personality traits on online behavior.

In line with personality research by Martin et al. (2011) and De Vries and van Gelder (2012), we calculated a correlation matrix to further analyze the relationship between the personality traits and the subcategories of the SeBIS questionnaire. A correlation matrix can easily identify whether there are strong or weak correlations between the different coefficients. With the combination of a simple regression and the correlation matrix we can identify which personality traits have an influence on the online behavior. Therefore, we can answer the hypotheses that there are differences in online behavior between personality traits.

Since previous research by Ögütçü et al. (2015) demonstrated an effect of age and education on risky online behavior, we analyzed whether an increase in age and education

level influences the security score. Regressing the dependent variable of security score and subcategories gives an insight in whether the independent variables age and education have a significant positive or negative effect on the security online. Since education is a categorical variable, an ANOVA test is performed to test whether an increase in level of the categorical variable has a significant impact on online behavior.

Results

For this research five regressions are made in order to test our hypothesis. The results of the regressions are reported in table 2. In table 3 the correlation matrix is reported. It is expected that there is a relationship between personality traits and online behavior. More specifically, we expect people that score high on Conscientiousness, Agreeableness, and Emotionality to behave more securely online. We also expect people who score high on Openness to Experience, Honesty-Humility, and Extraversion to behave less securely online. For the regressions, the dependent variables are Security Score (*M*= 73.73), Device Security (*M*=20.10), Password Generation (*M*=19.86), Proactive Awareness (*M*=16.24), and Updating (*M*=14.45). The independent variables in our dataset are the personality traits Honesty-Humility (*M* = 14.77), Emotionality (*M*=10.83), Extraversion (*M*=14.70), Agreeableness (*M*=12.42) Conscientiousness (*M*=13.82), Openness to Experience (*M*=13.38), and the demographics Age, Gender and Education.

VARIABLES	1 SecurityScore	2 DeviceSecurement	3 PasswordGeneration	4 ProactiveAwareness	5 Updating
Honesty-Humility	-0.313*	-0.0114	-0.127	-0.0660	-0.251*
	(0.379)	(0.158)	(0.117)	(0.120)	(0.140)
Emotionality	0.221	0.0575	0.0450	0.155	0.0180
	(0.362)	(0.151)	(0.112)	(0.115)	(0.134)
Extravert	0.423	0.375*	0.0249	-0.121	0.153
	(0.508)	(0.212)	(0.157)	(0.161)	(0.188)
Agreeableness	0.869**	0.131	0.0648	0.211*	0.300**
	(0.399)	(0.166)	(0.123)	(0.126)	(0.148)
Conscientiousness	1.094***	0.461***	0.188*	0.197*	0.261*
	(0.357)	(0.149)	(0.110)	(0.113)	(0.132)
Openness To Experience	0.419	0.115	0.168	0.207*	-0.0792
	(0.356)	(0.148)	(0.110)	(0.113)	(0.132)
Age	0.0889*	-0.0216	0.0241*	0.00174	0.0577**
	(0.0724)	(0.0302)	(0.0224)	(0.0229)	(0.0268)
Gender	0.441	0.401	0.00421	-1.034	0.900
	(2.526)	(1.053)	(0.781)	(0.800)	(0.936)
Education	0.275	-0.0943	0.192	0.0122	0.0972
	(0.678)	(0.283)	(0.210)	(0.215)	(0.251)
Constant	34.03**	5.043	13.71***	10.62**	5.978
	(13.16)	(5.486)	(4.070)	(4.166)	(4.875)
Observations	153	153	153	153	153
R-squared	0.137	0.121	0.063	0.108	0.118

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 2: Regression analysis

To test the effect personality traits have on online behavior, we made multiple regressions with Security Score and the four security subscales as dependent variables. High Security Scores indicate more secure online behavior. As expected, Conscientiousness has a positive significant effect on online behavior. This effect is visible in the regression analysis when regressing the Security Score as dependent variable. On average, scoring 1 point more on Conscientiousness increases the Security score by 1.094, ceteris paribus. This effect is

significant at a 1% significance level. On a subscale level, we only found an effect of Conscientiousness on Device Securement. When scoring 1 point on Conscientiousness, it raises the score of Device Securement with 0.461. This effect is significant on a 1% significance level. Although no significant effect is found in the other subscales, the coefficients were positive. To summarize and analyze the data further, we set up a correlation matrix which can be found in table 3. The goal of this correlation matrix was to observe patterns and significant correlations between the variables. This analysis is used in previous work by Martin et al. (2011) and De Vries and Van Gelder (2012). In our matrix the Security Score and the four subscales are correlated with the personality traits and the control variables. A significant positive correlation is found between Conscientiousness and the Security Score. Also, Conscientiousness shows a positive significant correlation with the subscales Device Securement and Updating. Positive correlations between Conscientiousness and the other two subscales was found, but these were not significant.

Personality Traits		Subscales of SeBIS			
	Security Score	Device Securement	Password Generation	Proactive Awareness	Updating
Honesty-Humility	-.037	.067	-.184**	-.159**	-.023
Emotionality	.042	.070	.010	.051	.046
Extraversion	-.051	.137	.018	-.098	.070
Agreeableness	.152**	.062	.023	.189**	.217**
Conscientiousness	.281**	.265**	.152*	.117	.195**
Openness to Experience	.076	.076	.121	.186	-.180*
Control Variables					
Age	.122*	-.029	.073	-.031	.176*
Gender	.054	.125	-.030	-.106	.073
Education	.017	-.015	.060	-.020	.008
Standard errors in parentheses					
*** p<0.01, ** p<0.05, * p<0.1					

Table 3: Correlation Matrix

As for the trait Agreeableness several significant results have been found. As expected, Agreeableness has a significant positive effect on Security Score. When scoring 1 point higher on Agreeableness, the Security score raises by 0.869, ceteris paribus. For the subcategories Updating a positive significant effect is found as well. Scoring 1 point in Agreeableness raises the score of Updating by 0.300, ceteris paribus. Agreeableness has a positive significant correlation with the Security Score. This indicates that a higher score on Agreeableness results into a higher Security Score, which is in line with our hypothesis. Also, a positive significant correlation was found between the trait Agreeableness and the subscales Proactive Awareness and Updating. For Device Securement and Password Generation no significant correlation is found, but the coefficients are positive.

For the trait Emotionality, no significant effect is found between the Security Score and the trait. This applies as well for the subscales as no significant effect is found between the subscales and the Emotionality trait. Therefore, no conclusions can be made based on the regressions for the traits Emotionality. The coefficients in the correlation matrix for Emotionality are positive. However, no significant correlation is found between Emotionality and the online behavior.

For the second hypothesis it is expected that the traits Honesty-Humility, Extraversion and Openness to Experience have a negative effect on online behavior. For the trait Honesty-Humility a negative effect is found between the trait and Security Score. On average, when scoring 1 point in Honesty-Humility it decreases the Security Score by 0.313, ceteris paribus. However, this effect is not significant. No significant effect is found between the trait and the subscales, but all coefficients except for Device Securement were negative. Although no significant effect for the Honesty-Humility trait is found in the regressions, the correlation matrix proves otherwise. No significant correlation is found between the Honesty-Humility trait and the Security Score, but there is a significant negative correlation found in two of the four subscales. Password Generation and Proactive Awareness show a negative significant correlation with the Honesty-Humility trait. For the remaining subscales negative correlations were found, but were not significant.

For the trait Extraversion no significant results have been found in both the regression table and the correlation matrix. What was interesting to see, is that most of the coefficients in the regression table showed a positive effect of the trait Extraversion on online behavior, which is in contrast to our expectations. The correlation matrix showed similar coefficients as the regression table did, because most of the coefficients show a positive correlation between the Extraversion trait and online behavior.

The findings for the trait Openness to Experience were also in contrast with our expectations. When regressing Security Score on the Openness to Experience trait, we found a positive effect. However, this effect is not significant. The subscale coefficients are almost all positive, except for Updating. None of these effects are significant as well. Again, the correlation matrix shows similar results regarding the coefficients. No significant correlation is found between the Openness to Experience trait and the online behavior.

For the remaining hypotheses, we analyze whether control variables Age and Education have any effect on the online behavior. To start with Age, we expect older people to behave more securely than younger people. To analyze this effect, we regress Age on Security Score. An additional year of age increases Security Score by 0.0889 points, ceteris paribus. However, this result is not significant. On a subscale level, we found a significant result for the effect of Age on Updating. An additional year of age significantly increases the score of Updating by 0.0577, ceteris paribus. Since a significant effect is only found for the effect of Age on Updating, we can say that the results are not in line with our expectations that Age has a positive significant effect on online behavior. Therefore, we reject the hypothesis that older people behave more securely online than younger people.

In order to answer the last hypothesis, we analyzed whether the categorical variable Education has any effect on online behavior. The regression displayed no effect between the level of Education and the Security Score. Also, no effect was found between Education and the subscales. To further analyze if there was any significant difference between different education levels, we performed an ANOVA test to check for differences in means and variance of the Security Score. With this analysis we found that the probability that every Education level has the same Security Score mean is 0.0523. To summarize and answer the hypothesis, the level of Education has no impact on online behavior. Although no significance effect was found in the regression, the means in Security Score of the Education levels were significantly different from each other.

Discussion

This study investigated the relationship between personality traits and online behavior. It was expected that some personality traits would display more secure online behavior than other traits. Previous literature by Van de Weijer and Leukfeldt (2017) analyzed the impact of the BF personality traits on online behavior. In their research they found that personality traits influence the online behavior. In our research, we use a more advanced measurement of personality, the HEXACO. We tested whether there is a relationship between HEXACO personality traits and online behavior. The main results in our paper indicate that Conscientiousness and Agreeableness have a positive significant effect on online behavior. The remaining personality traits showed no relationship with online behavior, which also applies for age and education.

According to research of Van de Weijer and Leukfeldt (2017) people who score high on Conscientiousness, Agreeableness and Emotionality are expected to behave more securely online. Van de Weijer and Leukfeldt (2017) found that when scoring high on Conscientiousness, Agreeableness, and Emotionality, there was a lower chance of becoming victimized by cybercrime. The findings in our paper support the research by Van de Weijer and Leukfeldt (2017), as a positive relationship is found between online behavior and the traits Agreeableness and Conscientiousness. We found no effect between Emotionality and online behavior, which goes against the existing literature by both Van de Weijer and Leukfeldt (2017) and Van Gelder and De Vries (2012). Research by Van Gelder and De Vries (2012) found a negative correlation between Emotionality and victimization. This indicated that scoring higher on Emotionality, results in a lower chance to become victimized. A research by Lodewyk (2017), who investigated the relationship between the HEXACO personality traits and victimization in school, is against the claim that Emotionality has no effect on victimization. He claimed that Emotionality and Extraversion are the sole predictors of victimization. This is not cybercrime victimization, but it indicates that Emotionality should have impacted victimization in general. In this case, we have to reject the hypothesis that when scoring high on the traits Emotional, Conscientiousness, and Agreeableness, an individual behaves more securely online. This is due to Emotionality not having any effect on online behavior. The other two personality traits displayed a positive effect on online behavior.

Furthermore, we expected people who score high on Openness to Experience, Extraversion and Honesty-Humility to behave less securely online. The expectations were based on previous literature by Van de Weijer and Leukfeldt (2017) and Van Gelder and De Vries (2012). Van de Weijer and Leukfeldt (2017) stated that people who score high on Openness to Experience and Extraversion were more likely to be victimized by cybercrime. In our research no significant negative effect was found between the traits Openness to Experience, Extraversion, and Honestly-Humility and online behavior. An interesting finding was that the coefficients of both Openness to Experience and Extraversion were positive instead of negative, indicating a positive relationship between the traits and online behavior. A research by Mulder and Aken (2013) supported the claim that there is a positive relationship between the traits Openness to Experience and Extraversion, and victimization. They investigated to which extend the BF personality traits affect whether a child will be victimized in the future. This is not cybercrime victimization, but due to a lack of research on this specific topic, crime victimization could be considered a good alternative as comparable research. Mulder and Aken (2013) found children who have high scores on Extraversion and Openness to Experience may protect them from being victimized in the future. This research may give us an indication as of why the coefficients were positive instead of expected negative coefficients.

As for Honesty-Humility we expected a negative relationship with online behavior based on research by Van Gelder and De Vries (2012). They stated that people who score high on Honesty-Humility tend are more likely to violate rules and therefore have a higher chance to become victimized. Although we found negative coefficients in our analysis for Honesty-Humility, no significant relationship is found between Honesty-Humility and online behavior. This finding can be supported by a research from Judges et al. (2017) who investigated the relationship between the HEXACO personality traits and fraud victimization. Regarding the trait Honesty-Humility, they explain that the relationship between victimization and Honesty-Humility can be interpreted in two ways. Honest individuals may be more likely to be victimized due to their optimistic expectation of others' honesty, or they may be protected by their desire to engage in fair behaviors, which results in a lower probability to become victimized. To put this in perspective, we did not find a relationship between Honesty-Humility and online behavior in our research, which could be due to Honesty-Humility having both a positive and negative effect on victimization.

For the relation between the control variables Age and Education we expected that older people and more educated people display a more secure behavior online based on previous findings by Ögütçü et al. (2015). Our results show no significant relationship between Age and online behavior. The most probable reason behind this finding is the abnormal Age distribution in our sample. Most participants were young adults which could cause a bias in our research. A specific research about the effect of Age on cybercrime has been done by Näsi et al. (2015). They claimed that due to younger people being more active Internet users, they have a more likely chance to become victims online. Therefore, we expect the insignificant result to be drawn from the abnormal age distribution.

For the other control variable Education, no effect is found between an educational degree and online behavior, which is against expectations and the research by Ögütçü et al. (2015). In a research about the relationship between phishing victims and risk factors by Leukfeldt (2014), he found that the probability of being a victim to phishing attacks is the same for all education levels. Becoming a victim of phishing attacks is a part of cybercrime, which is comparable to our research. A potential explanation of his findings is that there is no evidence of phishing perpetrators selecting their victims on education level or household with a lot of money. The findings by Leukfeldt (2014) can partly explain why no significant relationship is found between level of education and secure behavior online.

This research had some limitation in place. This research had a sufficient sample size, but participants were not that representative in terms of age. More than 50% of the participants was younger than 25 years old, which could have impacted the results. For our research we combined two brief questions which both had 24 statements. This is a limitation, as there are not many questions asked which could result in less accurate data. A recommendation for further research could be to use the 63-item HAIS-Q questionnaire by Parsons et al. (2014) instead of the SeBIS by Egelman and Peer (2015). Also, a research by Lee and Ashton provided evidence that expanding the HEXACO to a 60-item questionnaire could lead to more trustworthy results. The reason that we did not use that in our research, was because the expectation was that there would be a low participation when having a survey with 120 statements. The survey was provided online which could lead to some limitations as well. There was the possibility that people did not fill in their answers correctly, which could have impacted our results. Also, even when anonymous, tend to give socially desired answers to surveys or questionnaires (Carifo, 1994), which could lead to biased results as well. Recommendation

would be to test the relationship between online behavior and personality traits with a different research method, for example an experimental research. A big advantage of experimental research is that it provides researchers with a high level of control, which is not really the case when sending out surveys. It could be interesting to see if the results in this research hold when approaching it with experimental research.

Conclusion

Since a technical solution is not always the key to prevent cyber threats (Ng, Kankanhalli, & Xu, 2009), and humans can be seen as the most important factor in ensuring information security (Trček et al., 2007), we have dived into the relationship between personality traits and online behavior. Our research provided evidence that people who score high on the traits Agreeableness and Conscientiousness tend to behave more securely online. Also on subscale level, Agreeableness and Conscientiousness could be considered predictors of online behavior, as a significant positive relation is found between the traits and the subscales. For the other traits (Honesty-Humility, Extraversion, Openness to Experience, and Emotional) no significant relationship is found between the traits and online behavior. On a subscale level, only for Honesty-Humility a negative relationship is found between the trait and the subscales Password Generation and Proactive Awareness. The remaining traits had no significant relationship with the subscales of online behavior. We also analyzed whether our control variables Age and Education had any impact on the security online. In our research we did not find a significant positive effect that Age and Education could have on online behavior.

Personality traits have indeed an impact on online behavior, as Agreeableness and Conscientiousness have a positive significant effect on online behavior, even on subscale level. We managed to find two traits that could be considered predictors of secure online behavior and cybercrime victimization. Therefore, we conclude by saying that scoring high on Agreeableness and Conscientiousness has a positive influence on online behavior and decreases the chance of becoming victimized by cybercrime.

Bibliography

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

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

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*(pp. 36-58). Springer, Berlin, Heidelberg.

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making passwords secure and usable. In *People and Computers XII* (pp. 1-19). Springer, London.

Albladi, S. M., & Weir, G. R. (2017, November). Personality traits and cyber-attack victimisation: Multiple mediation analysis. In *2017 Internet of Things Business Models, Users, and Networks* (pp. 1-6). IEEE.

Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?. In *Advanced Computer and Communication Engineering Technology* (pp. 949-962). Springer, Cham.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Ashton, M. C., & Lee, K. (2007). Empirical, theoretical, and practical advantages of the HEXACO model of personality structure. *Personality and social psychology review*, *11*(2), 150-166.

Bensmann, L. (2009). Intelligent Search Strategies on Human Chosen Passwords. *Technishe Universtat Fakultat Für Informatik, Dortmond*.

Bradburry. (2019). Report Slams US Government for Poor Cybersecurity. *Infosec*, 1-6.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Chua, Y. P., & Chua, Y. P. (2017). Do computer-mediated communication skill, knowledge and motivation mediate the relationships between personality traits and attitude toward Facebook?. *Computers in Human Behavior*, *70*, 51-59.

De Vries, R. E., De Vries, A., De Hoogh, A., & Feij, J. (2009). More than the Big Five: Egoism and the HEXACO model of personality. *European Journal of Personality: Published for the European Association of Personality Psychology*, *23*(8), 635-654.

De Vries, R. E. (2013). The 24-item brief HEXACO inventory (BHI). *Journal of Research in Personality*, *47*(6), 871-880.

De Vries, R. E., Ashton, M. C., & Lee, K. (2009). De zes belangrijkste persoonlijkheidsdimensies en de HEXACO Persoonlijkheidsvragenlijst. *Gedrag en Organisatie*.

Ellrich, K., & Baier, D. (2016). The influence of personality on violent victimization–a study on police officers. *Psychology, Crime & Law*, *22*(6), 538-560.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *computers & security*, *31*(8), 983-988.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.

Galba, T., Solic, K., & Lukic, I. (2015). An information security and privacy self-assessment (ISPSA) tool for internet users. *Acta Polytechnica Hungarica*, *12*(7), 149-162.

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

Gulenko, I. (2013). Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. *Information Management & Computer Security*, *21*(2), 91-101.

Hansche, S. (2001). Designing a security awareness program: Part 1. *Information systems security*, *9*(6), 1-9.

Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 737-744). ACM.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220.

Ismail. (2019). Worldwide, targeted cyber attacks are on the rise. *Sonicwall*, 1-3.

Jardine, E. (2015). Global cyberspace is safer than you think: real trends in cybercrime. *Global Commission on Internet Governance Paper Series*, (16).

Jones, S. E., Miller, J. D., & Lynam, D. R. (2011). Personality, antisocial behavior, and aggression: A meta-analytic review. *Journal of Criminal Justice*, *39*(4), 329-337.

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in psychology*, *8*, 588.

Keszthelyi, A. (2013). About passwords. *Acta Polytechnica Hungarica*, *10*(6), 99-118.

Kokkinos, C. M., Antoniadou, N., Dalara, E., Koufogazou, A., & Papatziki, A. (2013). Cyber-bullying, personality and coping among pre-adolescents. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, *3*(4), 55-69.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security*, *25*(4), 289-296.

Lee, K., & Ashton, M. C. (2004). Psychometric properties of the HEXACO personality inventory. *Multivariate behavioral research*, *39*(2), 329-358.

Lodewyk, K. R. (2018). Associations between university students' personality traits and victimization and its negative affect in school physical education. *Journal of Physical Education and Sport*, *18*(2), 937-943.

Mak. (2017). The Human Factors in Cyber Security and Preventing Errors. *Vircom*, 1-7.

Martin, R. A., Lastuk, J. M., Jeffery, J., Vernon, P. A., & Veselka, L. (2012). Relationships between the Dark Triad and humor styles: A replication and extension. *Personality and Individual Differences*, *52*(2), 178-182.

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattison, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).

Mulder, S. F., & van Aken, M. A. (2014). Socially anxious children at risk for victimization: The role of personality. *Social Development*, *23*(4), 719-733.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47-66.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

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

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem?. *Computers in Human Behavior*, *52*, 424-435.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: two end user survey studies of motivation and security practices. *AMCIS 2004 proceedings*, 175.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133.

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113-118.

Trim, P., & Upton, D. (2016). *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Routledge.mation systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113-118.

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.

De Vries, R. E., & Van Gelder, J. L. (2013). Tales of two self-control scales: Relations with Five-Factor and HEXACO traits. *Personality and Individual Differences*, *54*(6), 756-760.

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

Violino. (2019). Cybercrime is increasing and more costly for organizations. *ZDnet*, 1-8.

Wilcox, P., Sullivan, C. J., Jones, S., & Van Gelder, J. L. (2014). Personality and opportunity: An integrated approach to offending and victimization. *Criminal Justice and Behavior*, *41*(7), 880-901.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330-340.

Appendix:

Survey

Dear participant,

Thank you for participating in our research. Your response is valued highly!
Participating in this research will only take 5-10 minutes.

By participating in this research, you have the chance to win 20 euros. This requires that you leave your e-mail address, but this is OPTIONAL. The address is only used to contact the winner. After that, all e-mail addresses will be deleted, and your answers will be analyzed strictly **anonymously**. The winner will be randomly picked between those who submit their email dresses.

First, there will be some personality statements where you can either agree or disagree with.

Q2
To what extend do you (dis)agree with these statements?

	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree
(O) I can look at a painting for a long time					
(C) I make sure that things are in the right spot					
(A) I remain unfriendly to someone who was mean to me (R)					
(X) Nobody likes talking with me (R)					
(E) I am afraid of feeling pain					
(H) I find it difficult to lie					
(O) I think science is boring (R)					
(C)I postpone complicated tasks as long as possible (R)					

	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree
(A) I often express criticism (R)					
(X) I easily approach strangers					
(E) I worry less than others (R)					
(H) I would like to know how to make lots of money in a dishonest manner (R)					
(O) I have a lot of imagination					
(C)I work very precisely					
(A) I tend to quickly agree with others					
(X) I like to talk to others					
(E) I can easily overcome difficulties on my own (R)					
(H) I want to be famous (R)					
(O) I like people with strange ideas (R)					
(C) I often do things without really thinking (R)					
(A) Even when im treated badly, I remain calm					
(X) I am seldom cheerful (R)					
(E)I have to cry during sad or romantic movies					
(H) I am entitled to special treatment					

Now, there will be some statements that ask you about your security online. You can either agree or disagree with these statements. Read them carefully!

To which extend do you (dis)agree with these statements?

	Never	Almost never	Sometimes	Almost always	Always
When I'm prompted about a software update, I install it right away	○	○	○	○	○
When my computer wants me to reboot after applying an update or installing software, I put it off (R)	○	○	○	○	○
I try to make sure that the programs I use are up-to-date	○	○	○	○	○
I manually lock my computer screen when I step away from it	○	○	○	○	○
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	○	○	○	○	○
I log out of my computer, turn it off, put it to sleep, or lock the screen when I'm done using it.	○	○	○	○	○
I use a PIN or passcode to unlock my mobile phone	○	○	○	○	○
I use a password/passcode to unlock my laptop or tablet	○	○	○	○	○
If I discover a security problem, I continue what I was doing	○	○	○	○	○

	Never	Almost never	Sometimes	Almost always	Always
because I assume someone else will fix it (R)					
When someone sends me a link, I open it without first verifying where it goes. (R)					
I verify that my anti-virus software has been regularly updating itself					
When browsing websites, I mouseover links to see where they go, before clicking them					
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.					
I backup my computer					
When I hear about websites that have been hacked, I wait to change my passwords until I have been personally notified (R)					
I use some kind of encryption software to secure sensitive files or personal information.					
I do not change my passwords, unless I have to. (R)					
I use different passwords for different accounts that I have					

	Never	Almost never	Sometimes	Almost always	Always
I do not include special characters in my password if it's not required. (R)					
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.					
When I'm done using a website that I'm logged into, I manually log out of it.					
I submit information to websites without first verifying that it will be sent securely (R)					
I use privacy software, "private browsing," or "incognito" mode when I'm browsing online					
I clear my web browsing history					

What is your age?

What is your sex?

- Male
- Female

What is your highest degree of education?

Thank you for participating in my Master Thesis. Your response is greatly appreciated! If you want to participate in a chance to win 20 euros, you can leave your email address below: