University of Twente

BSc. Psychology

Bachelor Thesis – Risk and Safety

Faculty of Behavioral, Management and Social Sciences

Relationship between personality variables and the perceived self-efficacy to protect against cyber-crime of young adults

Finished: 28.06.2021

Niklas Kindt
s2200627

Abstract

During the Covid-19 pandemic, the internet created opportunities to continue work, education, and social interaction without risking an infection. However, it also enabled criminals new opportunities and chances which were displayed in a significant increase of cybercrime. To counteract these developments in a growing body of literature focused on the underlying factors. Resulting, research and security experts reported that the human is the most error-prone part of cybersecurity while still, significant gaps exist in scientists' understanding of protective behavior determinants. This study explored the factor self-efficacy beliefs towards cybercrime protection, which were indicated by the Protection Motivation Theory as well as the Health Belief Model as a significant determinant for actual protection behavior. In specific, the study explored demographic as well as psychological variables influence on self-efficacy beliefs of young adults. This was tested through an online survey that was distributed on social media as well as the online service Sona. Results indicated, on the one hand, that there was a significant association between self-efficacy beliefs of young adults towards cybercrime protection behavior and their actual engagement in protection behavior. In other words, the results support the notion, of the Protection Motivation Theory, that actual protection behavior is influenced by the coping appraisal. On the other hand, that the demographic, as well as psychological factors of young adults could not be highlighted as a significant influence on their level of self-efficacy. Overall, the study indicated opportunities to develop a more detailed understanding of variables influencing the protection behavior to ultimately promote the safety of the Internet.

Contents

Relationship between personality variables and the perceived self-efficacy to protect against cyber-crime of young adults

In 2020 Covid-19 changed everyday life. To protect as many lives as possible, various governments had introduced policies to decrease interpersonal contact to the minimum while emphasizing the importance of “spatial distancing”. Schools and universities were forced to further educate their students in online classes while companies enabled their workers to home office as much as possible. While the internet is providing opportunities for people to work and socialize during the Covid-19 pandemic, the internet also enabled criminals opportunities and chances. According to Lallie et al (2021), the amount of cybercrime has significantly increased during the Covid-19 pandemic, while for example phishing being reported to have increased by 600% in March 2020.

Considering that Covid-19 had also forced many people without experience and know-how to use the internet frequently, a further rise in cybercrime can be expected. Supporting, Cheng, Chan, and Chau (2020) found evidence for a positive correlation between ICT use and cybercrime victimization. In regard to the increased use and dependence on the internet, protection against cybercrime became the focus of various nations. For example, former US-president Obama proposed, at the end of his administration, to spend more than 19 billion US-Dollars on cybersecurity (Van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). Especially, focusing on the human operating the system, while researchers and security experts reported that the human is the most error-prone part of cybersecurity (Van Bavel et al., 2019).

In spite of robust empirical evidence regarding the increase and hazardousness of cybercrime, significant gaps exist in scientists’ understanding of protective behavior determinants. More specifically, what influences individuals to engage in protective behavior against cybercrime. Furthermore, existing theories, for example the Protection Motivation Theory formulated by Rogers, did not take important factors, namely personality and demographics, into account. Consequently, the question arised to what extent we can connect recent research with existing literature to improve the understanding of protective behavior determinants. The present study explored the relationship between demographic variable, namely gender, as well as psychological variable, namely personality, in regard to the self-efficacy beliefs of young adults. Furthermore, the study examined if high self-efficacy beliefs are correlated to actual protection behavior.

Determinants of Cybercrime

Similar to traditional crime, cybercrime is difficult to define because it occurs in a variety of environments and forms. Gordon and Ford (2006) tried to define cybercrime as any crime that is planned or committed using a computer, network, or hardware device. Furthermore, Gordon and Ford (2006) separated cybercrime into two types: the first type is described as mostly technological nature, meaning the crime is focused on the hardware or data of the victim. Examples would be phishing attempts, identity theft, or manipulation of data mostly via hacking or viruses. The second type of cybercrime is focused on the human aspect, meaning the crime is focused on the victim and not on the hardware. Examples would be cyberstalking, harassment, blackmail, or child predation (Gordon & Ford, 2006).

Similar to Gordon and Fords' model, Furnell (2011) proposed to categorize cybercrime in a continuum ranging from crime which is entirely natural, to crime, which is entirely computer-based. According to Ibrahim, Nnamani, and Soeyele (2020) the most common types of cybercrimes can be classed into seven categories, the first is named “Biometric verification number scam” and includes cybercrimes that gather biometric information of the victim in order to access their bank accounts. The second type is called “Phishing” and includes all criminal activities in which the perpetrator is stealing personal data of unsuspecting targets to, for example, recreate their identity on the internet. The third type is named “ATM Fraud” and groups criminal behavior that focus on stealing credit cards and PINs throughout manipulated ATMs. Drawing back to the continuum proposed by Furnell, the first and second types can be categorized at the computer-based end of the continuum while the third type can be categorized on the natural end of the continuum because the computer is only the tool of the crime. The fourth type is named “Sales scam and counterfeit” and is focused on crimes in which the criminal is selling imitative goods or sometimes absent products. The next type is called “Cyber-plagiarism” and is grouping crimes in which the criminal is stating ideas or even complete texts of the victim as their own. The sixth type is called “Illegal e-lotteries” and includes all crimes in which the criminals try to get information and personal data in fake lotteries. The last type is called “Advanced fee-scam” and is grouping all crimes in which the criminal requesting money in advance while not delivering the acquisition (Ibrahim et al., 2020).

Furthermore, Ibrahim et al (2020) described three cybercrime prevention methods, the first is “Government interventions” and focus on the rules and regulations the government is implementing to decrease cybercrime. An example would be the implementation of new laws or the increasement of the fine. The second prevention behavior is “Personal security control" and is focused on self-protection, meaning the ICT user's protection behavior. In specific, it includes the competency in setting passwords as well as the caution to not publish confidential information. The third prevention method is "Knowledge-gaining practices" which highlights the importance that ICT users should update their know-how about protection methods constantly. Furthermore, ICT users should also gain knowledge about the types and procedures of cybercrime in order to better recognize cybercrime (Ibrahim et al., 2020).

The importance of protection behavior of the ICT user is highlighted, considering that two of the three prevention methods are focused on the personal initiative of the ICT user while researcher and security experts reported that the human is the most error-prone part of cybersecurity (Van Bavel et al., 2019). More specifically Van Bavel et al (2019) reported that criminals use knowledge about human behavior to explicitly focus on the human weakness in cybersecurity. Examples would be, phishing emails that seem to be written by authorities or at times when victims are busy (Van Bavel et al., 2019). These methods are often times very successful, highlighted by a survey conducted in the united states in which 64% of the participants stated that they had personally experienced cybercrime (Smith, 2017). The question arises what the defining factors are of human protection behavior in regard to cybersecurity and how can they be assessed in order to fight further cybercrime.

Human protection behavior when facing a threat

There are multiple theories accounting for human protection behavior when facing a threat that can also be applied to the threat of cybercrime. One of the most influential is the Protection Motivation Theory formulated by Rogers (1975), which is based on the assumption that the human is trying to engage in protection behavior when the protection motivation is sufficient (Norman, Boer, and Seydel, 2005). Furthermore, the protection motivation is influenced by two independent appraisal processes (Norman et al., 2005). The first appraisal process is called threat appraisal and is focused on the individuals' perception of the severity and vulnerability towards a specific threat (Norman et al., 2005). For example, people may consider the chance to become a victim of cybercrime as low or do not consider cybercrime as dangerous which will lead to low threat appraisal and, therefore, these people will not consider protecting themselves against cybercrime as important.

The second appraisal process is called coping appraisal and is focused on factors increasing or decreasing the probability of an adaptive response (Norman et al., 2005). Mainly consisting of response efficacy, the belief that a recommended behavior will be effective, and self-efficacy, the belief that one is capable of performing a recommended behavior (Norman et al., 2005). In combination with the response cost, which is defined as the costs or barriers that a specific protective behavior requires, it is defining to what extended adaptive behavior occurs (Norman et al., 2005). Drawing back to the example of cybercrime, an individual who thinks that protection behavior against cybercrime will reduce the chance of becoming a victim and who feels capable of protecting him or herself will be high in the coping appraisal.

Nevertheless, the Protection Motivation Theory formulated by Rogers does not take into account factors or predeterminants that are impacting the coping and threat appraisal. In other words, the Protection Motivation Theory is highlighting that the protection motivation is determined by the coping and threat appraisal but is dismissing information that further determines the coping and threat appraisal. Similarly, the Health Belief Model and the Protection Motivation Theory are based on similar underlying principles influencing human behavior. Meaning, both models account the threat appraisal as well as coping appraisal as the main factors influencing the behavior of an individual (Abraham & Sheeran, 2005). Both theories describe threat appraisal as the perception of the risk and coping appraisal as the self-efficacy beliefs of the individual. Nevertheless, the Health Belief Model further focuses on factors influencing risk perception and self-efficacy beliefs. In specific, the model named demographic variables, for example, class, gender, or age as influences as well as psychological variables, for example, personality or peer group pressure (Abraham & Sheeran, 2005). Considering that the Protection Motivation Theory formulated by rogers is neglecting factors influencing the coping and threat appraisal further development of the theory is necessary.

It is especially of importance to consider the growing body of literature that focuses on demographic as well as psychological variables, as existing literature underlines that personality, age and risk perception are closely connected. For example, people high in conscientiousness perceive risks concerning their physical health more intense than risks concerning the nature development (Chauvin, Hermand, & Mullet, 2007). Focusing on the risk of cybercrime, a study conducted on students in the Netherlands showed that the perceived risk of becoming a victim of cybercrime is generally lower than the actual risk (Seijen, 2021). Meaning, the students do not perceive the risk of becoming victims of cybercrime as high which leads to a low threat appraisal and no protection behavior. Nevertheless, this study found no correlation between demographic variables, such as gender, age, or social status, and the risk perception of the students. Additionally, there was also no correlation found between the psychological variables, specifically their personality, and their level of risk perception (Seijen, 2021).

Although there is a growing body of literature focusing on cybercrime research lacks the perspective on factors influencing ICT users to engage in more or less protection behavior. While it has been shown that protective behavior is influenced by the threat and the coping appraisal both need to be explored in order to understand why some people protect themselves better than others. Considering the finding that demographic, as well as psychological variables, are not influencing the threat appraisal further research should highlight their influence on the coping appraisal, while there exists a substantial gap in literature.

The coping appraisal – when and how to react to a threat

The coping appraisal, as described by the Protection Motivation Theory and Health Belief Model, is consisting of response efficacy, the belief that a recommended behavior will be effective, and self-efficacy, the belief that one is capable of performing a recommended behavior (Norman et al., 2005). Furthermore, the Health Belief Model is describing demographic as well as psychological factors influencing the coping appraisal.

In specific, the model is naming age, gender, and class as main demographic factors influencing the coping appraisal which, therefore, also appear to be relevant in cybercrime prevention and need to be taken into account. Putting it into the perspective, according to DeYoung and Spence (2004) females are less confident and more anxious about using the internet which would result in a lower coping appraisal and lower protection motivation. Regarding the factors age and socioeconomic status, existing literature highlights that teens and young adults, high in socioeconomic status, are the most prominent internet users (Lenhart, Purcell, Smith, & Zickuhr, 2010). Taking into account the finding of Cheng, Chan, and Chau (2020) that internet usage is positively correlate to cybercrime victimization, teens and young adults have the highest chances to become victims of cybercrime. Therefore, further research on cybercrime should be focused on teens and young adults while these are the most at risk.

Focusing on the psychological factors influencing the coping appraisal, existing literature explains the importance of personality and its impact on the behavior of individuals, nevertheless, lacks the connection to cybercrime protection motivation. One of the most cited theories is the HEXACO-model which divides the personality of an individual into six sub-categories (Ashton & Lee, 2009). The first sub-category is called “Honesty-Humility” and focuses on the extent to which an individual is sincere, fair, and modest (Ashton & Lee, 2009). The second sub-category is called “Emotionality” and highlights the extent to which an individual is fearful, anxious, and sentimental (Ashton & Lee, 2009). The third sub-category described in the HEXACO-model is named “Extraversion” and highlights the social selfesteem, social boldness, as well as sociability of an individual (Ashton & Lee, 2009). The fourth sub-category is named “Agreeableness” and highlights the forgiveness, gentleness, as well as patients of an individual (Ashton & Lee, 2009). The fifth sub-category is named “Conscientiousness” and describes the organization, perfectionism, and prudence of an individual (Ashton & Lee, 2009). The last sub-category of the HEXACO-model is named “Openness to Experience” and focuses on creativity and unconventionality of an individual (Ashton & Lee, 2009).

Connecting the personality traits of the HEXACO-model to the coping appraisal in the cybercrime protection perspective, being fearful and anxious could impact the perception of feeling capable of protecting oneself against cybercrime negatively. Consequently, this will result in a lower coping appraisal and, therefore, less protection motivation. In other words, being high in ‘Emotionality’ could, therefore, impact the coping appraisal negatively and lead to a lower cybercrime protection behavior and higher risk of becoming a victim. Furthermore, the personality trait ‘Conscientiousness’ could be important in understanding the differences in cybercrime protection behavior as well. Considering that individuals, categorized as high in the personality trait ‘Conscientiousness’, are described as perfectionistic, they probably would also choose a thoughtful and safe password. Next to that, being good in organization would also increase the protection organization which could result in more effective and efficient protection behavior.

The present research

Considering the importance of improving cybercrime protection and the existing gap in literature considering the coping appraisals of individuals regarding cybercrime protection, the following study is focused on supplementing the existing literature. Taking into account that existing literature focused foremost on the risk perception aspect of the coping appraisal the following study is focused on the self-efficacy beliefs of individuals protecting themselves against cybercrime. In specific, this study will explore the relationship between demographic variable, gender, as well as psychological variable, personality, in regard to the self-efficacy beliefs of individuals.

As mentioned above, the finding from Lenhart et al (2010), that teens and young adults are the most prominent internet users, and the finding from Cheng et al (2010), that internet usage correlates positively to cybercrime victimization, suggest that teens and young adults are the most prominent cybercrime victims. Therefore, the following study will focus on young adults in order to reveal underlying factors that could be used in future cybercrime prevention training to ultimately protect the most prominent cybercrime victims.

Overall, the research question: "To what extent do demographic as well as psychological variables influence young adults' level of perceived self-efficacy regarding cybercrime protection?" is divided into multiple sub-hypotheses. The first hypothesis states that females are lower in self-efficacy beliefs regarding cybercrime protection than males. The second hypothesis states that high "Emotionality" is connected to low self-efficacy beliefs regarding cybercrime protection. The third hypothesis defined that "Conscientiousness" is positively connected to the self-efficacy beliefs regarding cybercrime protection, meaning high "Conscientiousness" is connected to high self-efficacy beliefs. The last hypothesis is that the level of perceived self-efficacy and the extent of actual protection behavior are positively correlated.

Methods

Design

In order to assess whether demographic and/or psychological variables influence young adults' level of perceived self-efficacy regarding cybercrime protection, quantitative data was collected. In specific, a correlational survey design was implemented in which the effects of demographic and psychological variables on perceived self-efficacy were tested.

Participants

In total, 143 participants took part in the study from which 80, on the one hand, fulfilled the criteria of being between the age of 18 and 30 years old and on the other hand complete the study. Overall, 31 participants were male (38.8%) while 49 were female (61.3%), the mean age was 21.08 (SD=2.01) years old while 77.5 percent were German, 15 percent were Dutch, and 7.5 percent were from other European countries. Furthermore, 82.5 percent of the participants had a Highschool degree while 17.5 percent had a university degree. The mean time indicated as spend on the internet daily was 5.85 hours with a standard deviation of 2.62 hours.

Materials

Questionnaires

Self-efficacy In order to measure self-efficacy beliefs towards cybercrime protection the eight items, seven point Likert general self-efficacy scale developed by Chen, Guilly, and Eden (2001) was modified without changing the intent of the items (See appendix B). For example, item one stated originally: “I will be able to achieve most of the goals that I have set for myself” which was converted to “I will be able to achieve most of the protection goals that I have set for myself”. Overall, all eight items were modified in order to assess the self-efficacy beliefs towards each sub-category of cybercrime, specifically “Biometric verification number scam”, “Phishing”, “ATM Fraud”, “Sales scam and counterfeit”, “Cyber-plagiarism”, “Illegal e-lotteries”, “Advanced fee-scam” as indicated by Ibrahim et al (2020). Furthermore, the internal consistency was good with Cronbach’s alpha of .80.

Personality To investigate the relationship between personality and self-efficacy beliefs the Hexaco-60, developed by Ashton and Lee (2009), was administered (See appendix C). The Hexaco-60 is a self-report personality questionnaire consisting of 60 Items which are measured on a 5-point scale (strongly disagree – strongly agree). The Cronbach’s alpha for each subscale in this study range from .74 to .82. More specifically, the subscales ‘Honesty humility’ and ‘Agreeableness’ had the lowest Cronbach’s alpha of .74, followed by ‘Emotionality’ with a Cronbach’s alpha of .75. Openness to experience’ had a Cronbach’s alpha of .77 while ‘Extraversion’ was reported as .79. Overall ‘Conscientiousness’ had the highest Cronbach’s alpha of .82. Furthermore, the subscales of the Hexaco-60 correlate sufficiently with the subscales of the NEO-FFI while the self-observer agreement for all subscales were exceeding .45, which in fact, can be considered as reasonably high (Ashton & Lee, 2009).

Actual protection behavior To establish whether high self-efficacy beliefs towards cybercrime protection result in better protection behavior, the participants were asked to indicate to what extent they protect themselves (See appendix D). Therefore, two items were developed based on the prevention methods Ibrahim et al (2020) indicated as most effective. More specifically, Ibrahim et al (2020) highlighted that an individual had two possible protection behaviors that were effective against cybercrime, the first was named “Personal security control" and includes the competency in setting passwords. Therefore, the item was assessed on a 5-point scale (strongly disagree – strongly agree) to what extent participants choose their passwords thoughtfully. The second item was developed based on the method named “Knowledge-gaining practices” which highlights the importance that ICT users should update their know-how about protection methods constantly. The participants were asked to indicate on a 5-point scale (strongly disagree – strongly agree) if they informed themselves about specific threats in advance. In order to establish if actual protection behavior is impacted by the type of cybercrime, the two items developed were addressed to each sub-category of cybercrime as indicated by Ibrahim et al (2020). Overall, Cronbach’s alpha ranged between .43 and .61, which can be considered adequate while taking into account that only two items were used.

Procedure

Participants were recruited through social media as well as the respective online recruitment service of the University of Twente. The purpose of the study was briefly explained as well as the limitation that a sufficient level of the English language is required.

The active online informed consent (See appendix A) highlighted that the gathered data will be handled confidentially and that participant’s names as well as other potentially identifying information would not be accumulated. Following the informed consent, participants were asked questions about their self-efficacy beliefs towards cybercrime protection for each of the seven different forms of cybercrime. After that, the HEXACO-60 was administered to the participants in order to assess their personality characteristics. Which then was followed by questions about their actual protection behavior against each of the seven different cybercrime forms. Lastly, the demographic variables were recorded while participants were asked about their age, gender, education as well as how much time they spend on the internet each day (See appendix E).

Results

Correction of data

First and foremost, the data was imported from the online survey software ‘Qualtrics’ to the statistical program ‘SPSS’. To ensure reliability and validity, incomplete surveys were excluded from the data set. Next, 29 items of the HEXACO-60 were originally written in reversed polarity and needed to be recoded. Furthermore, the items that represent one personality trait, as indicated by the HEXACO-60, were grouped to achieve one comparable mean score for each personality trait. Lastly, an overall score of self-efficacy towards cybercrime protection was created by taking the mean of all self-efficacy sub-categories as well as an overall score of actual protection behavior by taking the mean of all actual protection behavior subcategories.

Preliminary analyses

In order to get a general overview of the data and to check for potential misleading information, for example flooring or ceiling effect, general descriptive statistics of all variables were made (Table 1). In general, the variables display a Gaussian function, in specific a mean that is close to the middle of the scale used and normally distributed. The only exception is the variable 'Time on Internet' which ranged from 1 to 15 with a mean of 5.85 and a standard deviation of 2.62.

Table 1.

Descriptive statistics of all variables

Variable	N	Minimum	Maximum	Mean	Std. Deviation
Time on Internet	80	1	15	5.85	2.62
Honesty-Humility	80	1.6	4	2.86	.46
Emotionality	80	2	3.7	3	.34
Extraversion	80	1.8	3.8	2.92	.37
Agreeableness	80	2	3.8	2.98	.37
Conscientiousness	80	2	4.1	3.07	.38
Openness to Experience	80	2	3.6	2.94	.34
Self-efficacy Mean	80	1.27	5.73	2.85	.75
Protection Behavior Mean	80	1	4.21	2.54	.75

Main analyses

Overall, we performed two general linear models. In the first, demographic and psychological factors were defined as independent variables and the level of perceived self-efficacy as the dependent factor. In the second, we defined perceived self-efficacy as independent factor while the level of actual protection behavior was defined as the dependent one.

More specifically, for the first hypothesis, we examined the effect of gender on the level of perceived self-efficacy towards cybercrime protection. We, therefore, conducted a general linear model with gender as the independent variable and the level of perceived self-efficacy dependent variable. For the second hypothesis, we assessed to what extent personality is influencing the level of perceived self-efficacy towards cybercrime protection. Meaning, we performed a general linear model with the different personality traits as independent variables and the perceived self-efficacy as the dependent variable, while highlighting the influences of emotionality and conscientiousness in specific. For the last hypothesis, we conducted a general linear model with the level of perceived self-efficacy as independent variable and the level of actual protection behavior as the dependent variable. To conclude, further analyses were performed in order to get a more detailed picture of the self-efficacy beliefs and actual protection behavior.

Gender on self-efficacy beliefs

Overall, the one-way between-subject analysis with gender as the independent variable and the level of self-efficacy beliefs as the dependent variable showed no significant difference while the mean score of all participants was balanced (*M*=2.85, *SD*=.75). In other words, the level of self-efficacy between males (*M*=2.75, *SD*=.63) and females (*M*=2.91, *SD*=.81) did not differ significantly (*F*(1,78)= 0.86, *p*=.36), which can be highlighted by an eta squared of .78.

Personality on self-efficacy beliefs

In order to assess to what extent personality is influencing the level of perceived self-efficacy a general linear model was conducted. Overall, no significant regression equation was found (R^2=.10, *F*(6,73)=1.40, *p*=.23). In other words, self-efficacy does not depend on honesty humility (*β*=.01, *p*<.959), emotionality (*β*=-.16, *p*<.196), extraversion (*β*=.13, *p*<.282), agreeableness (*β*=.13, *p*<.257), conscientiousness (*β*=.02, *p*<.922), nor openness to experience (*β*=.20, *p*<.111).

Self-efficacy beliefs on actual protection behavior

To assess the extend to which self-efficacy beliefs influence are associated with actual protection behaviors a general linear model was conducted. A significant causation was found (R^2=.26, *F*(1,78)=27.5, $p < .001$). Therefore, self-efficacy significantly predicted actual protection behavior scores (*β*=.51, *p*<.001).

Further analyses of self-efficacy beliefs

Follow-up analyses on the variable self-efficacy beliefs underlined, on the one hand, that time spent on the internet is not significantly associated with self-efficacy beliefs (*F*(1,78)=.94, *p*=.34). But on the other hand, that a significant regression equation between age and self-efficacy beliefs exists (R^2=.07, *F*(1,78)=6.11, *p*=.02). Consequently, age significantly predicted the level of self-efficacy beliefs (*β*=- .1, *p*<.016). In other words, as age increase self-efficacy decreased.

Further analyses of actual protection behavior

Follow-up analyses on actual protection behavior highlighted that no significant regression equation was found between personality traits and actual protection behavior (R^2=.14, *F*(6,73)=1.97, *p*=.08). Furthermore, time spend on the internet is not significantly associated with actual protection behavior (*F*(1,78)=.11, *p*=.74). Next, there was also no significant difference between males (*M*=2.71, *SD*=.71) and females (*M*=2.42, *SD*=.76) actual protection behavior found (*F(*1,78)=2.8, *p*=.1). Lastly, no significant regression equation was found between age and actual protection behavior (*F*(1,78)=33.02, *p*=.09).

Discussion

In the last years, the protection against cybercrime not only raised attention because of the increased occurrence and hazardousness but also because significant gaps exist in scientists' understanding of protective behavior determinants. Existing theories, thus far, attempted to explain protection behavior by assessing the threat and coping appraisal but did not consider determinants influencing the threat and coping appraisal. The present study is, therefore, assessing to what extent determinants, demographic as well as physiological, influence the coping appraisal towards cybercrime.

In line with the expectations, young adults that possessed higher self-efficacy beliefs were engaging in more actual protection behavior against cybercrime compared to young adults that possessed lower self-efficacy beliefs. Nevertheless, the difference in the level of self-efficacy beliefs possessed by young adults could not be explained by their personality traits. Furthermore, no difference in the level of self-efficacy was found by comparing males and females. These findings suggest that gender, as well as personality, are not determinants for self-efficacy beliefs, unlike age which had a negative impact on the level of self-efficacy beliefs possessed.

Further understanding of Protection behaviors and their determinants

The purpose of the study was to gain a better understanding of the factors influencing people to engage in protection behavior against cybercrime, specifically focusing on the factor self-efficacy beliefs. Our findings align with the original notion of the Protection Motivation Theory formulated by Rogers 1975, in which actual protection motivation is partially predicted by self-efficacy beliefs. The results provide supporting evidence for a positive correlation between self-efficacy beliefs and actual protection behavior, meaning that higher self-efficacy beliefs can be associated with more engagement in actual protection behavior (Norman et al., 2005). Consequently, individuals with high self-efficacy beliefs are focusing more on protection behavior than people with lower self-efficacy beliefs.

This finding also aligns with the Health Belief Model, which, equal to the protection motivation model, also defined self-efficacy beliefs as a determinant of actual protection behavior (Abraham & Sheeran, 2005). Considering that the Health Belief Model further defined demographic as well as psychological factors underlying self-efficacy, the results provide evidence for age as a defining factor (Abraham & Sheeran, 2005). In other words, increasing age was connected to a decrease in self-efficacy beliefs towards cybercrime protection behavior, therefore, younger people had higher self-efficacy beliefs compared to older people. This finding can be explained by the idea from Wang, Myers, and Sundaram (2013) who conceptualized 'Digital fluency'. 'Digital fluency' is defined as a continuum ranging from 'digital natives', young people who grow up using ICT and became fluent using it, to 'digital immigrants', mostly older people who grow up without ICT and were forced to implement ICT later on in their lives (Wang et al., 2013). This would explain the high self-efficacy believes in young adults because they grow up using these technologies, and the tendency that older adults do not feel as self-efficient, because they needed to implement them in their lives later on.

Nevertheless, further results do not align with the notion of the Health Belief Model, that self-efficacy beliefs are defined by the demographic variable gender or by the psychological variable personality. More specifically, the results are inconsistent with DeYoung and Spence's (2004) idea that females possess a lower coping appraisal and lower protection motivation because no significant difference between males and females were found for the level of self-efficacy nor for the engagement in actual protection behavior. These findings are also in line with the conceptualization of 'digital fluency' by Wang et al (2013) because demographics, for example age or socioeconomic status, were defined as determinants of 'digital fluency' but not the demographic factor gender. Wang et al (2013) explained that males and females do differ in their content usage of ICT but not in the extent of usage. Therefore, males and females feel similarly self-confident using ICT which results in similar self-efficacy beliefs protecting themselves against cybercrime. This finding implicates that gender does not impact the level of self-efficacy possessed by young adults but highlights that the self-efficacy beliefs are achieved throughout different content usage. This could be an interesting starting point for future research because training methods, to improve self-efficacy beliefs, could be tailored to the content preference for each gender to be as effective and efficient as possible.

Furthermore, contrary to the expectation that emotionality and conscientiousness are defining factors for self-efficacy, which were based on the HEXACO-model, no significant effect of personality on the level of self-efficacy was reported. As mentioned above, this could be a result of a sample that is too close to the 'digital native' end meaning personality would only be a determinant for people that need to implement ICT in their lives and not for people that grow up using it. Furthermore, it could be the case that personality is not influencing this specific protection behavior while still determining other protection behaviors. Especially, the personality trait emotionality could be impacted by the fact that the threat is not physical or actual visible, this would be in line with the findings of Seijen (2021) who reported that the average Dutch student underestimates the risk of becoming a victim of cybercrime. This finding highlights the importance of raising awareness for the increase and hazardousness of cybercrime. Moreover, future research could investigate if the personality trait emotionality is impacting the self-efficacy beliefs towards cybercrime protection behavior when the awareness of cybercrime is used as a moderation variable.

Limitations and strengths

The first limitation that needs to be considered is that only self-administered online questionaries were used in a limited sample. Therefore, the reliability and validity of the results were impacted, and actual significant results could be displayed as insufficient in the results or the other way around. Especially, tendencies, for example, age and actual protection behavior, which were slightly not significant, need to be considered further.

Another limitation of the study that needs to be taken into account is the limited age range of participants. In order to actually display the continuum described by Wang et al (2013) ranging from 'digital nomads' to 'digital natives' a broader age range is necessary. Considering that the mean age of the sample is 21.08 years old, and the standard deviation is 2.01 years the sample was not spread enough. In other words, the survey's sampling distribution was not sufficient in order to support reliable and valid age differences. Furthermore, it is possible that the wrong age group was chosen as the target group, considering that the majority of the sample could be identified as 'digital natives' while characteristics as personality or gender do not impact their self-efficacy to the extent it would impact 'digital nomads'.

Despite the limitations, the study had multiple strong points, for example, publishing the study online guaranteed that only people who had access to the internet were able to take part. Therefore, participating in this study had the same requirements as becoming a cybercrime victim. In other words, publishing the study online helped in reaching the people who are the most at risk of becoming cybercrime victims and, therefore, the people who need the most help in protecting themselves.

Future research

Based on these strengths and limitations, the research results indicate important tendencies which should be considered for future research in order to understand the determinant of protection behavior better. One of the most important findings is that the results are consistent with the previous literature about the Protection Motivation Theory, specifically that self-efficacy is a significant determinant for engagement in actual protection behavior. Therefore, future research should consider taking a closer look at self-efficacy to understand the underlying factors defining whether a person is high or low in self-efficacy beliefs towards cybercrime protection. One possible underlying factor of self-efficacy beliefs, as mentioned above, could be the 'digital fluency' continuum (Wang et al., 2013). People that can be categorized high on the 'digital native' end of the continuum are described as feeling comfortable and self-confident using ICT which could result in higher self-efficacy believes towards cybercrime protection. In comparison, people categorized high on the 'digital nomad' end of the continuum are described as inexperienced ICT users which therefore could be considered as low in self-efficacy believes towards cybercrime protection (Wang et al., 2013). Considering that, future research has to make sure that both categories are included in the sample.

Furthermore, the results indicated that an increase in self-efficacy believes would also increase the engagement in actual protection behavior against cybercrime. Future research should take this as a starting point in understanding the determinants of protection behavior better. Meaning, in order to fight cybercrime as effectively as possible, future research should further explore factors influencing people to engage in more actual protection behavior. The results supported the coping appraisal of the Protection Motivation Theory formulated by rogers, therefore, future research should further explore the theory in order to find as many determinants as possible that could be manipulated or trained to increase the actual protection behavior. An example would be to create workshops for digital training in which 'digital nomads' become the help they need to perfectly implement ICT in their lives while increasing their self-efficacy beliefs towards cybercrime protection to ultimately increase their engagement in actual protection behavior.

Sticking out, future research should redo the experiment while increasing the target group of the study by focusing on a broader variety of ages. As motioned above, a target group that is spread through multiple generations would enable the researcher to better assess the extent to which personality or gender is influencing the implementation of ICT for people closer to the 'digital nomad' end. Especially taking into account that Covid-19 forced many 'digital normative' people to use the internet frequently, for example home office or teaching from home, the determinants for their self-efficacy and protection motivation become increasingly important nowadays.

Conclusion

This research can be seen as a first step towards integrating behavioral theories in cybersecurity improvement. The results of this research provide supporting evidence for a significant association between self-efficacy believes and actual protection behavior, as conceptualized by the Protection Motivation Theory. Nevertheless, future research needs to consider improvements in order to understand further determinants of actual protection behavior that could be used to ultimately improve cybersecurity. Especially taking into account the increase and hazardousness of cybercrime, this study highlighted first opportunities and chances for training or development programs in order to ultimately improve actual cybercrime protection behavior in all generations. Implementing demographic as well as psychological variables in the research of cybersecurity, we look forward to harnessing the future research potential of this domain to develop a more detailed understanding of variables influencing the protection behavior of each and everyone in order to ultimately increase the security and promote the safety of the Internet.

References

Abraham, C., & Sheeran, P. (2005). The health belief model. *Predicting health behaviour*, *2*, 28-80. Retrieved from https://edc.iums.ac.ir/files/hshe soh/files/predicting_Health_ beh_avior.pdf#page=45

Alheneidi, H., AlSumait, L., AlSumait, D., & Smith, A. P. (2021). Loneliness and Problematic Internet Use during COVID-19 Lock-Down. *Behavioral Sciences*, *11*(1), 5. Doi: 10.3390/bs11010005

Ashton, M. C., & Lee, K. (2009). The HEXACO–60: A short measure of the major dimensions of personality. *Journal of personality assessment*, *91*(4), 340-345. Doi: 10.1080/00223890902935878

Chauvin, B., Hermand, D., & Mullet, E. (2007). Risk perception and personality facets. *Risk Analysis: An International Journal*, *27*(1), 171-185. Doi: 10.1111/j.1539-6924.2006.00867.x

Chen, G., Gully, S. M., & Eden, D. (2001). Validation of a New General Self-Efficacy Scale. *Organizational Research Methods*, *4*(1), 62-83. Doi: 10.1177/109442810141004

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, *108*, 106-311. Doi: 10.1016/j.chb.2020.106311

Cisco., 2017. Annual cybersecurity report. Retrieved from http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464170.

DeYoung, C., & Spence, I. (2004). Profiling information technology users: En route to dynamic personalization. Computers in Human Behavior, *20*, 55–65. Doi: 10.1016/S0747-5632(03)00045-1

Furnell, S. M. (2001). The Problem of Categorising Cybercrime and Cybercriminals. *2nd Australian Information Warfare and Security Conference 2001.* Retrieved from *https://cutt.ly/QntEKYx*

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20. Doi: 10.1007/s11416-006-0015-z

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *2010*(10), 16-18. Doi: 10.1016/S1361-3723(10)70134-2

Ibrahim, S., Nnamani, D. I., & Soyele, O. E. (2020). AN ANALYSIS OF VARIOUS TYPES OF CYBERCRIME AND WAYS TO PREVENT THEM. *International Journal of Education and Social Science Research*, *03*(02), 274–279. Doi: 10.37500/ijessr.2020.30221

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105,* 102-248.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. *Pew internet & American life project*. Retrieved from https://eric.ed.gov/?id=ED525056

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting health behaviour*, *81*, 126. Retrieved from https://new.iums.ac.ir/files/hshe-soh/files/predicting_Health_beh_avior(1).pdf#page=98

Seijen, S. T. (2021). Risk perception towards Cybercrime among Students in the Netherlands: The effect of multiple factors on Risk Perception (Bachelor's thesis, University of Twente). Retrieved from http://essay.utwente.nl/85576/

Smith, A. (2017). *Americans and Cybersecurity.* Pewresearch. Retrieved from: https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

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

Wang, Q. E., Myers, M. D., & Sundaram, D. (2013). Digital natives and digital immigrants. *Business & Information Systems Engineering*, *5*(6), 409-419. Doi: 10.1007/s12599-013-0296-y

Appendix A

Informed consent

I hereby declare that I have been clearly informed about the nature and methods of the study by the researcher. I fully agree to participate in this research. I reserve all rights to withdraw my agreement without having to give reason and have in mind that I can stop the research at any time. I have been informed that if the research is completed all information will be anonymized and cannot be tracked back to me, that my identity will stay hidden, and I stay anonymous throughout the whole research process. Without expressed consent, my personal data will not be accessed by third parties. If I want to get more information about the outcome of the research, I can contact the researchers Niklas Kindt (n.kindt@student.utwente.nl), and Iris van Sintemaartensdijk (i.vansintemaartensdijk@utwente.nl).

For complains about this research please contact the Secretary of ethics committee of faculty of behavioral science of the University of Twente, Dr. L.J.M. Kamphuis-Blikman (l.j.m.blikman@utwente.nl).

"By proceeding the study I consent to participate."

Appendix B

Self-efficacy assessment

How do you feel about protecting yourself against cyber criminality type 1: Criminals are acquiring personal data through phishing sites or phone calls for fraud activities on the bank account.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 2: "Phishing" includes all criminal activities in which the perpetrator is stealing personal data of unsuspecting targets in order to recreate their identity on the internet.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 3: "ATM Fraud" groups criminal behavior that focus on stealing credit cards and PIN throughout manipulated ATMs.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 4: "Sales scam and counterfeit" is focused on crimes in which the criminal is selling imitative goods or products that do not exist.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 5: “Cyber-plagiarism” is grouping crimes in which the criminal is stating ideas or even complete texts of the victim as their own.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 6: “Illegal e-lotteries” and include all crimes in which the criminals try to get information and personal data in fake lotteries

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

How do you feel about protecting yourself against cyber criminality type 7: “Advanced fee-scam” is grouping all crimes in which the criminal is requesting money in advance while not delivering the product or service.

1. I will be able to achieve most of the protection goals that I have set for myself.
2. When facing difficult protection processes, I am certain that I will accomplish them.
3. In general, I think that I can obtain protection behavior that is important to me.
4. I believe I can succeed at most protection behavior to which I set my mind.
5. I will be able to successfully overcome many challenges while protecting myself.
6. I am confident that I can perform effectively on many different protection behaviors.
7. Compared to other people, I protect myself very well.
8. Even when things are tough, I can perform protection behavior quite well.

Appendix C

Hexaco-60

1. I would be quite bored by a visit to an art gallery.
2. I plan ahead and organize things, to avoid scrambling at the last minute.
3. I rarely hold a grudge, even against people who have badly wronged me.
4. I feel reasonably satisfied with myself overall.
5. I would feel afraid if I had to travel in bad weather conditions.
6. I wouldn't use flattery to get a raise or promotion at work, even if I thought it would succeed.
7. I'm interested in learning about the history and politics of other countries
8. I often push myself very hard when trying to achieve a goal.
9. People sometimes tell me that I am too critical of others.
10. I rarely express my opinions in group meetings.
11. I sometimes can't help worrying about little things.
12. If I knew that I could never get caught, I would be willing to steal a million dollars.
13. I would enjoy creating a work of art, such as a novel, a song, or a painting.
14. When working on something, I don't pay much attention to small details.
15. People sometimes tell me that I'm too stubborn.
16. I prefer jobs that involve active social interaction to those that involve working alone.
17. When I suffer from a painful experience, I need someone to make me feel comfortable.
18. Having a lot of money is not especially important to me.
19. I think that paying attention to radical ideas is a waste of time.
20. I make decisions based on the feeling of the moment rather than on careful thought.
21. People think of me as someone who has a quick temper.
22. On most days, I feel cheerful and optimistic.
23. I feel like crying when I see other people crying.
24. I think that I am entitled to more respect than the average person is.
25. If I had the opportunity, I would like to attend a classical music concert.
26. When working, I sometimes have difficulties due to being disorganized.
27. My attitude toward people who have treated me badly is "forgive and forget".
28. I feel that I am an unpopular person.
29. When it comes to physical danger, I am very fearful.
30. If I want something from someone, I will laugh at that person's worst jokes.
31. I've never really enjoyed looking through an encyclopedia.
32. I do only the minimum amount of work needed to get by.
33. I tend to be lenient in judging other people.
34. In social situations, I'm usually the one who makes the first move.
35. I worry a lot less than most people do.
36. I would never accept a bribe, even if it were very large.
37. People have often told me that I have a good imagination.
38. I always try to be accurate in my work, even at the expense of time.
39. I am usually quite flexible in my opinions when people disagree with me.
40. The first thing that I always do in a new place is to make friends.
41. I can handle difficult situations without needing emotional support from anyone else.
42. I would get a lot of pleasure from owning expensive luxury goods.
43. I like people who have unconventional views.
44. I make a lot of mistakes because I don't think before I act.
45. Most people tend to get angry more quickly than I do.
46. Most people are more upbeat and dynamic than I generally am.

47. I feel strong emotions when someone close to me is going away for a long time.
48. I want people to know that I am an important person of high status.
49. I don’t think of myself as the artistic or creative type.
50. People often call me a perfectionist.
51. Even when people make a lot of mistakes, I rarely say anything negative.
52. I sometimes feel that I am a worthless person.
53. Even in an emergency I wouldn’t feel like panicking.
54. I wouldn’t pretend to like someone just to get that person to do favors for me.
55. I find it boring to discuss philosophy.
56. I prefer to do whatever comes to mind, rather than stick to a plan.
57. When people tell me that I’m wrong, my first reaction is to argue with them.
58. When I’m in a group of people, I’m often the one who speaks on behalf of the group.
59. I remain unemotional even in situations where most people get very sentimental. I remain unemotional even in situations where most people get very sentimental.
60. I’d be tempted to use counterfeit money, if I were sure I could get away with it.

Appendix D

Actual protection behavior assessment

Type 1: Criminals are acquiring personal data through phishing sites or phone calls for fraud activities on the bank account.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 2: “Phishing” includes all criminal activities in which the perpetrator is stealing personal data of unsuspecting targets in order to recreate their identity on the internet.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 3: “ATM Fraud” groups criminal behavior that focus on stealing credit cards and PIN throughout manipulated ATMs.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 4: “Sales scam and counterfeit” is focused on crimes in which the criminal is selling imitative goods or products that do not exist.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 5: “Cyber-plagiarism” is grouping crimes in which the criminal is stating ideas or even complete texts of the victim as their own.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 6: “Illegal e-lotteries” and include all crimes in which the criminals try to get information and personal data in fake lotteries

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.
2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Type 7: “Advanced fee-scam” is grouping all crimes in which the criminal is requesting money in advance while not delivering the product or service.

1. I protect myself by setting thoughtful passwords as well as the caution to not publish confidential information.

2. I gain knowledge about the type and procedure of this type of cybercrime in order to better recognize it.

Appendix E

Demographics

1. What is your Gender?
    a. Male
    b. Female
    c. Non-binary / third gender
    d. Preferer not to say

2. What is your Age?

3. What is your Nationality?
    a. German
    b. Dutch
    c. Other:
4. What is your highest academic degree?
    a. Primary school
    b. Highschool
    c. University
    d. Other:

5. How much time do you spend approximately on the internet?