University of Twente

BMS Faculty

Department of Psychology

June 28th, 2021

Supervisors:

I. van Sintemaartensdijk, Msc

Dr. S. J. Watson

The Risk Perception and Coping Mechanisms of Cybercrime

Michelle Walterscheid

Abstract

Cybercrime is increasing and hence an issue that must be fought against effectively. Each year financial losses are estimated to be in the billions, not accounting for the psychological damages that it inflicts. Research into the more psychological aspects of cybercrime is scarce but knowledge on peoples' judgements of the risks of cybercrimes and coping measures might be useful knowledge to be used against cybercrime. To establish that basis, this study aims to explore how risk perception differs depending on cybercrime and how factors like coping strategies or gender affect risk perception. To achieve this goal, a questionnaire was distributed online, mostly among students, and two scales were developed to measure risk perception and coping strategies for up to six cybercrimes. Multivariate analysis resulted in findings of positive relationships between risk perception and gender, education, coping strategies, victimization, knowledge and time spent on the internet, which were strongest for crimes of online violence and cyberstalking. Future research should go deeper and discover the causes for these findings. With this knowledge interventions can be developed to facilitate the usage of protective and coping measures by influencing risk perceptions and so reduce the impact of cybercrime.

Introduction

Since the inception of the internet, cybercrime is an issue that has been growing and developing alongside it (Kirhalla, 2020). Especially now, with the covid-19 pandemic the impacts of cybercrime have become more noticeable than ever before (Internet Organised Crime Threat Assessment [IOCTA], 2020; Kirhalla, 2020). Depending on the type of cybercrime, victims experience different types of damage and or losses. These can be financial in nature, for example, by purchasing fake concert tickets or by stolen bank passwords being abused to transfer money. For companies consequences of being victimized, like compromised private customer information, can lower their reputation or trustworthiness and lead to a loss in revenue since customers begin to look for alternative services. In the case of DDoS-attacks, online-services suffer disruptions that also lead to increasingly higher costs for companies as long as the attack persists. Other crimes that fall into the category of cyber-bullying can lead to psychological damages like anxiety, depression and trust issues (Arief, Adzmi, Azeem 2015).

Despite all that available information, research on cybercrime has a few issues, one of them being that there is no universal definition of cybercrime (Sabillon, Cano, Cavaller, Serra, 2016). Inevitably, this leads to researchers using different definitions or creating their own, all explaining and categorizing cybercrimes in various ways, making comparisons between such studies difficult. Indeed, cybercrime is an area that encompasses a great amount of diverse, rare and unique types of crimes, so it is appropriate to provide a short and general overview. The following definition also serves as the basic foundation of this study. This definition of cybercrime differentiates between various types and puts them into two major categories, making it more detailed, practical and concise than its contemporaries (Saxion, et al., 2020). The first category are cyber-dependent crimes that can only exist in an online environment. That is malware including viruses, worms, horses, spyware, ransomware, and DDoS attacks. It also includes hacking to destroy, interrupt or adapt data. The second category is for cyber-enabled crimes that previously existed outside of cyberspace and are now invading to benefit from new hunting grounds. This category consists of different forms of fraud like mail fraud, payment fraud, identity theft and advanced fraud. It also includes theft and selling of information, spoofing and skimming. Next, violence is comprised of activities such as extortion, cyber-bullying, insulting, stalking, discrimination, and threats. Lastly, there are obscenities encompassing grooming and child porn (Saxion, et al., 2020).

Apart from the great variety of definitions there is also an issue with the variety of laws of cybercrime. Different institutions have different laws on what is and is not a cybercrime (Alkaabi, Mohay, McCullagh, Chantler, 2010). For example, Alkaabi and colleagues (2010), during their investigation of classifications of cybercrime, found that the Council of Europe's taxonomy is missing crimes like identity theft and the United Nations' classification for computer crime was missing harassment. Specifically, what this can lead to is that victims of cybercrime do not file a report since they either do not know who to approach or how exactly they should report it. For example, in the United Kingdom it was estimated that only 120-150 per one million cybercrimes are reported to the police in a year (Wall, 2007). Some also do not see the point since, it is very difficult to pursue criminals that act through the internet (Bidgoli, Grossklags, 2016). Companies and services that are victimized often keep cyberattacks a secret since it could affect their revenue due to customers losing trust and leaving for other services that offer better cybersecurity measures (Hyman, 2013). That also makes research into cybercrime is also fairly difficult. Many annual crime reports give varying accounts on the number of crimes that are committed in a year so making definite statements on their frequency is risky with estimates ranging from 110 billion dollars to 1 trillion dollars (Hyman, 2013). But one thing that seems to be consistent over most reports is that the numbers are rising. The costs for cybercrime damage are estimated to be six trillion dollars annually by the year of 2021 (Kirhalla, 2020).

When shifting the attention to psychological aspects of cybercrime, it is often said that humans are seen as the weakest link in the security chain of cybercrime and cybersecurity (IOCTA, 2020). Individuals lacking awareness and general knowledge of such matters often become victimized. To be more specific, awareness of potential threats, usually determines precautionary or protective measures that are taken. This is in connection with risk perception as heightened risk perception often leads to the need to seek information and heightened awareness (Ferraro, 1995). The level of proficiency and knowledge of cybercrime and cybersecurity also determines if individuals are able to cope or to protect themselves from attacks (IOCTA, 2020). De Kimpe and colleagues (2021) also state that high levels of risk perception make taking up protective or coping measures more likely.

Considering that cybercrime is only ever increasing and with all the damages that it has already wrought it is perhaps worth considering opportunities to diminish its power and harm, starting with the potential victims themselves. Understanding differences in risk

perception or how people judge dangers of their online activities as well as their coping strategies (problem-focused coping strategies specifically) to protect themselves is a good first step to achieve that. But unfortunately, it is still unclear how individuals' judgements differ depending on cybercrimes, as such comparisons are rare (Martens, De Wolf, De Marez, 2019). Research that has been done in that regard did provide some interesting findings if a bit contradictory.

Risk Perception

Cybercrime is mainly seen as a technical issue so its more human or psychological aspects, such as human engineering, are often overlooked or neglected. This is unfortunate since more knowledge on this could help develop a better understanding on cybercrime. One psychological concept that has received little attention but is very relevant for understanding thought or judgment processes for these situations is risk perception. Most researchers use Ferraro's (1995) model of risk interpretation as their basis for studying either risk perception or levels of fear in relation to cybercrime, although the model did not take cybercrime into account at the point of its inception. In this model, perceived risk and fear have fairly similar roles with the main difference being that the perceived risk is a cognitive judgement of risk and fear is an emotional one. The judgements of risks are influenced by observations of the so-called micro and macro level factors. Macro-level factors are ecological forces such as crime rates, media information and available protection, while micro-level factors are based on personal and social characteristics, victimization and personal resources to use against threats. The outcome of these judgements are changes in the levels of fear and adaptive behaviours that are defined as either constrained or defensive actions with the purpose of mitigating risks (Ferraro, 1995). Such actions in the context of cybercrime could be using the internet less or installing anti-virus software respectively. The findings that research on this model has brought in relation to cybercrime is a positive relationship between perceived risk and fear levels, stating that risk perception also increases fear of victimization. Overall, this relation is established fairly well in the literature (Henson, Reyns, Fisher, 2013; Higgins, Ricketts, 2008; Yu, 2014).

Another common finding is that high levels of fear and risk perception leads to avoidance behaviour. More specifically, individuals spend less time on the internet than others and often avoid making purchases online, pursuing more local options instead (Reisig,

Pratt, Holtfreter, 2009; Riek, Böhme, Moore, 2015). Occasionally, researchers look at demographics to see if they can determine different levels of perceived risk and fear. Some have found support that women and individuals with low social status are more fearful than individuals who are neither of those (Virtanen, 2017). Virtanen (2012) states that women have higher fear levels when it comes to the crimes of online harassment, hacking, fraud and cyberattacks but not on computer viruses. There is also some research supporting that women have higher levels of risk awareness with cybercrime in general (Ismailova, Muhametjanova, Medeni, Medeni, Soylu & Dossymbekuly, 2019). However, others find no difference when it comes to gender even arguing, based on Ferraro's model, that differing risk perception levels based on gender should be diminished since the main reason women perceive higher levels of risk is that they are more vulnerable in face-to-face situations that cannot exist in an online environment (Reisig, et al., 2009). But Ferraro also states that women are especially fearful of sexual assault and crimes of similar nature while the study by Reisig and colleagues (2009) had its focus on credit card theft. In other words, it is likely that women usually have higher levels of fear for most cybercrimes, but exceptions might still occur.

When it comes to other factors such as previous victimization experiences, be they direct or indirect, increased levels of perceived risk and also increased avoidance behaviour are likely. For example, Riek and colleague (2015) found that victimization increases risk perception for online banking and shopping cybercrimes, which is likely also the case for other types of cybercrime. Multiple researchers have found that young people are more frequently victimized as well as those with lower levels of education or social status (Virtanen, 2017).

How age affects risk perception or levels of fear is unclear since studies come to inconsistent conclusions. For example, Yu (2014) did not find differences in levels of fear, while Henson and colleagues (2013) found that younger individuals are more fearful. Furthermore, Chen and colleagues (2020) took perceived IT-self-efficacy, also known as perceived skill capabilities to use IT devices, into account and found that individuals with high levels of perceived IT-self-efficacy have lower risk perceptions and are also less avoidant, which they found leads to more frequent victimization. This would mean that perceived knowledge could decrease the risk perception of cybercrimes. Concepts like confidence were also researched and showed that individuals with high confidence levels spend more time on the internet which makes them more vulnerable, but they also may be better at identifying risks (Riek, Böhme, Abramova, 2017; Virtanen, 2017).

To come to a conclusion, all the factors described in the last few paragraphs affect risk

perception in various ways as they are inherent abilities or characteristics of people, hence their potential influence should not be ignored when researching risk perception. However, the exact results of these effects are unclear or contradictory with some researcher finding either positive, negative or no effects at all. Something of note as well is that in some cases, the measures of risk perception tend to be rather simple. Some researchers only use one item that measures personal likelihood of being victimized (Riek, et al., 2015; Riek, et al., 2017; Yu, 2014). However, when looking at Ferraro's model (1995), it becomes apparent that risk perception of individuals is based on more than just general likelihood of victimization but also personal resources and environmental factors. So, there is a possibility that these simplified measures loose accuracy when it comes to risk perception. Additionally, most of this research looks only at specific types of cybercrimes or researched multiple types but put them all into one category at the end. This is something that has been critiqued before as well (Martens, et al., 2019). For example, the studies by Ismailova and colleagues (2019) and De Kimpe and colleagues (2021) do not differentiate between different types of crimes, while the study written by Reisig and colleagues (2009) had its focus solely on online credit card theft and Riek and colleagues (2015) looked only at cybercrimes related to online banking and shopping. This makes comparisons between cybercrime findings challenging, which consequently means that it is also difficult to examine potential differences in risk perception between types of cybercrimes, which is why more specified research is necessary.

Coping Mechanisms

Another concept that has received little attention in the area of cybercrime are coping mechanisms. All victims of a crime, or individuals perceiving the risk of becoming one, will utilize some sort of coping-strategy to mitigate its risks or consequences. A rather well-known definition for coping is by Lazarus & Folkman (1984), that defines coping as a continuous cognitive and behavioural adaptations to manage certain external and internal demands that are judged to surpass one's own personal resources. These demands or consequences can be both mental and physical in their nature. Mental issues are usually tied to tension and discomfort or feelings such as shame, fear, anger or anxiety while physical demands can include varying forms of damage or loss of property, including money (Green, Choi & Kane, 2010).

Besides that, risk perception and coping are closely connected since risk assessments

are usually followed by coping responses if deemed to be necessary. Ferraro (1995) included this in his model as the either defensive or constrained adaptive behaviours following the risk judgement and Green and colleagues (2010) also mentioned that if risks are judged as high, coping responses are also judged to gain importance. One group of researchers used the work of Lazarus & Folkman (1984) as a framework to categorize different coping behaviours of online banking fraud victims. Coping mechanisms are divided into problem-focused, avoidant-focused and emotion-focused coping, which are equivalent to the cognitive or behavioural adjustments mentioned previously. Problem-focused coping is a goal-oriented approach with the focus of actively solving a problem which can be further divided into technological and conventional coping, the former involving technology and the latter methods that do not require technology. Examples for technological coping would be acquiring double authentication for an account and conventional coping would be to regularly check for suspicious activities (Jansen, Leukfeldt, 2018). This kind of approach usually involves a process of generating a variety of options, followed by implementing those with the intent to solve the problem (Baker & Berenbaum, 2007). Problem-focused coping is likely to assist positive emotional outcomes, since this problem-solving process gives individuals a sense of control (Green, et al., 2010).

Emotion-focused coping strategies are more about managing emotions or stress stemming from the crime without approaching the actual problem. Emotion-focused coping encompasses a variety of strategies and hence is more complicated to define than the problem-focused approach. It can be an avoidant-focused approach that does not involve any form of problem solving, but it can also include strategies of venting emotions or seeking social support from family, friends, peers etc. (Green, et al., 2010). Apart from being difficult to define, the effectiveness of emotion-focused coping is also questionable since certain strategies such as avoidance is seen as more maladaptive towards personal health, thus leading to bad outcomes (Baker & Berenbaum, 2007). Due to these issues of contradiction and vagueness this study will have its focus on problem-focused approach.

Which type of coping strategies are used in the end depends on what the situation demands. Usually, the strategy that is deemed to lead to the most positive outcome is used. Often, new strategies emerge to solve problems resulting in an improved well-being. How well the chosen coping strategies help with the problem also determine if the outcome for the well-being is positive or negative. Coping strategies also gain more importance when the problem is perceived as severe, especially the emotional health of the victim benefits from the strategies (Green, et al., 2010). This also implies that high levels of risk perception could

benefit the usage of coping strategies. For instance, individuals perceiving risk of malware will install anti-virus software and in response to being victimized by malware, they install additional anti-malware software, or check security certificates on websites (Jansen, et al., 2018).

To summarize, there is a lack of research on cybercrime and the psychological mechanisms underlying it, risk perception being one of those. And although there is a good amount of literature on coping with crime in general, there is very little known about these behaviours in the context of cybercrime. How effective the different coping strategies are and how they would affect risk perception is also not known. More knowledge about the coping behaviours of cybercrime victims might reveal things that individuals find difficult to manage and so can be supported accordingly. Depending on what actions are taken or the lack thereof might demonstrate areas where the public needs to be better educated to reduce risk of victimization. The problem with that is that further research could be used to help internet users be more resilient towards cyber-attacks. Interventions could be developed to increase efficacy which would lead to less avoidant behaviour and in the ideal case reduce victimization.

The Present Study

This study aims to expand the literature through research that is supposed to uncover the basics of cybercrime and its relation to psychological concepts. The previously given definition of cybercrime will determine which types of cybercrime will be included; however, some will be excluded. For example, DDoSing, usually only affects companies and crimes like grooming and child porn are too sensitive to discuss. This then results in six main categories of cybercrimes. First, is malware (including viruses, worms and horses) also known as malicious software, that damages personal files. Next is spyware, which is software that can be used to spy on users' devices like files or force access attached applications like cameras or microphones. Ransomware encrypts personal and private files and demands money in return for decryption for a short period of time (Yaqoob, 2017). Lastly, there is cyberstalking, violence (cyberbullying, extortion, threats, defamation, spreading information) and forms of online fraud like mail, charity, theft or ticket fraud (Saxion, et al., 2020). With that in mind, the following research question is proposed: Do individuals perceive risks of cybercrimes (malware, spyware, ransomware, fraud, violence, stalking) differently and is that

risk perception influenced by problem-focused coping mechanisms and demographics of age, gender, education, knowledge, victimization, confidence and time spent on the internet?

Additionally, through the literature research which resulted in the compiling of various different factors that could affect risk perception, hypotheses have been constructed to examine the potential relationship between them and risk perception. For one, it is expected that women have higher levels of risk perception than to men. It is also expected that being victimized or knowing a victim of cybercrime increases levels of risk perception. Furthermore, low levels of education, usage of coping strategies and being young (adolescent) increases risk perception. Lastly, a high level of knowledge is expected to decrease risk perception.

Methods

Participants

There was a total of 125 participants, of which 111 were included in data analysis meaning that responses where participants had not given consent were deleted as well as responses that had a completion rate below 30% due to too little information available. Participants were recruited per snowball and convenience sampling. A link to the study was shared over Email and WhatsApp to available people and to one German college class. Additionally, the SONA-system was used for recruiting university students. The inclusion criteria included being 16 years or older. The participants had a mean age of 20.9 (*SD*age= 6.1). Additionally, 28 participants were male, 82 participants were female, and one participant identified themselves as non-binary. The majority of participants had an educational level of a bachelor (*n*=39) followed by a high school degree (*n*=53), the least participants had a masters (*n*=1) or trade school degree (*n*=4).

Design

This study employs a questionnaire survey design. The dependent variable is risk perception. The independent variables are problem-focused coping mechanisms followed by demographics of age, gender, level of education, level of knowledge and additional concepts such as time spend online, confidence in conducting activities online, activities online and general and victimization.

Materials

An online questionnaire was created using services provided by the website Qualtrics. The questionnaire had in total 47 questions. There is a section about the demographics of age, gender and education and a section of more general questions on the level of knowledge of cybersecurity and cybercrime, time spent online which was an estimate of time spent on the internet per day, the level of confidence in conducting activities online, which activities participants did in the online environment and lastly, if they or someone they know had been victim of certain cybercrimes. All of these questions excluding the time and activities questions used a seven point-Likert scale. This was followed by multiple scales also using a seven point-Likert scale which can be divided into the risk perception scale and the problem-focused coping scale which will be further elaborated on in the following paragraphs. The questionnaire and the study itself received ethical approval by the ethics committee of the university of Twente's faculty of behavioural, management and social sciences (BMS).

Risk Perception Scale

The risk perception scale is based on the risk perception of adolescents on drugs questionnaire by Benthin and colleagues (1992). This questionnaire employed 14 risk characteristics, which were used to rate 30 items of risky behaviours. It was partly chosen as basis since it assesses risk perception from multiple angles like risk for oneself, for others and perceived seriousness, unlike other studies who measured risk perception only through perceived likelihood of victimization. Additionally, items of the questionnaire showed good validity in other studies as well (Pailing, Reniers, 2018). The questions were reformulated to fit the cybercrime context and those questions that did not fit the context were left out. For example, the question: "To what extent are the potential risks (danger) associated with this activity frightening for people your age?" was reformulated to: "To what extent do you find this type of cybercrime as frightening?" or "If an accident or something bad happened because of this activity, would you expect the effects to be mild or serious?" was turned into: "If you were affected by it, would you expect the potential harm to be mild or serious?". The result of this is a risk perception scale with five items, those being risk to oneself, risk to others, seriousness of harm, fear and controllability. These five items where specifically developed, since they are expected to add a diverse perspective to the risk perception measure with the

first two items being fairly general and the rest being more specific aspects of it. Lastly, it has a seven point-Likert scale like the original questionnaire and the minimal obtainable score is five and the maximum is 35 per cybercrime. Additionally, for this questionnaire, the seven point-Likert scale scores are always the same, ranging from low risk (1) to high risk (7), while the original study had several reversed items. The five items of the risk perception scale are repeated for each cybercrime. This means that for the measure of the six different types of cybercrime the minimum score is 30 and the maximum score is 216. The total mean score for this sample is 124,59.

Problem-focused Coping Scale

This project additionally focuses on problem-focused coping as independent variable, which includes technological and conventional methods. When it comes to problem-focused coping strategies, there is a serious lack of questionnaires that examine the exact methods individuals utilize, especially when it comes to cybercrime. In order to construct this part of the questionnaire, interview studies of various types of cybercrime that compiled lists of coping strategies were used to develop scales (Alsayed, Bilgrami, 2017; Cross, Richards, Smith, 2016; Tokunaga, Aune, 2015; Michikyan, Lozada, Weidenbrenner, Tynes, 2014). The different coping strategies compiled in these lists were extracted and reformulated to turn them into statements for each cybercrime. To be more specific, statements for coping strategies for malware were as follows: “I would install anti-virus software.” or “I would scan files that I download.”. These where then followed by a seven point-Likert scale for participants to rate their likelihood of performing that coping strategy ranging from very unlikely (1) to very likely (7). This was done since no questionnaires about problem-focused coping behaviours in connection to cybercrime was found. Furthermore, the only other proper way to gather lists of coping methods would have been to additionally interview participants which is beyond the scope of this study. This resulted in six scales of coping strategies for each of the cybercrimes: malware, ransomware, spyware, fraud, cyberbullying, and stalking. The number of coping strategies ranged from at least six coping responses to a maximum of 12.

Procedure

Participants clicked the link to the survey and were redirected to the Qualtrics website. Here, the first step was to read the informed consent form and then agree to its terms and conditions to proceed. The next few questions were about demographics (age, gender, education, etc.), followed by measures of hours spend online, confidence online, activities, knowledge of cybercrime/cybersecurity and victimization. Afterwards, came the scales measuring risk perception and coping responses for each cybercrime in the following order: malware, spyware, ransomware, fraud, cyberbullying and lastly stalking. Each cybercrime had a small description as well. At the end of the study participants were debriefed and thanked for their participation and students recruited through the SONA-system received a quarter of a credit as well. The study took around 15 minutes to complete.

Analysis

For data analysis the statistical package of social sciences (SPSS) (version 25) will be used. First the data will be cleaned up meaning that what does not fit the inclusion criteria or that is insufficiently complete will be deleted. Then general frequencies and descriptive measurements of the dataset will be taken of, for example, the demographics and scales. Since the scales have been newly constructed for this study, they will be subjected to factor analyses to assess their validity. The Cronbach's alpha will also be calculated for the scales to measure their reliability. To examine the relationship between the dependent and independent variables, multivariate regressions for each of the six cybercrimes will be calculated and will always have risk perception as the dependent variable and as independent variables there will be age, gender, education, level of knowledge and confidence, time spent on the internet, coping strategies and victimization.

Results

First, the descriptive statistics of the measured factors will be summarized. Most participants use the internet to listen to music and to browse social media and they use it least for shopping and downloading files. When it comes to levels of confidence on conducting internet activities, the majority is somewhat (n=25) or fairly (n=45) confident and most see their knowledge on cybercrime and cybersecurity as either somewhat good (n=36) or somewhat bad (n=24) and a good number of participants would rate it neither good nor bad

(*n*=27). Most participants spend 5-6 hours (*n*=36) or 3-4 hours (*n*=38) on the internet daily. The least participants spend more 11-12 hours (*n*=2) or more (*n*=1) on the internet. There are overall 359 cases of victimization, with the majority being indirect victimization as can be seen in Table 1. Most participants have been victims of malware, followed by fraud and violence. The least of them were victimized by ransomware and spyware. When it comes to victimization of the participants' acquaintances, the majority were victims to fraud and cyberbullying they were the least victimized by spyware and ransomware.

Table 1. *Distribution of Direct and Indirect Cases of Victimization in Numbers and Percentages Categorized by Type of Cybercrime*

Victimization	Direct		Indirect	
	N	%	*N*	%
Malware	36	26.87	50	22.22
Spyware	12	8.96	18	8.00
Ransomware	12	8.96	14	6.22
Fraud	31	23.13	60	26.67
Violence	28	20.90	53	23.56
Stalking	15	11.19	30	13.33
Total	134	100	225	100

Next, the mean scores of the risk scale section are summarized (Table 2). Here, participants always judged their own risk of victimization to be a bit lower than the risk that others would be victimized. They also perceived the least risk for being stalked and bullied and the most risk being scammed or spied upon. Also, they perceived that others are most at risk for scams and spyware and the least of being stalked and being affected by ransomware. In general, spyware, bullying and stalking are perceived as more harmful and frightening than the other forms of cybercrime, but participants also perceive themselves to be of less risk of being affected by them (Table 2).

Table 2. *Mean Scores Ranging from 1-7 of the Risk Perception Scales Categorized by Type of Cybercrime*

	Malware	Spyware	Ransomware	Fraud	Violence	Stalking
Risk self	4.28	4.46	3.65	4.67	3.88	3.72
Risk other	4.56	4.68	3.95	5.23	4.58	4.30
Harm	4.78	5.32	4.54	4.61	5.16	5.25
Fear	4.68	5.68	4.59	4.47	5.03	5.64
Control	3.8	4.47	3.89	3.53	4.19	4.43

Following this, factor analyses were conducted for each subscale of the risk perception scale (malware, spyware, etc). The first step was to make sure that all of the three preliminary conditions for a factor analysis were met. The Bartlett's test of sphericity for all scales was significant ($p < .001$) and the number of correlations between items and factors that have values above 0.3 was also more than sufficient but not every scale had a high enough Kaiser-Meyer-Olkin which needs to be a value of at least 0.6 to be adequate. Specifically, the scales for malware, spyware, ransomware and stalking had a KMO value below 0.6, while violence had a KMO value of 0.692 and fraud had a KMO value of 0.631. Nevertheless, the factor analysis was still conducted out of exploratory reasons, with a varimax rotation for simplification as well. The factor analyses consistently resulted in two factors for each subscale one factor correlating with the items of risk for the self and risk for the others and the second factor correlating with the items of fear, harm and control. Taking that into account, it was decided to continue further analyses with these two factors as two risk scales, the first being for general risk perception since its items were more about risk perceptions in general and the second scale for more detailed risk perception since those items were made up of different aspects or parts that make up risk perception. For each of the two factors the Cronbach's alpha was calculated to judge their reliability. For the general risk perception, the Cronbach's alpha is 0.849 which is an adequate score that suggests high internal consistency. The Cronbach's alpha for detailed risk perception is slightly lower with 0.730 but still fairly adequate. Additionally, general risk perception has a score range of 2-84 with 4-80 being the score range of this sample. The mean score was 49.26 (SD= 14.93). For detailed risk perception the score range is 2-126 with an achieved range of 11-117 and a mean score of 79.63 (SD=19.90).

The analysis continued with calculating general and detailed risk perception scores for each cybercrime, that were then used as dependent variables for the multivariate regression analysis, with the independent variables of age, gender, education, level of knowledge and

confidence, time spent on the internet, coping strategies and victimization. The results are discussed in the following sections:

Gender

First the independent variable of gender yielded a few significant results. It showed that being female has a positive effect on the general risk perception of fraud and stalking, with the general risk perception of stalking being affected the strongest (Table 3). Being female had even stronger positive effects on the detailed risk perception of violence and stalking compared to the general risk ones. Summed up, there is a significant association of gender on risk perception, in particular for the perception of violence and stalking.

Table 3. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Gender*

	F	*df*	*p*	B
Risk-general				
Malware	3.708	1,110	.057	15.681
Spyware	.891	1,105	.348	4.009
Ransomware	.438	1,103	.510	3.098
Fraud	4.831	1,103	**.030**	42.919
Violence	1.504	1,103	.223	10.627
Stalking	6.508	1,103	**.012**	52.498
Risk-detail				
Malware	.612	1,110	.436	4.210
Spyware	.792	1,105	.376	6.323
Ransomware	.108	1,103	.743	.964
Fraud	2.012	1,103	.159	29.270
Violence	6.545	1,103	**.012**	117.714
Stalking	16.151	1,103	**.000**	193.006

Note. p-values < .05 are in boldface

Perceived Knowledge

Next, the independent variable of perceived knowledge of cybercrime and cybersecurity has yielded only one positive effect on the general risk perception of ransomware. (Table 4).

Table 4. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Knowledge*

	F	*df*	*p*	B
Risk general				
Malware	.094	1,110	.760	.396
Spyware	.144	1,105	.705	.647
Ransomware	5.696	1,103	**.019**	40.292
Fraud	.991	1,103	.322	5.112
Violence	.101	1,103	.752	7.11
Stalking	.166	1,103	.685	1.338
Risk detail				
Malware	2.712	1,110	.103	18.665
Spyware	.781	1,105	.379	6.232
Ransomware	.759	1,103	.386	6.753
Fraud	.480	1,103	.490	6.987
Violence	.000	1,103	.999	.000
Stalking	.289	1,103	.592	3.450

Note. p-values < .05 are in boldface

Level of Education

Furthermore, the level of education as independent variable yielded only one significant regression which shows a positive effect of education on the general risk perception of violence (Table 5).

Table 5. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Education*

	F	*df*	*p*	B
Risk general				
Malware	.007	1,110	.933	.030

Spyware	.005	1,105	.946	.021
Ransomware	.726	1,103	.396	.5.139
Fraud	.032	1,103	.859	.165
Violence	4.849	1,103	**.030**	34.263
Stalking	.514	1,103	.475	4.148
Risk detail				
Malware	.017	1,110	.896	.119
Spyware	.195	1,105	.660	1.555
Ransomware	.517	1,103	.474	4.593
Fraud	.145	1,103	.704	2.115
Violence	2.326	1,103	.131	41.829
Stalking	.218	1,103	.641	2.610

Note. p-values < .05 are in boldface

Coping Strategies

Moving on, to the independent variable of coping strategies which showed positive effects on general risk perception of ransomware and especially fraud. The regressions for detailed risk perception revealed a positive effect on detailed risk perception for spyware, ransomware and fraud. In general, the results of these regressions show that coping strategies have a positive relation with general and detailed risk perception of spyware, ransomware and fraud (Table 6).

Table 6. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Coping Strategies*

	F	*df*	*p*	B
Risk-general				
Malware	.013	1,110	.910	.055
Spyware	.040	1,105	.842	.179
Ransomware	4.481	1,103	**.037**	31.696
Fraud	14.604	1,103	**.000**	75.328
Violence	1.007	1,103	.318	7.115

Stalking	2.016	1,103	.159	16.263
Risk detail				
Malware	.005	1,10	.944	.035
Spyware	4.298	1,105	**.041**	34.282
Ransomware	5.548	1,103	**.021**	49.341
Fraud	4.204	1,103	**.043**	61.173
Violence	2.339	1,103	.130	42.072
Stalking	2.047	1,103	.159	24.461

Note. p-values < .05 are in boldface

Victimization

The next set of regressions were done with victimization as independent variable, including individuals who have been victimized themselves and those knowing other victims. Victimization of oneself had a positive effect on fraud and violence, while knowing of the victimization of others had a positive effect on malware, fraud and stalking. Additionally, the effects of victimization of oneself is always stronger than the victimization of others. Also, victimization of the self, had a positive effect on the detailed risk perception of malware and ransomware, the latter having a stronger relationship and victimization of others also had a positive effect on detailed risk perception of malware. All in all, victimization has a positive relationship with risk perception, which is weaker if others were victimized (Table 7).

Table 7. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Direct and Indirect Victimization*

Risk-general	*F*	*df*	*P*	B
Malware				
Self	2.818	1,110	.096	11.918
Other	6.740	1,110	**.011**	28.503
Spyware				
Self	1.795	1,105	.183	8.079
Other	2.574	1,105	.112	11.581
Ransomware				

Self	.017	1,103	.896	.122
Other	.073	1,103	.788	.516
Fraud				
Self	7.992	1,103	**.006**	41.221
Other	2.793	1,103	.098	14.407
Violence				
Self	17.285	1,103	**.000**	122.143
Other	5.814	1,103	**.018**	41.085
Stalking				
Self	2.909	1,103	.091	23.464
Other	5.040	1,103	**.027**	40.659
Risk-detail				
Malware				
Self	4.533	1,110	**.036**	31.201
Other	6.740	1,110	**.011**	28.503
Spyware				
Self	.041	1,105	.841	.324
Other	.548	1,105	.461	4.370
Ransomware				
Self	6.352	1,103	**.013**	59.485
Other	.221	1,103	.640	.1.964
Fraud				
Self	.004	1,103	.947	.065
Other	.008	1,103	.930	.114
Violence				
Self	1.374	1,103	.244	24.721
Other	.308	1,103	.580	5.533
Stalking				
Self	2.451	1,103	.121	29.290
Other	2.625	1,103	.109	31.368

Note. p-values < .05 are in boldface

Exploratory

Since the questionnaire also pertained questions on level of confidence and the amount of time spent on the internet, it was decided to include these additional factors in the multivariate analysis to see if they have a significant relationship with risk perception. The regressions for level of confidence had no significant results (Table 8). However, the regressions for the time spent on the internet did. The amount of time spent on the internet had a strong positive effect on fraud for both general and detailed risk perception (Table 9). There was also a positive relation between general risk perception on ransomware, albeit smaller.

Table 8. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Levels of Confidence*

	F	*df*	*p*	B
Risk general				
Malware	.803	1,110	.372	3.394
Spyware	.220	1,105	.640	.990
Ransomware	1.687	1,103	.197	11.932
Fraud	.907	1,103	.343	4.678
Violence	.005	1,103	.943	.036
Stalking	.016	1,103	.900	.129
Risk detail				
Malware	.093	1,110	.761	.638
Spyware	.912	1,105	.342	7.279
Ransomware	1.098	1,103	.297	9.761
Fraud	1.580	1,103	.212	22.998
Violence	1.091	1,103	.299	19.625
Stalking	.303	1,103	.583	3.619

Table 9. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Time spent on the Internet*

	F	*df*	*p*	B
Risk general				
Malware	.352	1,110	.555	1.487

Spyware	2.875	1,105	.093	12.983
Ransomware	4.489	1,103	**.037**	31.756
Fraud	3.974	1,103	**.049**	20.500
Violence	.414	1,103	.521	2.929
Stalking	2.796	1,103	.098	22.555
Risk detail				
Malware	2.192	1,110	.142	15.089
Spyware	.051	1,105	.822	.406
Ransomware	1.428	1,103	.235	12.702
Fraud	4.928	1,103	**.029**	71.701
Violence	.337	1,103	.563	6.057
Stalking	.025	1,103	.874	.300

Note. p-values < .05 are in boldface

Lastly, the regressions with age as independent variable did not have any significant results and was also mainly conducted for exploratory reasons, since the age range of this sample is not big enough to actually make proper conclusions on age (Table 10). To conclude, the factor analysis resulted in two factors or scales, those being general and detailed risk perception, and the linear regressions that were significant always showed positive effects.

Table 10. *F-Value, Degrees of Freedom, Significance and Intercept of the Multivariate Regressions with Age*

	F	*df*	*p*	B
Risk general				
Malware	.715	1,110	.400	3.024
Spyware	.008	1,105	.930	.035
Ransomware	.176	1,103	.676	1.244
Fraud	.000	1,103	.991	.001
Violence	.047	1,103	.829	.331
Stalking	.349	1,103	.556	2.816
Risk detail				
Malware	.993	1,110	.321	6.833
Spyware	.766	1,105	.384	6.110

Ransomware	.373	1,103	.543	.3.314
Fraud	.629	1,103	.430	9.147
Violence	.004	1,103	.947	.080
Stalking	1.397	1,103	.240	16.697

Discussion

The goal of this study was to extend the current findings of cybercrime literature by separating different types of cybercrime and comparing their differences to get a more detailed perspective. In order to achieve that a questionnaire of risk perception has been adapted to fit into the cybercrime context which was fairly successful. The factor analysis of this new scale found two factors, and the measured validity and the reliability scores were also adequate. With the factor analysis the scale was split in two different categories of risk perception, which were then used to test the hypotheses.

Summary

First of all, it was expected that women have higher levels of risk perception than men which was supported by the results showing that women do have higher levels of risk perception for fraud and especially for stalking and violence. Perceived knowledge was originally expected to decrease the levels of risk perception, since the study of Chen and colleagues (2020) found that IT-self efficacy also leads to lower risk perception, but the results of this study showed an increased risk perception for ransomware. The level of education was also expected to lower risk perception based on previous research (Virtanen, 2017), but instead the results showed that it has a positive effect, but only for the risk perception of violence. With the next hypothesis it was expected that the usage of coping strategies increases risk perception, based on the study of Green and colleagues (2010), stating that strategies gain value according to the degree of severity of problems. Fraud was perceived as riskiest, followed by ransomware and spyware. Another hypothesis was that being victimized and knowing victims of cybercrime increases risk perception which is supported by the results of positive relationships with malware, ransomware, fraud, stalking and especially violence. Additionally, the results for victimization also show that being personally victimized has a stronger effect on risk perception than knowing someone that has been victimized. Being young was also expected to have a positive effect on risk perception but this analysis did not yield any significant

results. Analysis on confidence and time spent on the internet were also conducted, with confidence having no significant results, but the measure of time spent on the internet showed that it increases risk perception of fraud and ransomware.

Theoretical Implications

Gender

The first finding that gender has an effect on risk perception, that being that women have higher levels of risk perception was expected since a fair number of other studies came to similar conclusions. These other studies often find higher risk perceptions for cybercrimes in women compared to men, although some other studies do not find such differences (Ismailova, et al., 2019; Reisig, et al., 2009). As stated previously, women may have higher levels of fear and risk perception simply because they perceive themselves as more vulnerable and defenceless against crimes, which could be the case for the results of this study (Henson, et al., 2013; Higgins, et al., 2008; Ismailova, et al., 2019; Yu, 2014). However, one thing unique to the findings of this study are the extremely high levels of risk perception of online violence, such as cyberbullying, and cyberstalking. Although this study cannot confirm it, there is a body of literature that states that women are more often victims of these two types of crimes than men (Reyns, Henson, Fisher, 2012; Snell, Englander, 2010). There is also the indication that women are more vulnerable to these crimes, since they spent more time on socializing activities than men and they also use more services that provide such means (Dowell, Burgess, Cavanaugh, 2009; Juvonen, J., Gross, E. (2008). Virtanen (2017) also suspects that women are more fearful of cybercrimes that have interpersonal contact aspects than crimes that do not involve that, arguing that other studies have found that women are more afraid of cyberbullying than computer viruses as well. This is also somewhat in line with Ferraro's (1995) statement that women are especially fearful of sexual assault and other crimes of similar nature, which would be the case for cyberstalking and cyberbullying. All this might explain the higher levels of risk perception found for women.

Perceived knowledge

Perceived knowledge of cybercrime and cybersecurity was also found to increases risk perception, however it was originally expected to decrease the levels of risk perception, since

the study of Chen and colleagues (2020) found that IT-self efficacy also leads to lower risk perception. They argued that the participants IT-knowledge led to overconfidence since the participants scoring high on IT-self efficacy were also more likely to be victims of cybercrime than those scoring lower who actively avoided getting into circumstances where they might be at risk. The results of this study however showed a relation between perceived knowledge and increased risk perception for ransomware. There are studies that have found that knowledge of crimes increases the likelihood to recognize them and that individuals with high scores of risk perception also find more signs for crimes (Rinke, 2020). Schreurs (2019) found that risk perception can also increase the willingness to research crimes, especially if the risks are perceived to be high. Additionally, Ismailova and colleagues (2019) study on students' perception of cybercrime also showed that crime risk awareness of cybercrimes increases with computer literacy rate as well. Another reason why ransomware has such high levels of risk protection may be because it is difficult to protect against, leading to perception of its dangers to be more severe (Yaqoob, 2017). These findings can either imply that heightened risk perception increase willingness to research and thus knowledge, or that knowledge increases awareness of crimes and thus could increase risk perception of cybercrimes. Both are possible explanations for the results of this study.

Level of education

The level of education was also expected to reduce risk perception based on previous research (Virtanen, 2017), but instead the results showed that it has a positive effect on the risk perception for cybercrimes under the category of violence. The reasons for these results could be similar to the ones of perceived knowledge of cybercrime and cybersecurity since both concepts are related to knowledge in general. The level of education might increase awareness for signs of crime, which would increase risk perception similar to how knowledge of cybercrimes increases awareness of crimes and risk perception (Schreurs, 2019). However, other studies examining education in relation to any sort of crime do not find such results (Russo, Roccato, Vieno, 2012; Virtanen, 2017). Additionally, since only a single measurement with education was significant this finding for education in connection to risk perception must be taken with caution.

Coping strategies

The findings of this study revealed a positive relation between the usage of problem-focused coping strategies and risk perception, specifically an increase that is exceptionally strong for ransomware and fraud. Here, it is likely that the perceived risk or severity of the crimes, increases the worth of coping strategies (Green, et al., 2010). Many other studies also find such a relation, that high levels of risk perception led to the usage of many coping strategies, although not necessarily in the areas of cybercrime (Van der Pligt, 1996; Vazquez, 2001). The experience or expectations of coping strategies could also have affected risk perception. Van der Pligt (1996) states that high levels of risk perceptions are likely to lead to coping responses, especially if the expectations of success are high. If the expectations are low, then usage of coping strategies is less likely. Both fraud and ransomware could have high risk perception in relation with coping, since they can be difficult to protect or mitigate against (Drew, Farrell, 2018; Yaqoob, 2017)

Victimization

The findings that victimization, be that direct or indirect experience, are positively related to risk perception already has a great body of literature supporting it (Riek, et al., 2015). With the experienced victimization of the crime, comes a certain assessment of the risks that individuals without such an experience do not have. There is also support that previous victimization experiences increases fear of cybercrimes (Henson, et al., 2013, Yu, 2014). Since fear is essentially the emotional counterpart to risk perception, which is more of a cognitive judgement, it is likely that victimization experiences also increase risk perception. Russo and colleagues (2012) also found that both direct and indirect victimization increases risk perception, albeit for more physical crimes. However, it is possible that this effect also applies to cybercrime.

Time spent on the internet

The last of the findings is that time spent on the internet has a positive effect on the risk perception of ransomware and fraud, with this effect being especially strong on fraud. One assumption for the positive relation between these variables is that with more time spent on the internet, individuals become knowledgeable and experienced users, hence they have more awareness of signs of cybercrime than individuals who spent less time on the internet (Riek,

et al., 2015; Rinke, 2020). This also means that time spent on the internet is also likely related with knowledge of cybercrime and cybersecurity. Fraud could have high risk perception in relation with time spent on the internet since it is difficult to protect against (Drew, et al., 2018).

Strengths and Limitations

One strength of this study is the extended or detailed measurement of risk perception compared to other studies. Previous studies that researched risk perception in connection to cybercrime used only one item for measurement, while this study has included different aspects that influence risk perception like fear, controllability or seriousness (Riek, et al., 2015; Riek, et al., 2017; Yu, 2014). Through this a more nuanced score of risk perception is gained as it takes multiple elements of risk perception into account. Although, the factor analysis revealed two factors, but those were extremely constant over all cybercrimes. To elaborate, one factor always included two items that were rather general, one about the perceived risk for oneself and the other for the perceived risk for others, which could be because to judge the risk of others and of oneself, the two are compared. The other factor on the other hand, always had the concepts of perceived fear, seriousness and controllability, which likely only includes perceptions that apply to oneself. Such kind of differentiations in risk perception are also rarely talked about, so this finding could be considered in future measure attempts of risk perception.

Another aspect of this study that has rarely been done before in this area of research is the addition of coping strategies. Especially when it comes to its relationship with risk perception in the area of cybercrime literature is scarce, however the two concepts are closely connected since one is usually followed by the other. Since coping strategies are seen as more valuable depending on severity of the problem, it was also expected that coping strategies increase risk perception. The analysis supported that hypothesis and showed the coping strategies' positive effects on risk perception that are especially strong for stalking and spyware.

This study is not without limitations; it has to be said that the effectiveness of the chosen coping strategies is not actually well known. But since they are problem-focused it is likely that they have positive effects, and this study also assumed that this is the case but to really confirm that more research is necessary. Still, it is unclear if the positive relation with

risk perception is due to effectiveness or ineffectiveness of the coping strategies. This means that the results pertaining coping strategies should be handled with caution. Additionally, for participants that were not victimized the questions and answers were rather hypothetical and thus might not reflect their true feelings, so those measures are slightly less accurate

Furthermore, there is a suspicion that the high number of young women that participated in this study might have had a stronger influence on the results than expected. Specifically, women made up more than 70% of the study population and previous research implied that women perceive more fear or risk in general and that they are likely to have even higher levels with violence and stalking as is the case for this study. Lastly, the population also consisted mainly of students around the age of 20, meaning these results are mainly applicable for that type of population and should not be generalized. Through this the effect of age on risk perception could also not be properly measured.

Future Research

For the future, more research dedicated to the types of cybercrime that did not show significant results like malware, spyware and ransomware should be conducted. With a larger and more diverse sample results might change, making it possible that comparisons between all the types can be conducted and it can be seen more clearly how much more violence and stalking are actually perceived to be riskier. Additionally, research should examine the relationships between risk perception and the factors more closely since in what direction they influence each other is also slightly vague. For example, the relation between coping strategies and risk perception could go either way, risk perception could be influenced by the success of past coping strategies, but risk perception could also affect the value coping strategies. It would be good to see which is more likely the case. Once that has been explored more thoroughly, research could also continue with examining the origins and causes of these findings which could then be used to heighten risk perception in areas where it may be useful and to reduce victimization.

Additionally, a study with a sample population of all ages would also be helpful since the possible differences or effects of that could not be found in this study and also since the effect of age on risk or fear perception is also still unclear (Henson et al. 2013). The study from Yu (2014) supports the notion that younger individuals are more fearful of cybercrime than other generations and here. In general, younger generations have a unique situation that

some of them were raised with the internet since birth while older generations have been introduced to it later in life. This difference could have an impact on the risk perception of cybercrimes that should be examined.

Since this study gives further support that women have higher risk perception than men, especially when it comes to violence and stalking, looking into the reasons for why that might be the case is also a good step for future research. Especially examining the differences of online behaviour of women and men would be the next best step. Lastly, more research into coping strategies used for cybercrimes is also recommended since the literature on that is lacking. More interview studies to get a general taxonomy of strategies would be helpful since the current ones often only focus on sub-categories of particular types.

Conclusion

This study aimed to expand the cybercrime literature through exploring risk perception and coping mechanisms in a more detailed manner than was previously done. Differences between cybercrimes were examined and found which partially support but also contradict old research. For all factors that were explored, positive relationships with risk perception were found. In order to get to these findings a more detailed risk perception scale and a coping scale have been developed that can be adapted or improved on for further use. However, the area of cybercrime, especially pertaining psychology, risk perception and coping, is still vastly unexplored so interesting and new discoveries lie to be uncovered. With more and more knowledge revealed, the threat of cybercrime could develop to be less damaging.

References

Alkaabi, A., Mohay, G., McCullagh, A., Chantler, N. (2010). Dealing with the problem of cybercrime. *Digital Forensics and Cyber Crime*, 1-18. Retrieved from https://eprints.qut.edu.au/38894/1/c38894.pdf

Alsayed, A., O., Bilgrami, A., L. (2017). E-Banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and Advanced Engineering, 7*(1), 109-115. Retrieved from: https://www.researchgate.net/profile/Alhuseen-Alsayed/publication/315399380_E-Banking_Security_Internet_Hacking_Phishing_Attacks_Analysis_and_Prevention_of_Fraudulent_Activities/links/58cfbf14aca27270b4acaeb5/E-Banking-Security-Internet-Hacking-Phishing-Attacks-Analysis-and-Prevention-of-Fraudulent-Activities.pdf

Arief, B., Adzmi, B., Azeem, M. (2015). Understanding cybercrime from its stakeholders' perspectives: part 2 – defenders and victims. *IEEE Security & Privacy, 13*(2), 84-88. Doi: 10.1109/MSP.2015.44

Baker J., P., & Berenbaum, H. (2007). Emotional approach and problem-focused coping: A comparison of potentially adaptive strategies. *Cognition and Emotion, 21*(1), 95-118. Doi: 10.1080/02699930600562276

Benthin, A., C., Slovic, P., Severson, H. (1992). A psychometric study of adolescent risk perception. *Journal of Adolescence. 16*(2), 153-268. Doi: 10.1006/jado.1993.1014

Bidgoli, M., Grossklags, J. (2016). End user cybercrime reporting: what we know and what we can do to improve it. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-6. Doi: 10.1109/ICCCF.2016.7740424

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

Cross, C., Richards, K., Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support. *Report to the Criminology Research Advisory Council Grant*: CRG 29/13-14). Retrieved from: https://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*. Doi: 10.1080/0144929X.2021.1905066

Drew, J., M., Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programmes. *Police Practice and Research, 19*(6), 537-549 Doi:10.1080/15614263.2018.1507890

Dowell, E., B., Burgess, A., W., Cavanaugh, D., J. (2009). Clustering of internet risk behaviours in a middle school student population. *Journal of School Health, 79*(11), 547-553. Doi: 10.1111/j.1746-1561.2009.00447.x

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. Albany, NY: State University of New York Press

Green, D., L., Choi, J., J., & Kane, M., N. (2010). Coping strategies for victims of crime: effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behaviour in the Social Environment, 20*(6), 732-743. Doi:10.1080/10911351003749128

Henson, B., Reyns, B., W., Fisher, B., S. (2013). Fears of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497. Doi: 10.1177/1043986213507403

Higgins, G., E., Ricketts, M. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice, 33*, 223-233. Doi: 10.1007/s12103-008-9041-3

Hyman, P. (2013). Cybercrime: it's serious, but exactly how serious? *Communications of the ACM, 56*(3), 18-20. Doi: 10.1145/2428556.2428563

IOCTA, (2020). Internet organised crime threat assessment. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Ismailova, R., Muhametjanova, G., Medeni, T., D., Medeni, I., T., Soylu D., & Dossymbekuly, O., A. (2019). Cybercrime risk awareness rate among students in central Asia: A comparative study in Kyrgyzstan and Kazakhstan. *Information Security Journal: A Global Perspective, 28*(4-5), 127-135. Doi: 10.1080/19393555.2019.1685142

Jansen, J., Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology, 6*(2), 206-228. Retrieved from https://repub.eur.nl/pub/120588/The-Cyborgian-Deviant.pdf#page=78

Juvonen, J., Gross, E. (2008). Extending the school grounds? - bullying experiences in cyberspace. *Journal of School Health, 78*(9), 496-505. Doi: 10.1111/j.1746-1561.2008.00335.x

Kirhalla, F., A., M. (2020). Statistics of Cybercrime from 2016 to the first half of 2020. *International Journal of Computer Science and Network, 9*(5), 2277-5420. Retrieved from: https://www.researchgate.net/profile/Fatma-Mabrouk-3/publication/347885650_Statistics_of_Cybercrime_from_2016_to_the_First_Half_of_2020/links/5fe5806c299bf140883f54de/Statistics-of-Cybercrime-from-2016-to-the-First-Half-of-2020.pdf

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

Michikyan, M. Lozada, F., Weidenbrenner, J., V., Tynes, B., M. (2014). Adolescent coping strategies in the face of their „worst online experience". *International Journal of Gaming and Computer-Mediated Simulations, 6*(4), 1-16. Doi: 10.4018/ijgcms.2014100101

Pailing, A., N., Reniers, R., L., E., P. (2018). Depressive and social anxious symptoms, psychosocial maturity and risk perception: Associations with risk-taking behaviour. *PLoS One, 13*(8). Doi: 10.1371/journal.pone.0202423

Reisig. M., D., Pratt, T., C., Holtfreter K. (2009). Perceived risk of internet theft victimization: examining the effect of social vulnerability and financial impulsivity. *Criminal Justice and Behaviour, 36*(4), 369-384. Doi: 10.1177/0093854808329405

Reyns, B., W., Henson, B., & Fisher, B., S. (2012). Stalking in the twilight zone: extent of cyberstalking victimization and offending among college students. *Deviant Behaviour, 33*(1), 1-25. Doi: 10.1080/01639625.2010.538364

Riek, M., Böhme, R., Abramova, S. (2017). Analyzing persistent impact of cybercrime on the societal level: evidence for individual security behaviour. *Thirty Eighth International Conference on Information Systems, South Korea*, 1-20. Retrieved from: https://informationsecurity.uibk.ac.at/pdfs/RAB2017_Cybercrime_Eurobarometer_longitudinal_ICIS.pdf

Riek, M., Böhme, R., Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2) 261-273. Doi: 10.1109/TDSC.2015.2410795

Rinke, J., (2020). The recognition of signs of crime by citizens. Enschede: University of Twente. Retrieved from: http://essay.utwente.nl/81931/

Russo, S., Roccato, M., Vieno, A., (2012). Criminal victimization and crime risk perception: a multilevel longitudinal study. *Social Indicators Research. 112*(3), 525-548. Doi: 10.1007/s11205-012-0050-8

Sabillon, R., Cano, J., Cavaller, V., Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176. Retrieved from: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/78507/1/p1_4-6.pdf

Saxion, De Haagse Hogeschool (2020). Cyberweerbarheid risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers. Retrieved from: https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/saxion--haagse-hogeschool---cyberweerbaarheid.-risicobewustzijn-en-zelfbeschermend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers..pdf

Schreurs, W. (2019). Crossing lines together: how and why citizens participate in the police domain. Enschede: University of Twente. Doi: 10.3990/1.9789036548496

Snell, S., Englander, E. (2010). Cyberbullying Victimization and behaviour among girls: applying research findings in the field. *Journal of Social Sciences, 6*(4), 510-514. Retrieved from: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1003&context=marc_pubs

Tokunaga, R., S., Aune, K., S., (2015). Cyber defence: A taxonomy of tactics for managing cyberstalking. *Journal of Interpersonal Violence*, 1-25. Doi: 0.1177/0886260515589564

Van der Pligt, (1996). Risk perception and self-protective behaviour. *European Psychologist, 1*(1), 34-43. Doi: 10.1027/1016-9040.1.1.34

Vazquez, E., L., (2001). Risk perception interactions in stress and coping facing extreme risks. *Environmental Management and Health, 12*(2), 122-133. Doi: 10.1108/09566160110389889

Virtanen, S., M., (2017). Fear of cybercrime in Europe: examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. Doi: 10.1080/13218719.2017.1315785

Wall, D., S. (2007). Policing cybercrimes: situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205. Doi: 10.1080/15614260701377729

Yaqoob, I., Ahmed, E., Rehman, M., H., Ahmed, A., I., A., Al-garadi, M., A., Imran, M., … Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. *Computer Networks, 129*(2), 444-458. Doi: doi.org/10.1016/j.comnet.2017.09.003

Yu, S., (2014). Fear of cybercrime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1), 36-46. Retrieved from: http://cybercrimejournal.com/yuijcc2014vol8issue1.pdf