Mental Wellbeing and Cybercrime:

The Psychological Impact of Cybercrime on Victims

Louisa von der Ahe

Department of Positive Clinical Psychology and Technology,

Faculty of Behavioural, Management and Social Sciences,

University of Twente

Under the supervision of Iris van Sintemaartensdijk and Kars Otten

June 29, 2022

Abstract

The prevalence of cyber-attacks is increasing constantly, all over the globe. However, the psychological impact of cybercrime is still understudied. There is limited research on the differences in psychological impact between different types of cybercrime. This study aimed to explore such differences regarding three types of cybercrime (hacking, person-centered, and financial cybercrime). According to the Shattered Assumption Theory, after experiencing cybercrime, the victim's assumption of the world is violated, which results in feelings of anger, anxiety, fear, shame/embarrassment, and loss of self-esteem. Those negative emotions were hypothesized to be especially severe after experiencing person-centered cybercrime, as the victim's interpersonal trust is most disrupted. Additionally, it was hypothesized that the negative impact of psychological impact would increase when the victim was familiar with the offender and had extensive contact with the offender before the crime. Participants read one scenario about each type of cybercrime, including several additions (describing familiarity and intensity of contact). Afterwards, their psychological impact was measured with a self-developed scale assessing those concepts. Results indicated that experiencing person-centered cybercrime led to a greater psychological impact and having intensive contact with the offender enhanced the psychological impact. However, knowing the offender did not influence the psychological impact. Consequently, future research should further investigate the impact of person-centered cybercrime, and how psychologists can improve their treatment of victims of such, as they need special attention. For the treatment of cybercrime victims, awareness about intensive contact with the offender is crucial. Generally, more research is required on the victim-offender relationship.

Keywords: Cybercrime, Hacking, Person-Centered cybercrime, Financial Cybercrime, Psychological Impact

Table of Contents

Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims

In the globalised world, technology plays an important part in people's lives. For instance, individuals use the internet to connect with others through various communication channels as well as to stream content and make online transactions (Deniz & Geyik, 2015). Consequently, the internet has become a big part of people's daily lives and some activities or services are held entirely online nowadays. Worldwide, around 4.95 billion people have access to the internet, which is around 62.5% of the population (Johnson, 2022). By 2023, this number is expected to increase up to 5.3 billion (Johnson, 2022). Especially adolescents interact to a large extent online, through platforms where they can express themselves freely (Agustina, 2019). More specifically, the internet and especially social media are of high importance for many individuals today, as their functions and services are deeply integrated into people's lives. This includes listening to music online or daily chatting with friends who live far away.

At the same time, this increase in internet usage makes individuals more vulnerable to potential risks of the online world, as it is another space for criminals (Kaakinen et al., 2018). With the rise of technology, criminals gained new opportunities for marketing scams, identity fraud, online stalking, getting unauthorized access to a system or device, and much more (Kerr et al., 2013; Short et al., 2014). This phenomenon is called cybercrime, which refers to "any criminal activity in which a computer (or networked device) is targeted or used" (Munanga, 2019, as cited in Burton et al., 2022, p. 1). Traditional crimes, e.g., embezzlement or fraud, are connected to a reduced risk for the perpetrator when executed online (Jahankhani et al., 2014). Keeping in mind the global internet access of 62.5 %, these 62.5 % are at risk for becoming a victim of cybercrime. Considering the importance of the internet in today's world, experiencing a crime online might cause severe psychological issues in the individual (from loss of trust to symptoms of post-traumatic stress disorder (PTSD) or suicide), as it potentially would after an offline crime (Borwell et al., 2021; Cross, 2015; Aiken et al, 2015). Cybercrime is especially harmful due to the many ways the perpetrator can get access to the victim's data, the difficulty of prosecuting it, and the lack of knowledge of preventive strategies for many internet users (Gupta & Mata-Toledo, 2016). Despite the rise of technology and its serious risks, until now most researchers focused on the impact of traditional crimes, and there is limited research on the impact of cybercrime (Borwell et al., 2021). This study will explore the psychological impact of cybercrime on victims.

Types of Cybercrime

Cybercrime is a problem all countries worldwide have to deal with (Cheng et al., 2020), and it is one of the fastest-growing threats worldwide (McAfee, 2018). One important factor for this growth is that time, space, and national borders are less of an obstacle to committing crimes (Koops, 2010). The Allianz Risk Barometer, which represents the estimates of risk management experts in Europe, Asia, America, Africa, and the Middle East, stated that cyber incidents are regarded as the most concerning risk in 2022 (Zandt, 2022). In Europe, 71% of people using the internet express concerns over cybercrime, according to research from the European Union Agency for Law Enforcement Cooperation (2019). Cybercrime is either broad or specific, meaning from the institutional level, such as cybercrime within organisations, companies, and institutions, to individual victim experiences (Burton et al., 2022). Cybercrime can be differentiated depending on what the crime is aimed at, such as a device, money, or the victim itself (Correia, 2019; Furnell, 2001). In other words, it is described as hacking, financial cybercrime, or person-centred cybercrime.

Hacking means that the criminal uses a technological device to get unauthorised access to a computer (system) to obtain data, or commit fraud (Jaquet-Chiffelle & Loi, 2020; Bregant & Bregant, 2014). A study by Reep-van den Bergh and Junger (2018) discovered that since 2010, 1.2-5.8% of the European population experience hacking every year. In the Netherlands, eight out of a hundred inhabitants were being hacked between 2012 and 2019 (Statista, 2021). Most of these hacking attacks were on a website or an online profile (Statista, 2021). Buil-Gil et al. (2020) investigated the shift of cybercrime suffered by individuals and organisations during one year of the pandemic (May 2019 to May 2020) in the UK. They observed that cyber-dependent crimes aimed at individuals, which are crimes that can only be executed with computers or networks, e.g., hacking or viruses, increased by 14.91% (Buil-Gil et al., 2020). Still, many of those cybercrime attacks remain undetected, due to their complex nature and difficulty to find footprints, and a large number of unreported crimes (Koops, 2010; De Kimpe et al., 2020).

Another type of cybercrime, namely financial cybercrime, consists of criminal online activities that are used for financial gain (Kaldor et al., 2019). The most prevalent form of financial cybercrime is phishing, in which a link is sent within an email or text message to lead the user to illegal websites, where passwords get stolen, viruses download automatically, or private information falls into the hands of unauthorized third parties (Kaldor et al., 2019). Regarding the individual financial impact, Hernandez-Castro and Boiten (2014) found that even though oftentimes there is no financial impact at all, they stated that 2.3% of the

population in the UK experienced financial losses of over £10.000. De Kimpe et al. (2020) stated that the psychological consequences of financial cybercrime might be as cruel to the victim as the financial impact itself.

Person-centered cybercrime deals with any crime where the victim is the main target, for example, online stalking, blackmailing, or cyberbullying (Borwell et al., 2021). Cyberstalking is defined as repeated and undesired contact administered through technology (Kaur et al., 2021). Blackmailing means to threaten the victim of exposing private information, if they do not fulfil the required demands, which can be an (illegal) action that needs to be done or money that needs to be sent (Mahdi Addai et al., 2022). The latter, cyberbullying implies that the victim is harmed intentionally by the offender, in a situation when they can hardly defend themselves (Olweus, 1999, as cited in Slonje et al., 2013). Oftentimes,in all three types there is a power-imbalance between the perpetrator and the victim in regards to technical skills and the facelessness of the offender (Kaur et al., 2021; Mahdi Addai et al., 2022; Slonje et al., 2013). According to Buil-Gil et al. (2020), online fraud against individuals increased by 51.99% during the Covid-19 outbreak.

Consequences of Cybercrime

It is crucial to look at the psychological consequences that these crimes can have more in-depth, as they are not yet widely acknowledged, since many cybercrimes remain unreported and the victims tend to suffer in silence (De Kimpe et al., 2020; Leukfeldt, 2017). The impact of such crimes can be severe, mainly depending on the type of crime (Freeman & Smith, 2014). However, most cybercrime victims tend to feel responsible for their victimisation and do not understand enough about what has happened to them, thus immersing themselves in a state of ‘learned helplessness’ (Das & Nayak, 2013). Within this frame of mind, individuals feel like any act of defense is ineffective, and as a result, behave rather apathic and passive (Peterson & Seligman, 1983). This in return leads to the victims oftentimes not seeking (professional) help and support, which frequently worsens their symptoms (Cross, 2015). Hence, getting insight into what victims of online crimes go through is essential for understanding the extent of such crimes, but also for finding ways to help them.

The psychological impact of online crimes has been studied separately for each type of cybercrime before, but not together. The three types appear to result in similarities, but also differences regarding the emotional consequences for the victim. Generally, victims of cybercrime tend to experience anxiety, fear, shame/embarrassment, symptoms of depression, and loss of self-esteem (Cross et al., 2016; Kaakinen et al., 2018). They are likely to be

anxious because they do not feel safe anymore, especially within the online environment, but also in the offline world (Cross et al., 2016). Furthermore, the victims fear that the offender has access to their personal information, also after the crime happened (Das & Nayak, 2013), for example to their bank account, which would affect them financially as well. Also, they fear that they become victimized again, as their evaluation of people already failed once, so it might easily happen again. They oftentimes blame it on themselves and their unreliable evaluation of others (Borwell et al., 2021). Due to self-blame, feelings of naiveness and them feeling less capable of navigating in the online world, victims are likely to experience shame and embarrassment (Cross, 2015; Cross et al., 2016). Their own feelings of helplessness, self-blame, fear, and anxiety about the consequences the crime might have, potentially result in symptoms of depression (Notté et al., 2021). This is more likely for victims who are already vulnerable to symptoms of mental illnesses, because through the traumatic experience of cybercrime those symptoms might be triggered again (Lazzari et al., 2020). Similarly, those feelings lead to loss of self-esteem, as the victims not only feel less confident about their internet skills but also about their evaluation of others (Borwell et al., 2021).

Especially through hacking, cybercrime victims experience fear and distress because they do not know to which data the offender might have access to (Palassis et al., 2021). This makes it stressful to think about the future, as the offender could use their data or access a certain account again. Furthermore, victims tend to be ashamed about having become a victim of online crime, which can lead to social isolation in some cases (Barnett et al., 1996). Also, many victims experience distress and feelings of violation due to losing their privacy and security (Palassis et al., 2021).

When looking at the psychological impact of financial cybercrime, it tends to be more crucial for greater financial losses (Kerr et al., 2013). Financial loss can be divided into indirect and direct loss (De Kimpe et al., 2020). Direct loss is the cost and disturbance the victim faces, such as money, time, or discomfort (Anderson et al., 2013). Indirect loss is the loss for society, for example, disruption of trust in certain companies or bank institutes (Anderson et al., 2013). A study by Modic and Anderson (2015) revealed that the emotional impact is closely affected by the financial loss, but the degree is dependent on the individual's wealth. However, they showed that after losing money several times, extremely wealthy individuals tend to experience similar psychological effects as those who are less wealthy. Emotions that victims felt after financial cybercrime were for instance anger, fear, distress, and worry, and depressive thoughts (Whitty & Buchanan, 2015). Additionally, victims were less likely to engage in online shopping or banking in the near future (Bada & Nurse, 2020).

After person-centered cybercrime, victims are more likely to experience symptoms of depression and anxiety, as well as feelings of shame and self-blame (Stevens et al., 2021; Short et al., 2014). Especially this type of cybercrime leads to severe psychological consequences such as PTSD or suicide attempts (Stevens et al., 2021). Victims become more self-conscious (especially online), distressed, and traumatized (Haron & Yusof, 2010). A reason for this is that the focus is on the victim itself, and they might feel more targeted as in other types of cybercrime, where they are mainly used to get access to e.g., the device or bank account (Borwell et al., 2021). They also focus more on themselves and, as a result, feel that their quality of life is reduced, because they cannot pay a lot of attention to other things, which makes them feel uninvolved with other parts of their lives (Haron & Yusof, 2010). Consequently, many victims of person-centered cybercrime have shown to experience insomnia.

Not only the type of cybercrime the victim experiences influences the psychological impact, but also if they know the offender, and if they had intensive contact with them before the crime (Borwell et al., 2021). For instance, the Shattered Assumption Theory (SAT) suggests that people develop elemental assumptions about themselves as an individual and the world, as well as their role in this world (Edmondson et al., 2011). These assumptions are usually stable and help them to navigate in society (Edmondson et al., 2011). One of the main assumptions is that good things will happen to good people, which gives people meaning in life, and the feeling that nothing bad will happen when they behave accordingly (Bai et al., 2021). Respectively, distressing events such as falling victim to cybercrime can disrupt individual worldviews, even though they are mostly stable (Bai et al., 2021). In the case of the victim knowing the offender, their assumption about the offender as a person is most likely violated. This is because they must have created an assumption about them beforehand, which presumably was disrupted when they found out that this person is an offender of cybercrime. Hence, this would result in greater psychological impact than when the victim does not know the offender. Additionally, when the victim had intensive contact with the offender before the crime, their assumptions about them will most likely be violated even more after the crime. When the victim engaged in contact with the offender, they must have made an assumption about them. Presumably, this assumption was not that this person is someone who threats others on the internet, as in this case they would have avoided the contact as much as possible, so that they did not fall victim to cybercrime. According to the SAT, this shattered assumption leads to feelings of anxiety, as the victim does not trust their own view of the

world anymore (Edmondson et al., 2011). Moreover, the victim tends to feel more betrayed as they have evaluated the offender incorrectly.

The Current Study

The aim of this study was to explore the psychological impact of hacking, person-centered, and financial cybercrime on victims, as well as the influence of familiarity and intensity of contact with the offender. Therefore, this study manipulated three scenarios in an online questionnaire, that described a situation for each type of cybercrime. These scenarios were applicable to everyone, but still very detailed so that the participants could imagine how it must feel like being a victim of cybercrime. Furthermore, to assess the anticipated psychological impact of familiarity and intensity of contact with the offender, four additions were manipulated (high familiarity, low familiarity, high intensity of contact, and low intensity of contact), which describe the scenario further with details of the given manipulation. The psychological impact was measured with the concepts of anxiety, fear, anger, shame/embarrassment, and self-esteem. Accordingly, I hypothesised the following:

Hypothesis 1: The psychological impact of person-centred cybercrime is higher than the psychological impact of financial cybercrime or hacking.

Hypothesis 2: The psychological impact of cybercrime is higher if the offender was familiar than if the offender was unfamiliar with the victim.

Hypothesis 3: The psychological impact of cybercrime is higher if the victim was in contact with the offender more intensively before the crime.

Method

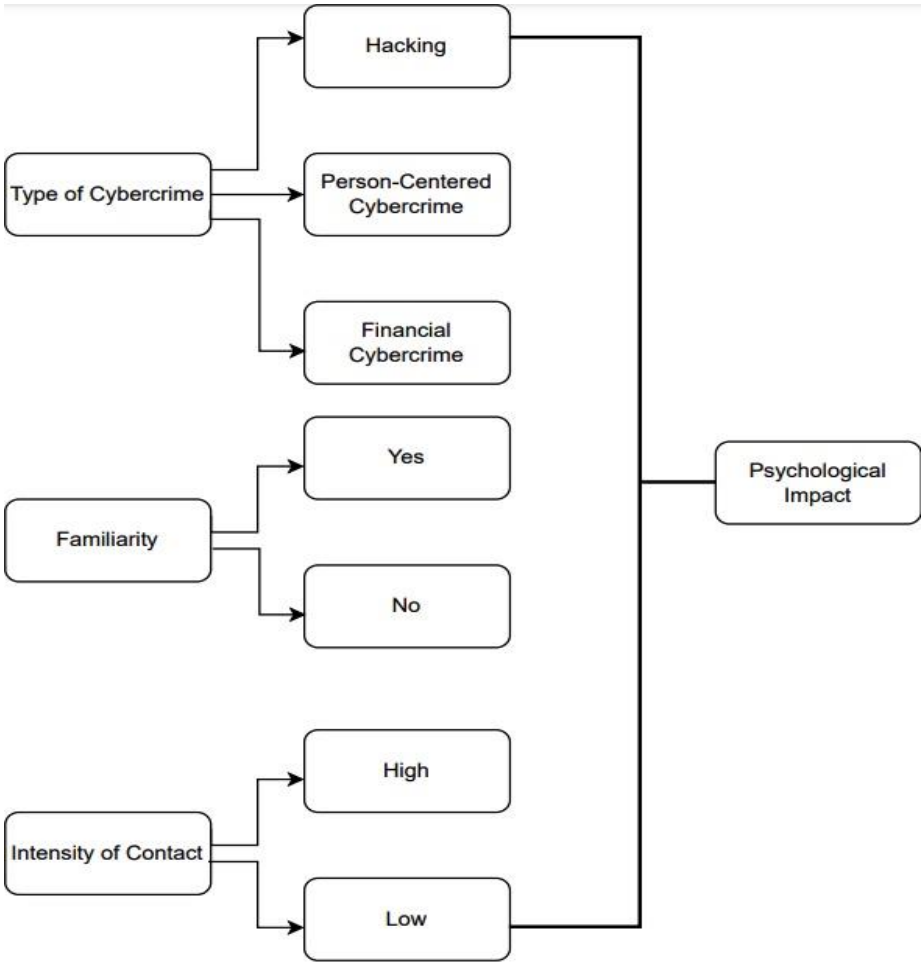
Design

I employed a within-subjects design. There were three independent variables, namely type of cybercrime, familiarity, and intensity of contact (see Figure 1). Every participant saw three scenarios for the type of cybercrimes, namely hacking, person-centered cybercrime, and financial cybercrime. Furthermore, everyone was exposed to four additions after every type of cybercrime. There were two additions to manipulate familiarity with the offender (yes/no) and two additions for the intensity of contact with the offender (high/low). The dependent variable was the psychological impact on the victim, which was measured repeatedly for all three independent variables, with the concepts of fear, anger, anxiety, shame/embarrassment, and self-esteem added together. Additionally, the design included seven different control variables

(Perceived Severity of Cybercrime, Perceived Knowledge of Cybercrime, Risk-Taking Behaviour, Internet Trust, Interpersonal Trust, Coping Strategies, and Sense of Security) further described in the material section.

Figure 1

Study Design



Participants

Out of the 127 participants, 14 had to be excluded because they either did not complete the questionnaire or had an unreasonable response time (< 500 seconds). Thus, there were 113 participants in this sample. The inclusion criterion was to have proficient English language skills. Thus, the exclusion criterion was not possessing sufficient English language skills. 50.4 % of the participants were German, 25.7 % were Dutch, and 23.9 % were of other nationalities. The participants' age ranged from 17 to 57, with a mean age of 21.96 (*SD* = 5.48). Furthermore, 69.9 % were female, 29.2 % were male, and 0.9 % identified as non-binary/third gender. Most participants, 77 %, indicated having finished secondary school, 17.7 % have finished their bachelor's or a similar higher, non-university degree, and 4.4 %

obtained a master's or another (post)graduate degree. Finally, 0.9 % finished primary school. Next, 92 % of the participants were students, and 8 % were (self) employed. Most respondents, namely 21.2 %, mentioned that they spend about four to five hours online daily, or seven or more hours (also 21.2 %). 19.5 % indicated that they spend about five to six hours online daily, and 18.6 % about three to four hours. Only 1 % said that they spend about zero to one hour online daily.

Materials

Scenarios and Additions

There were three different scenarios described in the questionnaire, one about hacking, one about person-centred and one about financial cybercrime (see Appendix D). These scenarios were created by the researcher, based on the criteria that the definitions of each type of cybercrime contain. Scenarios were used to let the participants easily imagine being in the given situation, as they described the way every type of cybercrime can happen, in a very personal way, but still applicable to everyone. For example, the scenario for person-centered cybercrime was *Imagine, that someone sends you a message on a social media platform saying that they have hacked into your webcam and now have images of you, e.g., from situations where you did not close your laptop and got undressed. They threaten you and say that unless you pay them 1000€, they will send them to all your social media contacts.* Every participant read all three scenarios, and the order in which the participants read them was randomised, as well as the order of the additions, which followed each scenario. This means that every scenario described one type of cybercrime, followed by four different additions. These additions each contained a little more information about either low or high familiarity with the offender, being in intensive contact with the offender before the crime, or not knowing them at all. An example for an addition describing a situation with high intensity of contact was *Before you notice that your account got hacked, you were chatting with someone on social media who seemed to be interested in the company you are working for, and was asking you some questions about it, such as how the atmosphere is in the company and with what kind of programs and systems you are working. Later, you find out that this person was the offender.* After each scenario and after each addition, there was a question about the psychological impact this type of cybercrime had on them.

Psychological Impact of the Victim Assessment

Psychological Impact

The psychological impact was measured to analyse what effect the different types of cybercrime, as well as familiarity with the offender, and intensity of contact, have on the

victim. The psychological impact that has been assessed was measured with the concepts of shame/embarrassment, anxiety, fear, anger, and self-esteem (see Appendix B). These items were chosen based on studies by Cross et al. (2016), Kaakinen et al. (2018), and Tennant et al. (2015), which investigated the emotional impact such crimes have, respectively. The mean score of these concepts represented the psychological impact. This was measured after each scenario, and after each addition. The participants were asked *How much more (e.g., anxious) would you likely be, compared to before the event?*, answering on a 5-point Likert scale, ranging from 1 (*None at All*) to 5 *(A Great Deal).* The mean score for psychological impact of hacking before the additions was 3.47 (*SD* = 0.84), for person-centered cybercrime before the additions it was 3.81 (*SD* = 1.07), and for financial cybercrime before the additions the mean score was 3.46 (*SD* = 0.77). Cronbach's alpha for this scale was proven to be good (α = .74).

Risk-Taking Assessment

DOSPERT Scale

The *DOSPERT-scale* was used to assess participants' risk-taking behaviour, which might influence the psychological impact (Duell & Steinberg, 2021), because individuals who enjoy taking risks more than others, might have less fear about the consequences that could occur (Wake et al., 2020). The scale consists of 30 items, in which respondents indicate to what extent they would engage in specific risky behaviours (see Appendix B). The items cover five life domains, such as ethical, financial, health/safety, social and recreational risks, with a 7-point rating scale ranging from 1 (*Extremely Unlikely*) to 7 (*Extremely Likely*). The item ratings across all items of a subscale are added to obtain scores for the subscales. A higher score represents greater risk-taking behaviour in the subscale domain. Sample items include "Going camping in the wilderness" (*Recreational*), "Drinking heavily at a social function" (*Health/Safety*), "Passing off somebody else's work as your own" (*Ethical*) and "Starting a new career in your mid-thirties" (*Social*). The internal reliability was proven to be good (α = .84), and the mean score of the scale was 3.55 (*SD* = 0.72).

Coping Style Assessment

Brief-COPE

Individuals who usually engage in rather beneficial coping strategies such as seeking emotional support are assumed to cope better with traumatic life events (Jansen & Leukfeldt, 2018). To assess the participant's coping mechanisms as a potential control variable, to see how respondents cope with such events usually, the *Brief-COPE* was used (see Appendix B). It is a 28-item questionnaire, and the answers indicate how frequent the respondents engage in the coping behaviour on a four-point Likert scale, ranging from 1 (*I haven't been doing this at*

all) to 4 (*I've been doing this a lot*). Higher scores indicate greater coping strategies. The scale assesses the respondent's primary coping style with scores on three subscales (*Problem-Focused Coping, Emotion-Focused Coping and Avoidant-Coping*). Fourteen facets are covered by this scale, however, the facets that were not necessary for this study were deleted. Thus, in this study, there were seven facets (*Active Coping, Emotional Support, Acceptance, Self-Blame, Self-Distraction, Denial and Behavioural Disengagement*), each with two items. The remaining facets (*Use of Informational Support, Positive Reframing, Planning, Venting, Humour, Religion and Substance Use*) were found to be either overlapping with other items (Carver, 1997) or not of value for this study. Sample items were "I've been giving up trying to deal with it", "I've been criticizing myself" or "I've been learning to live with it." Cronbach's alpha for the scale was proven to be adequate (α = .71). The mean scores of the subscales were the following: Active Coping had a mean score of 3.42 (*SD* = 0.86), Emotional Support of 3.42 (*SD* = 1.14), Acceptance of 3.66 (*SD* = 0.86), Self-Blame of 3.5 (*SD* = 1.08), Self-Distraction of 3.46 (*SD* = 0.95), Denial of 1.85 (*SD* = 1.01) and Behavioural Disengagement of 1.96 (*SD* = 0.95).

Perceived Severity Assessment

Perceived severity of cybercrime affects how serious the victim evaluates the crime (De Kimpe et al., 2020). More specifically, when the victim views cybercrime as a severe threat to society and/or themselves, their reaction to becoming a victim might be greater than when they assume that cybercrime is not severe. To assess the respondents' perceived severity of cybercrime as a potential moderator for the relationship of the type of cybercrime with the psychological impact, three items that were already used in a study by de Kimpe et al. (2020), were applied (see Appendix B). In that study, the authors used the items from a study by Witte (1996) and adapted them for the purpose of their own study. This adapted version was suitable for this study because it could be related to cybercrime, e.g., *I believe that cybercrime is significant.* A 5-point Likert scale was used to assess the answers, ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). Cronbach's alpha was good (α = .86), and the mean for perceived severity in this sample was 4.5 (*SD* = 0.62).

Perceived Knowledge Assessment

The level of knowledge the victim has about cybercrime influences the psychological impact as when the victim knows more about the potential risks and consequences, they might perceive the threat as more serious than others, who might not know much about cybercrime (Riek et al., 2016). The respondents' perceived knowledge about cybercrime was assessed to gain insight into how much they assumed to know beforehand and how this related to the

experienced psychological impact later. It has been assessed with two items from the Eurobarometer, which have been used in a study by de Kimpe et al. (2019), such as for example "I feel adequately informed about the risks of the internet." (see Appendix B). A 5-point Likert scale was employed, ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). They proved to have good internal reliability (α = .78). The mean score for perceived knowledge in this sample was 3.38 (*SD* = 0.93).

Interpersonal Trust Assessment

The victim is likely to have problems with establishing trustful relationships again when their trust was misused (Borwell et al., 2021). There were two self-developed items about interpersonal trust as a potential moderator included in the questionnaire. These items were asked after each scenario and the four additions for every type of cybercrime, to assess the impact on trust for each type (see Appendix B). An example of such an item was "I find it easy to trust others." Answers were given on a 5-point Likert scale, ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). The items correlate strongly after hacking (*r* = .65), person-centered cybercrime (*r* = .63), and financial cybercrime (*r* = .59). The mean score for hacking was 3.07 (*SD* = 0.96), for person-centered cybercrime it was 2.97 (*SD* = 0.96), and for financial cybercrime it was 3.04 (*SD* = 0.95).

Internet Trust Assessment

Victims tend to be more cautious when using the internet, because their fear becoming victimised again (Borwell et al., 2021). Internet trust was assessed with two items, to assess the influence of internet trust as a potential control variable for psychological impact (see Appendix B). The items have been used in a study by de Kimpe et al. (2019) before. An example item was, "I have every confidence that the internet is safe." Respondents could answer on a 5-point Likert scale, ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). The correlation between these items is strong after hacking (*r* = .72), person-centered cybercrime (*r* = .74), and financial cybercrime (*r* = .74). The mean score for internet trust after hacking was 1.81 (*SD* = 0.80), for person-centered cybercrime it was 1.73 (*SD* = 0.82), and for financial cybercrime it was 1.82 (*SD* = 0.81).

Sense of Security Assessment

The cybercrime victim's sense of security is likely to decrease after the event, as they tend to be more cautious about potential threats, online but also in their real life (Jansen & Leukfeldt, 2018). The respondent's sense of security was measured for each type of cybercrime. The question was: *After reading the scenario about hacking/person-centered cybercrime/financial cybercrime, and the additions, please indicate how concerned you are*

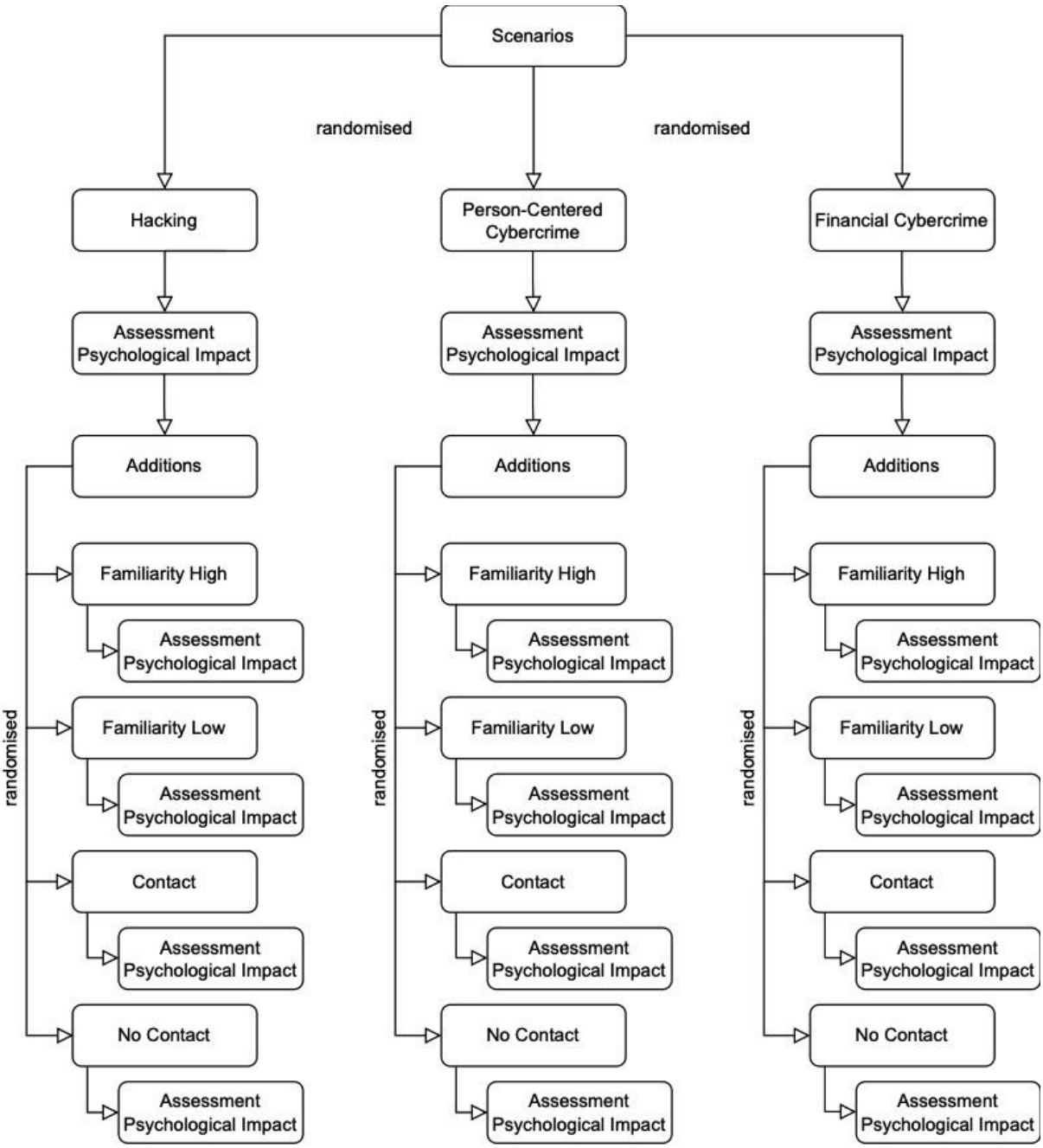
now about security on the Internet? (e.g., people reading your email, finding out what websites you visit, etc.). Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identity for you or for someone else (see Appendix B). The answers were based on a 5-point Likert scale, ranging from 1 (*Not at All Concerned*) to 5 (*Very Concerned*). There was one item saying, "I know I should be concerned, but I'm not." This item was scored as a midpoint item, with 3. The internal reliability for these items was good ($\alpha = .82$), and the mean score was 3.31 (*SD* = 0.79) for hacking, 3.42 (*SD* = 0.81) for person-centered cybercrime, and 3.31 (*SD* = 0.78) for financial cybercrime.

Procedure

First, the BMS Ethics Committee of the University of Twente ethically approved this study design. The study was conducted with Qualtrics, and participants were recruited through convenience sampling and the university's recruitment system (Sona systems). Respondents were informed about the goal, content, and course of the questionnaire, e.g., that they will be reading three different scenarios with 12 short additions, and that they should imagine being the victim and answer some questions about it (see Appendix A). Then, they indicated if they give consent and participate in the study or withdraw. Afterwards, participants started the study with demographic questions, followed by questions about their perceived severity, and perceived knowledge of cybercrime, their risk-taking behaviour, and questions about interpersonal trust and internet trust. Then, they read the first scenario, in which they should imagine being the victim of one of the three types of cybercrime. The order of the three scenarios was randomised (see Figure 2). After each scenario, there was a question about the psychological impact this type of cybercrime had on them. After this, they read four additions to this scenario, with also the order of these additions being randomised, and answered the question about the psychological impact after each addition again. The additions provided additional information about the situation regarding either being familiar with the offender, not being familiar with the offender, having intensive contact with them before the crime or not having any contact before. The same procedure was applied for the next two scenarios and additions, respectively. After each scenario and its additions, respondents were asked about their interpersonal trust and internet trust again, as well as their perceived sense of security. After that, they had to fill out the questions for the coping scale. Finally, the respondents were debriefed about the purpose of the study (see Appendix C). Overall, completing this questionnaire took approximately 15 min for most of the respondents.

Figure 2

Flowchart of the Procedure of the Study



Data analysis

The data were analysed with SPSS, the Statistical Package for the Social Sciences. To test if person-centered cybercrime has a greater psychological impact on the victim than hacking or financial cybercrime (H1), a general linear model with repeated-measures ANOVA and a contrast analysis were employed.

To test if being familiar with the offender has a greater psychological impact on the victim than not being familiar (H2), a repeated-measures ANOVA was used.

To test if having intensive contact with the offender before the crime has a significant effect on the victim's psychological impact (H3), a general linear model with repeated-measures ANOVA was applied.

Results

A repeated-measures ANOVA was run to assess the effect of person-centered cybercrime compared to the effect of hacking or financial cybercrime on the psychological impact (H1). The assumption of sphericity was violated, thus the Greenhouse-Geisser correction was employed. This showed a significantly different effect between the groups, $F(1.82, 224) = 10.645$, $p < .001$. The contrast analysis demonstrated that there is no significant difference between the psychological impact of hacking and financial cybercrime, $t(336) = 0.103$, $p = .918$. However, when comparing the impact of hacking with person-centered cybercrime, it proved to be significantly different, $t(336) = 2.823$, $p = .005$. More specifically, the mean score for psychological impact was higher after person-centered cybercrime ($M = 3.81$, $SD = 1.07$), than after hacking ($M = 3.47$, $SD = 0.84$). Furthermore, the impact of financial cybercrime and person-centered cybercrime was proven to be significantly different, $t(336) = 2.927$, $p = .004$. The mean score for the psychological impact after person-centered cybercrime proved to be higher than for financial cybercrime ($M = 3.46$, $SD = 0.77$). Therefore, I confirmed the first hypothesis.

For the second hypothesis, a repeated-measures ANOVA was employed, which showed that being familiar with the offender did not significantly increase psychological impact, $F(1,112) = 1.982$, $p = .162$, $\eta^2_p = .52$. When looking at the mean scores for the psychological impact when being familiar with the offender ($M = 3.41$, $SD = 0.78$), it showed a greater effect on psychological impact than not being familiar ($M = 3.32$, $SD = 0.90$), however, it did not seem to be significantly greater. Thus, I rejected the second hypothesis.

To test whether the intensity of contact with the offender significantly impacts the psychological impact (H3), a repeated-measures ANOVA was conducted. This analysis proved that there was a significant effect on psychological impact, $F(1,112) = 15.933$, $p < .001$, $\eta^2_p = .98$. The mean score for being in intensive contact with the offender before the crime ($M = 3.62$, $SD = 0.79$), showed a greater psychological impact than the mean score for not being in intensive contact ($M = 3.45$, $SD = 0.84$), hence, I confirmed the third hypothesis.

Additional Analyses

Besides testing the three hypotheses, additional analyses with the control variables were conducted. The variables included were Risk-Taking Behaviour, Perceived Severity of

Cybercrime, Perceived Knowledge of Cybercrime, Internet Trust, Interpersonal Trust, Coping Strategies, and Sense of Security. In order to check if these variables were associated with psychological impact, I looked at the Pearson correlation. Additionally, I decided to do several separate regression analyses with the variables that proved to be significantly correlated with the variable psychological impact. In this way, I could explicitly look at the individual impact of each variable on psychological impact.

First, I explored whether there is a correlation between psychological impact and risk-taking behaviours, which were found to be negatively correlated (see table 1). Conclusively, participants who had higher scores on the risk-taking scale were less likely to experience higher psychological impact. The linear regression showed that there was a significant effect of risk-taking behaviours on psychological impact, B = -0.23, T = -2.17, SE = .12, p = .032. Lastly, 4 % of the variance in psychological impact could be explained by the participant's risk-taking scores, (R^2 = .04).

Moreover, when looking at the correlation of perceived knowledge of cybercrime with psychological impact, they were shown to be negatively correlated (see table 1). Thus, participants who had high scores on perceived knowledge were less likely to have high scores on psychological impact. The linear regression demonstrated that perceived knowledge significantly influenced psychological impact, B = -0.22, T = -2.62, SE = .08, p = .010. Six percent of the psychological impact score can be attributed to the respondent's perceived knowledge scores (R^2 = .06).

Furthermore, I assessed if the variables of the coping inventory were correlated with psychological impact. More specifically, participants who scored high on the coping strategies self-blame and denial were found to be positively correlated with psychological impact (see Table 1), meaning that the higher participants scored on psychological impact, the more likely they were to have higher scores on these coping strategies. The linear regression analysis indicated that self-blame had a significant effect on the psychological impact, B = 0.15, T = 2.12, SE = .07, p = .036, as well as denial, B = .29, T = 3.99, SE = .07, p < .001. Four percent of the variance in psychological impact could be attributed to self-blame (R^2 = .04), and 13 % to denial (R^2 = .13).

Finally, I assessed whether the participant's sense of security correlated with psychological impact. The Pearson correlation showed that sense of security and psychological impact were significantly positively correlated (see table 1). This indicated that respondents who had greater concerns for security on the internet after the scenarios were more likely to have higher scores on psychological impact. The linear regression analysis

showed that sense of security had a significant effect on psychological impact, $B = 0.37$, $T = 3.35$, $SE = .11$, $p = .001$. Nine percent of respondents' psychological impact can be attributed to their sense of security ($R^2 = .09$).

To see whether perceived severity, interpersonal trust, internet trust, the coping mechanisms active coping, emotional support, acceptance, self-distraction, and behavioural disengagement are correlated with psychological impact, I also looked at the Pearson correlation of the variables. However, they were proven to have no significant correlation with psychological impact ($p > .05$) (see Table 1).

Table 1

Means (M), Standard Deviations (SD), and Correlations Between 13 Additional Variables and the Psychological Impact

Variables	*M*	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Risk-Taking	3.55	0.72														
2. Perceived Severity	4.5	0.62	-.21*													
3. Perceived Knowledge	3.38	0.93	.20*	-.10												
4. Internet Trust	2.05	0.86	.12	-.30**	.08											
5. Interpersonal Trust	3.5	0.86	-.13	.11	.10	.10										
6. Sense of Security	3.35	0.68	-.003	.05	-.01	-.32**	-.12									
7. Active Coping (C. M.)	3.42	0.86	.11	.13	.06	.05	-.15	-.09								
8. Emotional Support (C. M.)	3.42	1.14	-.08	.14	-.02	.03	.22*	.03	.23*							
9. Acceptance (C. M.)	3.66	0.86	.25**	.03	.32**	-.07	.06	-.02	.51**	.11						
10. Self-Blame (C. M.)	3.5	1.08	.03	.07	-.11	-.08	-.15	.08	.05	.15	-.15					
11. Self-Distraction (C. M.)	3.46	0.95	.17	-.04	.04	-.10	-.06	.01	-.04	.04	-11	.16				
12. Denial (C. M.)	1.85	1.01	-.04	-.12	-.17	.03	-.07	.26**	.07	.15	-.06	.30**	.11			
13. Behavioural Disengagement (C. M.)	1.96	0.95	.20*	-.08	.11	.13	.06	.15	-.16	.11	-.06	.36**	.32**	.50**		
14. Psychological Impact	3.47	0.84	**-.20***	.17	**-.24****	-.07	-.15	**.30****	.12	.14	-.10	**.20***	.05	**.35****	.09	

Note. N = 113, (C. M.) = Coping Mechanism

* Correlation is significant at the 0.05 level (2-tailed).

** Correlation is significant at the 0.01 level (2-tailed).

Discussion

With this study, I aimed to investigate how the psychological impact of cybercrime on victims differs depending on three different types of cybercrime (hacking, person-centered cybercrime, and financial cybercrime). It was hypothesized that person-centered cybercrime results in greater psychological impact, and that being familiar with the offender and having intensive contact with them before the crime increases this effect. Results indicated that after reading a scenario about person-centered cybercrime, victims indicated experiencing a greater psychological impact than after scenarios about hacking and financial cybercrime. Knowing the offender had no impact on the victim's psychological impact, however, when they imagined having intensive contact with them before the crime, they demonstrated experiencing a greater psychological impact.

Findings and Implications

Most importantly, victims experienced a significantly higher psychological impact after person-centered cybercrime, compared to hacking or financial cybercrime. One explanation for why this could have been the case, is the SAT, which indicates that the stable assumptions victims have developed about people and the world over a long period of time were completely disrupted (Edmondson et al., 2011). The cybercrime attack of person-centered crime tends to feel more personal, targeting the victim themselves, which oftentimes results in greater psychological impact (Van der Wagen & Pieters, 2018). In addition to the online crime itself, the victim’s interpersonal trust and assumptions are violated more extensively after person-centered cybercrime (Borwell et al., 2021). With the belief in a just world that individuals generally have, they experience their surroundings as fair and relatively stable, which proves to not be correct anymore after their victimization, and consequently results in emotional distress (Borwell et al., 2021). This means that it takes time and effort for the victim to establish a stable view of themselves and the world, and to build up trust again. As a result, victims of person-centered cybercrime should be especially supported with techniques for building trustful relationships, and they should be helped to develop new assumptions about the world and themselves. More specifically, psychologists who treat those victims should be aware that their worldview is violated, and they should empower them to re-build a new system that enables them to successfully operate in this world again (Figley, 1986). For example, they could help the individual change their behaviours by gaining new knowledge about secure internet usage, encouraging them to seek emotional support, or redefining the event. Redefining in this case means trying to view the event in a way that is consistent with the victim's prior assumptions, hence less traumatic (Figley, 1986).

Moreover, I found that being familiar with the offender had no significant influence on psychological impact. This is contrary to the results of the study by Borwell et al. (2021), who found that familiarity increased the psychological impact. The insignificant result in this study could be due to low reliability and validity of the scenarios, as they were not tested in another sample before. Thus, it was unclear how well they represent the types of cybercrime and the several additions. Also, the mean scores were proven to be slightly higher for the psychological impact when being familiar with the offender. Hence, the result might have been due to unreliable scenarios and additions.

Similar to the results of this study, van de Weijer et al. (2020) found that when the offender is known to the victim, they are less likely to report the crime. A reason for this might be that if the victim knows more about the offender, they might feel more empathetic towards them, and their wish for unpleasant consequences for the offender decreases (van de Weijer et al., 2020). This would reduce the psychological impact caused by the crime, respectively. Another important factor for this result might be that there is a difference between simply knowing the offender and having (had) a personal relationship with them (van de Weijer et al., 2020). The psychological impact likely increased the more intense the personal relationship with the offender was, as seen in a study by Johnson and Kercher (2009), who demonstrated that the victim-offender relationship plays an important part in the victim's psychological impact. In the additions of being familiar with the offender, the relationship with the offender seemed to be rather distant, for example, the offender was a party acquaintance or an old friend that is no longer a friend. Thus, this degree of victim-offender relationship might not have been enough to cause a significant effect on the psychological impact. This means that the psychological impact of cybercrime tends to be greater, the closer the victim's relationship with the offender is. For psychologists, this is an important factor that they should be aware of when treating cybercrime victims. When the relationship with the offender was relatively close, they will likely need more help and support. For instance, they might struggle with trusting other (important) people in their lives. The psychologist could help the victims establish trustful relationships (again), by first building rapport with them, for example by being authentic and expressing their feelings as well (as much as is recommended for a psychologist). Also, it it valuable to know that telling the victim about the identity of the offender, does not significantly increase the psychological impact. Thus when for instance the police investigated the case and the offender was found, there is no reason to keep the identity of the offender classified.

Furthermore, there was a significant effect of the intensity of contact with the offender before the crime on psychological impact. First of all, this might be explained with the SAT again, since through intensive contact with the offender, the victim establishes a personal and trustful relationship with them, which then results in greater loss and decrease of interpersonal trust (Borwell et al., 2021). Also, Leukfeldt et al. (2018) proved that the longer the victim was in contact with the offender, the greater was the decrease of trust. This might be because the victim feels like they could have avoided the crime by better evaluating the situation beforehand and the actions and behaviours of the offender, which makes them feel naïve and unintelligent. Preventing that the victim and offender have less intensive contact before the crime is only possible by making it harder for the offender to get in contact with the victim. Hence, it is especially important to increase the victim's awareness of cybercrime and knowledge about how to use the internet in the safest way possible, so that they can detect any signs of potential cybercrimes immediately on their own.

Nevertheless, even if the victims possess proficient internet skills, and are trained regarding online crimes, there is still a chance that they might fall victim to cybercrime (again). Therefore, psychologists or other professionals that these victims refer to, should not only be trained in how the victims can build new trustful relationships again, but also provide them with guidance on how they can learn to use the internet safely (Monteith et al., 2021). Many individuals, especially victims, may find it hard to find trusted and secure websites. It should be clear that it is not the psychologist's task to teach the victim about the potential online risks and ways to avoid them, but merely they should encourage the victim to think about what went wrong and provide them with secure websites or services that they can use (Monteith et al., 2021). In line with this, when psychologists use technology within their own treatment, they should provide guides and training of such for their patients.

Besides testing the hypotheses, I looked at the interactions between the additional variables and psychological impact, while I did not take into consideration the different types of cybercrime within this relationship. As the focus of this study was to find out which type of cybercrime has the largest psychological impact and how this impact is influenced by familiarity and intensity of contact, looking at the additional variables and taking their effect within this relationship into account would have been out of the scope of my research. The additional analyses revealed that self-blame and denial, two of the coping strategies assessed, correlated with the psychological impact, meaning that the more people used those strategies, the greater was the psychological impact. Also, both strategies were proven to predict the psychological impact to some extent.

In previous studies, self-blame was associated with ‘positive’ outcomes if the blame was about an individual’s behaviours, while it had a negative effect if the blame was related to one’s character (Voth & Sirois, 2009; Filipas & Ullman, 2006). A reason for this effect might be that behaviours are malleable, whereas character traits stay relatively stable, and it is difficult to control them (Voth & Sirois, 2009). So, when the individual blames themselves for a behaviour that they could have changed, they might change it in the future, and feel like they learned from it, thus it has a ‘positive’, productive outcome. In this study, the respondents might have felt like they could not have done anything differently in the described situation, as they did not see the threat coming. Therefore, when they blamed the crime on themselves, this resulted in a greater negative outcome compared to the respondents who did not blame it on themselves to that extent. Consequently, psychologists who treat victims of cybercrime should be aware that victims who experience a severe psychological impact tend to blame themselves for the crime. Then they should know how to help the victim shift that self-blame to blaming the offender and how they can cope with the situation.

Denial of the psychological impact was related to malfunctioning behaviours that will make the individual feel better for a short period of time, such as smoking, eating, drinking, and denying that the event occurred (Vos & de Haes, 2006). These strategies are ways to distract oneself from the situation, and the individual tends to feel out of control, pessimistic, and powerless, which are feelings similar to depression and proven to be malfunctioning (Vos & de Haes, 2006). Hence, psychologists should help the victim to learn not to deny their negative feelings about the crime, but instead rather provide them with guidance and support on how to deal with those feelings and explain to them that this will help them the most in the long term. Both coping mechanisms, self-blame, and denial, should consequently be regarded as potential moderators of the victims’ psychological impact in future research.

Furthermore, respondents who were highly risk-taking, were proven to experience a smaller psychological impact. This phenomenon can be explained with the concept of positive risks. Positive risks tend to be enriching activities that have productive outcomes, such as trying out a new sport (Duell & Steinberg, 2018). In contrast, negative risks tend to be illegal and hazardous, such as stealing something. Engaging in positive risks is proven to promote personal growth, which in turn leads to better wellbeing. Through taking (positive) risks, gaining new knowledge, and making new experiences, people feel more accomplished and personally develop a lot. This makes them feel good about themselves, proud, and satisfied with their own life (Duell & Steinberg, 2018). Hence, this might be a reason for why

participants who were more likely to engage in risky behaviours that are positive, experienced a smaller psychological impact.

Moreover, while Borwell et al. (2021) showed that the SAT is a suitable theory for explaining the impact of cybercrime on the victims, the victim's sense of security failed to predict that impact. Therefore, in this study, the perceived sense of security was included as an additional measurement, which showed that individuals who had higher concerns for security on the internet, were more likely to have higher scores on psychological impact. Also, I found that sense of security predicted the respondent's psychological impact to a significant extent. The victims question their capabilities and knowledge of the internet world and tend to be more cautious of repeating the mistake (Jansen & Leukfeldt, 2018). Hence, to help those individuals feel secure and confident in using the internet again, their feelings of trust need to be strengthened again (Coutu & Dupont, 2021). This can be done for example by gaining more awareness about potential risks and consequences of using the internet, and how to avoid them (Coutu & Dupont, 2021). Coutu and Dupont (2021) found out that very few prevention campaigns were proven to be successful until now. This shows that there is a large demand for improving such campaigns, as cybercrime is increasing constantly.

Strengths and Limitations

The strengths of this study are, most importantly, the scenarios. Through the scenarios, respondents could easily imagine what it must be and feel like being a victim of the specific type of cybercrime. They were written very detailed so that it was easy to imagine being in that situation, but still applicable to everyone. After thoroughly looking at other studies, this was the best way to get the most reliable answers to the questions, without harming the participants. Another important strength of this study is that it controlled for the individual effect of the participants. Every respondent read every scenario and answered the same questions, which gave the study a high power, with the relatively big sample size (n = 113).

Nevertheless, this study seems to have several limitations. Firstly, even though the scenarios were the best possible way to assess the psychological impact, it implies that only the respondent's anticipated psychological impact was measured. When people fall victim to cybercrime, their actual reaction might differ from their anticipated reaction. Also, I did not measure whether the participants had any prior experiences with cybercrime. This could have impacted the results as those who already fell victim might feel more strongly about it and their feelings of being a victim might come up again. However, when looking at other studies (Hernandez-Castro & Boiten, 2014; Dreßing et al., 2014), mostly very few participants indicated having experienced cybercrime, which did not affect the results tremendously.

Furthermore, there was no possibility of pilot testing for the scenarios, which implies that neither their reliability nor their validity was checked beforehand. Also, regarding the items for psychological impact, there was only one question for every concept, e.g., fear or anxiety. This measurement of psychological impact was not as valid as it could have been, due to the small availability of (short) validated scales. Thus, this showed that there is a need for scales that measure the psychological impact in a valid and reliable way. Additionally, the question about psychological impact, which was asked after each scenario, was formulated in a way that the respondent could only indicate to experience more anger, anxiety, etc. compared to before, a decrease or equal feelings of the psychological impact were not possible. Still, as the study aimed at finding a significant difference between the types of cybercrime, which was possible to identify with this question, it was sufficient for the purpose of this study. Another limitation might be that this study looked at the three most prevalent types of cybercrime, however, there are many more types which also result in a severe psychological impact for the victim (Yadav et al., 2021). Nevertheless, person-centered cybercrime proved to have a serious psychological impact, which needs to be investigated more in-depth.

Future Research Implications

The results show that there is a need to investigate person-centered cybercrime and its impact further, as the different kinds of person-centered cybercrime might translate into different aspects of psychological impact. For example, cyberstalking victims stated to have experienced feelings of helplessness, irritation, insomnia, and disruption of interpersonal trust (Dreßing et al., 2014), while victims of cyberbullying were found to experience mainly agony, sorrow, and resentment (Schenk et al., 2012). To understand and be able to help and treat victims of person-centered cybercrime, the subtle differences in the psychological impact must be considered. Another future research implication is that this study looked at the direct immediate psychological impact, while it is unclear how stable and persistent these effects might be. Hence, there is a need to investigate the long-term psychological impact of person-centered cybercrime. For example, victims of all types of person-centered cybercrime could be asked several times after different periods of time about their victimization. There might be different effects for cyberbullying than for cyberstalking, also in the long term. For the psychologists that are treating cybercrime victims, this study underlines that those who experienced person-centered cybercrime will likely need more support. Also, they should know how to help their patients establish interpersonal trust again, which is especially demanded by those victims who knew the offender well or those who were in intensive contact with them prior to the crime. Additionally, psychologists can try to help reduce the

prevalence of cybercrime by making their patients aware of potential risks of the internet, in particular when they are providing treatment online as well. Finally, future research should look into the different types of relationships that the victim can have with the offender, and how this relationship might influence the psychological impact. It would be valuable to know at what degree of relationship the victim experiences greater psychological impact.

Conclusion

This study revealed that person-centered cybercrime is a highly prominent predictor of psychological impact, and intensive contact before the crime increases this impact, while simply knowing who the offender is, has no (significant) effect. As a result, this suggests that psychologists who treat cybercrime victims need to be aware of the differences in the psychological impact of the different types of cybercrime. For example, victims of person-centered cybercrime should be regarded as more severely emotionally affected. Similarly, the psychologists should ask if the victim had intensive contact with the offender before the crime and if they knew the offender, and if so, how close their relationship was. Accordingly, they should adjust their treatment. However, the findings only reveal the surface of the differences in psychological impact and show that more extensive research needs to be done, especially on person-centered cybercrime as the impact might also differ among the specific types of person-centered cybercrime.

References

Agnew, R. S. (1985). Neutralizing the Impact of Crime. *Criminal Justice and Behavior, 12*(2), 221–239. https://doi.org/10.1177/0093854885012002005

Agustina, J. R. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology*, *9*(1), 35–54. https://doi.org/10.5281/zenodo.22239

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373–391. https://doi.org/10.1080/21582041.2015.1117648

Aljazzaf, Z. M., Perry, M., & Capretz, M. A. (2010). Online Trust: Definition and Principles. *2010 Fifth International Multi-Conference on Computing in the Global Information Technology*, 163-168. https://doi.org/10.1109/iccgi.2010.17

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (1 ed., pp. 265-300). Springer Berlin Heidelberg.

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. *Emerging Cyber Threats and Cognitive Vulnerabilities*, 73–92. https://doi.org/10.1016/b978-0-12-816203-3.00004-6

Bai, Q., Huang, S., Hsueh, F. H., & Zhang, T. (2021). Cyberbullying victimization and suicide ideation: A crumbled belief in a just world. *Computers in Human Behavior, 120*. https://doi.org/10.1016/j.chb.2021.106679

Barnett, O. W., Martinez, T. E., & Keyson, M. (1996). The Relationship Between Violence, Social Support, and Self-Blame in Battered Women. *Journal of Interpersonal Violence*, *11*(2), 221–233. https://doi.org/10.1177/088626096011002006

Borwell, J., Jansen, J., & Stol, W. (2021). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. *Social Science Computer Review*, https://doi.org/10.1177/0894439320983828

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. *The Encyclopedia of Criminology and Criminal Justice*, 1–5. https://doi.org/10.1002/9781118517383.wbeccj244

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(1), 47–S59. https://doi.org/10.1080/14616696.2020.1804973

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, *159*. https://doi.org/10.1016/j.exger.2021.111678

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). Victims of Cybercrime: Understanding the Impact Through Accounts. *Cybercrime in Context*, 137–156. https://doi.org/10.1007/978-3-030-60527-8_9

Carver, C. S. (1997). You want to measure coping but your protocol' too long: Consider the brief cope. *International Journal of Behavioral Medicine*, *4*(1), 92–100. https://doi.org/10.1207/s15327558ijbm0401_6

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

Correia, S. G. (2019). Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0099-7

Coutu C., Dupont B. (2021) The Impact of a Canadian Financial Cybercrime Prevention Campaign on Clients' Sense of Security. In: M. Weulen Kranenbarg., R. Leukfeldt (eds.) *Cybercrime in Context. Crime and Justice in Digital Society*. Springer, Amsterdam, pp. 157-172.

Cross, C. (2015). No laughing matter. *International Review of Victimology*, *21*(2), 187–204. https://doi.org/10.1177/0269758015571471

Cross, C., Richards, K., & Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support. *Final report for Criminology Research Grant 29.* 13-14. Australian Institute of Criminology, Australia.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*. https://doi.org/10.1016/j.chb.2020.106310

Deniz, M. H., & Geyik, S. K. (2015). An Empirical Research on General Internet Usage Patterns of Undergraduate Students. *Procedia - Social and Behavioral Sciences*, *195*, 895–904. https://doi.org/10.1016/j.sbspro.2015.06.369

DeValve, E. Q. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. *Applied Psychology in Criminal Justice*, *1*(2), 71-89. http://www.apcj.org/documents/1_2_victimization.pdf

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims. *Cyberpsychology, Behavior, and Social Networking*, *17*(2), 61–67. https://doi.org/10.1089/cyber.2012.0231

Duell, N., & Steinberg, L. (2018). Positive Risk Taking in Adolescence. *Child Development Perspectives*, *13*(1), 48–52. https://doi.org/10.1111/cdep.12310

Duell, N., & Steinberg, L. (2021). Adolescents take positive risks, too. *Developmental Review*, *62*, 100984. https://doi.org/10.1016/j.dr.2021.100984

Edmondson, D., Chaudoir, S. R., Mills, M. A., Park, C. L., Holub, J., & Bartkowiak, J. M. (2011). From Shattered Assumptions to Weakened Worldviews: Trauma Symptoms Signal Anxiety Buffer Disruption. *Journal of Loss and Trauma*, *16*(4), 358–385. https://doi.org/10.1080/15325024.2011.572030

European Union Agency for Law Enforcement Cooperation (2019). *in Brief 2018*. https://www.europol.europa.eu/publications-events/main-reports/europol-in-brief-2018

Figley, C. R. (1986). *Trauma and Its Wake, Volume II* (1st ed.). Brunner/Mazel.

Filipas, H. H., & Ullman, S. E. (2006). Child Sexual Abuse, Coping Responses, Self-Blame, Posttraumatic Stress Disorder, and Adult Sexual Revictimization. *Journal of Interpersonal Violence*, *21*(5), 652–672. https://doi.org/10.1177/0886260506286879

Freeman, K., & Smith, N. (2014). Understanding the relationship between crime victimisation and mental health: a longitudinal analysis of population data. *Crime and Justice Bulletin*, (177), 1–16. https://search.informit.org/doi/10.3316/agispt.20152782

Furnell, S. M. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, *1*(2), 35–44. https://www.jstor.org/stable/26486092

Gupta, P., & Mata-Toledo, R. A. (2016). CYBERCRIME: IN DISGUISE CRIMES. *Journal of Information Systems & Operations Management*, *10*(1). https://link.gale.com/apps/doc/A483829333/AONE?u=anon~170b596c&sid=googleScholar&xid=b3249339

Haron, H., & Yusof, F. B. M. (2010). Cyber stalking: The social impact of social networking technology. *2010 International Conference on Education and Management Technology*. https://doi.org/10.1109/icemt.2010.5657665

Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, *2014*(2), 5–8. https://doi.org/10.1016/s1361-3723(14)70461-0

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149–164). Syngress. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Jansen, J., & Leukfeldt, R. (2018). Coping with Cybercrime Victimization: An Exploratory Study into the Impact and Change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228. https://doi.org/10.21428/88de04a1.976bcaf6

Jaquet-Chiffelle, D.O., Loi, M. (2020) Ethical and Unethical Hacking. In: Christen, M., Gordijn, B., Loi, M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, (21), Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9

Johnson, J. (2022). *Internet usage worldwide - statistics & facts*. Statista. https://www.statista.com/topics/1145/internet-usage-worldwide/#dossierKeyfigures

Johnson, M. C., & Kercher, G. A. (2008). Identifying Predictors of Negative Psychological Reactions to Stalking Victimization. *Journal of Interpersonal Violence*, *24*(5), 866–882. https://doi.org/10.1177/0886260508317195

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426. https://doi.org/10.1016/j.techfore.2020.120426

Kerr, J., Owen, R., Nicholls, C. M., & Button, M. (2013). *Research on sentencing online fraud offences*. London: Sentencing Council.

Koops, B. J. (2010). The Internet and its Opportunities for Cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1738223

Lazzari, C., Shoka, A., Nusair, A., & Rabottini, M. (2020). PSYCHIATRY IN TIME OF COVID-19 PANDEMIC. *Psychiatria Danubina*, *32*(2), 229–235. https://doi.org/10.24869/psyd.2020.229

Leukfeldt, R. (2017). *Research Agenda The Human Factor in Cybercrime and Cybersecurity*. Eleven International Publishing.

Leukfeldt, E. R., Notté, R., J., Malsch, M. (2018). Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachofferschap van cybercrime en gedigitaliseerde criminaliteit [Victims of online crime: A study on the needs, consequences and responsibilities following the victimization of cybercrime and digitized crime]. Retrieved from http://hdl.handle.net/20.500.12832/2355

Mahdi Addai, S., Imad Kadhim, H., & Saleh Mahdi, G. (2022). A Pragmatic Approach of Blackmail in Online Messages. *Texas Journal of Multidisciplinary Studies, 7,* 304-309. https://zienjournals.com/index.php/tjm/article/view/1394

McAfee (2018). *Economic Impact of Cybercrime Report.* https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, *13*(5), 99–103. https://doi.org/10.1109/msp.2015.107

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(4). https://doi.org/10.1007/s11920-021-01228-w

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, *27*(3), 272–294. https://doi.org/10.1177/02697580211010692

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An Exploration of the Psychological Impact of Hacking Victimization. *SAGE Open*, *11*(4), 215824402110615. https://doi.org/10.1177/21582440211061556

Peterson, C., & Seligman, M. E. P. (1983). Learned Helplessness and Victimization. *Journal of Social Issues*, *39*(2), 103–116. https://doi.org/10.1111/j.1540-4560.1983.tb00143.x

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, *7*(1), 1-15. https://doi.org/10.1186/s40163-018-0079-3

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/tdsc.2015.2410795

Schenk, A. M., & Fremouw, W. J. (2012). Prevalence, Psychological Impact, and Coping of Cyberbully Victims Among College Students. *Journal of School Violence*, *11*(1), 21–37. https://doi.org/10.1080/15388220.2011.630310

Short, E., Linford, S., Wheatcroft, J. M., & Maple, C. (2014). The impact of cyberstalking: the lived experience - a thematic analysis. *Studies in health technology and informatics*, *199*, 133–137. https://doi.org/10.3233/978-1-61499-401-5-133

Statista (2021). *Cybercrime as share of total crime Singapore 2014–2020*. https://www.statista.com/statistics/1267252/singapore-cybercrime-as-share-of-total-crime/

Statista (2021). *Number of hacking offenses in the Netherlands 2012–2019*. https://www.statista.com/statistics/593923/number-of-hacking-offenses-in-the-netherlands/

Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376. https://doi.org/10.1089/cyber.2020.0253

Tennant, J. E., Demaray, M. K., Coyle, S., & Malecki, C. K. (2015). The dangers of the web: Cybervictimization, depression, and social support in college students. *Computers in Human Behavior*, *50*, 348–357. https://doi.org/10.1016/j.chb.2015.04.014

Van de Weijer, S., Leukfeldt, R., & van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/pijpsm-07-2019-0122

Van der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, *17*, 480 - 497. https://doi.org/10.1177/1477370818812016

Vos, M. S., & de Haes, J. C. J. M. (2006). Denial in cancer patients, an explorative review. *Psycho-Oncology*, *16*(1), 12–25. https://doi.org/10.1002/pon.1051

Voth, J., & Sirois, F. M. (2009). The role of self-blame and responsibility in adjustment to inflammatory bowel disease. *Rehabilitation Psychology*, *54*(1), 99–108. https://doi.org/10.1037/a0014739

Wagen, W. V. D. (2017). The Cyborgian Deviant: An Assessment of the Hacker Through the Lens of Actor-Network Theory. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 157–178. https://doi.org/10.21428/88de04a1.6a5d95c2

Wake, S., Wormwood, J., & Satpute, A. B. (2020). The influence of fear on risk taking: a meta-analysis. *Cognition and Emotion*, *34*(6), 1143–1159. https://doi.org/10.1080/02699931.2020.1731428

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194. https://doi.org/10.1177/1748895815603773

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). Various Types of Cybercrime and Its Affected Area. In *Emerging Technologies in Data Mining and Information Security* (pp. 305-315). Springer, Singapore.

Zandt, F. (2022) *The Biggest Business Risks in 2022*. Statista Infographics. https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/

Appendix A
Informed Consent

Dear participants,

thank you very much for taking part in this study about mental wellbeing and cybercrime. Please carefully read the following information.

With your help, I want to assess the impact of different types of cybercrime on the psychological wellbeing of the victim. Cybercrime is defined as “any criminal activity in which a computer (or networked device) is targeted or used” (Burton et al., 2022).

The study will take approximately 15 min. You will be asked some questions about your perspective on cybercrime, you will read 3 different scenarios and 12 short additions in which you should imagine being the victim and answer some questions about it.

Participating in this study is entirely voluntary. You can withdraw from it at any time, without any negative consequences for you.

There are no risks associated with this research study. It is ensured that your data will be treated anonymously and is only available to the researcher and the supervisor. After the study is finished, the data will be deleted. If you have any questions or concerns about this study, feel free to contact me, the researcher, or the supervisor.

Kind regards,
Louisa von der Ahe

Researcher: Louisa von der Ahe, [l.vonderahe@student.utwente.nl]
Supervisor: Iris van Sintemaartensdijk, [i.vansintemaartensdijk@utwente.nl]

By giving consent, you confirm that you understood everything and you agree to take part in this study.

Appendix B

Questionnaires

Demographic Items

What is your nationality?

1. Dutch
2. German
3. Other, namely…

What is your age?

(Respondents could insert a number)

What gender do you identify with?

1. Male
2. Female
3. Non-binary/Third gender
4. Prefer not to say

What is the highest degree or level of education you have **completed**?

1. No diploma
2. Primary school
3. Secondary school
4. Bachelor or higher non-university degree
5. Master/(Post)graduate degree

What best describes your current occupation?

1. Employed/Self-employed
2. Unemployed
3. Volunteer
4. Incapacitated
5. Student
6. Homemaker
7. Pensioner/Retired
8. None of the above
9. I prefer not to say

How many hours do you spend online daily?

1. 0-1h
2. 1-2h
3. 2-3h
4. 3-4h
5. 5-6h
6. 7 or more hours

Perceived Severity

**Assessed on a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree)*

In the following statements, please indicate how you perceive the severity of cybercrime.

1. I believe that cybercrime is significant.
2. I believe that cybercrime is serious.
3. I believe that cybercrime is severe.

Perceived Knowledge

** Assessed on a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree)*

In the following two questions, please indicate how informed you feel about cybercrime.

1. I feel adequately informed about the risks of the internet.
2. I feel adequately informed about how to avoid the risks of the internet.

Risk-Taking Behaviour (DOSPERT-Scale)

** Assessed on a 7-point Likert scale (1 = Extremely Unlikely; 7 = Extremely Likely)*

For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation.

1. Admitting that your tastes are different from those of a friend.
2. Going camping in the wilderness.
3. Betting a day's income at a casino.
4. Investing 10% of your annual income in a moderate growth mutual fund.
5. Drinking heavily at a social function.
6. Taking some questionable deductions on your income tax return.
7. Disagreeing with an authority figure on a major issue.
8. Betting a day's income at a high-stake poker game.
9. Having an affair with a married man/woman.

10. 10. Passing off somebody else's work as your own.
11. Going down a ski run that is beyond your ability.
12. Investing 5% of your annual income in a very speculative stock.
13. Going white-water rafting at high water in the spring.
14. Betting a day's income on the outcome of a sporting event.
15. Engaging in unprotected sex.
16. Revealing a friend's secret to someone else.
17. Driving a car wearing a seat belt.
18. Investing 10% of your annual income in a new business venture.
19. Taking a skydiving class.
20. Riding a motorcycle without a helmet.
21. Choosing a career that you truly enjoy over a more secure one.
22. Speaking your mind about an unpopular issue in a meeting at work.
23. Sunbathing without sunscreen.
24. Bungee jumping off a tall bridge.
25. Piloting a small plane.
26. Walking home alone at night in an unsafe area of town.
27. Moving to a city far away from your extended family.
28. Starting a new career in your mid-thirties.
29. Leaving your young children alone at home while running an errand.
30. Returning a wallet you found that contains $200.

Internet Trust

* *Assessed on a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree)*

In the following questions, please indicate how trustful you are.

1. I have every confidence that the internet is safe.
2. I am optimistic about the safety of the internet.

Interpersonal Trust

* *Assessed on a 5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree)*

In the following questions, please indicate how trustful you are.

1. I find it easy to trust others.
2. I generally assume that people act morally.

Sense of Security

* *Assessed on a 5-point Likert scale (1 = Not at All Concerned; 5 = Very Concerned)*

After reading the scenario about hacking and the additions, please indicate how concerned you are now about **security on the Internet**? (e.g people reading your email, finding out what websites you visit, etc.) Keep in mind that "security" can mean privacy, confidentiality, and/or proof of identity for you or for someone else.

* *Assessed on a 5-point Likert scale (1 = Not at All Concerned; 5 = Very Concerned)*

Psychological Impact

* *Assessed on a 5-point Likert scale (1 = None at All; 5 = A Great Deal)*

How much more … would you likely be compared to before the event?

- …anxious…
- …ashamed/embarrassed…
- …fearful…
- …angry…
- …unconfident…

Coping Strategies (Adapted Version of the Brief-COPE)

* *Assessed on a 4-point Likert scale (1 = I haven't been doing this at all; 4 = A Great Deal)*

Finally, I want to know more about the way you cope with stressful events in general. The following questions ask how you have sought to cope with a hardship in your life. Read the statements and indicate how much you have been using each coping style.

1. I've been turning to work or other activities to take my mind off things.
2. I've been concentrating my efforts on doing something about the situation I'm in.
3. I've been saying to myself "this isn't real."
4. I've been getting emotional support from others.
5. I've been giving up trying to deal with it.
6. I've been taking action to try to make the situation better.
7. I've been refusing to believe that it has happened.
8. I've been criticizing myself.
9. I've been getting comfort and understanding from someone.
10. I've been giving up the attempt to cope.

11. I've been doing something to think about it less, such as going to movies, watching TV, reading, daydreaming, sleeping, or shopping.
12. I've been accepting the reality of the fact that it has happened.
13. I've been learning to live with it.
14. I've been blaming myself for things that happened.

Appendix C

Debriefing

Thank you for taking part in this survey!

The purpose of the study was to analyze the psychological impact of the three different types of cybercrime (hacking, person-centered, and financial cybercrime), together with people's risk-taking behaviour, coping skills and perceived severity of cybercrime.
Also, I tried to measure what impact familiarity with the offender, as well as the intensity of contact have on the victim's wellbeing.

If you have any questions or concerns about this study, please contact the researcher

Louisa von der Ahe: l.vonderahe@student.utwente.nl

Appendix D

Scenarios And Additions

Hacking

Imagine, that you are working in a big company, and you are close friends with some of your colleagues. One day, when you try to login into your Facebook account, your password does not work. You try it several times, but you do not succeed. When you tell your colleagues about it, some of them mention that they have received suspicious messages from your account, in which they were asked for personal but also work-related information e.g., that they should tell you about the password for one of the companies' accounts, and some also received a link in which they should enter their credit card details.

Addition Intensive Contact

Before you notice that your account got hacked, you were chatting with someone on social media who seemed to be interested in the company you are working for, and was asking you some questions about it, such as how the atmosphere is in the company and with what kind of programs and systems you are working. Later, you find out that this person was the offender.

Addition No Contact

You did not have any further contact to the person who hacked into your account.

Addition Being Familiar

Later, you find out that the offender was someone you were working with in your previous job at another company, which is competing with the one you are working for right now.

Addition Not Being Familiar

Later, you find out the offender's identity, but you do not know this person.

Person-Centered Cybercrime

Imagine, that someone sends you a message on a social media platform saying that they have hacked into your webcam and now have images of you, e.g., from situations where you did not close your laptop and got undressed. They threaten you and say that unless you pay them 1000€, they will send them to all your social media contacts.

Addition Intensive Contact

You are sceptical if this is true and they indeed have these pictures, therefore you chat with the offender and say that you do not believe them. Also, because you do not have the money right now you also try to gain some time by chatting with them. You ask for proof,

and indeed they send you a picture where you took off your clothes. But because you did not send the money on time, they send the pictures they have of you to all your contacts.

Addition No Contact

You did not have any further contact with the offender, you directly send them the money.

Addition Being Familiar

Later, you find out that the offender was someone you were friends with in high school, but you stopped being friends after graduation.

Addition Not Being Familiar

Later, you find out the offender's identity, but you do not know this person.

Financial Cybercrime

Imagine, that you receive an email from Netflix, stating that you need to pay your annual subscription. You thought that your friend with whom you are sharing the account already paid this, but they are on vacation right now, and you don't want to bother them. So, you click on the link in the email and pay through online banking, meaning that you enter your credit card details. A few days later, you talk to your friend again, and they say that they indeed already paid this annual fee. You think it might be a mistake from Netflix, so you check the email address again, and you see that it contains one letter more than the 'real' Netflix email address, so it cannot be from Netflix.

Addition Intensive Contact

Before you transferred the money, you reply to the email because you are not sure if your friend already paid the subscription. You say that you probably already paid, but they respond that they did not receive any payment for your subscription.

Addition No Contact

You did not have any further contact with the offender, you transferred the money after you read the email.

Addition Being Familiar

Later, you find out that the offender was someone you know from a party where you talked about watching Netflix, and you mentioned that you are sharing your account with someone.

Addition Not Being Familiar

Later, you find out the offender's identity, but you do not know this person.