Mental well-being of Generation Z as potential victims of cybercrime:

The effect of risk perception and self-efficacy on mental well-being

Julia Mekler, s2261758

Department of Psychology, University of Twente

Bachelor Thesis – Positive Clinical Psychology and Technology

Faculty of Behavioral, Management and Social Sciences

Dr. Iris van Sintemaartensdijk

Kars Otten

June 26, 2022

Abstract

The development of technology leads to many advantages, such as being more flexible and having permanent access to information. However, it also brings many risks with it, as the screen time of many individuals rises dramatically while a lot of them still do not feel confident about using the internet. Especially there, individuals should be cautious in order to prevent cybercrimes, which are crimes on the internet aiming to steal data or gain access to private information. Generation Z, born between 1996 and 2009, is marked by the rise of technology, as they are referred to as high adopters of technology. Compared to other generations, they show the highest diagnosed mental illnesses which raises concerns about being more vulnerable to cybercrime. Therefore, this study focuses on how risk perception and self-efficacy toward becoming victimized by cybercrime affect the mental well-being of Generation Z. Risk perception and self-efficacy were measured within an online study that consisted of 175 valid participants. The results indicate that there is no relationship between risk perception/self-efficacy and mental well-being. However, gender correlates significantly with mental well-being which means that men show higher mental well-being compared to women. Additionally, problematic internet use also shows a significant association with mental well-being.

Keywords: Generation Z, mental well-being, cybercrime, risk perception, self-efficacy, technology

Mental well-being of Generation Z as potential victims of cybercrime:

The effect of risk perception and self-efficacy on mental well-being

The rapid development of technology leads to enormous changes in society which lead to advantages on one side, however, they also bring risks with it. According to Hertlein and Ancheta (2014), technology hinders relationships between people, as it creates barriers because of misinterpretations and individuals are confronted with feelings of jealousy and exclusion. Social media and digital devices are integrated into individuals' lives, as the screen time of users rises rapidly (Jensen et al., 2019). On the other side, users connect with friends and families, they keep themselves updated and are highly satisfied, as the internet allows quick exchange of information (Hertlein & Ancheta, 2014). Generally, technology creates an atmosphere of safety and privacy because of its anonymity where relationships can be kept alive (Palme & Berglund, 2002). However, many individuals are not aware of the downsides. Specific individual characteristics and the created atmosphere of safety and privacy make it easier for criminals to attack their victims online. The term cybercrime refers to crimes and offenses on the internet, ranging from data theft and stalking to financial fraud affecting many users (Arora, 2016). Even larger companies, such as Microsoft, Yahoo, or eBay were exploited by hackers (Rehman et al., 2018). For example, in 2017, there was a worldwide attack on Microsoft where the data of about 200.000 servers was encrypted (Rehman et al., 2018). Moreover, among all European internet users, almost 42% report that they have been confronted with different types of cybercrime in 2017 (De Kimpe et al., 2021). Since then, the number of cases has risen and offenders have found many ways to exploit their victims further.

Safety measures and rising use of technology

It is vital to address safety measures in order to prevent cybercrime attacks. Without individuals being aware of cybersecurity measures, criminals can have access to personal information, which they use to commit theft or even buy items, such as insurance (Arora, 2016). For example, in 2018, about two billion individuals' data have been stolen on the internet (Monteith et al., 2021). In order to protect oneself, it is already helping to block intrusive accounts or have strong passwords (Kennison & Chan-Tin, 2020). Many individuals indicate a lack of confidence regarding their knowledge of protective measures, which explains why many users fail to engage in safety measures in the online environment (LaRose et al., 2008). As a consequence, many users experience cyber-attacks in which they are exploited or hacked (De Kimpe et al., 2021).

Moreover, there are various reasons why individuals use the internet more often nowadays. Especially circumstances such as the pandemic lead to a dramatic rise in users' daily activity on the internet since many people work or study from home (Monteith et al., 2021). The increasing use of technology leads to a rising number of cybercrimes, which in turn impacts individuals' mental well-being (Monteith et al., 2021). Individuals who spend more than ten hours a day on the internet have an increased likelihood of being unhappy, up to even 56% (Owen et al., 2018). Furthermore, in 2020, cybercrime showed an estimated increase of 10% in each group of age (Sladek & Grabinger, 2014). Those results confirm that all individuals, no matter the age, are affected by the consequences of the accelerating development of technology.

Digital Natives: Generation Z

Especially Generation Z is marked by technology and its development, which is the reason why this research has its focus on those individuals born between 1996 and 2009. They are unlike

any other generation because these individuals grew up wholly in the digital era, they developed new values and dived into a life of fully modern expectations (Sladek & Grabinger, 2014). It should be mentioned that the letter Z is the last one in the alphabet, which stresses the ending of traditions and expectations that have been lived by the previous generations, as explained by Sladek and Grabinger (2014). Generation Z is marked by diversity and equity where all common roles and experiences are broken down into new ideas and lifestyles since they are encouraged by their parents and relatives to discover their individualism to develop unique skills and values (Sladek & Grabinger, 2014).

With the growing sense of equality and the rise of new and different talents, Generation Z is accompanied by the development of technology their entire life. While Generation Z is more highly educated, open-minded and showing greater economic well-being, they also tend to be less autonomous due to growing up in an overprotective parenting household, which interferes with their evolvement of emotional and social skills (Schroth, 2019). Moreover, they are also more likely to develop depression and anxiety compared to other generations. In the meantime, they have never missed the introduction and ongoing change of smartphones and social media for which reason Generation Z is referred to as a high adopter of technology (Debb et al., 2020). Combining the facts that Generation Z has grown up in a culture of safety while technology made great development, there are comprehendible concerns about their cybersecurity awareness.

According to Debb et al. (2020), there are notable results indicating that Generation Z engages less in online security behaviors compared to Millennials, born between 1980 and 1999. Furthermore, Generation Z shows the highest percentage of diagnosed mental illnesses compared to other generations, which is in accordance with Monteith et al. (2021), who assume that individuals who are mentally ill are also more vulnerable to cybercrime. These results raise interest

in why Generation Z engages in unprotective behaviors and to what extent those factors affect their mental well-being in potential cybercrime.

Protection Motivation Theory

In order to study why individuals engage in unprotective behaviors, the Protection Motivation Theory (PMT), developed by R. W. Rogers in 1975, is used. It explains the underlying cognitive processes of individuals engaging in unhealthy and unsafe behaviors (see Appendix A). The PMT is based on two factors, which are namely threat appraisal and coping appraisal (De Kimpe et al., 2021). These two cognitive processes affect individuals' protection motivation. Threat appraisal is an individual's risk perception which assesses the severity of a threat and one's vulnerability within a risky situation. Its goal is to decrease the risk of developing health problems by acknowledging issues beforehand (De Kimpe et al., 2021). When individuals are affected by the negative implications of cybercrime, they tend to increase their own motivation to engage in safety measures that prevent them from experiencing more harm.

The coping appraisal is about one's self-efficacy, which is an individual's belief that they can perform a certain task in order to reduce risks (De Kimpe et al., 2021). The aim of the coping appraisal is to prevent individuals from damage to their health by engaging in protective behaviors. As De Kimpe et al. (2021) explain, individuals take action through observational learning, their own personality characteristics, or prior incidents. Moreover, the PMT helps to understand individuals cognitive processes when they experience cybercrime and how they cope with the threats, as a higher self-efficacy indicates being more secure which facilitates safety behaviors to prevent cyber-attacks (De Kimpe et al., 2021).

Effect of risk perception and self-efficacy on mental well-being

As the PMT indicates, risk perception and self-efficacy are predictors affecting the mental well-being of individuals when it comes to potential threats. With regard to risk perception, Rogers et al. (2007) state that individuals evaluate a potential risk based on their emotions. This explains why individuals perceive the risk as low when it comes to a preferable activity, such as spending time on social media, because they assess their benefits as high. In short, negative emotions lead to higher risk perception and positive emotions cause lower risk perception (Rogers et al., 2007). Particularly Generation Z associates the internet with positive emotions as they are not only marked by technology but also contribute to its development (Sladek & Grabinger, 2014).

Additionally, individuals' risk perception is an important factor, as especially uncertainty and fear interfere with their mental health (Rogers et al., 2007). In line with this, De Kimpe et al. (2021) explain that the perceived knowledge of a risk and one's perceived effectiveness of safety measures decrease fear arousals in individuals since they have lower feelings of uncertainty.

Self-efficacy helps individuals to consider their broad skills and abilities in order to act confident when they are confronted with threats and reduce them. Lower self-efficacy leads to users being less careful, which is the reason why they are more at risk of being exposed to cybercrime (Cheng et al., 2020). As aforementioned, cybercrime leads to financial loss and physical danger, however, individuals are also affected mentally. Someone who already experienced cybercrime tends to have less trust in the internet after that (Cheng et al., 2020). Furthermore, individuals experience less perceived control and higher unfairness leading to feelings of helplessness (Cheng et al., 2020). All in all, low self-efficacy and the experience of

cybercrime explain why victims show a decreased well-being, as these factors often lead to fear of being victimized by cybercrime again.

As digital natives, Generation Z is born into the world of technology, the internet and social media. They are more often exposed to technology than any other generation which is the reason why especially Generation Z's mental well-being is of importance as they are also already vulnerable to anxiety and depression. According to the PMT, risk perception and self-efficacy are both crucial variables contributing to one's mental well-being. Generally, threats and risks, such as cybercrime should be reduced in order to not suffer mentally. Therefore, it is important to explore how far Generation Z's risk perception and self-efficacy affect them mentally in potentially experiencing cybercrime.

The present research

This study is going to focus on the research question "How can risk perception and self-efficacy toward becoming victimized by cybercrime affect the mental well-being of Generation Z?". This research question is divided into two sub-questions.

The first sub-question is "To what extent does risk perception toward becoming victimized by cybercrime affect the mental well-being of Generation Z?" and the hypothesis the higher the risk perception toward becoming victimized by cybercrime, the higher the mental well-being of Generation Z.

The second sub-question is "To what extent does self-efficacy toward becoming victimized by cybercrime affect the mental well-being of Generation Z?" and the hypothesis the higher the

self-efficacy toward becoming victimized by cybercrime, the higher the mental well-being of Generation Z.

Exploration

Four potential moderator variables are introduced, as it is expected that they have an effect on the relationship between independent variables and dependent variable: gender, problematic internet use, actual security behavior and risk-taking.

Gender is assumed to have an effect because the study of Oksanen and Keipi (2013) show that there is a significant association between gender and cybercrime victimization, as females indicate better offline social networks compared to men. The variables problematic internet use and actual security behavior are chosen since both predict risky online behaviors which could lead to being victimized by cybercrime (Hadlington, 2017). Further, risk-taking is a variable predicting individuals to be more vulnerable to be victimized by cybercrime (Van de Weijer & Leukfeldt, 2017).

Method

Design

The research consisted of a correlational design with two independent variables, which were namely risk perception and self-efficacy. It was measured to what extent those two variables correlated with the dependent variable of this study, the mental well-being of Generation Z. Additionally, potential moderation variables were included in order to test whether they affected the relationship between the independent variables and the dependent variable: gender, problematic internet use, actual security behavior and risk-taking.

Participants

In this study, 197 respondents were mainly recruited through SONA, an online platform for BMS students at the University of Twente. Next to that, social network sites were also used, like WhatsApp and Instagram where individuals received an anonymous online survey link. 22 participants were taken out after checking for the inclusion criteria, which were adults born between 1996 and 2006 who were at least 16 years old. Four participants were taken out because they did not fit into the ages of Generation Z, however, one participant also did not agree with the informed consent and there were 17 participants who agreed to the informed consent but did not indicate an answer for the whole survey, as they probably closed their screen after agreeing to the informed consent. Finally, the data set of 175 participants who gave informed consent was analyzed. The sample consisted of 55 males, 119 females and one non-binary person. Furthermore, the participants were between the ages of 16 and 26 years (M = 20.64, SD = 1.87). Concerning their nationalities, the sample consisted of 107 Germans, 36 Dutch participants and the remaining 32 respondents consisted of other nationalities. Out of the sample, one participant indicated they use the internet < 1 hour a day, 17 respondents 1-2 hours and 63 participants 2-4 hours. The majority of the respondents (N = 71) indicated they use the internet 4-6 hours a day. Additionally, eleven participants use the internet for 6-7 hours and twelve respondents > 7 hours a day. Furthermore, 43 participants experienced cybercrime, such as account hacking or credit card fraud.

Materials

Daily internet use

The *daily internet use* of the respondents was indicated within the question "How many hours per day do you spend on the internet (e.g., Email, Facebook, Instagram, WhatsApp, etc.)?"

(see Appendix D). Possible answer options were < 1 hour, 1 - 2 hours, 2 - 4 hours, 4 - 6 hours, 6 - 7 hours or > 7 hours.

Experience of cybercrime

Furthermore, the *experience of cybercrime* was asked: "Have you ever been a victim of cybercrime (e.g., Phishing, Identity theft, Account Hacking, Credit Card Fraud, etc.)?", as can be seen in Appendix E. Participants were able to click on no or confirm that they experienced cybercrime once and give an example of that.

Scale of Problematic Internet Use

Additionally, *problematic internet use* was measured with the Scale of Problematic Internet Use (SPIU) to track dubious cyberspace use of the respondents (see Appendix F). It consisted of eight items on a 5-point Likert scale ranging from 1 = 'Strongly disagree' to 5 = 'Strongly agree' and an example item is "I have stopped doing important things to stay connected". According to da Fonsêca et al. (2018), the SPIU was found to have good reliability and validity in university students as it can be used to estimate the problematic online behavior of participants. The Cronbach's alpha of this study was 0.74.

Scale of Security Behavior Self-Efficacy

The independent variable *self-efficacy* was measured with four items of the Scale of Security Behavior Self-Efficacy and additional two items constructed by Tsai et al. (2016). The scale aims to assess to what extent the participants believed they were able to engage in online safety measures. Altogether, the scale consisted of six items on a 5-point Likert scale ranging from 1 = 'Strongly disagree' to 5 = 'Strongly disagree', as can be seen in Appendix G. An example item

is "I feel comfortable taking measures to secure my primary home computer". According to Tsai et al. (2016), the scale has evidence of good reliability, as Cronbach's alpha lies at 0.82. However, in this study, the scale had a Cronbach's alpha of 0.54.

Online Security Behaviors and Beliefs Questionnaire

A possible moderator variable, which was the respondent's *actual security behavior* was measured using a sub-scale of the Online Security Behaviors and Beliefs Questionnaire (OSBBQ) consisting of 75 items and intending to assess an individual's cyber security behavior (Debb et al., 2020). The nine items of the sub-scale are named Cyber Security Behavior Items, measured on a 5-point Likert scale ranging from 1 = 'Strongly disagree' to 5 = 'Strongly agree' (see Appendix H). As an illustration, one item was labeled "I use different passwords for my different social media accounts (e.g., Facebook, Twitter, LinkedIn).". As stated by Schaffer & Debb (2019), the OSBBQ indicates good validity and strong internal consistency ($\alpha = 0.93$). In this sample, Cronbach's alpha lies at 0.67.

Risk Perception

Moreover, the second independent variable, *risk perception,* was measured by three items adapted from Liang and Xue (2010), as they changed the term ‘spyware’ into ‘malware’ (Tsai et al., 2016). The purpose of this scale was to indicate an individual's risk perception on the internet. As can be seen in Appendix I, an example item for this is "My chances of getting malware are great" and it was measured on a 5-point Likert scale ranging from 1 = 'Strongly disagree' to 5 = 'Strongly agree' indicating good reliability (Tsai et al., 2016). The Cronbach's alpha is nearly excellent with a value of 0.88 in this research.

Domain-Specific Risk-Taking Scale

Another potential moderator, called *risk-taking*, was measured. Thus, the Domain-Specific Risk-Taking (DOSPERT) Scale was used (see Appendix J). The DOSPERT evaluated widespread risks from five domains, such as ethical, financial, health, social, or recreational risks, and the likelihood to what extent an individual would engage in unsafe behaviors (Blais & Weber, 2006). It consisted of 30 items, measured on a 7-point Likert scale ranging from 1 = 'Extremely unlikely' to 7 = 'Extremely likely'. For instance, an item is "engaging in unprotected sex" referring to the health domain (Blais & Weber, 2006). The DOSPERT indicates good reliability in this study (α = 0.87).

Mental Health Continuum Short Form

The dependent variable of *mental well-being* was measured using the Mental Health Continuum Short Form (MHC-SF). The participants indicated how often during the past month they were in a certain mood in order to assess their general mental well-being (Petrillo et al., 2015). The MHC-SF consisted of 14 items measured on a 6-point Likert scale ranging from 1 = 'Never' to 6 = 'Every day' (see Appendix K). As an example, one item is "During the past month, how often did you feel interested in life?" and the scale indicates high internal reliability within this sample (α = 0.89).

Procedure

The online study was conducted with the online survey tool Qualtrics. The anonymous link was distributed via SONA, WhatsApp and Instagram. It was approved by the Ethics Committee of the Faculty of Behavioral, Management and Social Sciences (BMS) at the University of Twente

with application number 220210. First, participants agreed to the informed consent (see Appendix B) in order to continue with the questions. They also read general information about the study, such as what cybercrime is and that the study only focuses on the individuals of Generation Z. Thereafter, participants were asked about their demographics, like gender, age, nationality and highest education level (see Appendix C). Next, their daily internet use in hours and whether they ever experienced cybercrime was asked. If participants ever experienced cybercrime, there was an option for them to describe a specific situation in an open text field. After that, individuals received the SPIU in order to measure their internet use. Thereafter, items appeared concerning their self-efficacy which is one of the independent variables. Participants reflected on how they dealt with online threats and indicated to what extent the items applied to them. This was followed by the Cyber Security Behavior Items of the OSBBQ where respondents were asked to think about their actual security behavior. The upcoming items were gained from the Threat Susceptibility Scale in order to measure the independent variable, risk perception. After that, the DOPSERT Scale asked respondents to indicate the likelihood that they would engage in the described activity or behavior if they would find themself in that situation. Afterward, the last survey appeared, which was the MHC-SF in order to measure the dependent variable, the mental well-being of Generation Z. When the respondents finished the last survey, a final screen appeared which gave the participants insights into the aim of the research (see Appendix L). Moreover, in case they were interested in the results of the study, they had the possibility to send the researcher an email in order to be updated about the outcome in the future. Generally, the survey took the participants about 20 minutes. The data collection started on the 18th of March and ended on the 14th of April, which were 28 days in total.

Data Analysis

The final data set consisted of 175 participants after all outliers and errors were excluded. It was analyzed with IBM SPSS Statistics 25. For the purpose of gaining a general impression and a summary of the data, descriptive statistics and Pearson correlations were conducted on the variables gender, age, nationality, education, risk perception, self-efficacy, daily internet use in hours, the experience of cybercrime, problematic internet use, actual security behavior, risk-taking and mental well-being.

In order to answer the research question "How can risk perception and self-efficacy toward becoming victimized by cybercrime affect the mental well-being of Generation Z?" regression analyses were conducted. First, two separate regression analyses were conducted with only risk perception and mental well-being and then self-efficacy and mental well-being in order to explore the main effect of the independent variables on the dependent variable. After that, one regression analysis was conducted with both independent variables and the dependent variable to compare the results. This was followed by a multiple regression analysis to explore if the other variables affected the dependent variable. Further, it was tested for moderation effects of gender, problematic internet use, actual security behavior and risk-taking.

Results

Descriptive statistics and Pearson correlation

In order to gain a general impression of the participant's data (N = 175), a descriptive analysis was conducted with all variables to evaluate their means and standard deviations (see Table 1). Next to that, a Pearson Correlation is conducted to test how the items correlate. This is

helpful in assessing the relationship between two variables and making predictions about future behavior. All correlations can be seen in Table 1.

Table 1

Descriptives and Pearson correlation of all predictors for mental well-being of Generation Z

	M	SD	1	2	3	4	5	6	7	8	9	10	11	12
1.Gender**	1.70	0.48		-.31	-.10	-.08	-.03	.06	.16	.00	-.03	.18	-.38*	-.26
2.Age	20.64	1.87	-.31		.11	.23	-.06	.07	-.15	-.16	-.07	.07	.12	.17
3.Nationality***	1.99	0.63	-.10	.12		.17	.03	.13	.20	-.01	-.01	.03	.07	-.08
4.Education****	1.43	1.00	-.08	.30	.17		.06	.16	-.03	-.02	-.08	.07	.05	-.03
5.Daily internet use	3.63	1.00	-.03	-.06	.03	.06		.03	.23	.14	.02	-.04	.02	-.06
6.Experience of cybercrime*****	1.25	0.43	.06	.07	.13	.16	.03		.00	-.07	-.06	.11	.07	-.04
7.Problematic internet use	3.33	0.63	.16	-.15	.20	-.03	.23	.00		.04	-.11	.14	-.01	-.33*
8.Self-efficacy	3.26	0.55	.00	-.16	-.01	-.02	.14	-.07	.04		.53*	-.36*	-.03	.01
9.Actual security behavior	3.54	0.57	-.03	-.07	-.01	-.08	.02	-.06	-.11	.53*		-.37*	-.07	.10
10.Risk perception	2.76	0.85	.17	.07	.03	.07	-.04	.11	.14	-.36*	-.37*		.04	-.04
11.Risk-taking	3.43	0.76	-.38*	.12	.07	.05	.02	.07	-.01	-.03	-.07	.04		.12
12.Mental well-being	3.99	0.78	-.26	.17	-.08	-.03	-.06	-.04	-.33*	.01	.10	-.04	.12	

Note. ** Gender is coded as 1 = Male, 2 = Female, 3 = Non-binary, 4 = Prefer not to say

Note. *** Nationality is coded as 1 = Dutch, 2 = German, 3 = Other

Note. **** Education is coded as 1 = Secondary School Diploma, 2 = Bachelor's Degree, 3 = Master's Degree, 4 = PhD, 5 = Other

Note. ***** Experience of cybercrime is coded as 1 = No, 2 = Yes

Inferential statistics

Risk perception and mental well-being

The first regression analysis is conducted with mental well-being as a dependent variable and risk perception as an independent variable in order to test the first hypothesis and analyze whether risk perception toward becoming victimized by cybercrime has an effect on the mental well-being of Generation Z without any other variables. The analysis indicates that risk perception is not significantly correlated with the dependent variable (B = -.04, t (-.57), p = .57, SE = .07). Concluding, this means, that the first hypothesis, the higher the risk perception toward becoming victimized by cybercrime, the higher the mental well-being of Generation Z, can be rejected, as there is no significant correlation.

Self-efficacy and mental well-being

Next to that, the second regression analysis is conducted with mental well-being as a dependent variable and self-efficacy as an independent variable to conclude whether a higher self-efficacy toward becoming victimized by cybercrime is associated with the higher mental well-being of Generation Z. In this case, self-efficacy is also not significantly correlated with the dependent variable (B = .02, t (.19), p = .85, SE = .11). In conclusion, the second hypothesis is rejected as well, since there are no significant values indicating that the independent variable has a significant correlation with the mental well-being of Generation Z.

After, the regression analysis with both independent variables and mental well-being is conducted. However, the results do not indicate any significant correlations, which supports the findings from before, that both hypotheses can be rejected (B = -.04, t (-.54), p = .59, SE = .07).

Explorative analysis - All variables and mental well-being

Additionally, a multiple regression analysis is conducted with all existing variables. This explorative analysis is performed in order to explore if the remaining variables affect the mental well-being of Generation Z in this study. Risk perception and self-efficacy indicate no significant correlation with the dependent variable, which underlines the assumptions from the analyses before, that both hypotheses can be rejected (see Table 2). However, some significant effects emerged. The first one is gender which shows that there is a significant correlation between gender and mental well-being. Males (M = 4.29, SD = 0.73) have higher mental well-being than females (M = 3.85, SD = 0.77). The second significant variable is problematic internet use, in which an increase in problematic internet use leads to a decrease in mental well-being (see Table 2).

Table 2

Multiple regression analysis with all variables and mental well-being

	B	SE	t	Sig.
Gender	-0.31	0.14	-2.27	.03
Age	0.03	0.03	0.97	.33
Nationality	-0.06	0.09	-0.61	.55
Daily internet use	0.001	0.06	0.01	.99

Experience of cybercrime	-0.06	0.13	-0.48	.63
Problematic internet use	-0.34	0.09	-3.55	.001
Self-efficacy	0.03	0.12	0.20	.84
Actual security behavior	0.12	0.12	0.90	.37
Risk perception	0.06	0.07	0.78	.44
Risk-taking	0.04	0.08	0.53	.60

Moderation effects

First, four moderation analyses are conducted with risk perception as the main independent variable. Second, another four moderation analyses are conducted with self-efficacy as the main independent variable. Altogether, eight moderation analyses are performed to investigate whether a third variable has an effect on the relationship between the two independent variables of interest and the dependent variable. The analyses include the moderation effects of gender, problematic internet use, actual security behavior and risk-taking. Gender and problematic internet use are included as they show a significant correlation in the multiple regression analysis. Actual security behavior and risk-taking are incorporated as the researcher wants to explore whether there are other potential third variables. The first four analyses relating to risk perception can all be found in Table 3, while the last four analyses relating to self-efficacy are summarized in Table 4. The variable experience of cybercrime is not included in the moderation analysis because most of the participants did not experience cybercrime, therefore it is not assumed that there is a significant effect on the relationship between dependent and independent variables.

Risk perception

Table 3 points out the moderation effects on risk perception and mental well-being. It demonstrates that there is no variable that moderates the relationship between risk perception and mental well-being. The only significant effect that is shown, is the effect of gender on mental well-being. However, when risk perception and gender are combined, there is no significant effect. Concluding, no moderation effects are found.

Table 3

Moderation effects on the relationship between risk perception and mental well-being

	B	SE	df	F	Sig.
Risk perception	-0.32	0.25	1	0.001	.21
Gender	-0.94	0.41	1	6.87	.02
Risk perception*Gender	0.19	0.15	3	4.83	.19
Risk perception	0.46	0.31	1	0.00	.15

Problematic internet use	-0.02	0.28	1	1.99	.95
Risk perception*Problematic internet use	-0.14	0.09	3	7.59	.14
Risk perception	0.01	0.42	1	0.01	.97
Actual security behavior	0.14	0.35	1	1.25	.68
Risk perception*Actual security behavior	-0.01	0.11	3	0.52	.96
Risk perception	0.23	0.29	1	0.40	.45
Risk-taking	0.34	0.24	1	2.46	.17

Risk perception*Risk-taking	-0.08	0.08	3	1.22	.35

Self-efficacy

Looking at Table 4, which shows the moderation effects on self-efficacy and mental well-being, it can also be said that there is no significant third variable.

Table 4

Moderation effects on the relationship between self-efficacy and mental well-being

	B	SE	df	F	Sig.
Self-efficacy	-0.29	0.37	1	0.04	.43
Gender	-1.05	0.71	1	12.21	.14
Self-efficacy*Gender	0.19	0.21	3	4.51	.37
Self-efficacy	-0.52	0.51	1	0.14	.31

Problematic internet use	-0.95	0.49	1	20.55	.06
Self-efficacy*Problematic internet use	0.17	0.15	3	7.29	.26
Self-efficacy	0.86	0.60	1	0.31	.16
Actual security behavior	0.98	0.53	1	1.84	.07
Self-efficacy*Actual security behavior	-0.26	0.16	3	1.45	.12
Self-efficacy	0.33	0.47	1	0.06	.48
Risk-taking	0.41	0.44	1	2.41	.35
Self-efficacy*Risk-taking	-0.09	0.13	3	0.96	.50

Discussion

The purpose of this study was to test the research question "How can risk perception and self-efficacy toward becoming victimized by cybercrime affect the mental well-being of Generation Z?" and the corresponding hypotheses the higher the risk perception/self-efficacy toward becoming victimized by cybercrime, the higher the mental well-being of Generation Z. Both independent variables were not significantly correlated with the dependent variable. However, the analyses indicated that gender and problematic internet use had a significant association with the mental well-being of Generation Z. Next to that, the moderation analyses did not indicate a third variable which shows a significant effect on the relationship between the two independent variables and mental well-being. All in all, it can be concluded that the two hypotheses of this research can be rejected.

Implications

While this research focused on the hypothesis the higher the risk perception toward becoming victimized by cybercrime, the higher the mental well-being, the study of Conversano et al. (2010) assumes the contrary. Namely, that higher risk perception is associated with lower mental well-being. While De Kimpe et al. (2021) reasoned that one's risk perception decreases uncertainty and fear arousals leading to higher mental well-being. Conversano et al. (2010) argue that higher risk perception is accompanied by being too optimistic about a risk for which reason individuals could perceive themselves as being less at risk. This unrealistic idea of the risk makes them believe that they are also more capable of dealing with threats. Individuals considering themselves less at risk and still developing health issues are therefore mentally more affected by the outcome, as they did not prepare themselves because of their unrealistic optimism (Conversano

et al., 2010). Especially in terms of cybercrime, it is proven that individuals who are confronted with the threats of cybercrime are affected by feelings of anxiety (De Kimpe et al., 2021).

Moreover, my study supposed a higher self-efficacy could be associated with higher mental well-being because individuals' abilities lead to a specific outcome that satisfies them when they were capable of reducing risk (Cheng et al., 2020). On the other side, Jones et al. (2005) state that a higher self-efficacy correlates with low mental well-being. They interpret a higher self-efficacy, as estimating oneself to reach an outcome sooner with fewer resources. This overconfidence in one's abilities regarding a risk lead to disappointments when the outcome does not get along with one's expectations (Jones et al., 2005). Therefore, according to this argumentation, a higher self-efficacy corresponds with lower mental well-being.

Additionally, it could be that the PMT and the chosen variables were not related to Generation Z. Risk perception and self-efficacy were chosen, as the PMT explained why individuals engage in unsafe behaviors and how those two variables affect one's protection motivation (De Kimpe et al., 2021). However, in order to fight cybercrime, it should be known what affects it and even moving beyond it. For example, Miro (2014) argues for the Routine Activity Theory (RAT) which is widely known in the field of criminology as it focuses on crimes. The RAT is based on three conditions which are a likely offender, a suitable target and the absence of a capable guardian. It says that only the absence of one of the conditions could prevent a crime. Therefore, it should not only be Generation Z studied, who are the victims in this case, but also their environment, as potential offenders and guardians. Especially studying the behavior and motives of potential offenders could be relevant in understanding under which circumstances cybercrime happens in order to prevent them.

Furthermore, this study did not focus on a specific type of cybercrime. There are many different types of cybercrime that can have different causes and effects on the victims and offenders. It is especially difficult to find a consistent definition of cybercrime, which is a general problem in the analysis of cybercrime (Yar, 2005). Having a proper definition and classification of cybercrime could make it easier to find a suitable theory and target group that gives indications of common characteristics to prevent them.

Strengths and limitations

Strengths of this study were that it had many participants (*N*= 175) and all of them completed the survey. Furthermore, an advantage of this research was its online-based character which is a good point as the respondents could complete the survey whenever they wanted to without arranging an appointment. Additionally, this research gave information on variables, like gender and problematic internet use, correlating with mental well-being.

The limitations were that the whole study was conducted in English. This may interfere with the language skills of some participants, as they possibly did not understand all the items and survey descriptions which lead to unreliable answers. Further, the descriptive analysis also showed that the mean regarding the survey was always around the middle, which indicated that many respondents neither agree nor disagree with the items. This could be attributed to the issue stated before, that the survey was conducted in English. However, the social desirability bias could also have an impact on how the participants answered the items, as the topics could be too sensitive to them and they were afraid of giving an honest answer due to social expectations. An example item for this could be "Having an affair with a married man/woman".

Recommendations for future research

As this study only concentrated on Generation Z, other studies could also focus on different age groups and include maybe elderly individuals (Karagiannopoulos et al., 2021). There, it would be interesting to study the same independent variables in a different population, in order to conclude if the ages make a difference and compare the outcomes with the results of this study. Findings indicating that the elderly are more affected by cybercrime can be used to make cybercrime awareness training and build confidence regarding technologies in order to decrease cybercrime attacks.

Furthermore, this study focused on possible victims of cybercrime. However, it could also be helpful to analyze the behavior of potential offenders in order to evaluate their courses of action. This could prevent attacks even before they happen which could decrease harm (Butkovic et al., 2019). The knowledge of the causes and effects of cybercrime can be used to create preventive measures for organizations as well as individuals.

Another possibility to improve the study could be by translating the survey into different languages, such as German and Dutch which helps the respondents to understand the items better. Moreover, participants also would not be required to spend time by themselves translating the survey so they can fluently answer the items without being distracted.

Additionally, regarding the social desirability bias, it was already of great benefit that the survey was conducted online, however, it could help to inform the respondents from time to time that the survey was anonymous. Further, it could be beneficial to mention in the introduction of the survey that there were no right or wrong answers and that nobody will be judged based on their opinion.

Conclusion

The dangerous effects of cybercrime should be addressed and counteracted. Therefore, it is essential to find out which particular individual characteristics are common in cybercrime in order to give suitable training, such as cybersecurity awareness training or build confidence when users get in contact with technology. The current study contributed to this field, as the variables gender and problematic internet use can be further studied in order to incorporate outcomes in cyber security training. As the development of technology is an ongoing process, the causes and motives of victims and offenders should be acknowledged in order to protect future generations and fight cybercrime attacks with the main intention to ensure healthy mental well-being.

References

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, *8*, 540-542. https://doi.org/10.1016/j.pisc.2016.06.014

Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision making*, *1*(1). www.papers.ssrn.com/sol3/papers.cfm?abstract_id=1301089

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation*, *28*, 176-182. https://doi.org/10.1016/j.diin.2018.12.001

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, *108*, 106311. https://doi.org/10.1016/j.chb.2020.106311

Conversano, C., Rotondo, A., Lensi, E., Della Vista, O., Arpone, F., & Reda, M. A. (2010). Optimism and its impact on mental and physical well-being. *Clinical practice and epidemiology in mental health: CP & EMH*, *6*, 25. https://doi.org/10.2174/1745017901006010025

Da Fonsêca, P. N., Couto, R. N., do Vale Melo, C. C., Machado, M. D. O. S., & de Souza Filho, J. F. Scale of problematic internet use in university students: evidence of validity and reliability. https://doi.org/10.22235/cp.v12i2.1686

Debb, S., Schaffer, D., & Colson, D. (2020). A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 42-55. https://doi.org/10.52306/03010420GXUV5876

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*, 1-13. https://doi.org/10.1080/0144929X.2021.1905066

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hertlein, K. M., & Ancheta, K. (2014). Advantages and Disadvantages of Technology in Relationships: Findings from an Open-Ended Survey. *Qualitative Report*, *19*(11). https://doi.org/10.46743/2160-3715/2014.1260

Jensen, M., George, M. J., Russell, M. R., & Odgers, C. L. (2019). Young adolescents' digital technology use and mental health symptoms: Little evidence of longitudinal or daily linkages. *Clinical Psychological Science*, *7*(6), 1416-1433. https://doi.org/10.1177/2167702619859336

Jones, F., Harris, P., Waller, H., & Coggins, A. (2005). Adherence to an exercise prescription scheme: the role of expectations, self-efficacy, stage of change and psychological well-

being. *British journal of health psychology*, *10*(3), 359-378. https://doi.org/10.1348/135910704X24798

Karagiannopoulos, V., Kirby, A., Ms, S. O. M., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, *43*, 105615. https://doi.org/10.1016/j.clsr.2021.105615

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, *11*, 3030. https://doi.org/10.3389/fpsyg.2020.546546

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51*(3), 71-76. https://doi.org/10.1145/1325555.1325569

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 1. https://doi.org/10.17705/1jais.00232

Miró, F. (2014). Routine activity theory. *The encyclopedia of theoretical criminology*, 1-7. https://doi.org/10.1002/9781118517390.wbetc198

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), 1-9. https://doi.org/10.1007/s11920-021-01228-w

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309. https://doi.org/10.1080/17450128.2012.752119

Owen, S., Napoli, C., & Shin, J. (2018). The Gen Z Equation. www.wgsn.com/assets/marketing/toprightbox_assets/images/Gen_Z_Equation.pdf

Palme, J., & Berglund, M. (2002). Anonymity on the Internet. www.people.dsv.su.se/~jpalme/society/anonymity.pdf

Petrillo, G., Capone, V., Caso, D., & Keyes, C. L. (2015). The Mental Health Continuum–Short Form (MHC–SF) as a measure of well-being in the Italian context. *Social indicators research*, *121*(1), 291-312. https://doi.org/10.1007/s11205-014-0629-3

Rehman, H., Yafi, E., Nazir, M., & Mustafa, K. (2018). Security assurance against cybercrime ransomware. In *International conference on intelligent computing & optimization* (pp. 21-34). Springer, Cham. https://doi.org/10.1007/978-3-030-00979-3_3

Rogers, M. B., Amlôt, R., Rubin, G. J., Wessely, S., & Krieger, K. (2007). Mediating the social and psychological impacts of terrorist attacks: The role of risk perception and risk communication. *International review of psychiatry*, *19*(3), 279-288. https://doi.org/10.1080/09540260701349373

Schaffer, D. R., & Debb, S. M. (2019). Validation of the Online Security Behaviors and Beliefs Questionnaire with college students in the United States. *Cyberpsychology, Behavior, and Social Networking*, *22*(12), 766-770. https://doi.org/10.1089/cyber.2019.0248

Schroth, H. (2019). Are you ready for Gen Z in the workplace? *California Management Review*, *61*(3), 5-18. https://doi.org/10.1177/0008125619841006

Sladek, S., & Grabinger, A. (2014). Gen Z. *Introducing the first Generation of the 21st Century Available at*. www.xyzuniversity.com/wp-content/uploads/2018/08/GenZ_Final-dl1.pdf

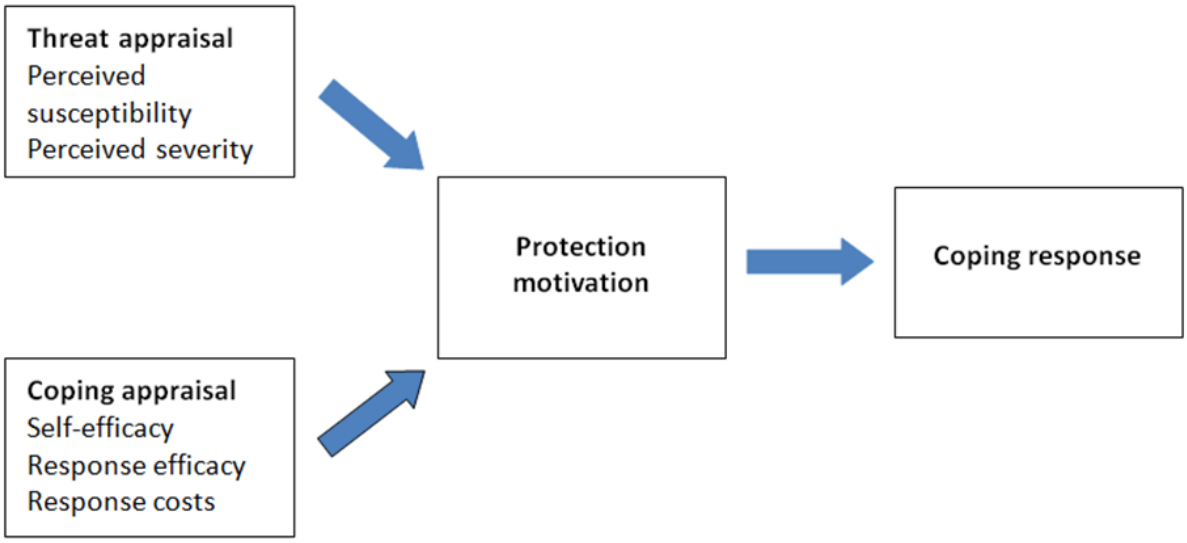
Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotton , S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412. https://doi.org/10.1089/cyber.2017.0028

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

Appendix A

Protection Motivation Theory by Rogers, 1983



Appendix B

Information Sheet and Informed Consent

Dear participant,

Thank you for your willingness to participate in this study. With this study, I aim to investigate to what extent different predictors affect individuals' mental well-being in cybercrime.

Cybercrime is crimes happening on the internet ranging from data theft and stalking to financial fraud. Offenders exploit their victims, steal data and money and use false identities. As cybercrime is more common nowadays, it is important to have a general knowledge about safety measures that protect oneself from criminals on the internet. Especially Generation Z is referred to as digital natives who never missed the introduction and ongoing change of smartphones and social media for which reason this study focuses only on those individuals.

Note that this survey is anonymous. The data provided by you cannot be used to identify who you are. Furthermore, you can also withdraw at any time in this study, without being forced to give an explanation. When you feel uncomfortable about your data, you can always contact me via email. Afterward, I will delete your data. Moreover, participating in this study is completely voluntary. Your contribution will help to make improvements in the area of cybercrime and mental well-being.

This Bachelor's thesis is part of my psychology program at the University of Twente. I am supervised by assigned supervisors who are Dr. Iris van Sintemaartensdijk and Rick Pinkster. Moreover, this study was reviewed and approved by the BMS Ethics Committee.

In case of any questions or concerns, feel free to contact me via email:

Julia Mekler (j.mekler@student.utwente.nl)

By selecting „I agree”, I confirm that I have read and understood the information above. I agree to participate voluntarily in this study and I understand that I can withdraw at any time.
[ ] I agree
[ ] I disagree

Appendix C
Demographics questions

The first part is about your demographics. Please indicate your gender.
[ ] Male
[ ] Female
[ ] Non-binary / third gender
[ ] Prefer not to say

How old are you?

What is your nationality?
Dutch
German
Other, namely:

What is your highest education level?
Secondary School Diploma
Bachelor's Degree
Master's Degree
PhD
Other, namely:

Appendix D
Hours spent per day

How many hours per day do you spend on the internet (e.g., Email, Facebook, Instagram WhatsApp, etc.)?
< 1 hour
1 -2 hours
2 - 4 hours
4 - 6 hours
6 - 7 hours
> 7 hours

Appendix E
Experience cybercrime

Have you ever been a victim of cybercrime (e.g., Phishing, Identity Theft, Account Hacking, Credit Card Fraud, etc.)?
No
If yes, please specify:

Appendix F

Scale of Problematic Internet Use (SPIU)

The following survey concerns your internet use. Please indicate to what extent you agree to each statement.

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
1. It is important to me to connect daily to Facebook, Twitter, Instagram, etc.	1	2	3	4	5
2. On some occasions, I have lost hours of sleep to use the Internet.	1	2	3	4	5
3. Sometimes I connect more than I should.	1	2	3	4	5
4. There are occasions when I prefer to stay connected to the Internet rather than being with my family or friends.	1	2	3	4	5
5. There are times	1	2	3	4	5

when I am in a bad mood because I cannot connect.					
6. When I am connected, I feel that time is passing fast, and when I realize it, I have spent hours on the Internet.	1	2	3	4	5
7. I have neglected my tasks by connecting to the Internet.	1	2	3	4	5
8. I have stopped doing important things to stay connected.	1	2	3	4	5

Appendix G

Scale of Security Behavior Self-Efficacy

The following questions reflect on how you deal with online threats.
Please indicate for each statement to what extent it applies to you.

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
1. I feel comfortable taking measures to secure my primary home computer.	1	2	3	4	5
2. Taking the necessary security measures is entirely under my control.	1	2	3	4	5
3. I have the resources and the knowledge to take necessary security measures.	1	2	3	4	5
4. Taking necessary security measures is easy.	1	2	3	4	5
5. I feel nervous when I think about online	1	2	3	4	5

security issues.					
6. In general, I am safe from online threats in my home.	1	2	3	4	5

Appendix H

Cyber Security Behavior Items of the OSBBQ (actual behavior)

The following statements are about your actual security behavior on the internet. Please indicate to what extent these statements apply to you.

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
1. I use different passwords for my different social media accounts (e.g., Facebook, Twitter, LinkedIn).	1	2	3	4	5
2. I usually review privacy settings on my social media sites (e.g., Facebook, Twitter, LinkedIn)	1	2	3	4	5
3. I keep the anti-virus software on my computer up to date.	1	2	3	4	5
4. I watch for unusual computer behavior/responses (e.g., computer	1	2	3	4	5

slowing down or freezing up, pop-up windows, etc.).					
5. I do not open email attachments from people whom I do not know.	1	2	3	4	5
6. I have never sent sensitive information (such as account numbers, passwords, and social security number) via email or using social media.	1	2	3	4	5
7. I back up important files on my computer.	1	2	3	4	5
8. I always act on any malware alerts that I receive.	1	2	3	4	5
9. I do not click on short URLs posted on	1	2	3	4	5

social
media
sites
unless I
know
where the
links will
really take
me.

Appendix I

Threat Susceptibility Scale (Risk perception)

The following statements concern your risk perception on the internet. Please, select to what extent you agree with the statements.

	Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree
1. It is extremely likely that my computer will be infected by malware in the future.	1	2	3	4	5
2. My chances of getting malware are great.	1	2	3	4	5
3. There is a good possibility that my computer will have malware.	1	2	3	4	5

Appendix J

DOSPERT Scale (Risk-taking)

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.

	Extremely unlikely	Moderately unlikely	Somewhat likely	Neither likely not unlikely	Somewhat likely	Moderately likely	Extremely likely
1. Betting a day´s income at the horse race.	1	2	3	4	5	6	7
2. Investing 10% of your annual income in a moderate growth mutual fund.	1	2	3	4	5	6	7
3. Investing 10% of your annual income in a new business venture.	1	2	3	4	5	6	7

4. Betting a day´s income at a high-stakes poker game.	1	2	3	4	5	6	7
5. Investing 5 % of your annual income in a very speculative stock.	1	2	3	4	5	6	7
6. Betting a day´s income on the outcome of a sporting event.	1	2	3	4	5	6	7
7. Engaging in unprotected sex.	1	2	3	4	5	6	7
8. Drinking heavily at a social	1	2	3	4	5	6	7

function.							
9. Driving a car without wearing a seatbelt.	1	2	3	4	5	6	7
10. Riding a motorcycle without a helmet.	1	2	3	4	5	6	7
11. Sunbathing without sunscreen.	1	2	3	4	5	6	7
12. Walking home alone at night in an unsafe area of town.	1	2	3	4	5	6	7
13. Admitting that your tastes are differe	1	2	3	4	5	6	7

nt from those of a friend.							
14. Disagreeing with an authority figure on a major issue.	1	2	3	4	5	6	7
15. Choosing a career that you truly enjoy over a more secure one.	1	2	3	4	5	6	7
16. Speaking your mind about an unpopular issue in a meeting at work.	1	2	3	4	5	6	7
17. Moving to a city far away	1	2	3	4	5	6	7

from your extended family.							
18. Starting a new career in your mid-thirties.	1	2	3	4	5	6	7
19. Going camping in the wilderness.	1	2	3	4	5	6	7
20. Going down a ski run that is beyond your ability.	1	2	3	4	5	6	7
21. Going white water rafting at high water in the spring.	1	2	3	4	5	6	7
22. Taking a skydiving class.	1	2	3	4	5	6	7

23. Bungee jumping off a tall bridge.	1	2	3	4	5	6	7
24. Piloting a small plane.	1	2	3	4	5	6	7
25. Taking some questionable deductions on your income tax return.	1	2	3	4	5	6	7
26. Having an affair with a married man/woman.	1	2	3	4	5	6	7
27. Passing off somebody else's work as your own.	1	2	3	4	5	6	7
28. Revealing a	1	2	3	4	5	6	7

friend's secret to someone else.							
29. Leaving your young children alone at home while running an errand.	1	2	3	4	5	6	7
30. Not returning a wallet you found that contains $200.	1	2	3	4	5	6	7

Appendix K

Mental Health Continuum Short Form (MHC-SF)

The last survey is about your general mental well-being. Please indicate, during the past month, how often did you feel...

	Never	Once or Twice	About Once a Week	About 2 or 3 Times a Week	Almost Everyday	Everyday
1. happy	1	2	3	4	5	6
2. interested in life	1	2	3	4	5	6
3. satisfied with life	1	2	3	4	5	6
4. that you had something important to contribute to society	1	2	3	4	5	6
5. that you belong to a community (like a social group, or your neighborhood)	1	2	3	4	5	6
6. that our society is a	1	2	3	4	5	6

good place or is becoming a better place, for all people						
7. that people are basically good	1	2	3	4	5	6
8. that the way our society works, makes sense to you	1	2	3	4	5	6
9. that you liked most parts of your personality	1	2	3	4	5	6
10. good at managing the responsibilities of your daily life	1	2	3	4	5	6
11. that you had warm and trusting relationships	1	2	3	4	5	6

with others						
12. that you had experiences that challenged you to grow and become a better person	1	2	3	4	5	6
13. confident to think or express your own ideas and opinions	1	2	3	4	5	6
14. that your life has a sense of direction or meaning to it	1	2	3	4	5	6

Appendix L

End of Survey

Thank you for your time spent taking this survey!

This study was conducted in order to gain insights into how different predictors affect the mental well-being of Generation Z in cybercrime. More specifically, I am interested in two predictors which are, namely, risk perception and self-efficacy of Generation Z.

The increasing use of technology leads to a rising number of cybercrimes, which in turn impact individuals' mental well-being. The perceived knowledge of risk and one's perceived effectiveness of safety measures decreases fear arousals in individuals since they have lower feelings of uncertainty. Therefore, it is important to measure if different predictors, such as risk perception and self-efficacy, correlate with Gen Z's mental well-being in cybercrime.

The primary focus lies on Gen Z because they never missed the introduction of technology and its rapid development. Generation Z is marked by a growing sense of equality and the rise of new talents whereby they also grow up in a culture of safety. Additionally, Gen Z is accompanied by the development of technology their entire life which leads to comprehendible concerns if this group of individuals is affected by cybercrime. Therefore, I aim to gain further knowledge about specific characteristics that increase an individual's mental well-being, as a higher risk perception could lead to higher mental well-being. These insights could help individuals to protect themselves from harm to their well-being in cybercrime.

If you are interested in the results of this study, please send an email to:

j.mekler@student.utwente.nl

Your response has been recorded.