# Ready, Set, Know: The Race Against Cybercrime and the Importance of Actual Knowledge

The Relationship Between Actual and Perceived Knowledge of Cybercrime and the Intentions to Engage in Self-Protective Behaviour to Prevent Cybercrime Victimisation

Kimberly Bluhm (2455773)
Faculty of Behavioural, Management and Social Sciences (BMS)
University of Twente
Supervisor: Dr. Iris van Sintemaartensdijk
Second supervisor: Dr. Steven Watson
15 March 2023

**Abstract**

Digitalisation offers criminals new ways to commit crimes, both new crimes and traditional crimes in the online environment. This is also known as cybercrime. Cybercrime can take place on an individual and societal level, and engaging in self-protective behaviour is crucial to prevent victimisation of these crimes. However, it was unclear how actual knowledge about cybercrime influences individuals' willingness to engage in self-protective behaviour, and if actual knowledge affects individuals' intentions to protect themselves after exposure to different cyberthreats. Using the Protection Motivation Theory, this study focused on self-protective behaviour to prevent cybercrime and the role of actual knowledge. Earlier studies suggested that constructs of the Protection Motivation Theory predicted individuals' intentions to engage in self-protective behaviour, and that actual knowledge may affect these intentions as well. As expected, a multiple, linear regression analysis showed actual knowledge was an essential indicator for the intentions to engage in self-protective behaviour. Moreover, it was a stronger predictor for the intentions for self-protective behaviour than perceived knowledge. Trust in the internet was an influential factor, since it was negatively correlated with actual knowledge, whereas it was positively correlated with perceived knowledge. The results also indicated that individuals' perceived vulnerability increased after reading about a cyberthreat. Lastly, actual knowledge was a stronger predictor for social protection measures than for technical protection tools. These findings provide directions to improve future interventions by emphasising the importance of actual knowledge about cybercrime combined with a continuing, critical view towards potential cyberthreats. Moreover, recommendations for future research to improve individuals' self-protective behaviour are provided in the discussion. These implications might contribute to create more awareness among individuals on their role in preventing cybercrime victimisation and the importance of actual knowledge, which will eventually lead to a safer, online society.

**Keywords:** *Cybercrime; Self-Protective Behaviour; Actual Knowledge; Perceived Knowledge; Cyberthreats; Protection Motivation Theory*

## Introduction

Digitalisation has considerably changed the way people live and communicate (Bossler & Holt, 2009). Offline activities, such as banking and shopping, are transferred into cyberspace, including crime (Bernik, 2014; Drew & Farrell, 2020). This resulted in the formation of new crimes and the execution of traditional crimes in a new and innovative manner. Thus, cybercrime is an umbrella term for all different forms of crime in which information- and communication technology (ICT) has a critical role in the execution of the crime (Domenie et al., 2013).

Cybercrime can be divided into two types. Cyber-enabled crimes are the first type, which are traditional crimes that are not focused on ICT, but ICT is used to commit the crime (e.g. online identity fraud). Second, there are cyber-dependent crimes, which are crimes focused on- and committed through the use of ICT (e.g. hacking) (Akdemir & Lawless, 2020; Drew & Farrell, 2020; Van de Weijer & Leukfeldt, 2017). Martens et al. (2019) also made a distinction between social cybercrimes, that rely on human error, and technical cybercrimes, for which technical knowledge is necessary to execute the crime. However, these types of cybercrime (i.e. social versus technical and cyber-dependent versus cyber-enabled) are intertwined, meaning that both cyber-dependent and cyber-enabled crimes have social and technical aspects. For instance, phishing is a more social crime, since a certain action needs to be performed by someone to shift from potential victim to actual victim. At the same time, offenders need a certain level of technical knowledge to execute the crime, as they have to create a spoofed website (i.e. a fake website that resembles the website of an official institution) (Ghazi-Tehrani & Pontell, 2021).

Cybercrime can take place on both an individual and a societal level. On the individual level, cybercrime offenders try to victimise people in various ways. Examples include consumer fraud and identity theft. According to the CBS (2022) seventeen percent of Dutch citizens was a victim of cybercrime in 2021, which is similar to the percentages of other, more traditional crime victims in 2021. The percentage of traditional crime victims reduces while the percentage of cybercrime increases. Therefore, it is to be expected that the percentage of cybercrime victimisation will surpass that of traditional crime victimisation. Cybercrime has unique characteristics, including greater anonymity, intangibility, and it is difficult to detect and prosecute, making it of increasing importance to study this topic (Borwell et al., 2021).

Cyberwar is a societal cybercrime threat and is a devious, invisible phenomenon fought out in cyberspace, which also has consequential effects in the offline world (Zeadally

& Flowers, 2014; McGraw, 2013). The attributes used are physical, such as computers and routers, but the interaction takes place in an online domain (Zeadally & Flowers, 2014 ;el Helow, 2021; Duddu, 2018). The current conflict between Russia and Ukraine can be defined as a hybrid war, since it is both a cyber war and physical war (Serpanos & Komninos, 2022). The comparison between how individuals react to different cyberthreats, and if different cyberthreats might influence individuals' intentions for self-protective behaviour has not been studied before. Therefore, this comparison was made in the current study.

**Self-Protective Behaviour**

One way to engage in self-protective behaviour to prevent cybercrime victimisation is by using protection measures or tools (Mamade & Dabala, 2021; Verma & Shri, 2022). These measures and tools can be used to engage in precautionary online behaviour to achieve online security (Jansen & van Schaik, 2017). Examples include technical tools, like firewalls or virus scanners. Individuals can also use protection measures, which include strategies or behaviours to prevent victimisation (e.g. checking sources and documents or coming up with hard-to-guess passwords) (Martens et al., 2019).

Protection measures can be divided into two categories: maladaptive and adaptive measures (Jansen & van Schaik, 2017; Martens & de Wolf, 2018). Maladaptive protection measures do not protect an individual from a cyber threat, but includes reducing certain online activities or avoiding the internet, which are only effective when users restrict their online behaviours excessively (Martens & de Wolf, 2018). Adaptive protection measures function to adequately protect users against cyber threats (Chou & Sun, 2017).

Martens & de Wolf (2018) also made a distinction between social adaptive measures (e.g. checking sources and documents) and technical adaptive measures (e.g. securing Wi-Fi networks).

**Perceived Knowledge**

To engage in self-protective behaviour, individuals need a certain level of knowledge. Perceived knowledge (i.e. what people think they know about cybercrime) is a strong predictor for individuals' willingness to engage in self-protective behaviour to prevent cybercrime victimisation, and a crucial factor to understand why individuals are overly optimistic about their tendencies to protect themselves (De Kimpe et al., 2022). De Kimpe et al. (2022) found that perceived knowledge was negatively related to the intentions to engage in self-protective behaviour. Thus, individuals who consider themselves well-informed about cybercrime, think that they do not need any (more) protection measures or tools to prevent cybercrime victimisation, as they perceive themselves as less vulnerable. De Kimpe et al.

(2022) also found that the feeling of being informed about cybercrime was, in part, a positive aspect, as individuals might feel more capable of using protection measures or tools, they are more assured of the effectivity of these protection measures, and it made them aware of the severity of cybercrime. Lastly, their study suggested that trust in the internet is an important predictor for making individuals more vulnerable for cybercrime victimisation, since individuals who trust the internet might think it is a reliable place and do not perceive cybercrime as a risk (De Kimpe et al., 2022).

**Actual Knowledge**

Actual knowledge was not included in the study of De Kimpe et al. (2022), but they suggested it might be a crucial indicator for individuals' willingness to engage in self-protective behaviour. Actual knowledge is what someone objectively knows about cybercrime, while perceived knowledge is what someone thinks they know about cybercrime (De Kimpe et al., 2022).

A study that focused on actual knowledge of cybercrime is from Van 't Hoff - de Goede et al. (2019) and they found that actual knowledge was positively related to safe, self-reported online behaviour. Their results suggested that individuals' who are informed about cybercrime are behaving more safely when sharing their personal information. Lastly, Arachchilage & Love (2014) studied the role of knowledge of phishing in relation to threat avoidance, and found that conceptual and procedural knowledge of phishing positively affected individuals' self-efficacy. This increased their phishing threat avoidance behaviour.

Moreover, it was unclear how actual knowledge affected the perception of different cyberthreats (individual threats versus societal threats) and the intentions for self-protective behaviour after reading about it. Newspapers are constantly publishing articles that focus on cyberthreats, however, it was unclear how these articles might influence individuals' willingness to engage in self-protective behaviour, and if actual knowledge played a role in these intentions. Earlier studies studied the effects of fear appeals on individuals' online information-sharing behaviour and compared two levels of fear appeals: strong versus weak arguments (Jansen & van Schaik, 2019). Their findings suggested that fear appeals have a positive effect on perceptions, attitudes and their behavioural intentions.

So far, there is little insight in how actual knowledge affects individuals' willingness to engage in self-protective behaviour to prevent cybercrime victimisation, and how actual knowledge affects their intentions after reading about different cyberthreats. The few studies that included actual knowledge of cybercrime as a variable have shortcomings. First, the role of actual knowledge combined with certain online behaviours has been studied, but only a

limited amount of protection measures and tools were included (Van ’t Hoff - de Goede et al., 2019). Second, De Kimpe et al. (2022) focused on perceived knowledge and intentions to use certain protection tools, but they did not include actual knowledge in their study, but acknowledge that actual knowledge may be an important indicator. Lastly, the literature on the perception of different cyberthreats and if actual knowledge might affect this, is scarce. Jansen & van Schaik (2019) focused on fear appeals. Fear appeals are persuasive messages focusing on a threat and try to evoke fear in order to motivate readers to take action (Johnston et al., 2023). However, it is unknown how actual knowledge affects and different cyberthreats influence these intentions, and if more coping-focused, compared to threat-focused, content leads to different intentions.

## Protection Motivation Theory

To study the relations between actual knowledge, perceived knowledge, and the intentions to engage in self-protective behaviour, the Protection Motivation Theory (PMT) from Rogers (1975) was used. Originally, the PMT was developed to study health promotions and prevention of diseases (Floyd et al., 2000), but recently the theory has also been applied to the context of cybercrime and self-protective behaviour (De Kimpe et al., 2022; Jansen et al., 2016; Martens et al., 2019). The two appraisal processes that initiate protection motivation are threat appraisal and coping appraisal, and the outcomes of both appraisal processes result in the intentions to engage in self-protective behaviours (De Kimpe et al., 2022).

### *Threat Appraisal*

Threat appraisal is a process in which an individual assesses the threat and it consists of two constructs: (1) *perceived severity*; and (2) *perceived vulnerability*. *Perceived severity* focuses on how severe an individual perceives the consequences of an occasion to be (De Kimpe et al., 2022). Therefore, perceived severity positively predicts the intentions to engage in protection measures (Crossler & Bélanger, 2014).

The second variable in the treat appraisal construct is *perceived vulnerability*. *Perceived vulnerability* is someone’s perception of their likelihood to become a victim of a threat (Rogers, 1975). Rogers (1975) found a positive relation between *perceived vulnerability* and intentions, but other studies found mixed results on the relation between *perceived vulnerability* and the intentions towards protective behaviour (Martens et al., 2019; Verkijika, 2018). Some studies found evidence for an increase of motivation towards protective behaviour (Thompson et al., 2017), whereas others found non-significant

relationships or contradicting results, in which *perceived vulnerability* negatively influenced individuals' self-protective behaviour (Crossler & Bélanger, 2014; Tsai et al., 2016). Follow-up studies found that a positive relationship between *perceived vulnerability* and engaging in security procedures only held for people who are familiar with IT or work in IT. Simultaneously, there was no significant relationship for individuals who had less experience with IT (Crossler & Bélanger, 2014; Herath & Rao, 2009). Given the theoretical support from the PMT, while considering the mixed results found in earlier studies, the current study followed the relationship from the original PMT.

***Coping Appraisal***

The second appraisal in the PMT is coping appraisal, and this is a process in which an individual assesses the components of the risk in relation to the potential strategies to avoid or reduce impact (Jansen & van Schaik, 2017). Coping appraisal consists of the following three constructs: *self-efficacy, response efficacy* and *response costs*. Both efficacy variables can be described as more cognitive processes, which are stimulated when an individual is confronted with a risk. These variables aim to increase individuals' protective behaviours to decrease a risk (Verkijika, 2018).

*Self-efficacy* is the belief an individual is able to successfully engage in protective behaviours (Tsai et al., 2016). Studies found a positive relation between *self-efficacy* and individuals' willingness to engage in self-protective behaviour (Anderson & Agarwal, 2010;Arachchilage & Love, 2014; Verkijika, 2018).

*Response efficacy* can be described as individuals' anticipated effectivity of using protection measures and tools to prevent cybercrime victimisation (Martens et al., 2019). Findings in the study of Tsai et al. (2016) suggested that *response efficacy* positively predicted *intentions* towards self-protective behaviour. They suggested that when individuals thought that using protective software is effective, they had a higher intentions to install and use it.

*Response costs* can be defined as the combination of monetary and non-monetary costs, with the latter including the time and effort for implementation of protection measures (Gurung et al., 2009). Some research found non-significant relationships between this variable and intentions towards self-protective behaviours, for example, Gurung et al. (2009). They claimed that engaging in self-protective behaviour was not related to the response costs, as a plethora of free protection measures is offered. For instance, when focusing on anti-spyware, companies offer this protection tools for free, but there are also anti-spyware programs that cost hundreds of euros. These companies also offer free versions for a certain

period of time. Most end-users might choose the free version over an expensive version, since this free version is effective enough (Gurung et al., 2009). Due to this reasoning, *response costs* was excluded in the current study.

### *Antecedents of Threat and Coping Appraisal*

*Perceived knowledge*, *actual knowledge*, and *internet trust* were added as constructs in this study. De Kimpe et al. (2022) found that *perceived knowledge* was a crucial predictor for individuals' intentions to use protection measures and tools. Moreover, they suggested that it was unclear how *actual knowledge* affect these intentions. Lastly, they suggested that *internet trust* was correlated with individuals' *perceived knowledge*.

**Perceived Knowledge.** *Perceived knowledge* is usually determined by participants' self-reporting of their perceived understanding of a subject, and it is a mixture of confidence and knowledge (Raju et al., 2015). An individual's perceived knowledge may differ from their actual knowledge (Jensen et al., 2005; McDonnell et al., 2014), as individuals frequently overestimate what they know about a topic (De Kimpe et al., 2022).

The findings in the study of De Kimpe et al. (2022) suggested that internet users with higher levels of *perceived knowledge*, perceived themselves as less susceptible. Consequently they had lower intentions to engage in self-protective behaviour. Moreover, *perceived knowledge* affects threat appraisal. Individuals with higher level of *perceived knowledge* may be aware of the general severity of cybercrime, but they may also see themselves as less vulnerable (De Kimpe et al., 2022). Lastly, perceived knowledge also affects coping appraisal. Findings in the study of De Kimpe et al. (2022) showed that perceived knowledge positively affected self-efficacy and response efficacy.

**Actual Knowledge.** The relationship between actual knowledge and intentions towards self-protective behaviour has not been widely studied in the field of cybercrime. Two studies were found that focus on this topic.

Van 't Hoff - de Goede et al. (2019) focused on online behaviour of Dutch citizens and they included actual knowledge in their study. Their results suggested that being knowledgeable was positively related to safer online behaviour. However, some differences were found between protection measures and tools. In case of sharing personal information online, actual knowledge seemed to lead to safer, online behaviour. On the contrary, in case of password management, more knowledge seemed to lead to a less safe password.

Another study that focused on actual knowledge, is from Arachchilage & Love (2014). They focused on the effect of conceptual and procedural knowledge about phishing

on user's self-efficacy to thwart phishing attacks. Their findings suggested that conceptual and procedural knowledge positively affected one's self-efficacy.

**Internet Trust.** *Internet trust* was the last antecedent in the current study. As trust is a complex concept that lacks a general definition, the definition of Pavlou (2003) was used and adapted to the topic of the current study. Pavlou (2003) described trust as 'the belief that the other party will behave in a socially responsible manner' (p. 106). Adapted to the current study, the internet can be seen as a safe space and its users behave in a responsible way (Riek et al., 2016). The findings in the study of De Kimpe et al. (2022) suggested that *internet trust* negatively affected *perceived severity* and *perceived vulnerability.*

## Current Study

The current study focused on the role of *actual knowledge* on *intentions* towards self-protective behaviour and was divided into two studies. Using an extended framework based on the Protection Motivation Theory (PMT), this study included constructs that influenced individuals' intentions towards self-protective behaviours. In the proposed model, *actual knowledge* was added as a predictor, and this was the main focus of the current study. The proposed model described individuals' *intentions* to engage in self-protective behaviour based on threat appraisal and coping appraisal. The current study only focused on the relations between these variables (Figure 1). The appraisals were influenced by the antecedents *perceived knowledge, actual knowledge* and *internet trust*. *Perceived knowledge* was added to compare the effect of *actual knowledge* versus *perceived knowledge* on intentions and appraisals. Lastly, De Kimpe et al. (2022) found that *perceived knowledge* and *internet trust* were correlated. Therefore, *internet trust* was added to determine how this variable affected *actual knowledge,* and it made a comparison possible between the role of *internet trust* on *actual knowledge* versus *perceived knowledge.*

*Intentions* towards self-protective behaviour for cybercrime in general were studied instead of focusing on one type of cybercrime, since various crimes are related (De Kimpe et al., 2022). For example, a victim of phishing can also become a victim of identity theft. Additionally, protection measures and tools often protect individuals against multiple cybercrimes, however, in some cases individuals might take specific measures or use certain tools to prevent victimisation from a particular crime.

The first study focused on individuals' *actual knowledge* and *intentions* towards self-protective behaviour, and the following exploratory research question was formulated: "How does actual knowledge affect individuals' intentions to engage in self-protective behaviour to prevent cybercrime victimisation?" (RQ1). Moreover, based on the studies mentioned before,

the following hypotheses were formulated to study the relations between the antecedents, constructs of the PMT and *intentions*:

**H1:** Perceived severity is a positive predictor of intentions towards self-protective behaviour.

**H2:** Perceived vulnerability is a positive predictor of the intentions towards self-protective behaviour.

**H3**: Self-efficacy is a positive predictor of intentions towards self-protective behaviour.

**H4:** Response efficacy is a positive predictor of intentions towards self-protective behaviour.

**H5:** Perceived knowledge is a negative predictor of the intentions towards self-protective behaviour.

**H6:** Perceived knowledge is a positive predictor of perceived severity (6a) and a negative predictor of perceived vulnerability (6b).

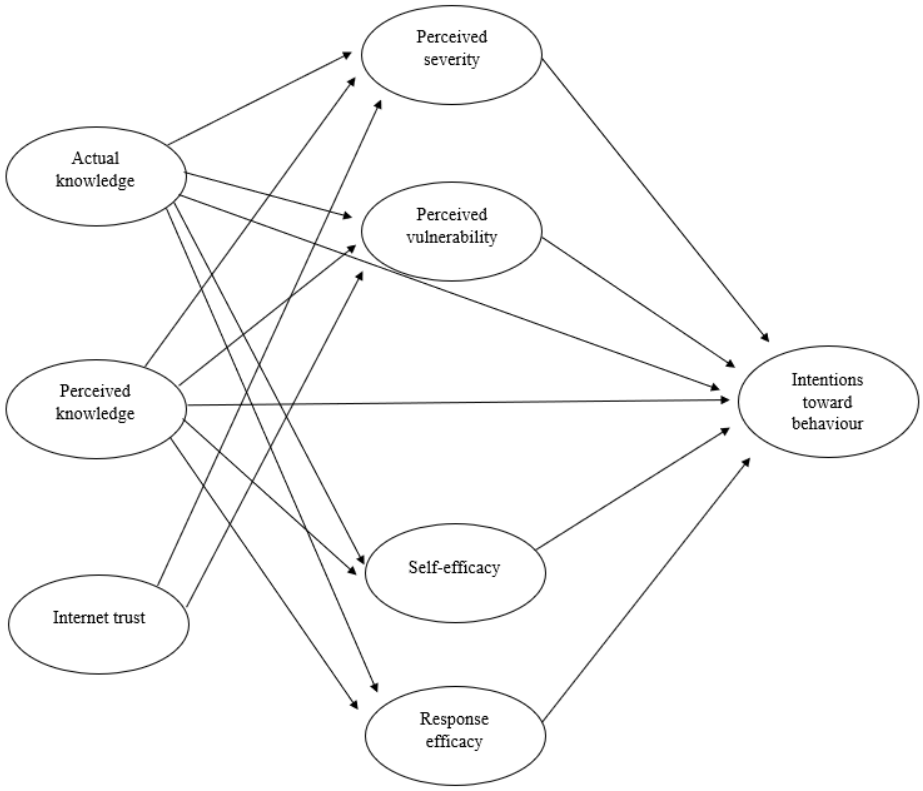
**H7:** Perceived knowledge is a positive predictor of self-efficacy (7a) and response-efficacy (7b).

**H8:** Actual knowledge is a positive predictor of self-efficacy.

**H9**: Internet trust is a negative predictor of perceived severity (9a) and perceived vulnerability (9b).

**Figure 1**

*Conceptual, Extended PMT Applied on Cybercrime and Intentions Towards Self-protective Behaviour*



The second study focused on individuals' *intentions* to engage in self-protective behaviour and the use of protection measures and tools after reading about different cyberthreats: a societal cyber-related issue (cyber warfare) versus an individual cyberthreat (cyber-attack on the Dutch emergency centre). Individuals' *actual knowledge* was also taken into consideration to determine if actual knowledge influenced individuals' *intentions*. Lastly, this study not only focused on two threat levels (societal versus individual), but also took the two types of appraisal of the Protection Motivation Theory into account (threat appraisal versus coping appraisal). Based on this, the following exploratory research question was addressed "In what way do individuals' intentions towards protective behaviour differ after exposure to a cyberwar threat level compared to exposure to a cybercrime threat level, also when taking into consideration the two appraisals of the Protection Motivation Theory and actual knowledge?" (RQ2). No hypotheses were formulated for this study due to the exploratory nature of the study.

## Methods

### Participants

The current research consisted of two studies, but all questions were asked in the same questionnaire (Appendix A). In total, nine participants were excluded. An exclusion criteria was age (<18). For this reason, two participants were excluded. Seven participants were excluded, because they did not consent to participate or because they answered each question with the same answer.

Participants were recruited per snowball and convenience sampling. They received a link to the study via What's App or Facebook. Moreover, the SONA-system of the University of Twente was used to recruit participants.

#### *Participants Study 1*

In total, 222 participants participated in the first study. The age range was between 18 and 67 years of age ($M$ = 29.99; $SD$ = 12.23). Most participants identified as female: 146 (65.8%), 70 (31.5%) as male, 3 (1.3%) as non-binary, 1 (0.4%) who preferred not to say their gender, and 2 (0.9%) who did not fill in their gender. Majority of the participants was Dutch: 128 (57.7%), 33 (14.9%) was German, 33 (14.9%) were from a non-European country, 24 (10.8%) were from another European country, and 4 (1.8%) preferred not to disclose their nationality. Most participants were students: 104 (46.8%), 64 (28.8%) participants were full-time employees, 42 (18.9%) participants were part-time employees, 7 (3.2%) participants

were unemployed, 2 (0.9%) participants were retired, and 3 (1.4%) preferred not to say their employment status.

***Participants Study 2***

In total, 172 participants participated in the second study. Fifty participants who participated in the first study, did not participate in the second study or did not finish the second study. The age range was between 18 and 67 years of age ($M$ = 29.13; $SD$ = 11.51). Most participants identified as female: 111 (64.5%), 55 (32.0%) identified as male, 3 (1.7%) identified as non-binary, 1 (0.6%) participant preferred not to say their gender, and 2 (1.2%) participants did not fill in their gender. Most participants were Dutch 89 (51.7%), 29 (16.9%) participants were German, 23 (13.4%) participants were from another European country, 28 (16.3%) participants were from a non-European country, and 3 (1.7%) preferred not to say their nationality. Most participants were students: 85 (49.4%), followed by full-time employees: 48 (27.9%), and part-time employees: 33 (19.2%). Five (2.9%) participants were unemployed and 1 (0.6%) participant preferred not to say their employment status.

**Design**

The current research was divided into two studies, in which the first study focused on the role of *actual knowledge* on the *intentions* towards self-protective behaviour, whereas the second study focused on threat levels and these *intentions*. *Actual knowledge* was also taken into consideration in the second study.

***Design Study 1***

The first study focused on victimisation of cybercrime and traditional crime to compare the victimisation rates, and the protection measures and tools to prevent victimisation of these two types of crimes. Moreover, *actual knowledge* was measured in this study, combined with the measurement of constructs of the PMT, and *intentions* towards self-protective behaviour. Participants were asked to fill in a questionnaire about these themes.

***Design Study 2***

The second study was a 2 (threat level: Societal versus Individual) x 2 (appraisal: Threat versus Coping) between-participants design. This study focused on *intentions* to engage in self-protective behaviours after exposure to different cyberthreats.

In the societal threat condition, participants read a fictious article about a cyberwar between Russia and Poland. This article was based on a real-life conflict between Ukraine and Russia to make the article as realistic as possible. The article focused on either threat appraisal (*perceived severity* and *perceived vulnerability*) or coping appraisal (*self-efficacy* and *response efficacy*).

In the individual threat condition, participants read a fictious article about a cyber-attack on the Dutch emergency centre. The event in this article was also based on a real incident that took place in June 2019, in which people were not able to reach the emergency centre for several minutes. This was an individual threat, as only the people who needed the emergency centre during the attack were disadvantaged. This article focused on either the constructs of threat appraisal (*perceived severity* and *perceived vulnerability*) or coping appraisal (*self-efficacy* and *response efficacy*).

In both threat appraisal conditions (i.e. for cyberwar and cybercrime) attention was devoted to the damage of the threat and prolonged consequences. Additionally, these articles focused on the vulnerability of citizens if a cyberattack takes place. This content was in line with the constructs of threat appraisal (i.e. *perceived severity* and *perceived vulnerability*).

In both coping appraisal conditions (i.e. for cyberwar and cybercrime) attention was given to the prevention of cyberattacks. The importance of using protection measures and tools was highlighted, combined with the role of citizens engaging in protection measures and tools to prevent cybercrime victimisation. This content was in line with the constructs of coping appraisal (i.e. *self-efficacy* and *response efficacy*).

## Measures

### *Study 1*

**Victimisation Cybercrime.** The selection of the cybercrimes in the victimisation questions was adapted by the studies of De Kimpe et al. (2022) and Martens et al. (2019), and includes the following crimes: (1) *phishing*; (2) *identity theft*; (3) *consumer fraud*; (4) *hacking*; (5) *malware*; and (6) *ransomware*. The first three crimes represented social cybercrimes, which rely on human error, whereas the latter three represented technical cybercrimes, for which technical knowledge is required (Martens et al., 2019). This selection entailed a varied collection of cybercrimes, which left room for comparison. Martens et al. (2019) suggested that individuals' intentions towards self-protective behaviour was constructed differently for malware (technical crime) compared to scams (social crime). Additionally, the impact individuals experience after victimisation of various cybercrimes might differ (Borwell et al., 2021). Therefore, the intentions towards self-protective behaviour might also differ for social crimes compared to technical crimes.

To study victimisation of *phishing*, respondents were asked: "Did you share sensitive information (passwords or credit card details) after you received a fraudulent message by email, phone, text or social media?" (Reyns, 2015). To study *online identity theft*, participants were asked "Did anyone ever steal your personal details (password, credit card details) online

and then pretended to be you?" (De Kimpe et al., 2022). To study *consumer fraud*, participants were asked: "Did you (partially) pay for something online without receiving the promised goods, services and/or prices in return?" (Leukfeldt & Yar, 2016). To determine whether participants have been a victim of *hacking*, they were asked: "Were you inconvenienced by someone accessing your email, social media accounts or the data on your computer, laptop, tablet or smartphone without your permission?" (Reyns, 2015). To study *malware* victimisation, participants were asked: "Were you inconvenienced by an infection of your computer, laptop, tablet or smartphone by a malicious type of software (e.g., viruses, Trojan horse, spyware)?" (Bossler & Holt, 2009). Lastly, to determine participants' victimisation of *ransomware*, they were asked: "Were the data on your computer, laptop, tablet or smartphone blocked, accompanied by the message that your data would only be unlocked if you paid a sum of money?" (Bergmann et al., 2018).

For each cybercrime, participants were asked if they have been a victim of this crime. Five answer options were provided: (1) "I have been a victim in the past twelve months"; (2) "I have been a victim more than a year ago, but less than five years ago"; (3) "I have been a victim more than five years ago"; (4) "I have never been a victim of this crime"; and (5) "I do not know". The *N* for each separate category was too small to compare the groups. Therefore, the answered were recoded, in which answer 1, 2, and 3 were categorised as 'Victim' and 4 and 5 were categorised as 'Not a victim'.

**Victimisation Traditional Crime.** To determine whether participants have been a victim of a traditional crime, five the crimes discussed in the study of Van Dijk (2010), were used: (1) *Theft of car*; (2) *Theft of bicycle*; (3) *Burglary*; (4) *Street robbery*; and (5) *Theft of personal property.* (sexual) Assault was excluded from the study, due to ethical considerations. Moreover, attempted burglary was excluded, since this study focused on victimisation and not attempted victimisation. *Pickpocketing* was added to the crimes. The answer options per traditional crime were equal to the ones in the cybercrime victimisation questions and after data collection, the answer options 1, 2, and 3 were recoded into 'Victim' and 4 and 5 were recoded into 'Not a victim'.

First, participants were asked if they have been a victim of *pickpocketing* ("Were items (jewels, money and/or other valuable items) stolen from you in public?'). Next, they were asked: "Did someone steal your car?" and "Did someone steal your bicycle?" to study *theft of car* and *theft of bicycle*. To study *burglary*, participants were asked: "Has someone unlawfully entered your residency? This usually, but not always, includes theft" (Catalano, 2010). To determine whether participants have been a victim of *street robbery*, they were

asked: ‘Did someone ever steal something from you in public while using force, threat or violence?’. Lastly, to study *theft of personal property*, participants were asked: “Did someone ever take and carry away your personal property with the intentions to permanently deprive it from you?”.

**Protection Tools Cybercrime.** To determine which protection tools or measures participants were using to prevent cybercrime victimisation, they were asked if they were using one or more of the following tools or measures: (1) “Install software e.g. anti-virus, anti-spyware, anti-phishing, crypto locker, backup software”; (2) “Set up software that is included with your operating system (e.g. firewall, defender)”; (3) “Update software in operating systems”; (4) “Secure a Wi-Fi network”; (5) “Set up difficult to guess passwords for accounts and home network”; (6) “Check the origin and the document itself on reliability”; (7) “Be on your guard when giving personal information to others”; (8) “Online backups”; (9) “Offline backups (physical/printed copies of important documents)”; and (10) “None of the above”. Participants were able to select multiple options, however, this was not possible if participants selected the last option ‘None of the above’. The first seven protection measures were based on the adaptive security measures (Martens & de Wolf, 2018). The first five protection measures (1 till 5) were technical adaptive measures, whereas the next two measures (6 and 7) were social adaptive protection measures (Martens & de Wolf, 2018). The last two social measures (8 and 9) were added by the researcher to create an equal division between technical and social measures.

**Protection Tools Traditional Crime.** The protection tools or measures to prevent victimisation of traditional crime used in this study, were based on outcomes of several studies focusing on one specific traditional crime. Participants were asked if they engage in one or multiple of the following protection measures: (1) “Particularly parking on driveways and in garages” (Farrell et al., 2011); (2) “Double locking habits for bicycles” (Van Lierop et al., 2015); (3) Taking additional security measures for the home, such as installing alarms, reinforced doors, and/or security locks” (San-Juan et al., 2012); (4) Avoiding passing through certain areas or streets of the city (San-Juan et al., 2012); (5) “DNA-kit (to mark your valuable items to let possible thieves know that you are protected)”; (6) “Identification spray (a spray used to mark offenders for days, weeks or even months)”; and (7) “None of the above”. Participants were able to select multiple options, as long as they did not select the last option.

**PMT Constructs.** The questionnaire in this study contained questions on the extended PMT constructs derived from previous studies and are adapted to this topic (Table

1). Additionally, the study of Anderson & Agarwal (2010) was used for the formulation of the items focusing on *intentions towards behaviour* against cybercrime.

All items were measured using a five-point Likert Scale (1 = "*totally disagree*" to 5 = "*totally agree*"), except for *perceived vulnerability*. The items for this construct were reversed, with 1 = "*totally agree*" to 5 = "*totally disagree*". After data collection, these items were recoded to align with the other items. Cronbach's Alpha (α) was calculated for all constructs, and *perceived severity, perceived vulnerability*, and *self-efficacy* had a Cronbach's Alpha α >.70 (Table 1), indicating a good internal reliability (George & Mallery, 2019). *Response efficacy* had a Cronbach's Alpha α = .57, which was lower than the other constructs, but still acceptable (George & Mallery, 2019).

**Actual Knowledge.** To estimate participants' actual knowledge of cybercrime, nine questions from the knowledge test in the study of Van 't Hoff - de Goede et al. (2019) were translated and included in the questionnaire of this study. The topics in these questions corresponded with the crimes in the victimisation questions, and focused on definitions of cybercrime-related topics, strong passwords and information provision on the internet (e.g. "Which of the following passwords is the strongest?" and "What is two-step verification?"). Participants were asked to select the correct definition or option. The answer options also included an "I do not know" option. Participants got a point for each correct answer and the sum of these nine question was their score for actual knowledge. This resulted in an average score of *M* = 4.73 (*SD* = 1.76).

**Table 1**

*Descriptive Statistics of Items (N = 222)*

| | *M* | *SD* | *α* |
|---|---|---|---|
| **Perceived knowledge** | **3.38** | **0.97** | **.86** |
| I feel adequately informed about cybercrime risks | | | |
| I feel adequately informed about how to avoid cybercrime risks | | | |
| **Internet trust** | **2.37** | **0.72** | **.78** |
| I am optimistic about the safety of the internet | | | |
| I have every confidence that the internet is safe | | | |
| I am satisfied with the safety of the internet | | | |
| **Perceived severity** | **4.33** | **0.59** | **.85** |
| I believe cybercrime is an important problem/phenomenon | | | |
| I believe cybercrime should be taken seriously | | | |
| I believe cybercrime is a severe problem | | | |
| **Perceived vulnerability** | **3.33** | **0.89** | **.87** |
| It is not likely that I become a victim of cybercrime | | | |
| It is not probable that I become a victim of cybercrime | | | |
| The risk is small that I become a victim of cybercrime | | | |
| **Self-efficacy** | **3.12** | **0.79** | **.76** |

| | | | |
|---|---|---|---|
| Using necessary protection tools against cybercrime is easy | | | |
| I feel comfortable using protection tools against cybercrime | | | |
| I possess the knowledge and skills to use the necessary protection tools against cybercrime | | | |
| **Response efficacy** | **3.54** | **0.56** | **.57** |
| Protection tools against cybercrime are effective in preventing cybercrime | | | |
| By using protection tools, I can avoid cybercrime | | | |
| I am less likely to become a victim of cybercrime of I use protection tools | | | |
| **Intention towards behaviour** | **3.87** | **0.64** | **.74** |
| I am likely to use protection tools against cybercrime | | | |
| I am sure I am going to use protection tools against cybercrime | | | |
| I am willing to use protection tools against cybercrime | | | |

***Study 2***

In the current study, a division was made between two threat levels (societal versus individual) and the two appraisals of the PMT (threat versus coping).

The Cronbach's Alpha (α) for all constructs can be found in Appendix B.

**Cyberwar Threat Appraisal.** Participants in the cyberwar threat appraisal condition were asked to rate the items to measure *perceived severity* (e.g. "I believe cybercrime is an important problem/phenomenon") and *perceived vulnerability* (e.g. "It is not possible that I become a victim of cybercrime").

A five-point Likert Scale was used to measure these items (1 = "*totally disagree*" to 5 = "*totally agree*"), except for *perceived vulnerability*, since the items for this construct were reversed.

**Cyberwar Coping Appraisal.** Participants in the cyberwar coping appraisal condition were asked to rate the items to measure *self-efficacy* (e.g. "Using necessary protection tools against cybercrime is easy") and *response efficacy* (e.g. "Protection tools against cybercrime are effective in preventing cybercrime").

A five-point Likert Scale was used to measure these items (1 = "*totally disagree*" to 5 = "*totally agree*").

**Cybercrime Threat Appraisal.** Participants in the cybercrime threat appraisal condition were asked to rate the items to measure *perceived severity* (e.g. "I believe cybercrime should be taken seriously") and *perceived vulnerability* (e.g. "The risk is small that I become a victim of cybercrime").

A five-point Likert Scale was used to measure these items (1 = "*totally disagree*" to 5 = "*totally agree*"), except for *perceived vulnerability*, since the items for this construct were reversed.

**Cybercrime Coping Appraisal.** Participants in the cybercrime coping appraisal condition were asked to rate the items to measure *self-efficacy* (e.g. "I feel comfortable using protection tools against cybercrime") and *response efficacy* (e.g. "By using protection tools, I can avoid cybercrime").

A five-point Likert Scale was used to measure these items (1 = "*totally disagree*" to 5 = "*totally agree*").

**Intentions Towards Self-Protective Behaviour.** To measure participants' intentions and appraisals after exposure to a threat level, all participants were asked to rate the items focusing on *intentions* towards self-protective behaviour for a second time. The phrasing in these items was slightly different compared to the items in study 1, since the participants were asked if they were more likely or willing to use protection tools (e.g. "I am more likely to use protection tools against cybercrime"). Participants were also asked if they would use any additional protection tools after reading the article. The protection measures and tools provided in this question were similar to the protection measures and tools asked in study 1, but the option "Other…." was included. Lastly, participants were requested to rate to what extent they agreed with statements focusing on the reality of cyberwar/cyber-attack in the article they read ("I believe it is likely that a cyberwar/cyber-attack, as described in the article, can take place"), and if they experienced any impact after reading the article (e.g. "I experienced emotional/psychological impact (e.g. anger, fear, or insecurity) after reading the article"). All items were measured using a five-point Likert Scale (1 = "*totally disagree*" to 5 = "*totally agree*").

**Procedure**

The current study was approved by the Ethics Committee of the BMS-lab at the University of Twente (request number: 221187) before data collection started.

Participants clicked on the link to the questionnaire in Qualtrics. First, participants had to read the informed consent and had to agree to the terms and conditions of this study to proceed. Second, participants were asked to fill in their demographics (e.g. age, gender and level of education), followed by questions related to their victimisation of cybercrime and traditional crime. Next, participants answered two questions about the protection measures and tools that they were currently using to prevent victimisation of cybercrime and traditional

crime. Afterwards, participants were asked to rate items related of the PMT and study 1 ended. After a short introduction to study two, participants were asked to read an article about a specific cyberthreat, followed by items related to that article. At the end of the questionnaire, participants were debriefed and thanked for their participation. It took the participants approximately 20 minutes to complete the questionnaire.

**Data Analysis**

For data analysis, the Statistical Package of Social Sciences (SPSS) version 28 was used. First, the data set was cleaned up. Incomplete responses or participants who did not meet the inclusion criteria were excluded. Additionally, irrelevant variables (e.g. starting time) were deleted.

To study the relationships in the model (Figure 1), correlations were calculated. Next, linear, multiple regressions were performed to measure which variables were the strongest predictors. First, a multiple regression was performed with the four original PMT constructs (*perceived severity, perceived vulnerability, self-efficacy,* and *response efficacy)* to study which one was the strongest predictor for *intentions* (H1 – H4). Next, a multiple regression was performed with *perceived knowledge* and *actual knowledge* to study which type of knowledge was the strongest predictor for *intentions* (H5). Afterwards, *actual knowledge, perceived knowledge,* and *internet trust* were included to study which antecedent was the strongest predictor for both *perceived severity* (H6a and H9a) and *perceived vulnerability* (H6b and H9b). Lastly, *perceived knowledge* and *actual knowledge* were included to study which one was the strongest predictor of *self-efficacy* and *response efficacy* (H7a, H8, and H7b). Due to the exploratory nature of *actual knowledge,* no hypotheses were formulated for this construct, except for the relationship between *actual knowledge* and *self-efficacy* (H8). The study of Arachchilage & Love (2014) focused on the relationship between actual knowledge of phishing and self-efficacy, and they suggested that there was a positive relationship between these variables.

## Results

**Study 1**

The first study focused on victimisation of cybercrime and traditional crime, protection measures against these two types of crimes, and *intentions* towards self-protective behaviour. The PMT was used to determine how the antecedents and constructs affected these intentions.

### *Victimisation and Protection Measures*

Participants were asked if they have been a victim of six cybercrimes and six traditional crimes. This resulted in the following scores for the various types of cybercrime and traditional crime (Table 2).

**Table 2**

*Victimisation Cybercrime and Traditional Crime (N = 222)*

| Cybercrime | *N* (%) | Traditional crime | *N* (%) |
|---|---|---|---|
| Phishing | 26 (11.6%) | Pickpocketing | 46 (20.5%) |
| Identity theft | 31 (13.8%) | Theft of car | 8 (3.6%) |
| Consumer fraud | 72 (32.1%) | Theft of bicycle | 90 (40.2%) |
| Hacking | 51 (22.8%) | Burglary | 43 (19.2%) |
| Malware | 88 (39.3%) | Street robbery | 14 (6.3%) |
| Ransomware | 24 (10.7%) | Theft of personal property | 29 (12.9%) |

Additionally, participants were asked which protection tools they were using to protect themselves against these two types of crimes (Table 3).

**Table 3**

*Protection Tools Used by Participants (N = 222)*

| Cybercrime protection tool | *N* (%) | Traditional crime protection tool | *N* (%) |
|---|---|---|---|
| Install software | 139 (62.1%) | Parking in driveways or garages | 79 (35.3%) |
| Firewall | 112 (50.5%) | Double locking bicycle | 89 (39.7%) |
| Update software | 112 (50.5%) | Additional measures at home | 89 (39.7%) |
| Secure Wi-Fi network | 153 (68.3%) | Avoiding certain areas | 123 (54.9%) |
| Difficult passwords | 126 (56.3%) | DNA-kit | 4 (1.8%) |
| Check origin documents | 102 (45.5%) | Identification spray | 4 (1.8%) |
| On guard when providing information | 151 (67.4%) | | |
| Online backups | 109 (48.7%) | | |
| Offline backups | 68 (30.4%) | | |

### *Preliminary Analyses Protection Motivation Theory (PMT)*

The PMT was used to study how *actual knowledge*, p*erceived knowledge*, and the constructs of threat appraisal and coping appraisal affected individuals' *intentions* towards self-protective behaviour.

Table 4 presents the correlations between the antecedents (*actual knowledge, perceived knowledge*, and *internet trust*), the constructs of threat and coping appraisal (*perceived severity, perceived vulnerability, self-efficacy* and *response efficacy*), and the intentions towards self-protective behaviour.

**Table 4**

*Pearson Correlation Between Variables*

| | ACK | PCK | ITR | PSE | PVU | SEE | REE | INT |
|---|---|---|---|---|---|---|---|---|
| ACK | | | | | | | | |
| PCK | .21 ** | | | | | | | |
| ITR | -.16 * | .24*** | | | | | | |
| PSE | .24*** | .09 | -.30*** | | | | | |
| PVU | .02 | -.20** | -.37*** | .15* | | | | |
| SEE | .17* | .45*** | .24*** | .01 | -.30*** | | | |
| REE | .19** | .12 | .07 | .01 | -.26 *** | .29*** | | |
| INT | .32*** | .30*** | -.08 | .32*** | .07 | .40*** | .20** | |

*$p$ <.05, ** $p$ <.01, *** $p$ <.001
ACK = actual knowledge, PCK = perceived knowledge, ITR = Internet trust, PSE = perceived severity, PVU = perceived vulnerability, SEE = self-efficacy, REE = response efficacy, and INT = intentions

Table 5 presents the linear, multiple regressions between the constructs measured in this study. The standardised Beta (β) was reported, since different measurements were used for the predictor variables (i.e. *actual knowledge* and the constructs of PMT).

**Table 5**

*Linear, Multiple Regressions*

| **H** | **From** | **To** | **β** | ***SE*** | ***t*** | $\eta_p^2$ |
|---|---|---|---|---|---|---|
| 1 | Perceived severity | Intentions | .27*** | .07 | 4.66 | .09 |
| 2 | Perceived vulnerability | Intentions | .18** | .05 | 2.92 | .04 |
| 3 | Self-efficacy | Intentions | .42*** | .05 | 6.66 | .18 |
| 4 | Response efficacy | Intentions | .13* | .07 | 2.02 | .02 |
| 5 | Perceived knowledge | Intentions | .24 *** | .04 | 3.74 | .06 |
| | Actual knowledge | Intentions | .26*** | .02 | 4.05 | .07 |
| 6a | Perceived knowledge | Perceived severity | .13 | .04 | 1.84 | .02 |
| | Actual knowledge | Perceived severity | .15* | .02 | 2.23 | .02 |
| 9a | Internet trust | Perceived severity | -.30*** | .06 | -4.46 | .09 |
| 6b | Perceived knowledge | Perceived vulnerability | -.12 | .06 | -1.76 | .01 |
| | Actual knowledge | Perceived vulnerability | -.01 | .04 | -1.58 | .00 |
| 9b | Internet trust | Perceived vulnerability | -.34*** | .08 | -5.13 | .11 |
| 7a | Perceived knowledge | Self-efficacy | .39*** | .05 | 6.02 | .19 |
| 8 | Actual knowledge | Self-efficacy | .12 | .03 | 1.85 | .01 |
| 7b | Perceived knowledge | Response efficacy | .06 | .04 | 0.85 | .01 |
| | Actual knowledge | Response efficacy | .18** | .02 | 2.62 | .03 |

*$p$ <.05, ** $p$ <.01, *** $p$ <.001

Significant, positive relations were found for all constructs of the PMT (i.e. *perceived severity* (H1), *perceived vulnerability* (H2), *self-efficacy* (H3) and *response efficacy* (H4)). Contrary to the expectation of a negative relation between the variables, there was a

significant, positive relation between *perceived knowledge* and *intentions* (H5). *Perceived knowledge* was positive related to *self-efficacy* (H7a). No significant relations were found between *perceived knowledge* and *perceived severity* (H6a), *perceived knowledge* and *perceived vulnerability* (H6b), and *perceived knowledge* and *response efficacy* (H7b). Both *actual knowledge* and *perceived knowledge* (H5) were positively related to *intentions*. *Actual knowledge* was positively related to *self-efficacy* (H8), *perceived severity, and response efficacy*. Lastly, *internet trust* was negatively related to *perceived severity* (H9a) and *perceived vulnerability* (H9b).

***Exploratory Analyses***

One multiple, linear regression was conducted to study how *actual knowledge* affected the use of social protection measures versus technical protection tools. This analysis showed that the score for the use of social measures (which rely on human error) had a higher contribution ($\beta = .49$, *SE* = .08, $p < .01$, $\eta_p^2 = .08$) for *actual knowledge* than the score for the use of technical tools, for which technical knowledge is required to execute the crime ($\beta = .29$, *SE* = .11, $p < .01$, $\eta_p^2 = .06$).

***Summary Study 1***

The results of this study indicated that *actual knowledge* was a stronger predictor for the *intentions* than *perceived knowledge*. For the original constructs of the PMT, all constructs were significantly related to *intentions. Self-efficacy* was the strongest predictor for *intentions*.

*Actual knowledge* and *perceived knowledge* were positively associated. When comparing *actual knowledge* with *perceived knowledge, actual knowledge* was negatively related to *internet trust*, whereas *perceived knowledge* was positively related to *internet trust.* Additionally, *perceived knowledge* was significantly related to *self-efficacy*, whereas *actual knowledge* was not. On the contrary, *actual knowledge* was significantly related to *response efficacy*, whereas *perceived knowledge* was not significantly related to this construct.

**Study 2**

The second study focused on *actual knowledge*, different threat levels, and the *intentions* to engage in self-protective behaviour.

***Preliminary Analyses***

An one-way between-group analysis of variance (ANOVA) was conducted to explore the impact of different threat levels and appraisals on the *intentions* to engage in self-protective behaviour. There was no significant difference in these *intentions* among the four

groups, $F$ (3, 180) = .55, $p$ = .65. When controlling for *actual knowledge*, there was still no significant difference in *intentions* between the four groups, $F$ (3,179) = .49, $p$ = .69. Also when comparing the different groups with planned contrast, no significant difference for *intentions* were found. These planned contrast included: (1) cyberwar versus cybercrime; (2) threat appraisal versus coping appraisal; (3) cyberwar threat appraisal versus cybercrime threat appraisal; and (4) cyberwar coping appraisal versus cybercrime coping appraisal.

A two-way ANOVA was conducted to study if threat levels (cyberwar versus cybercrime) and appraisals (threat versus coping) affected participants' *intentions* after reading the articles. This analysis showed that there was no significant main effect of appraisals on *intentions*, $F$ (1,180) = .15, $p$ = .70, and no significant main effect of threat levels on *intentions*, $F$ (1,180) = 1.30, $p$ = .26. Additionally, there was no significant interaction effect between threat levels and appraisals on *intentions*, $F$ (1,180) = .27, $p$ = .60.

To study whether *actual knowledge* affected participants' *intentions*, while also controlling for threat levels and appraisals, *actual knowledge* was added as a covariate in a two-way ANOVA. This analysis showed that there was no significant main effect of threat levels on *intentions*, $F$ (1,179) = 1.12, $p$ = .29, and no significant main effect of appraisals on *intentions*, $F$ (1,179) = .22, $p$ = 64. Lastly, there was no significant interaction effect between threat levels and appraisals on *intentions*, $F$ (1,179) = .17, $p$ = .68.

***Exploratory Analyses***

All constructs of the PMT were measured for a second time; after participants read the article. Therefore, a comparison could be made between the scores before and after reading the article. Paired *t*-tests were conducted to compare the constructs before and after reading the article.

***Threat Appraisal.*** There were no significant differences in *perceived severity* in both the cyberwar condition, $t$ (46) = -.82, $p$ = .42, and cybercrime condition, $t$ (49) = -1.70, $p$ = .10. There was a significant difference in *perceived vulnerability* in the cyberwar condition, $t$ (46) = -5.69, $p$ <.001; $d$ = .59. Participants' *perceived vulnerability* was higher after reading the article ($M$ = 3.67; $SD$ = 0.95) than before ($M$ = 3.18; $SD$ = 0.92). *Perceived vulnerability* was also significantly different for participants in the cybercrime condition, $t$ (49) -4.39, $p$ <.001; $d$ = .67. An increase in *perceived vulnerability* was found: after ($M$ = 3.83; $SD$ = 0.79) versus before ($M$ = 3.42; $SD$ = 0.93).

***Coping Appraisal.*** A significant difference was found for *self-efficacy* in the cyberwar condition, $t$ (42) = 2.82, $p$ = .01; $d$ = .58. Participants scored higher on this construct before

(*M* = 3.34; *SD* = 0.78) than after reading the article (*M* = 4.16; *SD* = 0.53). No difference was found for the cybercrime condition, *t* (43) = -1.79, *p* = .08. There was no significant difference for *response efficacy* in both conditions, *t* (42) = .77, *p* =.45 for cyberwar, and, *t* (43) = 1.56, *p* = .13 for cybercrime.

***Intentions.*** Only participants in the cyberwar coping appraisal condition showed a significant difference in *intentions*, *t* (42) = 2.47, *p* = .02; *d* = .70. Their score for the *intentions* was higher before the article (*M* = 4.16; *SD* = 0.53) than after (*M* = 3.89; *SD* = 0.72). For the other conditions, no significant differences were found.

***Summary Study 2***

There were no significant differences in *intentions* between the participants exposed to different threat levels and appraisals. Also when controlling for their actual knowledge, there were no significant differences.

When comparing the scores for the constructs of the PMT before and after the exposure to the threat level, significant differences were found for *perceived vulnerability* in both the cyberwar and cybercrime condition. The scores for this construct increased after being exposed to the threat. Additionally, a significant difference was found in the cyberwar condition, in which *self-efficacy* decreased after being exposed to the threat. Lastly, a significant difference was found for *intentions* in the cyberwar coping appraisal condition, as the score for this construct decreased after being exposed to the threat.

## Discussion

People are considered to be the weakest link in cyber security, and criminals use this vulnerability for the execution of their offences (Curtis & Oxburgh, 2022). People can protect themselves from cybercrime victimisation by using protection measures and tools, such as safe passwords or firewalls. However, it was unknown whether individuals' knowledge influenced their willingness to engage in self-protective behaviour to prevent cybercrime victimisation.

This research consisted of two studies and represents an attempt to gain insight into the position of actual knowledge in the willingness to engage in self-protective behaviour, while using an extended version of the PMT, and taking different threat levels into consideration.

The results of the first study indicated that more than one third of the participants was not using the more common protection tools, for instance, a firewall or software updates, and more than 50 percent of the participants did not check the reliability of incoming documents.

Additionally, the victimisation rates were high, as almost 40 percent of the participants was a victim of malware and almost one third was a victim of consumer fraud. The results also indicated that actual knowledge about cybercrime and protection measures and tools was more important to engage in self-protective behaviour than perceived knowledge. Additionally, the more knowledge individuals had, the less trust they had in the internet, while it is the other way around for individuals who perceived themselves to be informed about cybercrime. Moreover, the belief to be able to successfully implement these protection tools had the strongest positive relation to intentions. Lastly, these results confirm that the PMT is useful in the context of cybercrime and self-protective behaviour, since significant relationships were found between all constructs and intentions to engage in self-protective behaviour.

The findings in the second study suggested that different threat levels did not affect individuals' intentions to engage in self-protective behaviour. Also when taking individuals' actual knowledge into consideration, there was still no difference in these intentions. The perception of becoming a victim of cybercrime increased after exposure to both cyberthreats. The belief of successfully engaging in protective behaviour decreased after reading about the cyberwar.

**Actual Versus Perceived Knowledge**

The results of the current study suggested that actual knowledge was a crucial indicator for individuals' intentions to engage in self-protective behaviour, and a stronger predictor for these intentions than their perceived knowledge. This implies that it is more important that individuals have actual knowledge than that they think they have it. Additionally, the results indicated that actual knowledge and perceived knowledge were positively correlated, suggesting that when someone increases their actual knowledge, their perceived knowledge will increase as well.

Trust in the internet also affected both types of knowledge. Actual knowledge was negatively related to internet trust, whereas perceived knowledge was positively related to internet trust. Thus, individuals who are informed about cybercrime have less trust in the internet and may be more careful when using it. Whereas individuals who think they have knowledge of cybercrime may overestimate their skills to recognise a cyberthreat and consider the internet as a safe place. An explanation for the latter might be the optimism bias from Slovic (1987), also described in Martens et al. (2019). When people are aware of obvious attempts, they may think they will recognise another attempt as well, as they feel knowledgeable. They may think they are safe on the internet, due to both their trust in the

internet and perceived knowledge. Consequently, they underestimate the possibility of becoming a victim and are more vulnerable to become a victim of cybercrime (Drew & Farrell, 2020). The results of the study of De Kimpe et al. (2022) suggested that fifteen percent of the population can be considered as users who have trust in the internet, thus being more vulnerable to become a victim.

Moreover, the two types of knowledge had different influences on individuals' perceived severity. Actual knowledge had a positive effect on perceived severity, whereas a non-significant result was found for perceived knowledge. Thus, individuals with actual knowledge perceived cybercrime as a severe threat, whereas individuals with perceived knowledge lacked this perception. Perceived knowledge is, in part, a positive aspect, as it was a stronger predictor for individuals' self-efficacy, meaning that individuals feel capable of successfully engaging in self-protective behaviour.

Lastly, the results showed that one third of the participants did not use the common protection measures and tools, for instance to install software or secure a Wi-Fi network, to prevent cybercrime victimisation, making them more vulnerable to become a victim.

Therefore, it is crucial that future interventions, like awareness campaigns, trainings, or media coverage, should focus on increasing individuals' actual knowledge, without only awakening perceived knowledge. When the level of perceived knowledge increases, this may negatively affect individuals' perception of the severity of cybercrime and may increase the perception that the internet is a reliable place. On the contrary, when individuals have higher levels of actual knowledge, without higher levels of perceived knowledge, this might result in a better understanding of the severity of cybercrime and highlights their susceptibility, which consequently might also lead to higher intentions to engage in self-protective behaviour (De Kimpe et al., 2022). However, it should be emphasised that increasing actual knowledge might also lead to an increase in perceived knowledge. All in all, a continuing, critical view towards cyberthreats should be emphasised, while a balance between actual and perceived knowledge is safeguarded. It seems crucial that this balance between these two types of knowledge will be established.

**Protection Motivation Theory Versus Extended Parallel Process Model**

To go beyond the cognitive focus of the PMT, the extended parallel process model (EPPM), developed by Witte (1992), can be used. This framework includes similar constructs as the PMT, and recognises two process: danger control process and fear control process. Danger control is triggered when there are high levels of both perceived threat and efficacy, resulting in the premise of fear motivating an individual to protect oneself, while when the

latter is triggered, there is a high level of perceived threat and a low level of perceived efficacy, resulting in maladaptive coping (De Kimpe et al., 2022; Johnston et al., 2023). Thus, individuals need to a certain degree of fear to get into action, as being scared might help to increase their willingness to engage in self-protective behaviour. In the current study, individuals' perceived vulnerability increased after reading about the cyberthreats, while their self-efficacy, response efficacy, and intentions did not significantly differ from the scores before reading the article, which is in line with maladaptive coping, as described in the EPPM.

Therefore, it seems crucial that future research first establishes if individuals do not feel the need to engage in self-protective behaviour after exposure to different cyberthreats or that other cyberthreats might motivate them to engage in (more) self-protective behaviour. Second, the EPPM could be used to determine the motivation to engage in self-protective behaviour and compare several protection measures and tools, as has been done in this study. Earlier studies focused on one or two types of protection measures (e.g. Johnston et al., 2023), but future research could include multiple protection tools to determine which tools individuals are planning to use after exposure to a cyberthreat.

**Cyberwar Versus Cybercrime**

When focusing on different threat levels, the results from the cyberwar coping appraisal condition showed that individuals' self-efficacy and intentions decreased after reading about the cyberwar, and non-significant results were found for the other conditions. These results are in line with the findings in the study of Boss et al. (2015), who implied that when a strong fear message was included in an article, significant relations were found for all assumptions of the PMT. However, when the article did not include enough fear, significant relations between constructs vanished and protection motivation decreased dramatically. Another study from Yoon et al. (2012) focused on security behaviours of students and implied that security behaviours start with awareness of an external risk or the tension on information security. When looking at the results in the current study, the level of fear in the articles might not have been enough to increase individuals' willingness to engage in self-protective behaviour.

Another explanation might be that the hybrid war between Russia and Ukraine might have influenced individuals' intentions for self-protective behaviour, as the fictional war between Poland and Russia in the article is based on a real attack that took place in the war between Russia and Ukraine. This is close to an ongoing reality, and it might have reminded readers of the current war between Russia and Ukraine. They may see the physical and online damage

caused by these events, which increases their awareness of the risks or the surrounding pressure, but not to a sufficient extent to feel the need to protect oneself. Therefore, it seems crucial that individuals need to be scared to some extent to increase their intentions to protect themselves, and future research could focus on what level of fear is necessary to do this, and how real-life events could be incorporated in increasing individuals' willingness to engage in self-protective behaviour.

**Social and Technical Protection Tools**

Another finding in this study suggest that actual knowledge was more likely to predict engagement in social protection measures than technical protection tools. Social protection measures had a higher contribution to individuals' actual knowledge than technical protection tools. One explanation for this finding might be that knowledge about cybercrime is necessary to engage in the social protection measures used in this study. These findings are in line with the findings in the study of Van 't Hoff - de Goede et al. (2019), who suggest the more knowledge an individual has, the higher their self-reported safe, online behaviour is (i.e. which protection measures and tools they use). Another explanation might be that users may have a higher perception of control over social measures compared to technical tools, as social protection measures are more likely to be behaviours that individuals can execute to prevent victimisation. It is crucial to understand what motivates individuals to use certain protection measures and tools, and whether this is related to individuals' actual knowledge. This might provide implications to enhance self-protective behaviour.

**Strengths and Limitations**

The first strength of the current study is that it was a first attempt to study the relationship between individuals' actual and perceived knowledge and their willingness to protect themselves from cybercrime victimisation. Earlier studies focused on one type of crime (e.g . Arachchilage & Love, 2014), but literature focusing on the relation between actual knowledge and cybercrime in general is scarce. Another aspect of this study that has not been studied before, is the role of different cyberthreats, like a cyberwar, and how these threats affect individuals' willingness to protect oneself. The effect of fear appeals has been studied, but did not include different threat levels. Additionally, fear appeals are persuasive message with the explicit intention to scare people (Johnston et al., 2023), while the articles used in the second study were similar to news articles, and were based on events that have happened in the past.

This study also had several limitations. First, intentions were measured in this study instead of actual behaviour. Actions are controlled by intentions, but not all intentions

become actions (Ajzen, 1985), also known as the behavioural-intention gap (Sheeran, 2002). Intentions might also change over time (Sheeran, 2002), which can influence individuals' willingness to engage in self-protective behaviour. It is unknown whether the participants of the current study implemented (new) protection measures and tools after reading the articles. A longitudinal study would therefore yield valuable insights, as this can focus on the implementation of protection measures and tools.

Second, the sample of the current study was too small to compare the intentions from victims of different cybercrimes and differences in time of victimisation. Participants were asked if they have been a victim of cybercrime and if so, whether this was in the past year, more than a year ago but less than five years ago, or more than five years ago. This should have made it possible to compare different moments of victimisation and study whether moment of victimisation affected individuals' intentions to engage in self-protective behaviour. However, due to the sizes of the groups, it was not possible to make a comparison. An earlier study focusing on the relationship between victimisation of cybercrime and using protection measures found no significant difference in the use of protection measures between individuals who have been a victim of cybercrime and participants who have not been a victim (Drew, 2020). However, a dichotomous question (yes/no) was used to study victimisation and the moment of victimisation was not taken into consideration. Additionally, Drew (2020) suggested that other aspects, such as polyvictimisation or moment of victimisation might influence individuals' protection behaviour. Therefore, future research could incorporate a similar measurement style to study whether moment of victimisation might influence the intentions to engage in self-protective behaviour.

## Conclusion

Cybercriminals are constantly finding new and innovative ways to execute cybercrimes, which means that society has to keep up and prevent cybercrime victimisation. In conclusion, this study has made an essential contribution to the understanding of what should be included in cybercrime prevention interventions. This study highlights the importance of actual knowledge about cybercrime, as this is beneficial for the willingness to engage in self-protective behaviour. Attention is drawn to different protection measures and tools, both social and technical, and the results also suggested that there was still a group who did not actively protect themselves online. Protection measures cannot guarantee complete prevention from cybercrime victimisation, but the group that does not protect themselves and people who overestimate the safety of the internet are especially vulnerable to become a

victim of cybercrime. The implications in this study might provide input to keep up in the continuing race against cybercriminals and contribute to create a safer, online society with informed end-users.

## References


Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In *Action Control* (pp. 11–39). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-69746-3_2

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

Anderson, & Agarwal. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613. https://doi.org/10.2307/25750694

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727

Bernik, I. (2014). *Cybercrime and cyber warfare*. John Wiley & Sons.

Borwell J, Jansen J, & Stol W. (2021). Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions. *Journal of Digital Social Research*, *3*(3), 85–110.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864.

Bossler, A., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*.

CBS. (2022). *Veiligheidsmonitor 2021 [Safety monitor 2021]*.

Chou, H.-L., & Sun, J. C.-Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education*, *112*, 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in ‘real world’ policing and law enforcement. *The Police Journal: Theory, Practice and Principles*, 0032258X2211075. https://doi.org/10.1177/0032258X221107584

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). 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*, *41*(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

Domenie, M. M. L., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J., & Stol, W. Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit [Victimization in a digitized society: A study among citizens of e-fraud, hacking, and other common crimes]*. Boom Lemma Uitgevers.

Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, *6*(1), 17–33. https://doi.org/10.1108/JCRPP-12-2019-0070

Drew, J. M., & Farrell, L. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, *6*(1), 17–33. https://doi.org/10.1108/JCRPP-12-2019-0070

Duddu, V. (2018). A Survey of Adversarial Machine Learning in Cyber Warfare. *Defence Science Journal*, *68*(4), 356–366.

El Helow, K. R. (2021). The role of cyber security in facing the challenges of cyber warfare and cyber-attacks. *International Journal of Computers*, *6*. http://www.iaras.org/iaras/journals/ijc

Farrell, G., Tseloni, A., & Tilley, N. (2011). The effectiveness of vehicle security devices and their role in the crime drop. *Criminology & Criminal Justice*, *11*(1), 21–35. https://doi.org/10.1177/1748895810392190

FLOYD, D. L., PRENTICE-DUNN, S., & ROGERS, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

George, D., & Mallery, P. (2019). *IBM SPSS Statistics 26 Step by Step*. Routledge. https://doi.org/10.4324/9780429056765

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders*, *16*(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*, *17*(3), 276–289. https://doi.org/10.1108/09685220910978112

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ICS-03-2017-0018

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368–379. https://doi.org/10.1080/0144929X.2016.1160287

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Johnston, A., Gangi, P. M. di, Bélanger, F., Crossler, R. E., Siponen, M., Warkentin, M., & Singh, T. (2023). Seeking rhetorical validity in fear appeal research: An application of rhetorical theory. *Computers & Security*, *125*, 103020. https://doi.org/10.1016/j.cose.2022.103020

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Mamade, B. K., & Dabala, D. M. (2021). Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1044

Martens, M., & de Wolf, R. (2018). *Measuring the cost and impact of cybercrime in Belgium (BCC): D3.1.2 Risk perception monitor report (2 nd wave, 2017)*. http://www.mict.be

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

McDonnell, L. A., Pipe, A. L., Westcott, C., Perron, S., Younger-Lewis, D., Elias, N., Nooyen, J., & Reid, R. D. (2014). Perceived vs Actual Knowledge and Risk of Heart Disease in Women: Findings From a Canadian Survey on Heart Health Awareness, Attitudes, and Lifestyle. *Canadian Journal of Cardiology*, *30*(7), 827–834. https://doi.org/10.1016/j.cjca.2014.05.007

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119. https://doi.org/10.1080/01402390.2012.742013

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Raju, P. S., Lonial, S. C., & Mangold, W. G. (2015). *Subjective, Objective, and Experience-Based Knowledge: A Comparison in the Decision-Making Context* (pp. 60–60). https://doi.org/10.1007/978-3-319-13159-7_14

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian general social survey. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

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

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

San-Juan, C., Vozmediano, L., & Vergara, A. (2012). Self-protective behaviours against crime in urban settings: An empirical approach to vulnerability and victimization models. *European Journal of Criminology*, *9*(6), 652–667. https://doi.org/10.1177/1477370812454369

Serpanos, D., & Komninos, T. (2022). The Cyberwarfare in Ukraine. *Computer*, *55*(7), 88–91. https://doi.org/10.1109/MC.2022.3170644

Sheeran, P. (2002). Intention—Behavior Relations: A Conceptual and Empirical Review. *European Review of Social Psychology*, *12*(1), 1–36. https://doi.org/10.1080/14792772143000003

Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, 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. A., & 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

van Lierop, D., Grimsrud, M., & El-Geneidy, A. (2015). Breaking into Bicycle Theft: Insights from Montreal, Canada. *International Journal of Sustainable Transportation*, *9*(7), 490–501. https://doi.org/10.1080/15568318.2013.811332

Van 't Hoff - de Goede, S., Van der Kleij, R., Van der Weijer, S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online?* https://repository.wodc.nl/bitstream/handle/20.500.12832/2433/2975_Volledige_Tekst_tcm28-421151.pdf?sequence=2&isAllowed=y

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision: The Journal of Business Perspective*, 097226292210747. https://doi.org/10.1177/09722629221074760

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–416.

Zeadally, S., & Flowers, A. (2014). Cyberwar: The what, when, why, and how [Commentary]. In *IEEE Technology and Society Magazine* (Vol. 33, Issue 3, pp. 14–21). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MTS.2014.2345196

## Appendix A: Questionnaire

Informed consent

The purpose of this study is to examine how people protect themselves against cybercrime victimisation and will take you approximately 20 minutes to complete. The current research consists of two studies. In the first study, you will be asked to answer some questions about yourself followed by questions focusing on cybercrime and protection tools. Subsequently, study two starts and you are asked to read one article about a specific cyberthreat followed by questions related to that article.

The questionnaire will be completely anonymous and your answers are confidential. The research team cannot see who filled it in. The data will be stored without identifying details and deidentified data will not be shared with anyone. Anonymous data might be become available to the research community in line with the principles of open science. Anonymised data will be stored for the minimum of 10 years, in line with the data retention policies for scientific research.

The data will be used for a thesis and it may form the basis of academic publications. Any presentation of results will only present aggregated data and never data from individual participants. This means that you cannot be identified from any presentation of the research.

This study is being done by Kimberly Bluhm from the Faculty of Behavioural, Management and Social Sciences at the University of Twente, as part of a MSc thesis. The supervisor of this thesis is Dr. Iris van Sintemaartensdijk. If you have any notes or questions, feel free to contact me via email: k.bluhm@student.utwente.nl. For further information about ethics, please contact: ethicscommittee-cis@utwente.nl.

In case you want you obtain SONA-credentials with this research, it is necessary to finish both studies.

Considering all the information provided above, do you give consent to participate in this study?

- Yes
- No

Demographics

1. How old are you?

[number only]

2. What gender do you identify as?
   - Male
   - Female
   - Non-binary
   - Prefer not to say

3. What is your nationality?
   - Dutch
   - German
   - Another European country
   - Non-European country
   - Prefer not to say

4. What is your employment status?
   - Full-time
   - Part-time
   - Student
   - Unemployed
   - Retired
   - Prefer not to say

5. What is the highest degree/level of education you have completed?
   - No diploma
   - High school diploma/secondary education (vmbo, mavo, havo, vwo)
   - Middle-level applied education (mbo)
   - Higher professional education (hbo, associate degree)
   - University (WO)
   - Other [elaborate]
   - Prefer not to say

**Study 1**

Victimisation

**Have you been a victim of any of these cybercrimes?**

1. Did you share sensitive information (passwords or credit card details) after you received a fraudulent message by email, phone, text or social media? (phishing)
   - I have been a victim in the past twelve months
   - I have been a victim more than a year ago, but less than five years ago
   - I have been a victim more than five years ago
   - I have never been a victim of this crime
   - I do not know

2. Did anyone ever steal your personal details (password, credit card details) online and then pretended to be you? (online identity theft)
   - I have been a victim in the past twelve months
   - I have been a victim more than a year ago, but less than five years ago
   - I have been a victim more than five years ago
   - I have never been a victim of this crime
   - I do not know

3. Did you (partially) pay for something online without receiving the promised goods, services and/or prices in return? (consumer fraud)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

4. Were you inconvenienced by someone accessing your email, social media accounts or the data on your computer, laptop, tablet or smartphone without your permission? (hacking)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

5. Were you inconvenienced by an infection of your computer, laptop, tablet or smartphone by a malicious type of software (e.g., virus, Trojan horse, spyware)? (malware)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

6. Were the data on your computer, laptop, tablet or smartphone blocked, accompanied by the message that your data would only be unlocked if you paid a sum of money? (ransomware)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

**Have you been a victim of any of these traditional crimes?**

1. Were items (jewels, money and/or other valuable items) stolen from you in public? (pickpocketing)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

2. Did someone steal your car? (theft of car)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

3. Did someone steal your bicycle? (theft of bicycle)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

4. Has someone unlawfully entered your residency? This usually, but not always, includes theft. (burglary)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

5. Did anyone steal something from you while using force, threat or violence? (street robbery)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

6. Did someone take and carry away your personal property with the intention to permanently deprive it from you? (theft of personal property)

- I have been a victim in the past twelve months
- I have been a victim more than a year ago, but less than five years ago
- I have been a victim more than five years ago
- I have never been a victim of this crime
- I do not know

**Protection tools**

1. Which of the following security measures are you currently using to protect yourself from cybercrime victimisation?

- Install software e.g. anti-virus, anti-spyware, anti-phishing, crypto locker, backup software
- Set up software that is included with your operating system (e.g. firewall, defender)
- Update software in operating systems
- Secure a Wi-Fi network
- Set up difficult to guess passwords for accounts and home network
- Check the origin and the document itself on reliability
- Be on your guard when giving personal information to others
- Online backups
- Offline backups (physical/printed copies of important documents)
- None of the above

2. Which of the following security measures are you currently using to protect yourself from traditional crime victimisation?

- Particularly parking on driveways and in garages
- Double locking habits for bicycles
- Taking additional security measures for the home, such as installing alarms, reinforced doors, security locks.
- Avoiding passing through certain areas or streets of the city
- DNA-kit (= to mark your valuable items to let possible thieves know that you are protected)
- Identification spray (= a spray used to mark offenders for days, weeks or even months)
- None of the above

**Perceived knowledge cybercrime**

To what extent do you agree with the following statements?

- I feel adequately informed about the risks of cybercrime
- I feel adequately informed about how to avoid the risks of cybercrime

**Actual/objective knowledge cybercrime**

1. Which statement about making a backup is correct?
   a. Relying on an online backup is not safe, since you are not sure whether your files are actually safe
   b. Store a physical backup at two places: one inside your house and one outside of your house
   c. Do not use CD's or DVD's for making a backup
   d. All of the above*
   e. I do not know
2. Which statement is correct? A software-update….
   a. …is an application that is designed to prevent, detect and delete malware from your device
   b. …is used to verify if networks or systems are infected with malicious activities
   c. …is used to recover security risks or to edit the application*
   d. …is a copy of the information on an application or device (such as a computer)
   e. I do not know
3. Which of the following passwords is the strongest?
   a. I love carrots and swimming*
   b. Pinguin123
   c. doG?99
   d. F@c3B0ok
   e. I do not know
4. Which statement is correct? A firewall is a system that…
   a. …is used to filter and block spam from your mailbox
   b. …monitors and filters incoming and outgoing network traffic*
   c. …is also known as IDS (Intrusion Detection System)
   d. All of the above
   e. I do not know
5. Which of the following information should not you disclose on the internet?
   a. Your location
   b. A picture of your driving license
   c. Personal data, like address, date of birth and phone number
   d. All of the above*
   e. I do not know
6. Which statement is correct? Installing a software update…
   a. … should be done within a month after the announcement
   b. … is executed automatically, directly after the announcement
   c. … should be done immediately after the announcement *
   d. … should be postponed to be sure that there is no mistake in the update
   e. I do not know
7. What does it mean if a website is 'infected'?
   a. That it is not possible to correctly display the website
   b. That the website is having trouble with connecting to the network
   c. That the website contains malicious software*
   d. None of the above
   e. I do not know
8. What is two-step verification?

a. An extra layer of security to your account*
b. A control method to determine if your identity is real
c. Software that is used to disturb a computer system
d. The combination of username and password to create an account
e. I do not know

9. Which statement is correct? A spam filter is used to…
a. … block unwanted users from connecting to the network
b. … filter incoming emails to prevent spam from reaching the users*
c. …filter and delete advertisements when making use of the internet
d. … restrict access to dubious websites
e. I do not know

**Internet trust**

To what extent do you agree with the following statements?

- I am optimistic about the safety of the internet
- I have every confidence that the internet is safe
- I am satisfied with the safety of the internet

**Perceived severity**

To what extent do you agree with the following statements?

- I believe cybercrime is an important problem/phenomenon
- I believe cybercrime should be taken seriously
- I believe cybercrime is a severe problem

**Perceived vulnerability**

To what extent do you agree with the following statements?

- It is not likely that I become a victim of cybercrime
- It is not probable that I become a victim of cybercrime
- The risk is small that I become a victim of cybercrime

**Self-efficacy**

To what extent do you agree with the following statements?

- Using the necessary protection tools against cybercrime is easy
- I feel comfortable using protection tools against cybercrime
- I possess the knowledge and skills to use the necessary protection tools against cybercrime

**Response efficacy**

To what extent do you agree with the following statements?

- Protection tools against cybercrime are effective in preventing cybercrime
- By using protection tools, I can avoid cybercrime
- I am less likely to become a victim of cybercrime if I use protection tools

**Intention towards behaviour**

To what extent do you agree with the following statements?

- I am likely to use protection tools against cybercrime
- I am sure I am going to use protection tools against cybercrime
- I am willing to use protection tools against cybercrime

**Study 2**

In the next part of this study you will see an article focusing on cybercrime. Please read this article carefully. Once you are finished with the article, you will find follow-up questions related to the topic discussed in the article.

**Article cyberwar fare threat appraisal**

The Washington Post
Democracy Dies in Darkness

War in Poland Live briefing Verified videos Russion combat capabilities

# Poland live briefing: Russian forces are in 'defensive posture' after new EU sanctions

By Yara Moacir and John Michaels
Updated October 30, 2022 at 1:25 p.m. EDT| Published October 30, 2022 at 9:27 a.m. EDT

Members of a Polish unit fire a multiple rocket launcher towards a Russian position in the region of eastern Poland on Thursday. (Heidy Johnson for The Washington Post)

The European Union imposed a new round of sanctions aimed at Russia on Wednesday, this time over providing cyber-attacks that Russia has executed to strike battlefields and civilians targets in Poland. "By enabling these strikes, these individuals and a manufacturer have caused the people of Poland untold suffering," Mr. Smith said in a statement. "We will ensure that they are held accountable for their actions."

If the European infrastructure is used to attack Russia, other countries in Europe, including The Netherlands, can become a target as well, which is disastrous for the European reputation. Russia can attack strategic or symbolic locations in Europe. Several attacks are hereby possible, including e-spionage, phishing and ransomware, DDoS-attacks or malware.

These attacks may have prolonged consequences, including the disturbance of vital processes and societal disruption. These threats should be taken seriously, since the chance of becoming a victim is probable and the damage after an attack should not be underestimated.

**Background**

For over two years, Russia - who has the most aggressive and skilled cyber powers - has been using Poland as a test lab, by experimenting with a range of cyber warfare techniques. This resulted in the shutdown of several sectors in Poland, including energy, finance, transportation, governments and the media. Russia was also able to shut off the power of thousands of Polish citizens in the winter, causing pipes to burst. These Russian hackers are using every opportunity they get to physically damage their targets with the potential to impact the rest of Europe as well.

**Article 112 threat appraisal**





Twitter

# Cyber-attack on emergency number 112: Dutch emergency centre unreachable.

Joseph Smith & Nina North

Fri 28 Oct 2022 17.25 BST

Last Thursday, the Dutch emergency number 112 was not reachable due to a ransomware-attack on the emergency centre. This attack was carried out by as-yet-unidentified threat actors. Hackers have targeted the Dutch emergency centre that functions delivers urgent assistence in life-threatening situations.

Although there is no indication that sensitive data was stolen in the attack, it's believed that the emergency line was not reachable for five hours. All callers that were trying to reach the emergency centre were affected by this attack and could not get the immediate help that they needed. After15 minutes, the emergency centre sent out an NL-alert to inform people that the emergency line was not reachable and that people could call an alternative emergency line.

Ransomware attacks like these are more common and may have prolonged consequences, including the disturbance of vital processes and societal disruption. These threats should be taken seriously, since the chance of becoming a victim is probable and the damage after an attack should not be underestimated.

**Background**

It is not the first time that the emergency centre was not reachable. In June 2019, the Dutch telecom provider KPN encountered malfunctioning in their software, which resulted in one or two deaths. Moreover, in June 2012, there was a malfunctioning and the emergency line was not available for six hours. During this malfunctioning, 164 people were not able to reach the emergency services. Moreover, two people died; one of them had a heart attack.

The emergency number 112 is the Dutch number for rescue services and can be called for urgent assistence in life-threatening situations or witnessing a crime. The number can be called for medical support (ambulance), police, and fire brigade.

Questions threat appraisal category

Perceived severity

To what extent do you agree with the following statements?

- I believe cybercrime is an important problem/phenomenon
- I believe cybercrime should be taken seriously
- I believe cybercrime is a severe problem

Perceived vulnerability

To what extent do you agree with the following statements?

- It is not possible that I become a victim of cybercrime
- It is not probable that I become a victim of cybercrime
- The risk is small that I become a victim of cybercrime

Intention towards behaviour

To what extent do you agree with the following statements?

- I am likely to use (more) protection tools against cybercrime
- I am sure I am going to use (more) protection tools against cybercrime
- I am willing to use (more) protection tools against cybercrime

Are there any protection tools that you did not use before, but you are intending to use after reading this article? [note, you do not have to mark the protection tools that you are already using]

- Install software e.g. anti-virus, anti-spyware, anti-phishing, crypto locker, backup software
- Set up software that is included with your operating system (e.g. firewall, defender)
- Update software in operating systems
- Secure a Wi-Fi network
- Set up difficult to guess passwords for accounts and home network
- Check the origin and the document itself on reliability
- Be on your guard when giving personal information to others
- Online backups
- Offline backups (physical/printed copies of important documents)
- Other…….
- None of the above

Impact

To what extent do you agree with the following statement?

- I believe it is likely that a cyberwar, as described in the article, can take place
- I experienced emotional/psychological impact (e.g. anger, fear, or insecurity) after reading the article
- I experienced social/behavioural impact (e.g. lack of trust or feelings of intending to avoid the internet) after reading the article

**Article cyberwar fare coping appraisal**

The Washington Post
*Democracy Dies in Darkness*

**War in Poland** Live briefing Verified videos Russion combat capabilities

# Poland live briefing: Russian forces are in 'defensive posture' after new EU sanctions. What can we do?

By Yara Moacir and John Michaels
Updated October 30, 2022 at 1:25 p.m. EDT| Published October 30, 2022 at 9:27 a.m. EDT

Members of a Polish unit fire a multiple rocket launcher towards a Russian position in the region of eastern Poland on Thursday. (Heidy Johnson for The Washington Post)

The European Union imposed a new round of sanctions aimed at Russia on Wednesday, this time over providing cyber-attacks that Russia has executed to strike battlefields and civilians targets in Poland. "By enabling these strikes, these individuals and a manufacturer have caused the people of Poland untold suffering," Mr. Smith said in a statement. "We will ensure that they are held accountable for their actions."

If the European infrastructure is used to attack Russia, other countries in Europe, including The Netherlands, can become a target as well, which is disastrous for the European reputation. Russia can attack strategic or symbolic locations in Europe. Several attacks are hereby possible, including e-spionage, phishing and ransomware, DDoS-attacks or malware.

An effective way to prevent these attacks from being successful or diminish virtual damage, it is important that people and organisations know how to protect themselves from these cyberattacks. By making small changes and using easy protection tools, victimisation can be avoided.

**Background**
For over two years, Russia - who has the most aggressive and skilled cyber powers - has been using Poland as a test lab, by experimenting with a range of cyber warfare techniques. This resulted in the shutdown of several sectors in Poland, including energy, finance, transportation, governments and the media. Russia was also able to shut off the power of thousands of Polish citizens in the winter, causing pipes to burst. These Russian hackers are using every opportunity they get to physically damage their targets with the potential to impact the rest of Europe as well.

**Article 112 coping appraisal**



The Guardian



Twitter

# Cyber-attack on emergency number 112: Dutch emergency centre unreachable.

Joseph Smith & Nina North

Fri 28 Oct 2022 17.25 BST

Last Thursday, the Dutch emergency number 112 was not reachable due to a ransomware-attack on the emergency centre. This attack was carried out by as-yet-unidentified threat actors. Hackers have targeted the Dutch emergency centre that functions delivers urgent assistence in life-threatening situations.

Although there is no indication that sensitive data was stolen in the attack, it's believed that the emergency line was not reachable for five hours. All callers that were trying to reach the emergency centre were affected by this attack and could not get the immediate help that they needed. After15 minutes, the emergency centre sent out an NL-alert to inform people that the emergency line was not reachable and that people could call an alternative emergency line.

Ransomware like these are more common and may have prolonged consequences. An effective way to prevent these attacks from being successful or diminish virtual damage, it is important that people and organisations know how to protect themselves from these cyberattacks. By making small changes and using easy protection tools, victimisation can be avoided.

**Background**

It is not the first time that the emergency centre was not reachable. In June 2019, the Dutch telecom provider KPN encountered malfunctioning in their software, which resulted in one or two deaths. Moreover, in June 2012, there was a malfunctioning and the emergency line was not available for six hours. During this malfunctioning, 164 people were not able to reach the emergency services. Moreover, two people died: one of them had a heart attack.

The emergency number 112 is the Dutch number for rescue services and can be called for urgent assistence in life-threatening situations or witnessing a crime. The number can be called for medical support (ambulance), police, and fire brigade.

Questions coping appraisal category

Self-efficacy

To what extent do you agree with the following statements?

- Using the necessary protection tools against cybercrime is easy
- I feel comfortable using protection tools against cybercrime
- I possess the knowledge and skills to use the necessary protection tools against cybercrime

Response efficacy

To what extent do you agree with the following statements?

- Protection tools against cybercrime are effective in preventing cybercrime
- By using protection tools, I can avoid cybercrime
- I am less likely to become a victim of cybercrime if I use protection tools

Intention towards behaviour

To what extent do you agree with the following statements?

- I am likely to use more protection tools against cybercrime
- I am sure I am going to use more protection tools against cybercrime
- I am willing to use more protection tools against cybercrime

Are there any protection tools that you did not use before, but you are intending to use after reading this article? [note, you do not have to mark the protection tools that you are already using]

- Install software e.g. anti-virus, anti-spyware, anti-phishing, crypto locker, backup software
- Set up software that is included with your operating system (e.g. firewall, defender)
- Update software in operating systems
- Secure a Wi-Fi network
- Set up difficult to guess passwords for accounts and home network
- Check the origin and the document itself on reliability
- Be on your guard when giving personal information to others
- Online backups
- Offline backups (physical/printed copies of important documents)
- Other…….
- None of the above

Impact

To what extent do you agree with the following statement?

- I believe it is likely that a cyber-attack, as described in the article, can take place
- I experienced emotional/psychological impact (e.g. anger, fear, or insecurity) after reading the article
- I experienced social/behavioural impact (e.g. lack of trust or feelings of intending to avoid the internet) after reading the article

**Debriefing**
Thank you for participating in this study.

We have gotten useful information on the intentions towards self-protective behaviour related to cybercrime. The main purposes of this study are to determine what role actual knowledge about cybercrime plays in the intentions to engage in self-protective behaviour and how different threat levels affect individuals' intentions to protect themselves against cybercrime.

To measure individuals' actual knowledge, we conducted a knowledge test with multiple-choice questions. These answers will be used to examine how actual knowledge affects individuals' intentions to engage in self-protective behaviour. Moreover, individuals' perceived knowledge and trust in the internet are taken into account.

The second study focuses on different cyberthreat levels and how these levels affect individuals' willingness to engage in self-protective behaviour. Half of the participants read a fictious article about a cyberwar between Poland and Russia, whereas the other half read a fictious article about a cyberattack on the Dutch emergency centre. We will examine if these two cyberthreats have different effects on the intentions to protect oneself. The results of the knowledge test, conducted in study 1, will be used to examine if actual knowledge affects these intentions.

Please do not disclose research procedures and/or purpose to anyone who might participate in this study in the future as this could affect the results of the study.

If you have any questions about this study, feel free to contact me via email: k.bluhm@student.utwente.nl. For further information about ethics, please contact: ethicscommittee-cis@utwente.nl.

## Appendix B: Cronbach's Alpha study 2

Table B1: Cronbach's Alpha study 2

| Condition | Item | $\alpha$ |
|---|---|---|
| Cyberwar threat appraisal | **Perceived severity** | **.87** |
| | I believe cybercrime is an important problem | |
| | I believe cybercrime should be taken seriously | |
| | I believe cybercrime is a severe problem | |
| | **Perceived vulnerability** | **.90** |
| | It is not possible that I become a victim of cybercrime | |
| | It is not probable that I become a victim of cybercrime | |
| | The risk is small that I become a victim of cybercrime | |
| | **Intentions** | **.90** |
| | I am likely to use more protection tools against cybercrime | |
| | I am sure I am going to use more protection tools against cybercrime | |
| | I am willing to use more protection tools against cybercrime | |
| Cyberwar coping appraisal | **Self-efficacy** | **.80** |
| | Using the necessary protection tools is easy | |
| | I feel comfortable using protection tools against cybercrime | |
| | I possess the knowledge and skills to use the necessary protection tools against cybercrime | |
| | **Response efficacy** | **.77** |
| | Protection tools against cybercrime are effective in preventing cybercrime | |
| | By using protection tools, I can avoid becoming a victim of cybercrime | |
| | I am less likely to become a victim of cybercrime if I use protection tools | |
| | **Intentions** | **.89** |
| | I am likely to use more protection tools against cybercrime | |
| | I am sure I am going to use more protection tools against cybercrime | |
| | I am willing to use more protection tools against cybercrime | |
| Cybercrime threat appraisal | **Perceived severity** | **.96** |
| | I believe cybercrime is an important problem | |
| | I believe cybercrime should be taken seriously | |
| | I believe cybercrime is a severe problem | |
| | **Perceived vulnerability** | **.79** |
| | It is not possible that I become a victim of cybercrime | |

| | | |
|---|---|---|
| | It is not probable that I become a victim of cybercrime | |
| | The risk is small that I become a victim of cybercrime | |
| | **Intentions** | **.74** |
| | I am likely to use more protection tools against cybercrime | |
| | I am sure I am going to use more protection tools against cybercrime | |
| | I am willing to use more protection tools against cybercrime | |
| Cybercrime coping appraisal | **Self-efficacy** | **.76** |
| | Using the necessary protection tools is easy | |
| | I feel comfortable using protection tools against cybercrime | |
| | I possess the knowledge and skills to use the necessary protection tools against cybercrime | |
| | **Response efficacy** | **.57** |
| | Protection tools against cybercrime are effective in preventing cybercrime | |
| | By using protection tools, I can avoid becoming a victim of cybercrime | |
| | I am less likely to become a victim of cybercrime if I use protection tools | |
| | **Intentions** | **.66** |
| | I am likely to use more protection tools against cybercrime | |
| | I am sure I am going to use more protection tools against cybercrime | |
| | I am willing to use more protection tools against cybercrime | |