What We Think We Know About Cybersecurity: An Investigation of the Relationship between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context

De Kimpe, L., Walrave, M., Verdegem, P. and Ponnet, K.

This is an accepted manuscript of an article published by Taylor & Francis in Behaviour & Information Technology, DOI: 10.1080/0144929X.2021.1905066.

The final definitive version is available online:

https://doi.org/10.1080/0144929X.2021.1905066

What We Think We Know About Cybersecurity: An Investigation of the Relationship between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context

Lies De Kimpe [a]

lies.dekimpe@uantwerpen.be

Michel Walrave [a]

michel.walrave@uantwerpen.be

Pieter Verdegem [b]

p.verdegem@westminster.ac.uk

Koen Ponnet [a,c*]

koen.ponnet@ugent.be

[a] Department of Communication Studies, University of Antwerp, Sint-Jacobsstraat 2, 2000 Antwerp, Belgium

[b] Communication and Media Research Institute (CAMRI), University of Westminster, Watford Road, Northwick Park, Middlesex HA1 3TP, UK.

[c] Department of Communication Studies, imec-mict-Ghent University, Korte Meer 11, 9000 Ghent, Belgium

*corresponding author

Abstract

Individual internet users are commonly considered the weakest links in the cybersecurity chain. One reason for this is that they tend to be overoptimistic regarding their own online safety. To gain a better understanding of the cognitive processes involved in this assessment, the current study applies an extended version of the protection motivation theory. More specifically, this study includes perceived knowledge and internet trust to discover how these antecedents influence the threat and coping appraisal processes. Based on representative survey data collected from 967 respondents, we found that people who feel well-informed about online safety feel less vulnerable to cybercrime and are less inclined to take security measures. At the same time, feeling informed is associated with being more convinced of the severity of cybercrime. High levels of trust in the safety of the internet are linked to the feeling that one is less vulnerable to cybercrime and the perception that cybercrime is not a severe threat. Future interventions should remind internet users about their own perceived vulnerability and the risks that exist online while ensuring that internet users do not lose their trust in the internet and confidence in their own online knowledge.

Keywords: Protection motivation theory; Cybercrime; Optimism bias; Perceived knowledge; Internet trust

1. Introduction

In today's digitized society, internet users are increasingly confronted with cybercrime. In 2017, at least 42% of European internet users indicated they had been the victim of a certain type of cybercrime, such as online consumer fraud (16%) or malware infection (42%) (Eurobarometer, 2017). In 2018, one in twelve Dutch internet users were victims of cybercrime (Statistics Netherlands, 2019). A similar proportion of cybercrime victims was found among Belgian internet users (Belgian Federal Police, 2019). These experiences can have a myriad of negative financial and emotional effects on victims (e.g., Jansen & Leukfeldt, 2018; Kaakinen et al., 2018; Modic & Anderson, 2015).

Even though no consensus exists about the exact definition of cybercrime, the term is usually applied to refer to two types of incidents: cyber-enabled/computer-assisted crimes, and cyber-dependent/computer-focused crimes (e.g., Cross, 2019; Holt & Bossler, 2016; McGuire & Dowling, 2013). The former category refers to crimes that already have an offline equivalent (e.g., fraud, identity theft), and where the online environment offers additional ways for perpetrators to approach their targets. The latter category represents new forms of crime that depend on the online infrastructure and technology to reach their goal (e.g., malware, DDoS attacks). It is particularly important to focus on ways to better protect individual users against these criminal activities, as the end user has often been identified as one of the weakest links in the cybersecurity chain (Abawajy, 2014; Dodel & Mesch, 2019; Europol, 2016; Wordsworth, 2017). One reason for this is that internet users have a tendency to be overoptimistic regarding their own online safety (Campbell et al., 2007; Cho et al., 2010; Wash & Rader, 2015), which results in people actually performing fewer security behaviors (Cain et al., 2018). However, internet users keep engaging in online risk behaviors (Campbell et al., 2007; Whitty et al., 2015). So far, we have little insight into

the way feelings of overoptimism are intertwined with the cognitive processes involved in determining intention to take protective measures against cybercrime. Studying these processes would provide insights that can help us to guide users into acting in their own best interests.

To achieve this goal, an extended framework based on the protection motivation theory (PMT; Rogers, 1975) will be applied. In previous studies, the PMT has proven to be a valuable framework to study the cognitive processes that take place when individuals are confronted with a threat in a cybercrime context (e.g., Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Herath & Rao, 2009; Lee & Larsen, 2009; Tsai et al., 2016). However, the antecedents of these processes have rarely been investigated. Therefore, the current study will extend the PMT by taking into account two trust-related variables that are particularly relevant when exploring the processes that trigger overoptimism. More specifically, the current study will consider to what extent people (1) trust the safety of the internet (i.e., internet trust), and (2) believe they have enough knowledge about online risks and security measures (i.e., perceived knowledge). This study will take into account how these two dimensions are related to coping appraisal and threat appraisal processes identified by the PMT. To the best of our knowledge, previous cyber security research has not considered antecedents of these two processes yet. This approach will provide useful information about the way threat appraisal and coping appraisal can be influenced by intrapersonal processes and how these could result into attitudes towards online safety that are not always rational.

2. The protection motivation theory

At its core, the PMT states that two cognitive processes influence people's protection motivation (i.e., the intention to perform a recommended action or behavior): threat appraisal and coping appraisal (Norman et al., 2005). Threat appraisal is a cognitive process that evaluates how serious

a specific risk is. It takes into account the general *severity* of a risk as perceived by the individual and the perceived *vulnerability* or susceptibility of the individual to that specific risk. Coping appraisal focuses on one's ability to cope with or prevent the risk in question (Rippetoe & Rogers, 1987). First, it includes an assessment of the effectiveness of the recommended countermeasure(s) in tackling the threat, which is called *response-efficacy*. Moreover, *self-efficacy* is evaluated, which is the belief that one is capable of performing the required actions to reduce the threat (Norman et al., 2005). According to Rogers (1983), both appraisals can be initiated by several sources of information or antecedents, such as observational learning, personality variables, or prior experience with the threat. The outcome of the appraisal processes is the intention to initiate, maintain, or refrain from coping behaviors (Floyd et al., 2000).

The original PMT has been adapted and extended by other authors to move beyond its cognitive focus (Nabi et al., 2008). For example, Witte (1992) developed the extended parallel process model (EPPM), which acknowledges the importance of negative emotional arousal (Wang, Li, & Rao, 2017). The EPPM makes a distinction between a *danger control process* and a *fear control process*. The former is triggered when perceived threat and efficacy are high enough to prompt adaptive reactions, while the fear control process is activated when perceived threat is high but not met with sufficient perceived efficacy. This results in more maladaptive coping strategies. Another extension of the PMT proposed in recent years is the technology threat avoidance theory (TTAT) (Liang & Xue, 2010). This framework was designed specifically to study technology-related threats. Like the EPPM, the TTAT stresses the possible maladaptive actions following a lack of perceived efficacy. Even though the added value of these theories should be acknowledged, they all include components offered by the PMT at its core. Given our focus on individual

cognitive antecedents of threat and coping appraisal, the PMT model is especially useful as a framework in the current study.

Specifically within the online environment, the PMT (Rogers, 1975, 1983) is one of the theoretical frameworks (among, e.g., routine activities theory, general theory of crime) that has already made a considerable contribution to the study of cybercrime. The strength of this framework lies in the possibility for scholars to gain a better understanding of the cognitive processes that determine intention to take protective measures against a threat (Ifinedo, 2012). This is a necessary focus, as perceptions about online threats and available coping strategies are considered to be the most important determinants of online protective behavior (Dodel & Mesch, 2017). Moreover, studying individuals' protection motivation in relation to cybercrime is especially pertinent, as for these types of cyber threats, individual actions can actually make a difference and improve online safety. Based on the acquired insights, suggestions can be made to improve communication strategies persuading internet users to take appropriate measures against cybercrime victimization.

Some studies have used the PMT framework to study specific online risks, such as online harassment (Lwin et al., 2012), malware infection (Dang-Pham & Pittayachawan, 2015), and privacy concerns (Youn, 2009). Others have applied a broader approach and looked more closely at internet users' general intention to implement security measures (Anderson & Agarwal, 2010) (e.g., Anderson & Agarwal, 2010; Hooper & Blunt, 2020; Ifinedo, 2012; Tsai et al., 2016). Crossler and Bélanger (2014), for example, used the PMT framework to test a unified security practices scale, which is a measure to examine the use of several security measures in one scale (e.g., automatic updates, strong passwords, security education, firewalls, browser safety) instead of using individual measures per security practice, as was often done in prior research. The study

provided evidence of the effectiveness of such an inclusive scale. Therefore, the current study will also opt for a more holistic approach and focus on perceptions towards cybercrime and online security measures in general instead of one specific type of crime or countermeasure. This makes sense, as several types of cybercrime are closely related (e.g., phishing can result in identity theft or hacking, malware infections can result in online fraud) and specific countermeasures often protect against more than one threat at once (e.g., the installation of a firewall can protect a computer against hacking, viruses, and spyware). Moreover, taking one specific measure is not sufficient to protect oneself against the range of risks one might encounter. A more inclusive approach is thus needed.

3. Antecedents of threat and coping appraisal

It should be noted that most studies on cybercrime and cybersecurity that use the PMT framework recognize the value of the theory, but also acknowledge the importance of extending the original framework and adapting it to the online environment by including one or several additional variables, such as exposure to media coverage on security (Anderson & Agarwal, 2010), experience with the internet (Anderson & Agarwal, 2010; Youn, 2009), prior experience with online threats (Anderson & Agarwal, 2010), digital safety skills (Dodel & Mesch, 2018, 2019), or knowledge (Youn, 2009). These studies illustrate that extending the PMT framework creates a better understanding of people's protection motivation. However, all of these studies have in common that they investigate how these additional variables influence intention or behavior. To create a deeper understanding of the cognitive processes that initiate protection motivation, it is also important to explore the antecedents of the appraisal processes. Up until now, these antecedents have rarely been studied in a cybersecurity context, even though this could greatly increase our understanding of the cognitive processes that take place when people are confronted

with online threats. To gain more insight into the overoptimistic tendencies of internet users, the present study will contribute to exploring valuable extensions of the original PMT by including two trust-related variables and considering them antecedents of the two appraisal processes. These two factors are *perceived knowledge* regarding online safety and *trust in the safety of the internet* (cf. figure 1). We will elaborate on this further in the hypotheses development.

4. Research model and hypotheses

This study applies the PMT to cybercrime and, more particularly, to the intention to take online security measures. In the context of our study, we perceive cybercrime as "any crime that is facilitated or committed using a computer, network or hardware device" (Gordon & Ford, 2006, p. 14). It entails several crimes, which can be presented on a continuum ranging from Type I cybercrimes, which are mostly technology-related (e.g., hacking, malware) to Type II cybercrimes, which are more human-related (e.g., cyberstalking). Given that different types of cybercrime and the according safety measures are closely intertwined, it makes sense to study cybercrime as a whole (Crossler & Bélanger, 2014). We will discuss our research model, as shown in figure 1, by first elaborating on threat appraisal and coping appraisal and consequently clarifying the hypothesized relationships between perceived knowledge, internet trust, and the PMT.

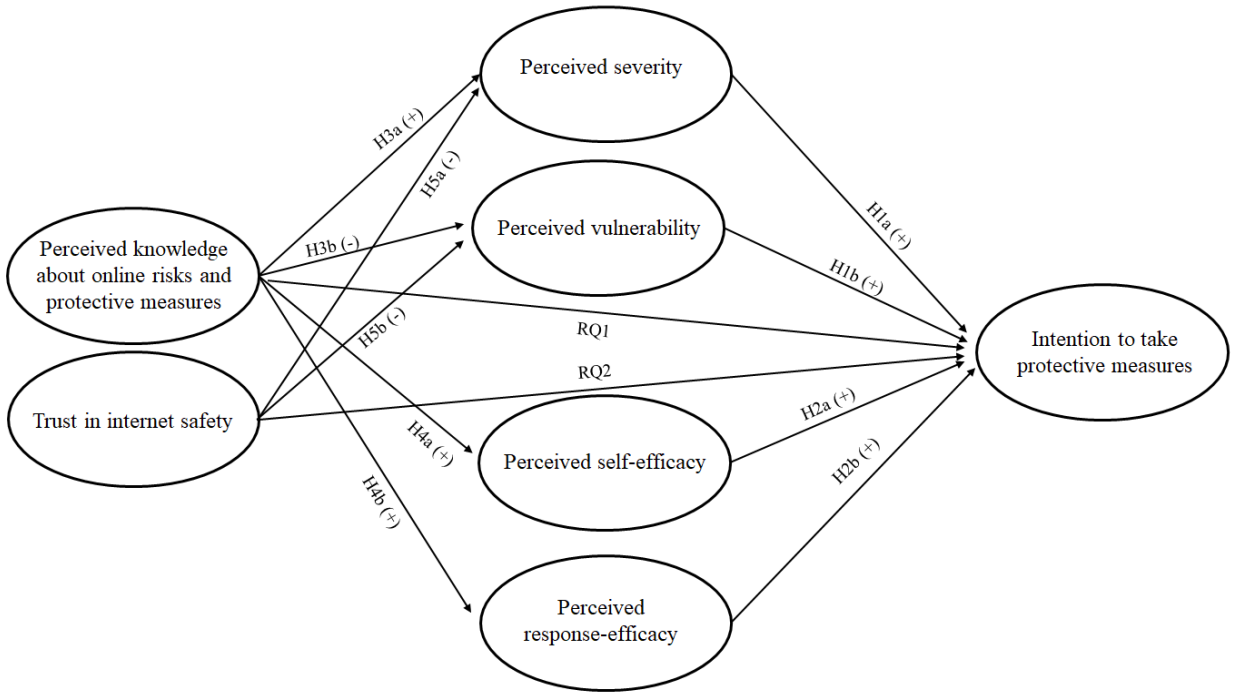

Figure 1 - Conceptual model of the extended PMT, applied on cybercrime

4.1. Threat appraisal

Threat appraisal is determined by perceived severity and perceived vulnerability. *Perceived severity* entails how serious the consequences of a certain event are perceived by an individual. Although a cybercrime incident might have severe implications for internet users and companies, individuals may assess the treat or the extent of the damage differently in terms of severity (Ng et al., 2009). Research shows that the perceived severity of malware threats increases internet users' motivation to perform malware avoidance behavior (Dang-Pham & Pittayachawan, 2015). This result is consistent with earlier findings from more general studies on cybersecurity. Anderson and Agarwal (2010) proved that being concerned about security threats resulted in a more positive attitude towards taking action, and a study by Crossler and Bélanger (2014) showed that perceived severity has a positive influence on implementing security practices. Based on these findings, we articulate the following hypothesis (H):

H1a: Perceived severity of cybercrime is positively related to the intention to take protective measures against cybercrime.

The second threat appraisal concept is *perceived vulnerability*, or a person's assessment of the probability of being confronted with threatening events, such as becoming a victim of cybercrime (Ifinedo, 2012). It is believed that individuals who perceive something as a threat often adapt their behaviors according to the level of risk they perceive (Ifinedo, 2012). More specifically, a more intense perceived threat increases the motivation to avoid the threat (Liang & Xue, 2010). In the case of e-mail safety, for example, perceived vulnerability to infected attachments has proven to be positively related to computer security behavior (Ng et al., 2009). Hence, we expect that perceived vulnerability to cybercrime will be related to protection motivation in a similar way. We hypothesize:

H1b: Perceived vulnerability is positively associated with the intention to take protective measures against cybercrime.

4.2. Coping appraisal

The second appraisal process assesses the countermeasures that can be taken against a threat. This assessment depends in part on how an individual evaluates their own abilities to perform the suggested behavior. *Self-efficacy* in the context of the current study refers to perceived skills or ability to perform online protective measures, such as installing antivirus software or changing passwords regularly. Previous studies have indicated that perceived self-efficacy is a useful predictor of individuals' online security behavior (Crossler & Bélanger, 2014; Ng et al., 2009) or intention to take protective measures (Dang-Pham & Pittayachawan, 2015; Hooper & Blunt, 2020; Ifinedo, 2012). Individuals who feel capable of performing a certain behavior thus appear to be

more likely to perform this particular behavior. With this reasoning in mind, the following hypothesis is articulated:

H2a: Perceived self-efficacy is positively related to the intention to take protective measures against cybercrime.

It is also important that the suggested measures are indeed perceived as effective in protecting internet users against online threats, which is referred to as *response-efficacy*. This will determine whether an individual applies the suggested behavior or not (Rippetoe & Rogers, 1987). Again, the relationship between perceived response-efficacy and intention has been established several times in the context of cybersecurity measures (Dang-Pham & Pittayachawan, 2015; Ifinedo, 2012; Lee & Larsen, 2009; Tsai et al., 2016). Hence, focusing on cybercrime measures, we expect:

H2b: Perceived response-efficacy will positively predict the intention to take protective measures against cybercrime.

4.3. Perceived knowledge and internet trust

The present study expands the core of the PMT by taking into account two trust-related antecedents that might influence the appraisal processes (Rippetoe & Rogers, 1987). The first of those two variables is self-perceived knowledge (i.e., what one thinks one knows), which can be considered a proxy of confidence in one's own knowledge. Perceived knowledge and actual knowledge on a specific topic do not necessarily coincide. They might overlap, but often do not, as people often overestimate what they actually know about a certain topic (Jensen et al., 2005). In particular, perceived knowledge (rather than actual knowledge) will be taken into account in the current study, as in comparison to actual, objective knowledge, it has proven to be a stronger

motivator in performing behaviors and a more important factor in understanding reactions to emotion-based persuasive messages (Eastman et al., 2002; Nabi et al., 2008).

According to a European study on attitudes toward cybersecurity, 51% of internet users feel rather uninformed about cybercrime, while 46% consider themselves well informed (Eurobarometer, 2017). There is thus a considerable proportion of European users with rather high perceived knowledge. However, perceived knowledge has received little attention in prior research on cybersecurity or in studies applying the PMT, even though this has proven to be an important concept in other contexts. For example, a study by Nabi et al. (2008) about breast or testicular self-examination stressed the importance of taking into account individual characteristics such as perceived knowledge, as they found that high perceived knowledge can constrain fear arousal. This might be explained by the fact that perceived knowledge reduces the amount of uncertainty one feels about a threat. We expect the same negative relationship between perceived knowledge and perceived vulnerability in an online context, as a previous study by Wash and Rader (2015) has shown that those people who feel like they are able to protect themselves actually feel less vulnerable online. In particular, people with higher education, and thus presumably more self-perceived knowledge, believe that online threats are less likely to target them. Consequently, we expect that internet users who feel highly informed about the internet and its risks perceive cybercrime as less of a personal threat.

In line with the unrealistic optimism effect, which states that people in various contexts believe that negative events are less likely to happen to them than to other people (Weinstein & Klein, 1996), we do believe that internet users with high perceived knowledge might acknowledge the general severity of cybercrime. Campbell and colleagues (2007) found that heavy internet users are more concerned with online risks than less experienced users, even though heavy users are

convinced that these events are less likely to happen to them. As a result, these findings suggest that feeling more knowledgeable might have a positive effect on perceived severity. Consequently, we hypothesize:

H3: Perceived knowledge is positively related to perceived severity (H3a) and negatively related to perceived vulnerability (H3b).

Perceived knowledge has been defined as a combination of knowledge and self-confidence (Raju et al., 2015). Consequently, (perceived) knowledge and self-efficacy are closely intertwined (Arachchilage & Love, 2014). Prior studies on privacy concerns have shown that those who are more knowledgeable about the subject, perceive greater control over their personal information (Youn, 2009), and knowledge on phishing risks proved to be positively related to perceived self-efficacy (Arachchilage & Love, 2014). Perceived knowledge is assumed to be equally important when studying perceived response-efficacy. To establish a degree of confidence in the efficiency of the security measures at hand, internet users first need to feel like they are well informed about the measures available. Therefore, perceived knowledge and the assessment of coping mechanisms are expected to be related in the following manner:

H4: Perceived knowledge is positively related to perceived self-efficacy (H4a) and response-efficacy (H4b).

The second variable included in the extended protection motivation framework to study its relation to the cognitive processing of threats is trust in the safety of the internet, which we will call *internet trust* in the remainder of this paper. Taking into account that (online) trust is a complex concept with no clear definition, we consider trust to be "the belief that the other party will behave in a socially responsible manner" (Pavlou, 2003, p. 106). In the context of internet trust, this

translates into the belief that the internet is safe and its users will act in a responsible manner (Wang & Emurian, 2005). Trust is believed to be the counterpart of perceived risk (Riek et al., 2014) and in fact reduces the amount of risk that is perceived (Pavlou, 2003). In performing risky online acts, such as online banking, trust alleviates existing uncertainty (Montazemi & Saremi, 2013). Trust is therefore expected to be negatively related to perceived severity of and perceived vulnerability to cybercrime. Meanwhile, we have no theoretical basis to assume that confidence in the safety of the internet is related to the way coping mechanisms are assessed. Consequently, we do not link internet trust to coping appraisal. In sum, we expect:

H5: Internet trust is negatively related to perceived severity of cybercrime (H5a) and perceived vulnerability to cybercrime (H5b).

So far, we have hypothesized that perceived knowledge and internet trust have an influence on intention via threat and coping appraisal. At the same time, it should be taken into consideration that these two antecedents might also have direct relationships with the intention to take protective measures. For example, it has been found that self-identified experts in the field perform less secure behaviors online compared to self-identified non-experts (Cain et al., 2018), which could indicate that perceived knowledge can lower people's intention to take the necessary measures. However, there is little research available on this specific matter. Therefore, we will explore the link between perceived knowledge, internet trust and intention without making predictions about their exact relationship. This results in two exploratory research questions (RQ):

RQ1: Is there a significant relationship between perceived knowledge and the intention to take protective measures?

RQ2: Is there a significant relationship between internet trust and the intention to take protective measures?"

5. Method

5.1. Data collection and sample

To test our model, data from the BCC project (Belgian Cost of Cybercrime) were used. In 2015, a link to an online survey was sent via e-mail to 6,670 panel members of the professional market research agency iVOX, who were representative of the Belgian population. After three weeks, 1,289 participants had filled out the survey, implicating a response rate of 19.33%. A total of 1,033 questionnaires were completely filled out. After omitting participants who did not pass the attention check (i.e., please respond with "totally agree") that was incorporated in the survey, 967 surveys were assessed as valid. Only these respondents were taken into account in further analyses.

Our sample is representative of the active Belgian internet population based on the distribution of gender, age, and residence. In total, the sample consists of 49.8% male (n = 482) and 50.2% female (n = 485) participants between the ages of 18 and 88 (M = 47.73; SD = 15.89). More than half of them (52.9%; n = 512) live in Flanders (the Dutch-speaking northern part of Belgium), 36.1% (n = 349) live in Wallonia (the French-speaking southern part of Belgium), and the remaining 11.0% (n = 106) reside in Brussels. Furthermore, 10.5% (n = 102) of the respondents have a master's or postgraduate degree, 21.4% (n = 207) have a bachelor's degree or a higher non-university degree, 41.0% (n = 396) have finished secondary school, 20.0% (n = 193) have completed the first three years of high school, and the remaining 7.1% (n = 69) have a primary school degree or no diploma. Focusing on the frequency of the internet use within the sample, a distinction was made between internet use at work, internet use at home during workdays and at home during the weekends. Of all respondents, 48.5% uses the internet at work less than weekly or never, while 18% uses the internet for more than three hours at work. When people are home during workdays, 2.9% of the sample uses the internet less than weekly or never, 48.2% between

one and three hours per day, and 28.4% is online for more than three hours per day. During weekends, 3.5% uses the online environment less than weekly or never, 41.5% between one and three hours per day, and 35.9% is online more than three hours per day.

5.2. Measures

The online survey contained questions on all PMT variables as well as items estimating self-declared trust in the safety of the internet and perceived knowledge about online risks and appropriate countermeasures. All items were presented using a five-point Likert scale ranging from 1 = "totally disagree" to 5 = "totally agree." Descriptive statistics for all variables and the exact formulation of all items can be found in table 1.

5.2.1. Perceived knowledge

Perceived knowledge has typically been measured by subjects' self-reports of their knowledge of a specific topic (Raju, 1995). Two items from the Eurobarometer (2013) were used to assess to what extent respondents believe they are well informed about online safety and risks (example item: "I feel adequately informed about the risks of the internet"). The internal reliability proved to be good ($\alpha = .82$).

5.2.2. Internet trust

Three items measured the level of confidence participants claimed to have in the safety of the internet (e.g., "I have every confidence that the internet is safe"). The wording of these items was based on De Jonge et al. (2007) and was adapted to the current research topic. Cronbach's alpha indicated this scale was reliable ($\alpha = .88$).

5.2.3. Protection motivation theory

All measures used for testing the PMT were based on validated measures derived from previous research and were adapted to the current research topic. The wording of the items used to estimate perceived severity, perceived vulnerability, and response-efficacy was based on the risk behavior diagnosis scale by Witte (1996). Moreover, a study by Anderson and Agarwal (2010) on online security behavior intentions of home computer users was used as inspiration for the formulation of the items estimating perceived self-efficacy and intention to take protective measures against cybercrime. Participants were told that protective measures are measures that one can take as an internet user to protect oneself against internet-related risks. Examples given were using anti-virus software, changing privacy settings, and using software that blocks pop-up windows. All constructs were measured using three items, except for perceived self-efficacy, which had a four-item measure. Based on the Cronbach's alpha of each construct, the scales measuring perceived vulnerability ($\alpha = .77$), perceived severity ($\alpha = .85$), perceived self-efficacy ($\alpha = .75$), and intention ($\alpha = .83$) can be considered reliable. For perceived response-efficacy ($\alpha = .64$), the internal reliability is somewhat low but still sufficient given that a three-item scale was used (Field, 2009).

5.2.4. Socio-demographic variables

Covariates of interest were age, gender (*male* (= 0*)* and *female* (= 1)) and educational level. To measure the highest educational attainment, respondents were offered six options: *no diploma* (= 1)*, primary school* (= 2), *lower secondary school* (= 3), *higher secondary school* (= 4), *bachelor or higher non-university degree (*= 5), and *master/(post-)graduate* (= 6).

5.3. Data analysis

We performed structural equation modeling (SEM) with the bootstrapping procedure using Mplus 7.4. (Muthén & Muthén, 2012) to study the relationship between threat and coping appraisal and intention, and to examine how the variables perceived knowledge and internet trust influenced

these appraisal processes and intention. We started by estimating a measurement model and investigating its fit, and then tested the structural model. To assess the fit of the models, multiple goodness-of-fit indices were consulted. First of all, the chi-square test was taken into account; however, since this test is sensitive to sample size, its value is almost always significant (Byrne, 2012). Therefore, the comparative fit index (CFI), Tucker-Lewis index (TLI), root mean square error of approximation (RMSEA), and standardized root mean squared residual (SRMR) were evaluated as well. The CFI ranges from 0 to 1.00; the closer to 1, the better the model fits. As a rule of thumb, .90 is often used as a cut-off value (Hu & Bentler, 1999). The TLI is interpreted in the same way, although this measure is more strict and includes a penalty for model complexity. The value of RMSEA should be kept as low as possible, with values below .08 representing a good fit and values up to .10 indicating a mediocre fit. The SRMR ranges from 0 to 1 and should be kept as low as possible (Byrne, 2012). A relatively good model fit is indicated when the SRMR is smaller than .08 (Hu & Bentler, 1999).

	M	SD	Factor loading (CFA)
Perceived knowledge	**3.23**	**.92**	
I feel adequately informed about the risks of the internet			.82
I feel adequately informed about how to avoid the risks of the internet			.85
Internet trust	**2.81**	**.84**	
I am optimistic about the safety of the internet			.82
I have every confidence that the internet is safe			.89
I am satisfied with the safety of the internet			.84
Perceived severity	**4.36**	**.61**	
I believe that cybercrime is significant			.75
I believe that cybercrime is serious			.85
I believe that cybercrime is severe			.84
Perceived vulnerability	**3.30**	**.71**	
It is possible that I will be a victim of cybercrime			.67
It is likely that I will be a victim of cybercrime			.84
There is a great risk that I'll be a victim of cybercrime			.70
Perceived self-efficacy	**3.40**	**.71**	
Taking the necessary security measures is entirely under my control			.66
Taking the necessary security measures is easy			.71
I feel comfortable taking security measures			.59
I have the knowledge and skills to take the necessary measures			.67
Perceived response-efficacy	**3.66**	**.62**	
Security measures are effective in preventing crime			.59
By taking security measures, I can prevent cybercrime			.68
If I take security measures, I am less likely to be a victim of cybercrime			.58
Intention	**3.47**	**.69**	
I am likely to take (more) security measures			.81
I am certain that I will take (more) security measures			.83
It is possible that I will take (more) security measures			.74
Age	**47.73**	**15.89**	
Educational level	**4.04**	**1.15**	

*Table 1***.** Descriptive statistics of all study variables (n = 967)

6. Results

6.1. Bivariate correlations

Table 2 displays the correlations between the study variables. Significant associations are found between all constructs of the PMT (i.e., perceived severity, perceived vulnerability, perceived self-efficacy, perceived response-efficacy and intention). Perceived knowledge and internet trust are significantly correlated, just as there is a significant association between perceived knowledge and vulnerability, self-efficacy, and response-efficacy. No significant correlation was found between perceived knowledge and perceived severity. Internet trust is significantly correlated with all appraisal constructs but not with intention. In addition, there is only a weak correlation between perceived knowledge and intention.

	KNO	**TRU**	**SEV**	**VUL**	**SEF**	**REF**	**INT**
KNO							
TRU	.51***						
SEV	-.03	-.19***					
VUL	-.22***	-.23***	.18***				
SEF	.49***	.32***	.10**	-.24***			
REF	.28***	.20***	.27***	-.10**	.54***		
INT	-.07*	-.04	.32***	.28***	.20***	.28***	

*Table 2***.** Pearson correlations between study variables.

* $p < .05$, ** $p < .01$ *** $p < .001$; SEV: perceived severity, VUL: perceived vulnerability, SEF: perceived self-efficacy, REF: perceived response-efficacy, INT: intention, KNO: Perceived knowledge, TRU: internet trust

6.2. Measurement model

The measurement model included assessments of the latent constructs—perceived knowledge, internet trust, perceived severity, perceived vulnerability, perceived self-efficacy, perceived response-efficacy, and intention. All factor loadings were significant and had a standardized value of .58 or higher. Based on the model fit information, we concluded a good fit with the data: χ^2 (168) = 685.65 ($p < .001$); RMSEA = .056 (CI: .052 - .061); CFI = .94; TLI = .93 and SRMR = .05. Subsequently, age, gender, and educational level were included in the model as control variables. Several significant associations with the sociodemographic variables considered were established. Age had a positive significant relationship with perceived severity (β = .20, SE = .03, $p < .001$) and perceived response-efficacy (β = .12, SE = .04, $p < .01$). Older internet users thus perceive cybercrime as more severe and online security measures as more effective than their younger counterparts. Gender was significantly related to perceived knowledge (β = - .10, SE = .04, $p < .01$), perceived vulnerability (β = - .11, SE = .04, $p < .01$), intention (β = .10, SE = .03, $p < .01$); male respondents have higher levels of perceived knowledge and perceived vulnerability than women, while the latter have a significantly stronger intention to take countermeasures than men. Last, educational level proved to be significantly related to internet trust (β = - .11, SE = .04, $p < .01$) and perceived self-efficacy (β = - .12, SE = .03, $p < .001$), implicating that internet users with a higher level of education trust the internet less and are less convinced that they have the skills necessary to implement countermeasures. The structural model below was adjusted for the effect of these covariates.

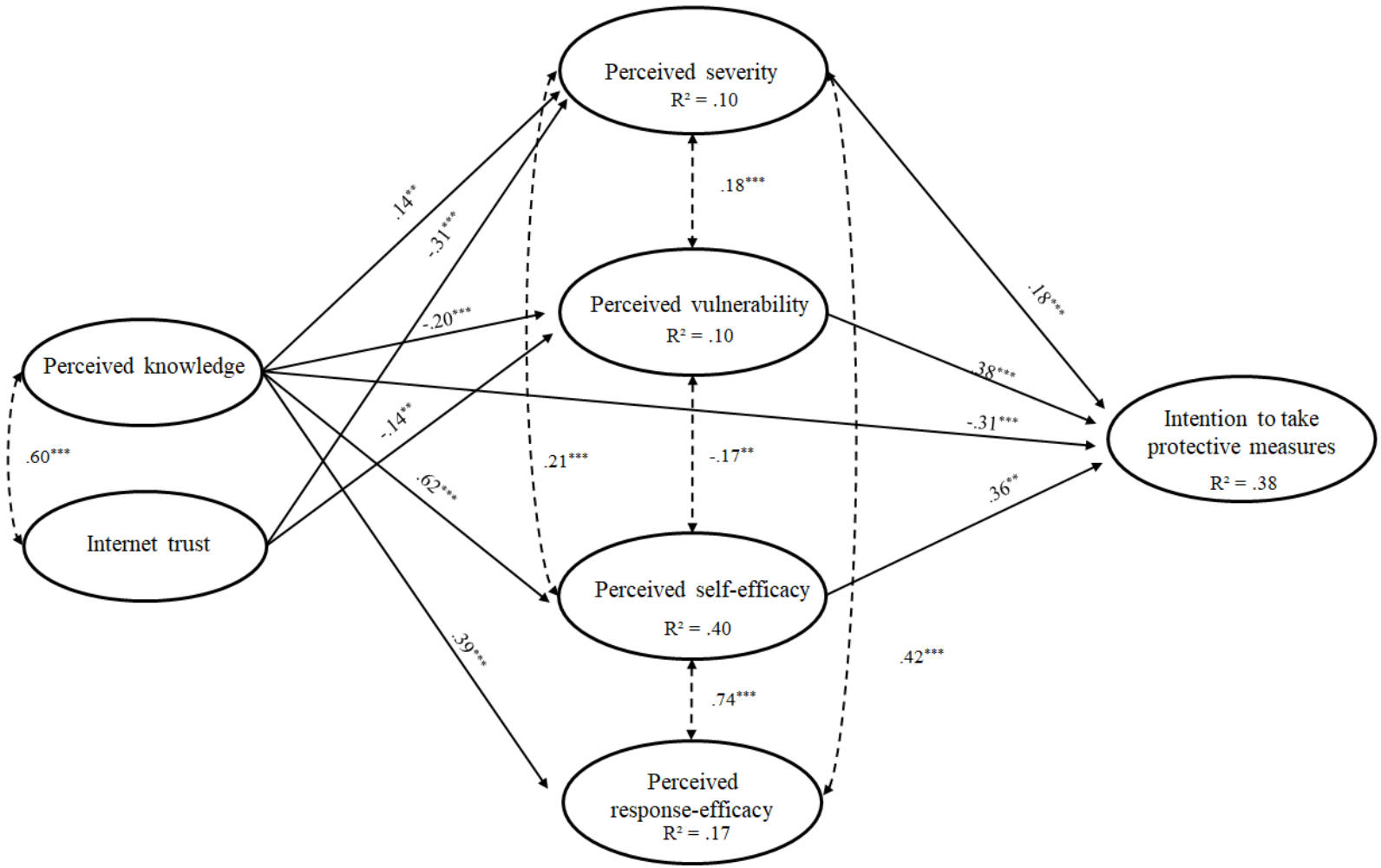

Figure 2 - Extended protection motivation model. Note: All reported coefficients are standardized values adjusted for the influence of covariates. Non-significant paths are not shown. Dashed lines refer to correlations. * $p < .05$, ** $p < .01$; *** $p < .001$.

6.3. Structural model

In the structural model, the hypothesized relationships between all constructs were tested. Based on the model fit indices, the complete model as shown in figure 2 proved to be a good fit with the data: $\chi^2(212) = 811.759$ ($p < .001$); RMSEA = .054 (CI: .050 - .058); CFI = .93; TLI = .91 and SRMR = .04. The analyses showed that perceived severity (H1a), perceived vulnerability (H1b), and perceived self-efficacy (H2a) are significantly and positively associated with the intention to take online security measures. No such association was found between perceived response-efficacy and intention ($\beta = .16$, $p = .22$), so hypothesis H2b could not be confirmed. Both perceived knowledge and internet trust were significantly related to all threat and coping appraisal constructs. Perceived knowledge was negatively related to perceived vulnerability (H3b) and positively related to perceived severity (H3a), perceived self-efficacy (H4a), and perceived response-efficacy (H4b). As expected, a significant inverse relationship between internet trust and perceived severity (H5a) and perceived vulnerability (H5b) was found. Moreover, the direct effects of perceived knowledge and internet trust on intention were explored. A negative relationship between perceived knowledge and intention was found (RQ1), but such a significant association was absent between internet trust and intention (RQ2).

7. Discussion and conclusion

Given that "information security is only as strong as its weakest link" (Abawajy, 2014, p. 237) and internet users' tendency to be overoptimistic can make them vulnerable online, this study represents an attempt to gain more insight into the cognitive processes involved in users' intention to take protective measures against cybercrime. We used an extended protection motivation framework (Rogers, 1975, 1983) that focused on two trust-related antecedents of the appraisal processes, namely perceived knowledge and internet trust. The results indicate that when internet

users believe that cybercrime is a more severe risk (i.e., perceived severity) and that they are more vulnerable to cybercrime (i.e., perceived vulnerability), they are more inclined to take protective measures. Moreover, perceived self-efficacy, or the belief that one is capable of implementing the suggested measures, is positively related to intention. These results confirm that the PMT framework is particularly valuable in a cybercrime and cybersecurity context (Crossler & Bélanger, 2014; Tsai et al., 2016).

Interestingly, the belief that one has enough knowledge about online risks and countermeasures is directly related to a reduction in protection motivation. Moreover, internet users with higher levels of perceived knowledge perceive themselves as less vulnerable to cybercrime. There are also positive relationships between perceived knowledge, perceived severity of cybercrime, and perceived self-efficacy and response-efficacy of security measures. Feeling informed about online risks and countermeasures is thus a good thing, at least in part, as it might result in people feeling more capable of applying online security measures, people being convinced that these countermeasures are effective, and internet users being aware of the severity of cybercrime. However, these positive links are counterbalanced by the negative association between perceived knowledge and intention as well as by the negative link between perceived knowledge and vulnerability. These results provide more insight into the cognitive processes at work among overoptimistic internet users. People who believe that they are informed well enough about online risks do not feel the need to take any (more) countermeasures against cybercrime, as they think that they are less vulnerable in the online environment even though they do acknowledge the general severity of cybercrime and feel capable of taking the right security measures. The present study identifies perceived knowledge as a crucial factor in understanding internet users' overoptimistic tendencies. It has to be stressed that the present study measured perceived

knowledge and not actual knowledge. Research found that actual digital knowledge is limited among the general population. Moreover, the level of knowledge varies by education level and age (Vogels & Anderson, 2019). Therefore, future research could incorporate a measurement of actual knowledge on how to avoid online risks, to investigate how actual knowledge (and not perceived knowledge) is related to taking countermeasures.

Given that almost half of European internet users consider themselves well-informed about cybercrime (Eurobarometer, 2017), these findings have important implications for future cybercrime campaigns, who should carefully tailor their communications. On the one hand, the current study shows that increasing people's awareness and (perceived) knowledge about online risks and measures might be beneficial to a certain extent, as it will increase perceptions of severity and self-efficacy. On the other hand, however, people should not be made to feel invincible online as a result of gaining knowledge. As such, we recommend that future interventions explicitly stress that every internet user can become a cybercrime victim. Providing vivid, relatable, self-relevant messages (e.g., through media coverage) might serve as a form of indirect experience of cybercrime, which might highlight the personal vulnerability of every internet user (Cho et al., 2010). More research is needed to determine to what extent stressing personal vulnerability would have a positive influence on users' protection motivation and behavior. Based on the Extended Parallel Process Model (Witte, 1994), awareness raising efforts should not only focus on stimulating perceived threat, in terms of perceived severity of cybercrime victimization and individuals' perceived susceptibility. At the same time, prevention strategies must be presented as effective and feasible. This would stimulate individuals' perceived response efficacy and self-efficacy and lead to danger control responses, which form adaptive behavior to prevent cybercrime victimization. By contrast, if only fear is triggered, without integrating recommendations that are

feasible and effective, fear control is stimulated which leads to defensive mechanisms as to reduce fear rather than engaging in protective behavior that would diminish the threat (Popova, 2012). In addition, interventions could also stress that technology alone cannot safeguard the online environment (Dodel & Mesch, 2017), and that each user has a personal responsibility to make the internet safer. It has been proven that, combined with providing vicarious experience with online protective measures, stressing personal responsibility can have a positive effect on protection motivation if the message is adapted to the knowledge level of the individual (Shillair et al., 2015).

Moreover, trust in the safety of the internet should be tempered to some extent. Although internet trust has no direct relationship with intention to take security measures, internet trust does have a negative relationship with perceived severity and vulnerability. This implies that people who trust that the internet is a safe place perceive cybercrime as less of a threat and something they are less susceptible to, which consequently results in internet users feeling less inclined to take protective measures. Hence, it might be useful to temper this dimension of trust to some extent to emphasize the fact that the online environment cannot be trusted blindly. A report by the Home Office (HO RICU, 2015) points out that 15% of the population can be considered "trusting" internet users and are therefore especially vulnerable. Those people should thus be addressed specifically and taught to adopt a more critical attitude online. Again, this could be done through awareness campaigns, interventions, or media coverage, but also within the daily accessed online environment (e.g., personalized warning messages in the browser or e-mail service, add-ons). However, it is not a good idea to interrupt people's tasks and thought processes too brusquely, as this can degrade users' decision-making efficiency and accuracy (Tan et al., 2020), nor is it desirable to scare internet users too much, since perceived risk has proven to be associated with people refraining from performing specific internet activities (e.g., online shopping). This results

in individuals missing out on opportunities the internet has to offer, which translates into a considerable opportunity cost to society in general (Riek et al., 2014). Self-efficacy of adaptive coping mechanisms in particular, such as installing protective software, changing settings, or developing a critical attitude online, should thus be stressed.

8. Limitations

Some limitations of our study should be acknowledged. In the questionnaire, we asked respondents about their intention to take protective measures in general. Based on the current study, we thus cannot determine which specific countermeasures users intend to take and to what extent they are effective. Although the wording of the items was based on an existing scale (Witte, 1996), some items were stated in a rather absolutist way, which might also account for the strength of the effects (of in case of response efficacy the absence of significance). In future studies related to the topic, it might therefore be interesting to also present the items to an expert panel in order to test the relevance, wording and clarity (i.e. content validity) and thereafter to ask a group of lay people to evaluate each item and to indicate if they feel ambiguity or difficulty in replying to the items (i.e. face validity). Furthermore, we have no insight into users' actual protective behaviors. For future research, it would therefore be interesting to measure both protection motivation and behavior in a more specific way. A longitudinal approach would also yield valuable additional insights. Because a cross-sectional design was used in the current study, it was not possible to establish causal relationships. Still, the current study illustrates that studying the association between intrapersonal processes and threat and coping appraisal is worth exploring further.

Since only two antecedents were included, future research could increase our understanding of the way threats and coping mechanisms are evaluated by integrating complementary variables. For instance, the effect of perceived knowledge on threat and coping

appraisal could be studied alongside the effect of actual knowledge. Although it was not taken into account in the current study, the actual knowledge of respondents might be an important factor to consider in future research. It would be interesting to examine whether there is a structural mismatch between perceived and actual knowledge or whether these two concepts are positively associated. Based on this information, vulnerable targets, such as internet users with high levels of perceived knowledge but low levels of actual knowledge, could be identified and targeted. In addition, those individuals who trust the internet the most should be given explicit attention in future research. Both groups of internet users could subsequently be targeted by interventions to temper their self-confidence and/or trust in the internet and to stimulate them to be more critical online. In addition, including an affective dimension (e.g., fear) and taking maladaptive responses into account in future studies would allow us to move beyond the cognitive focus of the PMT. Lastly, it would be valuable to move beyond a mere psychological focus and take other factors into account, such as experience or technological features.

Bibliography

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Bada, M., & Sasse, A. (2014). *Cyber security awareness campaigns: Why do they fail to change behaviour?* http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf

Belgian Federal Police. (2019). *Veiligheidsmonitor 2018.* Federale Politie DGR - Informatie en ICT.

Byrne, B. M. (2012). *Structural equation modeling with Mplus: Basic concepts, applications, and programming*. Routledge.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, *5*(2), 120–131.

Crossler, R. E., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51–71.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281–297.

De Jonge, J., Van Trijp, H., Jan Renes, R., & Frewer, L. (2007). Understanding consumer confidence in the safety of food: Its two-dimensional structure and determinants. *Risk Analysis*, *27*(3), 729–740.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367.

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information Communication & Society*, *21*(5), 712–728.

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security*, *86*, 75–91.

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403–418.

Eastman, J. K., Eastman, A. D. A., & Eastman, K. L. (2002). Insurance sales agents and the Internet: The relationship between opinion leadership, subjective knowledge, and Internet attitudes. *Journal of Marketing Management*, *18*(3–4), 259–285.

Eurobarometer. (2017). *Special Eurobarometer 464a: Europeans' attitude towards cyber security*. European Commission.

Europol. (2016). *Internet organised crime threat assessment 2016*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Field, A. (2009). *Discovering statistics using SPSS*. Sage publications.

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.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20.

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.

HO RICU. (2015). *Serious and organised crime protection public interventions model*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502960/Gov.uk_Serious_Organised_Crime_deck_vF.pdf

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 862–874.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Information Security Forum. (2014). *From Promoting Awareness to Embedding Behaviours: Secure by choice, not by chance*. Information Security Forum.

Jansen, J., & Leukfeldt, E. R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228.

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.

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129–137.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence*, *35*(1), 31–41.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence* (No. 75; pp. 1–34). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

Modic, C., & Anderson, R. (2015). It's all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security & Privacy*, *13*(5), 99–103.

Montazemi, A. R., & Saremi, H. Q. (2013). Factors affecting Internet banking pre-usage expectation formation. *System Sciences (HICSS), 2013 46th Hawaii International Conference On*, 4666–4675.

Muthén, L., K., & Muthén, B., O. (2012). *Mplus User's Guide. Seventh Edition.* Muthén & Muthén.

Nabi, R. L., Roskos-Ewoldsen, D., & Dillman Carpentier, F. (2008). Subjective knowledge and fear appeal effectiveness: Implications for message design. *Health Communication*, *23*(2), 191–201.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting Health Behaviour: Research and Practice with Social Cognition Models*, 81–126.

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.

Popova, L. (2012). The extended parallel process model: illuminating the gaps in research. *Health Education & Behavior, 39*(4), 455-473. https://doi.org/10.1177/1090198111418108

Raju, P. S., Lonial, S. C., & Mangold, W. G. (2015). Subjective, objective, and experience-based knowledge: A comparison in the decision-making context. *Proceedings of the 1993 Academy of Marketing Science (AMS) Annual Conference*, 60–60.

Riek, M., Böhme, R., & Moore, T. (2014). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. *Workshop on the Economics of Information Security (WEIS)*.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596–604.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social psychophysiology* (pp. 153–176). Guilford Press.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Statistics Netherlands. (2019). *Digitale veiligheid & criminaliteit 2018*. https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

Tan, M. K. S., Goode, S., & Richardson, A. (2020). Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security. *Behaviour & Information Technology*, 1–30.

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.

Vogels, E. A., & Anderson, M. (2019). *Americans and digital knowledge. Pew Research Center, https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/*

Wang, J., Li, Y., & Rao, H. R. (2017). Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. *Information Systems Research*.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105–125.

Wash, R., & Rader, E. J. (2015). Too much knowledge? Security beliefs and protective behaviors among United States internet users. *SOUPS*, 309–325.

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology*, *15*(1), 1–8.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs, 61*, 113-134. https://doi.org/10.1080/03637759409376328

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), 317–342.

Wordsworth, R. (2017, August 16). *The biggest challenge in cybersecurity? Human nature*. http://www.wired.co.uk/article/wired-security-allison-miller-google-rachel-botsman

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.