IADIS International Journal on Computer Science and Information Systems
Vol. 20, No. 1, pp. 23-39
ISSN: 1646-3692

KNOWING BETTER, DOING BETTER: THE ROLE OF ACTUAL AND PERCEIVED KNOWLEDGE OF SELF-PROTECTIVE BEHAVIOUR ON PROTECTION MOTIVATION

Kimberly Bluhm[1], Steven Watson[2], Jurjen Jansen[1,3] and Iris Van Sintemaartensdijk[2]
[1]*Cybersafety Research Group, NHL Stenden University of Applied Sciences. P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands*
[2]*Section of Psychology of Conflict, Risk and Safety, University of Twente. P.O. Box 217, 7500 AE Enschede, The Netherlands*
[3]*Dutch Police Academy, P.O. Box 834, 7301 BB Apeldoorn, The Netherlands*

ABSTRACT

In an era characterised by increasing cyber threats, there is a pressing need to gain a deeper understanding of how to enhance digital resilience at the individual level. In this study, we compared the role of actual knowledge with individuals' perceived knowledge, and the influence on the intentions to engage in self-protective behaviour. Participants (N = 222) completed an online questionnaire, which included an actual knowledge test focusing on protection measures and items measuring constructs of Protection Motivation Theory. Our regression analyses showed that actual knowledge is a predictor to engage in self-protective behaviour, with a stronger influence than perceived knowledge. Both actual and perceived knowledge are vital for self-protective behaviour, however, they activate different types of efficacy. Actual knowledge is a stronger predictor of response efficacy, whereas perceived knowledge better predicts self-efficacy. We explored implications for intervention and future research in the discussion, by highlighting the need for prioritising knowledge dissemination, increasing user confidence, and the effectiveness of interventions. This paper is a substantial adaptation of a previous conference paper (Bluhm et al., 2025).

KEYWORDS

Cybercrime, Actual Knowledge, Perceived Knowledge, Protection Motivation Theory, Self-Protective Behaviour

1. INTRODUCTION

Digitalisation has offered society new ways to communicate, and offline activities are transferred into the online domain, including crime. Cybercrime is an umbrella term which includes all forms of crime in which information- and communication technology (ICT) plays a critical role in the execution of the crime (i.e., cyber-dependent and cyber-enabled crimes) (Domenie et al., 2013). In The Netherlands, 16% of the population aged 15 years and older were a victim of cybercrime in 2024 (Arends et al., 2025). The impact of victimisation of cybercrime should not be underestimated: the impact of cybercrime on victims can be equal to – and sometimes even higher than - the impact of victimisation of traditional crimes (Bluhm et al., 2022; Borwell et al., 2025; Leukfeldt et al., 2018). Therefore, it is imperative that the public protect themselves against the negative effects of cybercrime (Arifi & Arifi, 2024). Self-protective measures to achieve online security and to prevent cybercrime victimisation are increasingly available (Mamade & Dabala, 2021; Verma & Shri, 2022), for instance anti-virus software and firewalls (Van 't Hoff - de Goede et al., 2019). However, to date, we still observe that even basic measures to increase online security are not taken by individuals (NCTV, 2023). Prior research has indicated that awareness of security threats and coping responses are important predictors of self-protective behaviour (Martens et al., 2019). Specifically, Martens et al. (2019) identified that threat awareness motivated protective intentions via increased perceptions of threat severity and vulnerability, while coping awareness motivated self-protective intentions through self-efficacy and perceptions of response efficacy. This study implies that how much people think they know about relevant security threats and countermeasures is an important precursor to taking self-protective behaviour. However, studies measuring the effects of awareness on self-protective behaviour, often rely on participants' subjective evaluations of their knowledge. It cannot be assumed that such research accurately estimates participants' actual knowledge of security threats. In this paper, we assess whether objectively rated knowledge has a different effect on security behaviour intentions compared to participants' perceptions of their level of knowledge.

1.1 Perceived Versus Actual Knowledge

Huang et al. (2021) argue that the lack of knowledge about information security risks can lead to the over- or underestimation of security levels in information systems. Individuals need a certain level of knowledge to engage in appropriate self-protective behaviour. Tambariki et al., (2024) studied the relationship between perceived knowledge (i.e., what individuals think they know) and protection habits on cybersecurity behaviour and their findings indicate that perceived knowledge was positively associated with threat and coping awareness. Their findings suggest that individuals' perception of being informed about relevant security threats and countermeasures serves as a critical positive determinant of their engagement in self-protective behaviour. In contrast, De Kimpe et al. (2022) also studied the role of perceived knowledge in relation to self-protective behaviour and found that as perceived knowledge increased, individuals' intentions to engage in self-protective behaviour against cybercrime victimisation strongly decreased. Therefore, individuals who consider themselves as well-informed might believe that they do not any (additional) protection measures to protect themselves from cybercrime victimisation, hence creating unsafe situations. Furthermore, Shillair et al. (2015) studied the role of perceived knowledge in relation to the encouragement of self-protective

behaviour. They measured perceived knowledge by asking participants to what extent they were familiar with spyware and Trojans. Their findings imply an association between self-reported knowledge about spyware and Trojans and the intentions to take self-protective measures. Namely, individuals with low levels of knowledge should not be overloaded with information about these threats, as this may result in a subsequent disregard for protection measures. Whereas individuals with high levels are more likely to act safely by using protection measures. This study also hints that individuals might have an inaccurate perception of their knowledge, which eventually makes them more vulnerable to become a victim of cybercrime. However, if this self-proclaimed expertise is inaccurate, then such confidence will create unsafe situations.

Compounding this concern, is the tendency for optimism bias, where people feel they are less likely than others to experience negative events, or have overly positive beliefs in their abilities to avoid negative outcomes (Weinstein, 1980). A recent meta-analysis has shown that such effects do occur with cyber security assessments, and most commonly lead to suboptimal self-protective behaviours (Alnifie & Kim, 2023). The presence of optimism bias implies that perceived knowledge may not accurately capture how well-equipped people are to protect themselves online and the roles of perceived and actual knowledge in self-protective behaviour may even conflict. Therefore, it is necessary to determine whether actual knowledge is a better predictor of self-protective behaviour once these biases are eliminated.

Actual knowledge (i.e., what individuals objectively know about cybercrime) is rarely included in earlier studies, making its effects on intentions unclear (De Kimpe et al., 2022). The role of actual knowledge has been studied in an organisational context (Roberts, 2021). The findings of this study suggest that as employee's knowledge improved, so did their attitude toward cybersecurity. Additionally, Zwilling et al., (2022) studied the relationship between cybersecurity awareness and knowledge related to cyberattacks. They measured participants' educational awareness (i.e., to what extent their current education influences their awareness around cybersecurity), previously attended IT-trainings, awareness of threats and the intentions to improve their cyber security awareness. While actual knowledge is not directly measured, their findings imply that attending cybersecurity programs and formal education programs has a positive impact on participants' level of attitude towards cybersecurity. Lastly, they imply that individuals with higher levels of self-reported cybersecurity knowledge are more willing to take protective measures, especially when these measures are easy to use and familiar to them. Limna et al. (2023) studied the interplay between cybersecurity knowledge, cybersecurity awareness and behavioural choice protection within the context of mobile banking. Their results indicate that actual knowledge about cybersecurity was positively associated with cybersecurity awareness, which is in line with the findings in the study of Zwilling et al. (2022). Therefore, it is likely that actual knowledge plays a crucial role in individuals' engagement in self-protective behaviour, because individuals with high actual knowledge are by definition more aware of threats and countermeasures (Tambariki et al., 2024; Zwilling et al., 2022).

Individuals' perceived knowledge might also differ from their actual knowledge, leading them to take different actions to those with greater actual knowledge, because they misunderstand which threats to prioritize and/or suboptimal protection decisions. Limited research examined the role of actual knowledge on (related aspects of) self-reported online behaviour. The studies that we found, suggest actual knowledge is positively related to safer online behaviour when sharing personal information (Van 't Hoff - de Goede et al., 2019), and there is a positive association between procedural knowledge and self-efficacy (Arachchilage & Love, 2014). Studies in non-cybercrime contexts have also explored the association between actual knowledge and self-protective behaviour (e.g., Alinejad et al. (2023) and Sayed et al.

(2022)). These studies indicate that actual knowledge plays a crucial role in the engagement of self-protective behaviour when for example focusing on knowledge of COVID-19. Nonetheless, there remains little insight about how actual knowledge affects individuals' willingness to engage in self-protective behaviour to prevent cybercrime victimisation (Haag et al., 2021).

1.2 Protection Motivation Theory

It is likely that actual and perceived knowledge affect individuals' ability to make more informed decisions about risks. Protection Motivation Theory (PMT) is a dominant model of appraising how individuals make risk decisions related to information security behaviours (De Kimpe et al., 2022; Haag et al., 2021; Jansen, 2018; Shillair et al., 2015). Over the years, PMT has become one of the best explanatory theories for predicting individuals' intention for protective behaviour (Floyd et al., 2000). PMT distinguishes two appraisal processes: threat appraisal and coping appraisal. The outcomes of these processes result in protection motivation, i.e., behavioural intentions (De Kimpe et al., 2022; Martens et al., 2019; Rogers, 1975; Van 't Hoff-de Goede et al., 2025).

Threat appraisal comprises evaluations of an individuals' perceived vulnerability to negative outcomes, and the perceived severity of those outcomes (Bekkers et al., 2023; De Kimpe et al., 2022). Several studies have suggested that both evaluations are positively associated with individuals' self-protection intentions (Haag et al., 2021; Martens et al., 2019; Rogers, 1975; Van 't Hoff-de Goede et al., 2025). Coping appraisals capture whether individuals believe they can enact strategies to prevent or reduce threat impacts, and comprises the personal capability to implement security measures (self-efficacy), the extent to which an individual considers these measures as effective (response efficacy), and the relative costs for a given security measure (response costs) (De Kimpe et al., 2022; Haag et al., 2021; Martens et al., 2019; Rogers, 1975; Van 't Hoff-de Goede et al., 2025). Earlier studies demonstrated that both self-efficacy and response efficacy positively affected individuals' intentions (e.g., De Kimpe et al. (2022) and Martens et al. (2019)). However, contradictory results were found for the association between response costs and intentions for self-protective behaviour (Mou et al., 2022). Gurung et al. (2009) suggested that response costs do not predict self-protective behaviour due to the plethora of easily accessible free protection measures that are available. Therefore, we do not further consider response costs.

We propose that actual and perceived knowledge serve as distinct antecedents of threat and coping appraisals within an extended PMT framework. Actual knowledge is predicted to be positively related to threat and coping appraisals, because knowledgeable individuals should be aware of both genuine risks and counter measures. Perceived knowledge is expected to be positively associated with coping appraisals, but negatively associated with threat appraisals in line with prior studies (e.g., De Kimpe et al. (2022)). Lastly, we include internet trust as a third antecedent. We define trust as: "The belief that the other party will behave in a socially responsible manner" [p. 106] (Pavlou, 2003). We include internet trust, because too much trust can lead to over-confidence, eventually resulting in careless behaviour (Furnell, 2008). The findings of the study of De Kimpe et al. (2022) indicate that internet trust is positively correlated with perceived knowledge and negatively affected perceived severity and perceived vulnerability. A negative relationship between trust and perceived risk, and between trust and protection motivation have also been demonstrated elsewhere (Colquitt et al., 2007; Jansen & van Schaik, 2018). Overall, we expect internet trust to be related to reduced threat appraisal.

Thus, the current study focuses on the role of actual and perceived knowledge on individuals' intentions to engage in self-protective behaviour, while also including internet trust. Therefore, we tested the following sixteen hypotheses:

H1: Perceived severity (1a), perceived vulnerability (1b), self-efficacy (1c), and response efficacy (1d) are positive predictors of intentions toward self-protective behaviour.

H2: Actual knowledge is a positive predictor of perceived severity (2a), perceived vulnerability (2b), self-efficacy (2c), response efficacy (2d), and intentions (2e).

H3: Perceived knowledge is a positive predictor of perceived severity (3a), self-efficacy (3b) and response efficacy (3c), and a negative predictor perceived vulnerability (3d) and intentions (3e).

H4: Internet trust is a negative predictor of perceived severity (4a) and perceived vulnerability (4b).

2. METHODS

2.1 Procedure and Participants

Data were collected via Qualtrics survey software. Data collection took place between November and December 2022. Before data collection started, this study was approved by the Ethics Committee of the University of Twente (request number: 221187). We have addressed potential common method bias and the likelihood of participants giving socially desirable answers by guarantying anonymity (Podsakoff et al., 2003).

First, participants read information about the topic and duration of the study. If they consented to participate, they provided their demographics, followed by two items measuring their perceived knowledge. Subsequently, their actual knowledge was tested. Lastly, participants were asked to rate PMT statements and were debriefed about the study. Data collection took place between November and December 2022. It took participants approximately 20 minutes to complete the survey. Part of this study was spent with participants completing tasks not related to our research questions[1].

In total, 222 participants completed our study. The age range was between 18 and 67 years (M = 29.9; SD = 12.2). Most participants (145, 65,3%) identified as female, 70 participants (31.5%) identified as male, three participants (1.4%) as non-binary, and one participant (0.5%) did not want to share their gender.

Participants were recruited with snowball and convenience sampling procedures. Additionally, the SONA-system of the University of Twente was used. This is an internal participant recruitment system.

2.2 Measures

2.2.1 PMT Constructs

The items in our questionnaire for internet trust, threat and coping appraisals are derived from previous studies (De Kimpe et al., 2022; Martens et al., 2019) and were adapted to our study

[1] These tasks were related to another study that was part of the thesis.

(Table 1). Intentions toward self-protective behaviour were measured using items from Anderson & Agarwal (2010). De Kimpe et al. (2022) argue that protections and vulnerabilities against different cybercrimes are often related. Consequently, the measures taken to prevent victimisation typically safeguard individuals against multiple types of cybercrime. Therefore, we studied intentions toward protection measures in general.

All items were all measured using a five-point Likert Scale (1 = "totally disagree" to 5 = "totally agree"), except for perceived vulnerability. The formulation of these items for this construct were reversed, with a corresponding five-point Likert Scale (1 = "totally agree" to 5 = "totally disagree"). We did this to reduce response bias and prevent acquiescence bias (Schriesheim & Hill, 1981). By changing the response scale, participants had to read the items carefully, which should prevent them from selecting the same answer to every item. Lastly, Cronbach's Alpha (α) was calculated for all PMT constructs, and are presented in Table 1 alongside descriptive statistics for all measures ($\alpha = .57$)[2] (Tavakol & Dennick, 2011).

Table 1. Descriptive Statistics of PMT Items ($N = 222$)

Construct/item	*M*	*SD*	α
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 if I use protection tools			
Intention toward 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			

2.2.2 Actual Knowledge

To measure participants' actual knowledge, we used questions on nine different topics (Table 2) from the actual knowledge test of Van 't Hoff - de Goede et al. (2019). Participants were asked to select the correct answer in a multiple choice format. For instance, "Which statement about making a backup is correct?", with the following answer options: (a)" Relying on an online backup is not safe, since you are not sure whether your files are actually safe"; (b) "Store

[2] We performed additional tests to find an explanation for our low alpha of response efficacy. These tests included a factor analysis, a reliability analysis and correlations between the items. However, the outcomes of these tests do not provide any clarification for this. Additionally, these items are based on items used in earlier studies, in which the alpha for response efficacy was considerably higher. Therefore, we proceeded to use the full scale for our analyses.

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"; and (e) "I do not know". Participants received a point for each correct answer ($M = 4.74$; $SD = 1.76$), which is in with the findings of Van 't Hoff - de Goede et al. (2019). Lastly, Cronbach's Alpha was calculated and this test had a Cronbach's Alpha of $\alpha = .58$. While this Alpha is also low, we believe this reflects variable expertise about specific topics, and so it is appropriate to maintain all items in the scale to ensure the knowledge scale has construct validity, and does not only include knowledge of the most commonly known protections. We capture this variation in how well known different protective measures are in Table 2.

Table 2. Score Knowledge Test per Topic ($N = 222$)

Topic	*N (%) correct*
Infected websites	187 (83.5%)
Disclosing information on the internet	176 (78.6%)
Spam filter	170 (75.9%)
Two-step verification	138 (61.6%)
Software-updates	103 (46.0%)
Software-updates	93 (41.5%)
Firewall	89 (39.7%)
Making backups	55 (24.6%)
Password strength	48 (21.4%)

2.2.3 Perceived Knowledge

To measure participants' perceived knowledge, we used two items: (1) "I feel adequately informed about cybercrime risks"; and (2) "I feel adequately informed about how to avoid cybercrime risks." (De Kimpe et al., 2022). These items were measured using a five-point Likert Scale (1 = "totally disagree" to 5 = "totally agree"). This construct had a Cronbach's Alpha, $\alpha = .86$, indicating a good internal reliability (George & Mallery, 2019). This resulted in an average score of $M = 3.38$ ($SD = 0.97$).

2.2.4 Internet Trust

To measure participants' internet trust, we added three items to measure this construct: (1) "I am optimistic about the safety of the internet"; (2) "I have every confidence that the internet is safe"; and (3) "I am satisfied with the safety of the internet" (De Kimpe et al., 2022). We used a five-point Likert Scale (1 = "totally disagree" to 5 = "totally agree"). Cronbach's Alpha was also calculated for internet trust and this construct had an alpha of $\alpha = .78$, indicating a good internal reliability (George & Mallery, 2019). This construct had an average score of $M = 2.37$ ($SD = 0.72$).

2.3 Data-Analysis

For data analysis, we used the Statistical Package of Social Sciences (SPSS) version 28. First, the dataset was cleaned by excluding incomplete responses ($N = 44$), participants who did not meet our age inclusion criteria ($N = 4$), and participants who completed the questionnaire in a very short amount of time ($N = 12$). Lastly, we deleted irrelevant variables, for instance time to

complete the questionnaire. This process led to a final sample of 222 participants, from 282 that initiated the study.

To study the relationships between the constructs, correlations were calculated. The hypotheses were tested via a series of multiple linear regressions.

3. RESULTS

3.1 Preliminary Analyses

3.1.1 Correlations

Correlations were calculated to study the relations between the antecedents and the constructs, the antecedents and intentions, and the constructs and intentions (see Table 3). A positive correlation was found between actual and perceived knowledge. We also found a positive association between perceived knowledge and internet trust, whereas we observed a negative association between actual knowledge and internet trust. These findings indicate that participants who *consider* themselves well-informed have more trust in the internet, whereas participants who *are* actually well-informed have less trust in the internet. Lastly, significant positive associations were found between the original PMT constructs and intentions, except for perceived vulnerability. Greater internet trust was also associated with lower perceived severity and vulnerability to online risks.

Table 3. Pearson Correlations Between Variables

	ACK	PCK	ITR	PSE	PVU	SEE	REE	INT
ACK								
OCK	.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

3.1.2 Regressions

Seven linear, multiple regression analyses were conducted to study the predictors of threat and coping appraisal, and the intentions toward self-protective behaviour. The standardized regression (β) was reported, as the measurement of the predictor variables differed and we are interested in the relative rather than absolute strength of predictors (Bring, 1994). The first multiple, linear regression included all variables (i.e., the four original PMT constructs, actual knowledge, perceived knowledge and internet trust) to study the predictive power of these variables on intentions (Table 4). This regression shows that self-efficacy was the strongest predictor of intentions, followed by perceived severity, perceived vulnerability, and actual knowledge.

Table 4. Linear, Multiple Regression

From	To	β	*SE*	*t*	ηp2	*p*
PSE	INT	.22	.07	2.69	.17	<.001
PVU	INT	.17	.05	5.17	.05	.008
SEE	INT	.35	.06	1.68	.20	<.001
REE	INT	.10	.07	2.46	.07	.095
ACK	INT	.15*	.02	1.86	.13	.015
PCK	INT	.12	.04	-.70	.13	.064
ITR	INT	-.05	.06	3.59	.07	.482

PSE = perceived severity, PVU = perceived vulnerability, SEE = self-efficacy, REE = response efficacy, and INT = intentions, ACK = actual knowledge, PCK = perceived knowledge, ITR = internet trust

The previous regression analysis was followed by six linear, multiple regression analyses that separately assessed the hypotheses (Table 5).

Table 5. Linear, Multiple Regressions with Hypotheses

H	From	To	β	*SE*	*t*	ηp2	*p*	H confirmed?
1a	PSE	INT	.28	.07	4.66	.09	<.001	+
1b	PVU	INT	.18	.05	2.92	.04	.004	+
1c	SEE	INT	.42	.05	6.66	.18	<.001	+
1d	REE	INT	.13	.07	2.02	.02	.041	+
2a	ACK	PSE	.17	.02	2.23	.02	.011	+
2b	ACK	PVU	-.01	.03	-.133	.00	.895	ns
2c	ACK	SEE	.08	.03	1.30	.01	.197	ns
2d	ACK	REE	.18	.02	2.56	.03	.011	+
2e	ACK	INT	.27	.02	4.05	.07	<.001	+
3a	PCK	PSE	.12	.04	1.84	.02	.070	ns
3b	PCK	PVU	-.12	.06	-1.77	.01	.079	ns
3c	PCK	SEE	.43	.05	6.96	.19	<.001	+
3d	PCK	REE	.08	.04	1.23	.01	.221	ns
3e	PCK	INT	.24	.04	3.74	.06	<.001	-
4a	ITR	PSE	-.30	.06	-4.46	.09	<.001	+
4b	ITR	PVU	-.34	.08	-5.15	.11	<.001	+

H = Hypothesis, PSE = perceived severity, PVU = perceived vulnerability, SEE = self-efficacy, REE = response efficacy, and INT = intentions, ACK = actual knowledge, PCK = perceived knowledge, ITR = internet trust,
+ = statistically significant effect in the hypothesised direction, ns = non-statistically significant result,
- = statistically significant effect in the opposite of the hypothesised direction.

Significant, positive relationships were found for all original PMT constructs on intentions (i.e., perceived severity (H1a), perceived vulnerability (H1b), self-efficacy (H1c), and response efficacy (H1d)). The positive relationships between actual knowledge and perceived severity (H2a), response efficacy (H2d) and intentions (H2e) were significant, whereas the associations between actual knowledge and perceived vulnerability (H2b) and self-efficacy (H2c) were not significant. We found non-significant relationships between perceived knowledge and perceived severity (H3a), perceived knowledge and response efficacy (H3c), and perceived knowledge and perceived vulnerability (H3d). The positive relationship between perceived knowledge and self-efficacy (H3c) was significant. Unexpectedly, we found a significant, positive relationship between perceived knowledge and intentions (H3e). Lastly, we found significant negative relationships between internet trust and perceived severity (H4a), and internet trust and perceived vulnerability (H4b).

3.2 Additional Analyses

An additional exploratory, multiple regression analysis was performed to determine whether actual and perceived knowledge independently predicted intentions, while also accounting for the relationship between self-efficacy and intentions. Self-efficacy was included as it was the strongest predictor of intentions, and we hypothesized that there might be conceptual overlap between perceived knowledge and self-efficacy. This analysis showed that actual knowledge ($\beta = .23$, $SE = .02$, $p < .01$, $\eta p2 = .06$) and self-efficacy ($\beta = .31$, $SE = .06$, $p < .01$, $\eta p2 = .09$) were independently significant positive predictors of intentions, while perceived knowledge was no longer related to intentions after self-efficacy was included ($\beta = .11$, $SE = .06$, $p = .10$, $\eta p2 = .01$).

4. DISCUSSION

A key finding of this study is that actual knowledge is a crucial indicator for the willingness to engage in self-protective behaviour to prevent cybercrime victimisation. Additionally, actual knowledge was positively related to perceived severity and response efficacy but not self-efficacy, and negatively correlated with internet trust. On the contrary, perceived knowledge self-efficacy and internet trust were positively correlated, with internet trust negatively associated with perceived risk and perceived knowledge having no direct relationship with perceived risks. While perceived knowledge was itself positively correlated with protection intentions, combined our results indicate that the effects of perceived knowledge are not uniformly positive, and likely lead people to overestimate estimate their ability to stay safe online.

Our findings are largely in line with the study of De Kimpe et al. (2022), as they indicate that individuals' own evaluations of their expertise are often inaccurate, ultimately increasing their susceptibility to vulnerabilities. An overestimation of one's own ability to protect oneself against internet threats can negatively influence individuals' actual behaviour to implement protective measures (Komatsu et al., 2013). The tendency for individuals to overestimate their protection skills can be explained through optimism bias (Slovic, 1987). When people are aware of obvious attempts at cybercrime, they might believe they can identify future other attempts as well, as they perceive themselves as knowledgeable (e.g., an increase of perceived knowledge) (Lee et al., 2023; Martens et al., 2019). Subsequently, they may underestimate the severity of cybercrime risks and mistakenly consider the internet to be safe (De Kimpe et al., 2022; Lee et al., 2023). For instance, Lee et al. (2023) demonstrated that higher levels of self-efficacy might increase individuals' risk of becoming a victim of phishing, as self-efficacy might reduce individuals' susceptibility to become a victim. On the contrary, when self-efficacy is low and perceived threat is high, individuals might feel unable to prevent victimisation, potentially resulting in maladaptive responses, e.g., denial. Feelings of helplessness, compounded by a lack of knowledge, may further lead individuals to either accept the likelihood of becoming a victim of cybercrime or entirely reject the possibility (Bada & Nurse, 2020). Therefore, both over- and underestimations of ability are likely to lead to poorer protective behaviours.

In contrast, as actual knowledge increases, so does the realization that susceptibility to risks are high. Furthermore, perceived severity was positively associated with actual knowledge, whereas it was not related to perceived knowledge. Actual knowledge was also a stronger

indicator for individuals' intentions than perceived knowledge. Lastly, actual knowledge was negatively associated with internet trust, whereas perceived knowledge was positively associated with this construct. These findings suggest that being well-informed about cybercrime is more important for protection motivation than the mere perception of being well-informed. Additionally, this indicates that individuals who are genuinely well-informed perceived cybercrime as a (more) severe threat, whereas individuals who only considered themselves as well-informed lacked this perception. Consequently, individuals may consider themselves as less vulnerable and disregard protection measures, since they believe they are not a target to become a victim, which eventually makes them more vulnerable to become a victim (Alnifie & Kim, 2023; Drew & Farrell, 2020). Therefore, this study highlights the importance of future cybercrime prevention interventions focusing on increasing individuals' actual knowledge, rather than solely enhancing perceived knowledge.

The association of only perceived and not actual knowledge with trust is also an important finding. Past research has indicated that when people lack experience, they tend to rely on affective processes when making trust judgements (Dunn & Schweitzer, 2005). That we observed a relationship between only perceived knowledge and trust, but not actual knowledge and trust, further suggests that non-experts rely on affective processes when making risk judgements. This is because trust is used to simplify decision making by increasing willingness to make oneself vulnerable to trusted entities (Siegrist, 2021), and so that there was no association with actual expertise and trust indicates that any the association between trust and perceived knowledge does not reflect an accurate appraisal of the actual trustworthiness of the internet. Given the evidence that affective process impact on decisions about risk (Loewenstein et al., 2001; Watson et al., 2017), it is important that we better understand affective processes in protective behaviour online. However, the role of affect in risk judgements in online settings has rarely been considered (van Schaik et al., 2020). We recommend that attempts to improve protective behaviours account for the likelihood that many decisions are made heuristically rather than in a carefully considered manner. This is critical because our results indicate that heuristic and affective decisions are especially likely to be used by the target audience of such interventions – people with limited expertise in cybersecurity. One option is to design interventions that target users emotions to motivate appropriate behaviour, however this can itself be risky, as it relies on being able to reliably associate an emotive response with an appropriate action – something hard to control in applied settings (Shiota et al., 2023). Therefore, the more promising route is to develop interventions that genuinely increase expertise, rather than only confidence. The separate predictive power of trust and self-efficacy in our sample reinforces that while trust and confidence are often strongly associated, they remain separate constructs (Siegrist, 2021). It remains a challenge to develop measures that clearly differentiate between the two constructs (Siegrist, 2021) but doing so is important for us to better understand how decisions about protective behaviours are made. This knowledge can then be used to ensure that we can increase individuals' confidence in keeping themselves safe online, but where this confidence is based on genuine expertise.

We do not claim that increasing perceived knowledge is always detrimental. Both actual and perceived knowledge were positively correlated, indicating that perceived knowledge is likely at least partly derived from actual knowledge. Perceived knowledge clearly has its benefits, as it can enhance individuals' capability to engage in self-protective behaviour (De Kimpe et al., 2022; Tambariki et al., 2024). Additionally, it is positively associated with intentions (Huang et al., 2021) and our study shows that as well. However, the association between perceived knowledge and self-protection intentions might be explained by the covariance between

perceived knowledge and self-efficacy. Individuals with high levels of perceived knowledge consider themselves well-informed and capable of self-protective behaviour. This may result in higher levels of self-efficacy, which can reflect the confidence necessary to engage in protective behaviours (Bada & Nurse, 2020; Tambariki et al. 2024). Our analysis showed that perceived knowledge no longer predicted intentions once self-efficacy was included in the same regression model, which again suggests that primary benefit of perceived knowledge lies in its relationship with individuals confidence in their ability to protect themselves. In contrast, actual knowledge continued to independently predict intentions when including self-efficacy. Actual knowledge was not related to self-efficacy, but it was positively associated with response efficacy. This finding suggests that people who are well-informed view protection measures to enhance their self-protective behaviour as effective. However, it also shows that people who have actual knowledge, but may underestimate the depth of their knowledge, could lack the self-efficacy required to fully motivate protective behaviours. Increased response efficacy is a strong benefit of increased actual knowledge. A meta-analysis focusing on the strength of PMT constructs on intentions indicates that the relationship between response efficacy and protection motivation was one of the most robust relationships (Mou et al., 2022), indicating that it is crucial to improve individuals' perception of the effectiveness of protection measures. However, without an accompanying increase in perceived knowledge, the benefits on self-efficacy may be limited, and in our analysis self-efficacy was the strongest individual predictor of protective intentions. This highlights the need for both motivational and factual education, as the two types of efficacies may be based on different types of knowledge.

Knowledge seems to be a key factor that influences the gap between individuals' security perceptions and their actual behaviour (Huang et al., 2011). However, a balance between actual and perceived knowledge should be safeguarded. It is crucial that future interventions (e.g., crime prevention programs or awareness campaigns), by for instance IT-practitioners, government or internet providers, focus on increasing individuals' actual knowledge without only awakening perceived knowledge. Additionally, the necessity to improve public education is reinforced through only a small proportion of individuals who engage in advanced protection measures that require a deeper level of cybersecurity knowledge (Zwilling et al., 2022).

These two types of knowledge activate different types of efficacies, indicating the need for both factual and motivational elements in education. However, these education programs should be tailored to individuals' level of knowledge (Martens et al., 2019; Shillair et al., 2015), their preferences, characteristics and current behaviours (Kievik, 2017). Future research is necessary to draw definitive conclusions about what works for whom, when, and which conditions are necessary in interventions focusing on improving individuals' self-protective behaviour (Bluhm & Jansen, 2025). Additionally, the design in systems or processes could also promote safe, online behaviour (De Bruine, 2018). Indeed, underestimating online threats may encourage individuals to behave unsafely. On the other hand, overestimating the threats can also have negative effects, such as avoiding the usage of internet (Jansen, 2018). It is therefore crucial that this balance between actual knowledge and perceived knowledge will be established.

5. LIMITATIONS

As we measured intentions toward behaviour in the current study, it is important to note that intentions do not always result in actual behaviour (Van 't Hoff - de Goede et al., 2025), which

is also known as the behaviour-intention gap (Sheeran, 2002). A longitudinal study, preferably observing or measuring actual behaviour, would allow a direct test of what form of knowledge is most associated with behaviour over time. Moreover, longitudinal or experimental research approaches are necessary to observe cause-and-effect-sequences, as our study is limited to measuring associations at one point in time. Nonetheless, intentions could be a reasonable predictor of behaviour (Scholz et al., 2008), and PMT relationships might be generally stronger in a personal setting than in a workplace setting (Mou et al., 2022).

We also need to consider that participants self-reports of protection measures may be inaccurate and reflect low knowledge. For example, many modern computers come with a firewall already installed. Therefore, if a participant reports not using a firewall this may reflect a lack of knowledge more than their genuine security situation. Nonetheless, this would still indicate a lack of clear action to take a protection measure and so would not likely invalidate any of our claims which centre around knowledge predicting deliberate self-protection behaviours.

Another limitation is the validity of the knowledge test used in this study. This test might be one of the scarce few measures focusing on actual knowledge. The Cronbach's Alpha for this test was relatively low, but still considered reasonable given the explorative nature of the study, and our desire to capture more and less well known security measures. Nonetheless, it is unclear whether our questions cover the most critical issues for assessing individuals' actual knowledge; and the requires knowledge will differ depending on specific protection behaviours. Future research could employ a different approach (for instance a Delphi study) to identify knowledge individuals need to keep themselves safe and use this input for an updated knowledge test. It should also be noted that advice for self-protective behaviour may change over time, potentially limiting the longevity of the construct. Therefore, it is crucial to continually update the measure to validate it or develop a measure that focuses on stable principles rather than details that will likely change over the years.

6. CONCLUSION

Actual knowledge seems to be an important predictor for individuals' willingness to engage in self-protective behaviour to prevent cybercrime victimisation. Additionally, it was positively associated with perceived severity and negatively associated with internet trust. These findings suggest that people who overestimate their knowledge or consider the internet as a safe place are especially vulnerable to become a victim of cybercrime, as they perceive protection measures as less effective than people with higher levels of knowledge.

To motivate users to take concrete protection measures we show that increasing risk perceptions, self-efficacy, and response efficacy are all effective, which aligns with the premise of PMT Additionally, actual knowledge was more effective than perceived knowledge in affecting perceived risks and response efficacy. Perceived knowledge was however most strongly associated with self-efficacy, which plausibly reflects that training requires a motivational and not only a factual element. Studies measuring the success of these interventions should therefore also focus on actual knowledge and not only perceived knowledge to validate whether these interventions are effective. It matters what you know, not only what you think you know.

REFERENCES

Alinejad, N. et al. (2023). Effect of educational intervention based on health belief model on nurses' compliance with standard precautions in preventing needle stick injuries. *BMC Nursing*, Vol. 22, No. 1, 180. https://doi.org/10.1186/s12912-023-01347-0

Alnifie, K. M., and Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis. *Journal of Information Security*, Vol. 14, No. 02, pp. 93-110. https://doi.org/10.4236/jis.2023.142007

Anderson, C., and Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, Vol. 34, No. 3, 613. https://doi.org/10.2307/25750694

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

Arends, J., Derksen, E., and Morren, M. (2025). *Online Veiligheid en Criminaliteit 2024*. https://www.cbs.nl/-/media/_pdf/2025/16/online-veiligheid-en-criminaliteit-2024-_-cbs.pdf

Arifi, D., and Arifi, B. (2024). Cybercrime Victimization. In T. Pajuste, H. Bellani (Miço), and S. Maslo Cerkic (eds.) *Legal Perspectives in the Modern Era of Technological Transformations*. ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, pp. 193-204. https://doi.org/10.62768/ADJURIS/2024/1/12

Bada, M., and Nurse, J. R. C. (2020). The Social and Psychological Impact of Cyber-Attacks. In V. Benson, and J. Mcalaney (eds.) *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elvesier, pp. 73-92.

Bekkers, L. et al. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, Vol. 127, 103099. https://doi.org/10.1016/j.cose.2023.103099

Bluhm, K., Borwell, J., and Stol, W. (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift Voor Veiligheid*, Vol. 21, No. 3-4, pp. 13-31. https://doi.org/10.5553/TvV/.000045

Bluhm, K., and Jansen, J. (2025). *Oud en Wijs Genoeg voor een Digitale Wereld*.

Bluhm, K. et al., 2025. Ready, Set, Know: The Relationship Between Actual and Perceived Knowledge of Cybercrime and the Intentions to Engage in Self-protective Behaviour. In M. Baptista Nunes, P. Isaías, P. Powell, & P. Kommers (eds.) *International Conferences IADIS Information Systems 2025 and e-Society 2025*. IADIS Press, pp. 339-346.

Borwell, J., Jansen, J., and Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, Vol. 31, No. 1, pp. 156-181. https://doi.org/10.1177/02697580241282782

Bring, J. (1994). How to standardize regression coefficients. *The American Statistician*, Vol. 48, No. 3, 209-213. https://doi.org/10.1080/00031305.1994.10476059

Colquitt, J. A., Scott, B. A., and LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, Vol. 92, No. 4, pp. 909-927. https://doi.org/10.1037/0021-9010.92.4.909

De Bruine, H. (2018). Organiseren van Veiligheid. In F. Guldenmund (ed.) *Gedrag en Veiligheid* Vakmedianet, pp. 153-168.

De Kimpe, L. et al. (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*, Vol. 41, No. 8, pp. 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

Drew, J. M., and 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*, Vol. 6, No. 1, pp. 17-33. https://doi.org/10.1108/JCRPP-12-2019-0070

Dunn, J. R., and Schweitzer, M. E. (2005). Feeling and Believing: The Influence of Emotion on Trust. *Journal of Personality and Social Psychology*, Vol. 88, No. 5, pp 736-748. https://doi.org/10.1037/0022-3514.88.5.736

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp. 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Furnell, S. (2008). *Securing information and communications systems: Principles, technologies, and applications*. Artech House.

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

Gurung, A., Luo, X., and Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*, Vol. 17, No. 3, pp. 276-289. https://doi.org/10.1108/09685220910978112

Haag, S., Siponen, M., and Liu, F. (2021). Protection motivation theory in information systems security research. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 52, No. 2, pp. 25-67. https://doi.org/10.1145/3462766.3462770

Huang, D.-L. et al. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, Vol. 69, No. 12, pp. 870-883. https://doi.org/10.1016/j.ijhcs.2011.07.007

Huang, P.-C. et al. (2021). Expanding protection motivation theory to explain willingness of COVID-19 vaccination uptake among Taiwanese university students. *Vaccines*, Vol. 9, No. 9, 1046. https://doi.org/10.3390/vaccines9091046

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Open Universiteit.

Jansen, J., and van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, Vol. 87, pp. 371-383. https://doi.org/10.1016/j.chb.2018.05.010

Kievik, M. (2017). *The time of telling tales: the determinants of effective risk communication*, Doctoral Dissertation, University of Twente. https://doi.org/10.3990/1.9789036544269

Komatsu, A., Takagi, D., and Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security*, Vol. 21, No. 1, pp. 5-15. https://doi.org/10.1108/09685221311314383

Lee, Y. Y., Gan, C. L., and Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, Vol. 20, No. 4, 3514. https://doi.org/10.3390/ijerph20043514

Leukfeldt, R., Notté, R., and Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Available at: https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Limna, P., Kraiwanit, T., and Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, Vol. 7, pp. 1133-1151. https://doi.org/10.25147/ijcsr.2017.001.1.123

Loewenstein, G. F. et al. (2001). Risk as feelings. *Psychological Bulletin*, Vol. 127, No. 2, pp. 267-286. https://doi.org/10.1037/0033-2909.127.2.267

Mamade, B. K., and 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., and 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*, Vol. 92, pp. 139-150. https://doi.org/10.1016/j.chb.2018.11.002

Mou, J., Cohen, J., Bhattacherjee, A., and Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising. *Journal of the Association for Information Systems*, Vol. 23, No. 1, pp. 196-236. https://doi.org/10.17705/1jais.00723

NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Available at: https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp. 101-134. https://doi.org/10.1080/10864415.2003.11044275

Podsakoff, P. M. et al. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, Vol. 88, No. 5, pp. 879-903. https://doi.org/10.1037/0021-9010.88.5.879

Roberts, S. A. (2021). *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors*.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, Vol. 91, No. 1, pp. 93-114. https://doi.org/10.1080/00223980.1975.9915803

Sayed, S. H., Al-Mohaithef, M., and Elgzar, W. T. (2022). Effect of digital-based self-learned educational intervention about COVID-19 using protection motivation theory on non-health students' knowledge and self-protective behaviors at Saudi Electronic University. *International Journal of Environmental Research and Public Health*, Vol. 19, No. 22, 14626. https://doi.org/10.3390/ijerph192214626

Scholz, U. et al. (2008). Beyond behavioural intentions: Planning mediates between intentions and physical activity. *British Journal of Health Psychology*, Vol. 13, No. 3, pp. 479-494. https://doi.org/10.1348/135910707X216062

Schriesheim, C. A., and Hill, K. D. (1981). Controlling Acquiescence Response Bias by Item Reversals: The Effect on Questionnaire Validity. *Educational and Psychological Measurement*, Vol. 41, No. 4, pp. 1101-1114. https://doi.org/10.1177/001316448104100420

Sheeran, P. (2002). Intention—behavior Relations: A conceptual and empirical review. *European Review of Social Psychology*, Vol. 12, No.1, pp. 1-36. https://doi.org/10.1080/14792772143000003

Shillair, R. et al. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, Vol. 48, pp. 199-207. https://doi.org/10.1016/j.chb.2015.01.046

Shiota, M. N., Vornlocher, C., and Jia, L. (2023). Emotional Mechanisms of Behavior Change: Existing Techniques, Best Practices, and a New Approach. *Policy Insights from the Behavioral and Brain Sciences*, Vol. 10, No. 2, pp. 201-211. https://doi.org/10.1177/23727322231195907

Siegrist, M. (2021). Trust and Risk Perception: A Critical Review of the Literature. *Risk Analysis*, Vol. 41, No. 3, pp. 480-490. https://doi.org/10.1111/risa.13325

Slovic, P. (1987). Perception of risk. *Science*, Vol. 236, No. 4799, pp. 280-285. https://doi.org/10.1126/science.3563507

Tambariki, C. (2024). Drivers of Banking Consumers' Cybersecurity Behavior: Applying the Extended Protection Motivation Theory. *GATR Journal of Management and Marketing Review*, Vol. 9, No. 1, pp. 01-12. https://doi.org/10.35609/jmmr.2024.9.1(1)

Tavakol, M., and Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, Vol. 2, pp. 53-55. https://doi.org/10.5116/ijme.4dfb.8dfd

van Schaik, P. et al. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, Vol. 90, 101651. https://doi.org/10.1016/j.cose.2019.101651

Van 't Hoff - de Goede, M. S., et al. (2025). Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers in Human Behavior Reports*, 100649. https://doi.org/10.1016/j.chbr.2025.100649

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

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

Watson, S. J., Zizzo, D. J., and Fleming, P. (2017). Risk, Benefit, and Moderators of the Affect Heuristic in a Widespread Unlawful Activity: Evidence from a Survey of Unlawful File-Sharing Behavior. *Risk Analysis*, Vol. 37, No. 6, pp. 1146-1156. https://doi.org/10.1111/risa.12689

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, Vol. 39, No. 5, pp. 806-820. https://doi.org/10.1037/0022-3514.39.5.806

Zwilling, M. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, Vol. 62, No. 1, pp. 82-97. https://doi.org/10.1080/08874417.2020.1712269