

# The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization



M. Susanne van 't Hoff-de Goede, E. Rutger Leukfeldt,  
Rick van der Kleij, and Steve G. A. van de Weijer

## Introduction

Cybercrime is common and its impact can be significant for victims (Cross, Richards, & Smith, 2016; Jansen & Leukfeldt, 2018; Leukfeldt, Notté, & Malsch, 2019). Cybersecurity professionals have tried to reduce victimization with technical measures such as anti-virus scanners and firewalls. However, these measures often have only a limited effect and much victimization can be traced back to human behaviour (Jansen, 2018; Leukfeldt, 2017). For example, internet users may fill in information on a phishing<sup>1</sup> website when they should not, thereby allowing

---

<sup>1</sup> Phishing is a form of an online scam, in which criminals copy the emails or websites of legitimate organisations to mislead victims in order to obtain login details and gain access to online accounts.

---

M. S. van 't Hoff-de Goede (✉)  
Centre of Expertise Cyber Security, The Hague University of Applied Sciences,  
The Hague, The Netherlands  
e-mail: [m.s.vanthoff-degoede@hhs.nl](mailto:m.s.vanthoff-degoede@hhs.nl)

E. R. Leukfeldt  
Centre of Expertise Cyber Security, The Hague University of Applied Sciences,  
The Hague, The Netherlands

Netherlands Institute for the Study of Crime and Law Enforcement (NSCR),  
Amsterdam, The Netherlands

R. van der Kleij  
Centre of Expertise Cyber Security, The Hague University of Applied Sciences,  
The Hague, The Netherlands

The Netherlands Organisation for Applied Scientific Research (TNO),  
The Hague, The Netherlands

S. G. A. van de Weijer  
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR),  
Amsterdam, The Netherlands

criminals to misuse that information. Therefore, research into internet users is essential to reduce victimization (Leukfeldt, 2017; Rhee, Kim, & Ryu, 2009; Talib, Clarke, & Furnell, 2010).

If we want to prevent cybercrime victimization, we must first explain victimization. Previous cybercrime victimization studies have focused on establishing a risk profile for victims and have attempted to identify factors that could increase the risk of victimization. In these studies, personal characteristics and routine activities are often central, for example, by assuming that certain routine activities, such as using social media, make potential victims more visible to cybercriminals. However, taking the studies together, it does not seem possible to establish an unambiguous risk profile (Bossler & Holt, 2009, 2010; Holt & Bossler, 2013; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Van de Weijer & Leukfeldt, 2017). Cybercriminals are apparently not too picky and do not select whom they attack: Everyone is a potential victim of cybercrime. Moreover, it appears that certain online activities are only related to the risk of victimization of specific forms of cybercrime. There do not seem to be any routine activities that are by definition risk-increasing (Leukfeldt & Yar, 2016). It is thus not possible to outline a profile of high-risk personal characteristics or routine activities for cybercrime victimization (Leukfeldt, 2014).

The current study focuses on the behaviour of internet users in explaining online victimization. It has been widely recognized that humans are the “weakest link” in cybersecurity. Unsafe online behaviour, such as using weak passwords and not updating software regularly, may increase the risk of cybercrime victimization (Leukfeldt, 2014; Shillair et al., 2015). However, knowledge about how citizens defend themselves against cybercrime is scarce (for an overview, see, for example, Leukfeldt, 2017). It is still unknown how well internet users protect themselves against cybercrime, partly because how people *say* or *think* they behave online is not always the same as how people *actually* behave online (Crossler et al., 2013; Debatin, Lovejoy, Horn, & Hughes, 2009; Workman, Bommer, & Straub, 2008). However, such knowledge is indispensable for the empirical foundation of possible behavioural interventions. It is therefore necessary to gain more insight into the way internet users actually behave online and which factors are associated with this.

This chapter will outline the development of the research tool for the online behaviour and victimization study that can measure actual online behaviour along with possible explanatory factors. The added value of this research instrument is evident: we go beyond existing studies that are often based on self-report by measuring both perceived and actual behaviour among a large-scale sample. Moreover, we do aim to explain not only victimization of specific forms of cybercrimes, but also several clusters of online behaviour. After all, there are many types of behaviour that increase the risk of certain cybercrimes. In addition, simultaneously, it does not have to be the case that a certain behaviour always leads to a certain form of victimization. On one occasion, falling for a phishing email can lead to an empty

bank account, while on another, it can lead to a ransomware<sup>2</sup> infection or be the start of a spear phishing<sup>3</sup> attack on the company where the victim works (see, for example, Leukfeldt, Kleemans, & Stol, 2017; Lusthaus, 2018). Therefore, the research instrument presented in this chapter objectively measures a number of behaviours that we know to be directly related to the victimization of various cybercrimes, such as sharing personal information and using weak passwords. Furthermore, this research instrument is innovative because it measures various explanations for online behaviour and victimization, while existing studies often only examine attitudes or awareness. Finally, the tool includes several experiments to determine, for example, whether persuasion techniques used by criminals make individuals more likely to engage in unsafe online behaviour.

## Online Behaviour and Cybercrime Victimization

### *Unsafe Online Behaviour as a Predictor of Online Victimization*

Unsafe online behaviour can directly contribute to increased risk of victimization. Victims of online banking fraud, for example, often appear to have inadvertently given their personal information to fraudsters, for example by clicking on a hyperlink in a phishing email or entering information on a phishing website (Jansen, 2018; Jansen & Leukfeldt, 2015, 2016).

An important condition for online safety is therefore safe online behaviour (i.e. cyber hygiene behaviour, Cain, Edwards, & Still, 2018). People who behave safely online—or cyber hygienically—adhere to “golden” rules (best practices). For example, they avoid unsafe websites, prevent clicking on unreliable hyperlinks, use strong passwords and keep their technical security measures up to date (Cain et al., 2018; Crossler, Bélanger, & Ormond, 2017; Symantec, 2018). Based on previous empirical studies, we identified seven central behavioural clusters for this study: password management, backing up important files, installing updates, using security software, being alert online, online disclosure of personal information and handling attachments and hyperlinks in emails. When internet users display safe behaviour within each cluster, this may protect them from cybercrime victimization (for more information, see Cain et al., 2018; Crossler et al., 2017; Van Schaik et al., 2017).

Previous studies, based on both self-reported behaviour and actual behaviour in experimental settings, have shown that many people only behave safely online to a limited degree or even display patently unsafe online behaviour, on each of the

---

<sup>2</sup>Ransomware is a malicious software that blocks a computer or encrypts files. Only when you pay a ransom you are able to use the computer or files again.

<sup>3</sup>Spear phishing is a targeted phishing attack against a person or a specific group of people.

seven behavioural clusters. Many people do not have a malware<sup>4</sup> scanner or firewall on their home computer, or do not keep them up to date (Cain et al., 2018; Van Schaik et al., 2017). In addition, young people are lax with their smartphone security (Jones & Heinrichs, 2012; Tan & Aguilar, 2012). While the use of unique strong passwords is an important security measure, studies have shown that 50–60% of passwords are reused across platforms, and that many people would share their passwords with others (Alohali, Clarke, Li, & Furnell, 2018; Cain et al., 2018; Kaye, 2011). Another example of unsafe online behaviour is that people share personal information on social media on a large scale (Christofides, Muise, & Desmarais, 2012; Debatin et al., 2009; Talib et al., 2010), which can be used to make phishing emails more credible (spear phishing) or to commit identity fraud. For example, many of the respondents in the study by Talib et al. (2010) shared their full name and email address (62%), date of birth (45%), or full address (7%) on an online social network. Finally, online deviant behaviours, such as illegal downloading, online bullying and threatening others, are common and contribute to online victimization, possibly especially among young people (Bossler & Holt, 2009; Holt & Bossler, 2013; Maimon & Louderback, 2019; Ngo & Paternoster, 2011).

A further conclusion that can be drawn from the literature is the added value of focusing on behaviour rather than on specific cybercrimes. Hacking victimization, for example, can be caused by many different behaviours. For example, people can be hacked because they have shared personal information, downloaded malware, or do not have up-to-date security. Moreover, these behaviours can also lead to victimization of other forms of cybercrime, such as online fraud or identity fraud. Studies that focus on specific crimes only provide insight into a small part of the complexity of online behaviour and cybercrime. By focusing on online behaviour, on the other hand, a wide range of cybercrimes can potentially be tackled.

## *Explaining Online Behaviour*

Although safe online behaviour may be of great importance to prevent cybercrime victimization, unsafe online behaviour is common. How can this be explained? Based on two theories that have previously been used to explain behaviour, Protection Motivation Theory (PMT) (Floyd, Prentice-Dunn, & Rogers, 2000; Norman, Boer, & Seydel, 2005) and the COM-B framework (Capability, Opportunity, Motivation, Behaviour) (Michie, Van Stralen, & West, 2011), several constructs can be distinguished that each may play a role in unsafe online behaviour. These are motivation for safe online behaviour, knowledge about safe online behaviour (i.e. awareness) and opportunity for safe online behaviour. After discussing these factors and previous studies on their relationships with online behaviour, this chapter will also focus on other potentially relevant factors.

---

<sup>4</sup>Malware is malicious software that is installed on your computer unsolicited and usually unnoticed. Examples of malware are viruses, Trojan horses, worms, and spyware.

## Motivation

According to PMT, how well we protect ourselves is influenced by the degree to which we are motivated to protect ourselves (Floyd et al., 2000; Norman et al., 2005). People with high protection motivation supposedly act more cautiously and take measures to protect their safety (Crossler & Bélanger, 2014; Floyd et al., 2000). It is argued in PMT that protection motivation is influenced by coping appraisal and threat appraisal; a persons' evaluation of the threat and the measures against this threat (Floyd et al., 2000). Both threat appraisal and coping appraisal have several components. The components of threat appraisal are perceived vulnerability (assessment of one's own vulnerability to the threat) and perceived severity (assessment of the severity of the threat). Coping appraisal includes the components response-efficacy (whether a measure will be effective against the threat), self-effectiveness (whether he/she is able to implement an effective measure) and response costs (whether the estimated costs of taking measures are worth it).

PMT has previously been applied to online behaviour. Previous studies found that estimated response-efficacy, self-efficacy and response costs seem to be important predictors of safe online behaviour (Arachchilage & Love, 2014; Crossler et al., 2017; Crossler & Bélanger, 2014; Jansen & van Schaik, 2017; Rhee et al., 2009; Van Schaik et al., 2017; Workman et al., 2008). However, perceived vulnerability may not be related to safe online behaviour in the expected manner. People who consider themselves vulnerable to online attacks do not behave differently (Jansen, 2018) and may even behave less safely (Crossler & Bélanger, 2014). Related to perceived vulnerability, Boss, Galletta, Lowry, Moody, and Polak (2015) found that fear of victimization did not seem to affect the intention of computer users to back up their files, while it did seemed to increase their intention to use anti-malware software. Finally, most studies find a relationship between perceived severity and online behaviour (Crossler et al., 2017; Jansen, 2018; Jansen & van Schaik, 2017). However, Downs, Holbrook, and Cranor (2007) did not find the estimated severity of the consequences of a successful phishing attack to be a predictor for precautionary behaviour in their sample of 232 computer users.

Unfortunately, very few studies have gone beyond studying protection motivation and attitudes to measure online behaviour. The few that did mainly focused on self-reported precautionary behaviour. It remains unclear how motivation may be related to actual online behaviour.

## Knowledge/Awareness

The theoretical COM-B framework (Michie et al., 2011) suggests that in addition to motivation, a necessity for safe online behaviour is capacity (i.e. knowledge about online safety), also referred to as awareness. Examples are knowledge about online threats, information security, safety measures and being able to recognize malicious URLs.

Previous studies that investigated the extent to which knowledge of IT and cybersecurity influences online behaviour yielded ambiguous results (Alohali et al., 2018; Arachchilage & Love, 2014; Cain et al., 2018; Downs et al., 2007; Holt & Bossler, 2013; Ovelgönne, Dumitras, Prakash, Subrahmanian, & Wang, 2017; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Shillair et al., 2015). For example, Arachchilage and Love (2014) showed that knowledge, such as recognizing an unreliable URL, increases self-efficacy and may contribute to phishing risk-avoiding behaviour. In addition, people who are able to evaluate URLs, understand internet icons and internet terms may be less vulnerable to phishing attacks (Downs et al., 2007). Furthermore, people who say they are IT experts seem less likely to display unsafe online behaviour (Alohali et al., 2018). On the other hand, Ovelgönne et al. (2017) found that software developers exhibit risky online behaviours more often than other respondents do. Although this may be related to people overestimating their knowledge of internet security in some cases, thereby unjustly classifying themselves as an IT expert (Debatin et al., 2009), Cain et al. (2018) found that people who considered themselves experts in IT behave less safely online. Moreover, no difference in safe behaviour was found between those who were trained in IT or cybersecurity and those who were not. These studies have made an important step towards exploring the relationship between knowledge and online behaviour. However, findings are still undecided and more research is needed, in particular to study actual online behaviour and its association with knowledge.

## Opportunity

According to the COM-B framework, knowledge and motivation alone may not be enough to elicit safe online behaviour. Opportunity is also needed, which refers to the social and material environment that make behaviour possible or impossible (Michie et al., 2011). While the association between opportunity and behaviour has attracted the attention of researchers in other fields, such as dietary behaviour (Michie et al., 2011), research into the influence of the opportunity on online behaviour is scarce.

The social environment refers to how the people around us influence our behaviour. For example, the privacy settings of users of online social networks are related to the number of online friends with private profiles (Lewis, Kaufman, & Christakis, 2008). Moreover, Herath and Rao (2009) showed that social influence of direct colleagues and managers can have a major impact on safe online behaviour within organizations. To our best knowledge, however, the relationship between social environment and online behaviour in private settings has not been studied further.

The material environment refers to the availability of financial resources, time and tools that support safe practices. Many companies offer their employees tools, such as privacy screens, that should enable safe online behaviour. Such tools and resources can help strengthen self-confidence in displaying desired behaviour (self-effectiveness) among employees (Herath & Rao, 2009). To date, however, the role that the material environment plays in online behaviour outside companies has been

the subject of few studies. It is therefore unclear how the material environment influences online behaviour in a private setting where tools are available in a different way than in companies; citizens must actively purchase and implement safety measures and keep these up to date themselves. Financial opportunity is therefore a relevant factor: people who know they should not send personal photos with free transfer websites (knowledge) and are motivated to use a safer—paid—option (motivation) also need financial leeway to do this (opportunity).

## Other Factors

Another factor that can influence online behaviour is people's previous experiences, such as previous cybercrime victimization. Past experiences can be an important predictor of future behaviour (Debatin et al., 2009; Rhee et al., 2009; Vance, Siponen, & Pahlila, 2012). People may adjust their online behaviour after they have become victims of a cyberattack and start to behave safer. For example, Facebook users who have had unpleasant experiences because they had shared personal information on the platform seem to be more aware of the risks and better able to protect themselves (Christofides et al., 2012; Debatin et al., 2009). However, not all studies point in this direction and previous victimization may not always directly lead to a change in online behaviour (Cain et al., 2018).

It has also been argued that self-control is related to online behaviour (Bossler & Holt, 2010; Ngo & Paternoster, 2011). Self-control theory states that people with low self-control are impulsive, do not avoid risks and mainly focus on the short term (Gottfredson & Hirschi, 1990), which could increase their risk to be victims of cybercrime more frequently (Ngo & Paternoster, 2011). The link between self-control and online victimization, however, may be indirect through other factors, such as motivation (Floyd et al., 2000) being more active online (Van Wilsem, 2013), delinquent behaviour and associating with offenders (Bossler & Holt, 2010). It remains unclear, however, if and how the relationship between self-control and online victimization is influenced by online behaviour or how self-control is related to online behaviour.

Another potentially important predictor of online behaviour is "locus of control", a term that refers to the sense of responsibility that people have with regard to their own safety (Rotter, 1966). Whether someone considers themselves responsible (i.e. internal locus of control) or places that responsibility on others, such as the police or the bank (i.e. external locus of control), may affect the actions that they take to prevent a successful cyberattack, i.e. the way they behave online (Debatin et al., 2009; Jansen, 2018; Workman et al., 2008). It is expected that someone with a high internal locus of control will take responsibility and is motivated to take their online safety into their own hands. Indeed, previous studies found a positive significant association between locus of control and safe online behaviour (Jansen, 2018; Workman et al., 2008). However, it is also possible that a greater sense of responsibility leads to an unjustified sense of security. When people consider themselves responsible and capable of protecting themselves from cybercriminals, they may underestimate online risks (Rhee et al., 2009), which may result in unsafe online behaviour.



## Measuring Online Behaviour

Online behaviour, and the degree to which it is safe or unsafe, has so far been measured in two ways. Some researchers have measured perceived behaviour by asking how respondents typically behave or how they would behave in a fictional online situation. In other studies, actual online behaviour has been observed. This section will provide an overview of the methods used in previous studies.

### *Research into Self-Reported Behaviour*

Most previous studies into online behaviour have focused on self-reported behaviour. Respondents in these studies were asked about their behaviour using items (e.g. “I open emails from unknown senders”) or questions (“What percentage of your passwords do you change every three months?”) (Cain et al., 2018; Crossler & Bélanger, 2014). An example of a research tool that works with propositions is the Human Aspects of Information Security Questionnaire (i.e. HAIS-Q; Parsons et al., 2014, 2017). In particular, this instrument measures knowledge, attitudes and perceived behaviour on a number of relevant topics, such as password management.

Self-reported behaviour can also be investigated in questionnaires research using vignettes and role-play (Downs et al., 2007; Jong, Leukfeldt, & van de Weijer, 2018; Sheng et al., 2010). These methods make it possible to ask respondents about the behaviour they think they would exhibit in a fictitious situation set out by the researchers (Vance et al., 2012). An important advantage of this research method is that it enables researchers to determine situational factors that could cause bias in questionnaire research. In a role-play, researchers can, on the one hand, equate certain factors among everyone (e.g. “imagine your name is Tom Johnson and you work at a bakery”). On the other hand, researchers can manipulate factors, whereby subgroups of respondents are presented with an adapted situation. For example, researchers may differentiate between subgroup one (“imagine you have never been a victim of a crime”) and subgroup two (“imagine you have been defrauded in an online web shop in the past”). Based on the outlined circumstances, respondents are asked how they would act in this situation (Downs et al., 2007; Jong et al., 2018; Sheng et al., 2010).

Questionnaire research has several advantages as a research method. For example, the investments needed for questionnaire research are relatively low, while a large representative research population can be achieved. The answers to standardized questions are also suitable for quantitative analysis in order to distinguish explanatory factors and easily compare answers between respondents.

However, there are also drawbacks to researching behaviour using questionnaires and vignettes. In studies of self-reported behaviour, researchers focus on how people say they typically behave online or would behave in a hypothetical situation. Although most people indicate that cybersecurity is important (Madden & Rainie,



2015), their self-reported behaviour does not always correspond to their actual behaviour (Smith & Louis, 2008; Spiekermann, Grossklags, & Berendt, 2001). When research focuses solely on self-reported online behaviour, it may result in an incorrect picture of how people actually behave online.

## *Research into Actual Online Behaviour*

Instead of self-reported behaviour, research can also measure actual behaviour. Previous studies where actual behaviour has been measured are scarce within the domain of cybersecurity. The studies that have been carried out mostly focus on phishing victimization. These studies often use phishing tests, using both fake phishing emails and legitimate emails, to measure the degree of susceptibility to phishing, i.e. to test their resistance to phishing attacks (see, for example, Cain et al., 2018, for an overview). By measuring how often the hyperlinks in the emails are clicked and how often people who click actually leave confidential or personal information on a legitimate or phishing website, it can be determined how safe people behave online regarding phishing. An important objection of this method is that people are misled for research purposes as participants in a phishing test often have not given permission to participate in advance.

Kaptein, Markopoulos, De Ruyter, and Aarts (2009) looked at how easy it is to persuade people to give out personal information. More specifically, they looked at a type of information that cybercriminals can use in phishing attacks: email addresses. Participants first completed a survey that consisted of so-called dummy questions: the questions did not matter. The actual measurement took place after respondents completed the survey. Respondents were asked to provide email addresses of friends and acquaintances who may also want to participate in the survey. Various persuasion techniques were applied to this request. For example, respondents were told that other respondents had already given different email addresses to the researchers (social proof) or that they would have the results of the study sent to them if they provided at least one email address (reciprocity). Applying a persuasion technique resulted in significantly more email addresses being retrieved.

Junger, Montoya Morales, and Overink (2017) have gone a step further. They looked at how easy it is to entice people to provide personal information that can be used in a more effective form of phishing, namely spear phishing, where the victim's personal information is used to give him or her a false sense of security. In the study, people were approached on the street to take part in a survey. In this survey, a number of questions were asked about online shopping behaviour: whether they had ever bought something online, and if so, where and what. They were also asked to provide part of their personal identification number and email address. Surprisingly, people were willing to give such personal information to the interviewers. With this information, a very targeted and effective (spear) phishing attack can potentially be carried out.

There are, however, several downsides to these types of studies. Although they provide better measurements of actual online behaviour, the studies are often performed on a small scale and few other factors are observed. Therefore, the observed actual online behaviour cannot be contributed to explanatory factors. Moreover, measurements of actual behaviour are not feasible in all situations, for example if we want to know how people behave during an actual ransomware attack. In addition, such measurements can be costly to perform and time consuming.

### ***Self-Reported Behaviour Versus Actual Behaviour***

Online behaviour can thus be measured in various ways. We argue that measures of actual behaviour are preferable to self-reports of behaviour. Self-reports can deviate from reality because they appeal to the memory of respondents or because respondents may give socially desirable answers. Therefore, measures of actual online behaviour can make a major contribution to our knowledge of the circumstances that influence online behaviour (Maimon & Louderback, 2019). However, such measurements also have practical disadvantages. For each study, it will therefore be necessary to determine the most suitable way of measuring online behaviour in terms of costs and benefits.

A combination of the best of both worlds can be achieved through a “population-based survey experiment”, also called an “experimental survey” (Mutz, 2011). This method combines the advantages of questionnaire research, such as the possibility to study a large representative sample, with the advantages of experimental research, in which actual behaviour can be measured and causal relationships can be determined (Mullinix, Leeper, Druckman, & Freese, 2015). In practice, such an experimental survey often consists of an online questionnaire with built-in experiments. Respondents can be manipulated through these experiments (such as by imposing time pressure). In addition, measurements of actual behaviour can be taken during the survey.

## **Online Behaviour and Victimization Study**

### ***Outline of the Research Instrument***

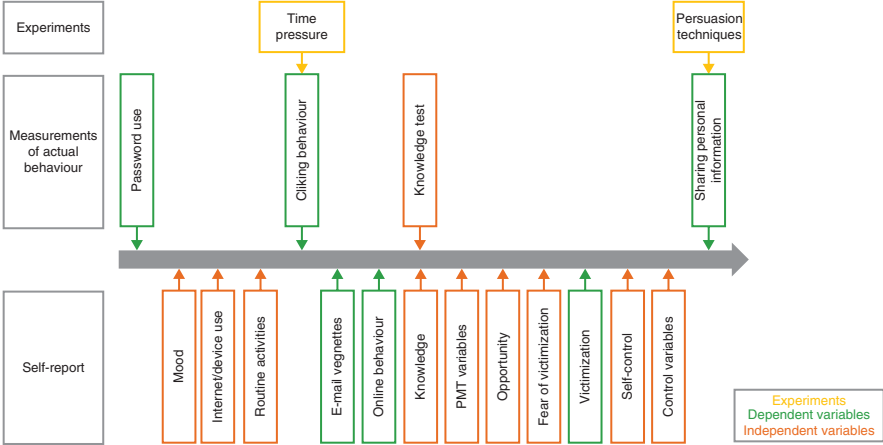
The aim of the online behaviour and victimization study was to build a research instrument that can measure actual online behaviour simultaneously with possible explanatory factors that have emerged from the literature. A population-based survey experiment was used, consisting of a questionnaire containing questions and vignettes on self-reported online behaviour and explanatory factors (presented in Table 1 and discussed in section “Explaining Online Behaviour”), as well as measurements of actual online behaviour with experimental manipulations. Moreover,

**Table 1** Overview of survey topics, other than online behaviour

Section	Theoretical model	Topics
Motivation	PMT & COM-B	Protection motivation
Knowledge	COM-B	Self-reported knowledge of online safety
		Knowledge test (objective)
Opportunity	COM-B	Material opportunity
		Social opportunity
Mood		Mood (PANAS)
Victimization		Fear of victimization
	PMT	Previous online victimization
Self-control		Self-control (BSCS)
Device		Type of device used to fill out survey
		Use of online devices
		Security measures
Time pressure		Time pressure
Persuasion technique		Authority
		Reciprocity
Threat appraisal	PMT	Perceived vulnerability
		Perceived severity
Coping appraisal	PMT	Response-efficacy
		Self-effectiveness
		Response costs
Locus of control		Locus of control
Control factors		Gender
		Education level
		Age
		Daily activity/occupation
		Cohabiting (yes/no)
		Children (< age 16) in household
Routine activities		Internet use
		Online activities

background characteristics of respondents (e.g. age, gender, educational level, occupational status), respondents' mood (e.g. the degree to which someone feels optimistic or depressed) and the device that was used are measured to include as control variables. Figure 1 schematically shows the order in which the different sections of the survey are presented to the respondents.<sup>5</sup> The used items are based on existing questionnaires, which, if necessary, were translated into Dutch and adapted to the specific context of this study. If no questionnaire was available, such as for measuring opportunity, a questionnaire was developed by the researchers themselves.

<sup>5</sup>An English translation of the original Dutch questionnaire is available upon request from the authors.



**Fig. 1** Schematic overview of the order of survey sections

*Measuring Seven Clusters of Online Behaviour*

The research instrument presented in this chapter measures seven behavioural clusters, based on the literature study. In this experimental survey, online behaviour is measured in three ways. First, all behavioural clusters are measured through self-reports (see Table 2 and items in Appendix). Second, real phishing emails were adapted to be used as vignettes in order to measure respondents’ handling of (phishing) emails. Respondents are shown three emails addressed to a fictional person: two phishing emails, supposedly from a bank and a festival organization, and one legitimate email from an internet provider. Respondents are asked to pretend to be this fictional person. Respondents are then asked to choose from nine options on how they would respond to each of these emails (e.g. reply, click on link, etc.). Respondent behave unsafely if they reported opening the linked website from one or both phishing emails.

Third, respondents encounter (fictitious) cyber-risk situations while completing the survey (see section “Measuring Seven Clusters of Online Behaviour” for more details), in order to measure actual online behaviour within the clusters “password management”, “being alert online” and “online disclosure of personal information”. It proved impossible to measure actual online behaviour within the other behavioural clusters for a number of reasons. First, mimicking cybercrime is not always possible or morally justified, for example, in the case of testing technical preventive measures. In some cases, it has also been proven technically unfeasible to incorporate a measurement in the questionnaire in a satisfactory manner. Therefore, a pragmatic approach was taken, and it was decided only to measure behaviour in an objective manner if this was possible in a practically feasible and morally responsible manner. Table 2 provides an overview of the ways in which each online behaviour cluster is measured in the survey.

**Table 2** Overview of measurements of online behaviour per behavioural cluster

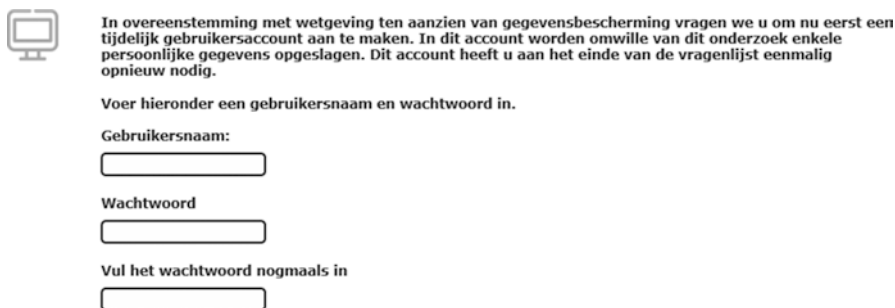
Online behaviour	Method		
	Self-report: questionnaire	Self-report: vignette	Objective measurement
1. Password management	Yes		Yes: <i>password strength</i> No <i>experimental condition</i>
2. Backing up important files	Yes		
3. Installing updates	Yes		
4. Using security software	Yes		
5. Being alert online	Yes		Yes: <i>clicking behaviour</i> <i>Experimental condition:</i> <i>Time pressure</i>
6. Online disclosure of personal information	Yes		Yes: <i>disclosure of personal information</i> <i>Experimental condition:</i> <i>Persuasion techniques</i>
7. Handling attachments and hyperlinks in emails	Yes	Yes	

**Detailed Description of the Measurements of Actual Online Behaviour**

The measurements of actual online behaviour in the experimental survey of the online behaviour and victimization study will now be described in detail. There are three objective measurements of online behaviour included in the survey (Table 2). While completing the survey, respondents encounter, unbeknownst to them, three simulated cyber-risk situations, and how respondents deal with these situations is registered. First, at the beginning of the questionnaire, respondents are asked to create a username and password for privacy reasons (see Fig. 2).<sup>6</sup> While the chosen password is not registered, the strength of the chosen password is measured. This allows researchers to determine the strength of the passwords respondents choose to protect their personal information. At the end of the survey, respondents are asked a control question to investigate if they would normally choose a similar type of password: “did you choose a password similar to those you would normally choose to protect your personal data?”

<sup>6</sup>The objective measurement of password management is displayed in the picture, a print screen of the survey. In English, this states: In accordance with Dutch privacy legislation, we now ask you to create a temporary user account. For the purpose of this study, your personal data will be stored in this account. You will need to use this account one more time, at the end of the questionnaire. Please enter a username and password below.

Username:  
Password:  
Re-enter password:



In overeenstemming met wetgeving ten aanzien van gegevensbescherming vragen we u om nu eerst een tijdelijk gebruikersaccount aan te maken. In dit account worden omwille van dit onderzoek enkele persoonlijke gegevens opgeslagen. Dit account heeft u aan het einde van de vragenlijst eenmalig opnieuw nodig.

Voer hieronder een gebruikersnaam en wachtwoord in.

Gebruikersnaam:

Wachtwoord

Vul het wachtwoord nogmaals in

Fig. 2 Screenshot of measurement of password management

**Voordat u de volgende vraag beantwoordt, vragen wij u eerst een kort filmpje over online winkelen te bekijken (30 seconden). Klik in onderstaande scherm op de afspeelknop .**



Fig. 3 Screenshot of measurement of being alert online

Later in the survey, the extent to which respondents are alert while online is measured. Respondents are asked to watch a short video before answering the next question. However, the video does not start playing. Suddenly, a pop-up appears stating that software needs to be downloaded, called “Vidzzplay” (see Fig. 3).<sup>7</sup> This software supposedly comes from an unknown source (thus unreliable). Here

<sup>7</sup>The objective measurement of clicking behaviour is displayed in the picture, a print screen of the survey. In English, this states: Before you answer the next question, we ask you to watch a short video on online shopping (30 s). Click on the play button in the screen below. //This video is being processed. Try again later. //We are sorry. //User account management. //Do you allow the following program from an unknown publisher to make changes to this computer? //Program name: Vidzzplay. //Publisher: unknown // Origin: <http://vidzzplay.play>//yes/no.

researchers can see which choice the respondents make: download the software (unsafe choice), not download (safe choice) or skip the question (safe choice).

Third, at the end of the questionnaire, respondents are asked to share personal information. This starts with standard questions, such as marital status, but the privacy value of the information increases with each question, such as their full name, date of birth and email address, and ends with asking for the final three digits of their bank account. For each question, respondents are able to click on the button “I’d rather not say”, which is considered the safe choice. If respondents fill out their personal information, the contents of their answer are not registered but only that they have answered the question. The more types of personal information respondents share, the more unsafe their behaviour is.

## *Experiments*

In two of the measurements of actual online behaviour, experimental conditions are included (Table 2). In these cases, variations to an objective measurement of actual online behaviour are presented to different subgroups of respondents. In the first experiment, during the objective measurement of “clicking behaviour”, where respondents are asked to download software, time pressure is imposed on half of the respondents. Respondents are asked to fill out a part of the survey in no more than 5 min. In the experimental condition, respondents are told that this was not sufficient time for previous respondents, and are urged to work fast-paced. Other respondents are informed that 5 min is sufficient time and that they can continue working at their own pace. Then, respondents are asked about their online routine activities. Hereafter, the respondents are asked to watch a video and the pop-up requesting permission for a software download appears (measurement of actual clicking behaviour). Control questions concerning the time pressure experienced are asked hereafter.

The second experiment takes place during the objective measure of “online disclosure of personal data”, in which respondents are asked to enter personal data such as their address and the last three digits of their account number. Various persuasion techniques are used to manipulate respondents’ willingness to share personal information (1/3 the “authority” persuasion technique, 1/3 the “reciprocity” persuasion technique, 1/3 no persuasion technique). All respondents are told, “we would like to ask you some final questions”. One third of the respondents moves on to the questions for personal information without a persuasion technique. In the reciprocity category (one third of respondents), respondents are promised a chance of winning a gift certificate if they fully complete all questions concerning personal information. In the authority category (one third of respondents), the researchers urge the respondents to fully complete all their personal information because of the importance of the scientific study.



## Discussion

This chapter outlined the development of a research instrument for the online behaviour and victimization study. The literature review that was conducted at the start of this study clearly shows that there is a lack of studies that measure actual online behaviour. One explanation for this is that this research area is still relatively young. Most studies that have been conducted can be seen as exploratory or mainly test whether existing criminological or psychological models can be used to explain self-reported unsafe online behaviour or cybercrime victimization (for an overview, see Leukfeldt, 2017). The available studies in which actual online behaviour has been measured had to deal with limitations because, for example, a non-representative sample was used. Moreover, while these studies have yielded valuable results on the prevalence of unsafe online behaviour, they have seldom focused on a broad range of explanatory factors. A possible connection between factors such as knowledge and motivation and the prevalence of actual (objectively measured) online behaviour has hardly been investigated to date. Moreover, the association between unsafe actual online behaviour and online victimization has rarely been researched. While some studies have described online victimization that can be led back to unsafe online behaviour, such as sharing personal information online, it remains unclear how unsafe online behaviour affects the risk of online victimization, or how this may be related to individual or contextual factors.

In the online behaviour and victimization study, a research instrument has therefore been developed that offers new possibilities for the research field in various ways. It was deliberately decided to measure both self-reported and actual online behaviour. After all, we know that although most people indicate that cybersecurity is important, people's actual behaviour is not always equal to their attitudes or perceived behaviour. By using a population-based survey experiment—a method that combines the advantages of questionnaire research with the benefits of experiments—the added value of this research instrument is therefore evident: this instrument makes it possible to go beyond existing studies by measuring actual online behaviour in a large representative sample. Moreover, this instrument is innovative in another way: we do aim to explain not only victimization of specific forms of cybercrimes, but also several clusters of online behaviour. After all, it is behaviour that increases the risk of all kinds of online crime.

While designing the experimental survey, several ethical issues arose that should be discussed in detail. During the experimental survey, respondents are presented with various fictitious cyber-risk situations. Respondents are also asked to create a password and enter personal details. In addition, there was concern that (compared to other studies) striking questions and situations would deter respondents, which could result in high levels of abandonment or contacts with the help desk.<sup>8</sup> A university ethics committee has therefore approved the instrument. Requesting a password and personal data is ethically permitted, if the answers are not registered. It remains

---

<sup>8</sup> However, during a pilot of the research tool, this only occurred in low frequencies.

therefore unknown to the researchers, for example, which password respondents choose, only how strong this password is. In addition, the personal data that respondents fill in is not released to the researchers, only whether or not respondents answer a specific question about personal information. Finally, all respondents are informed (as much as possible) in advance by means of “informed consent” and are subsequently notified of the cyber-risk situations and manipulations to which they had been “exposed” by means of a “debriefing” (whether or not respondents completed the survey).

Like any measurement instrument, this research instrument also has limitations. First, the research instrument measures both dependent and at the same point in time. A second wave of data collection, in which cybercrime victimization in particular is measured over time, is necessary to examine causal relationships between behaviour and victimization.

Second, the objective measurements and experiments also each have their own limitations. Due to the length of the questionnaire, it was not possible to include objective measures and experiments for all seven behavioural clusters. Moreover, password strength is determined but it remains unknown if the password is unique and never used in other applications by the respondent, which is an explanatory factor second condition for safe password management. In addition, in accordance with the GDPR,<sup>9</sup> the information that respondents share is not recorded, thus it cannot be verified whether these are actual/correct data. When measuring whether or not respondents downloaded unsafe software (i.e. clicking behaviour), the instrument uses a pop-up made in the style of the Windows operating system. Non-Windows users are less familiar with the pop-up, which may make them more suspicious and less likely to say yes. Further development of this objective measurement is necessary, with various pop-ups that are technically actual pop-ups and are adapted to different devices and operating systems.

Third, although the method—a survey with experiments—is very suitable for doing this kind of research, it is possible that respondents feel safe in the online environment of the survey. As a result, they may be quicker to make unsafe choices than in actual cyber-risk situations in real life. This may mean that in the home environment, the percentage of unsafe behaviour is lower than is determined by the research instrument. However, it is important to mention that the purpose of the research instrument is to measure online behaviour in an apparently safe environment—criminals often also imitate a safe environment (for example, an online bank or web shop) and entice people to click on a hyperlink or give away personal information.

Finally, it is possible that participants will differ from non-participants on unregistered properties. Given the aim of the study, respondents are not fully informed in advance about the content of the study. Respondents expect to answer questions only about what they do online. Certain questions may scare participants that are of a suspicious nature. Therefore, respondents who are more suspicious/observant may drop out faster.

---

<sup>9</sup>General Data Protection Regulation, applicable in Europe; <https://gdpr-info.eu/>

Despite the limitations mentioned here, this research instrument makes it possible to study self-reported online behaviour and actual online behaviour, as well as the differences between them, and explain the occurrence of unsafe online behaviour and cybercrime victimization. This is relevant for interventions that will be developed in the future that focus on making online behaviour safer.

## Appendix: Survey Items Self-Reported Online Behaviour

Items
<i>Password management</i>
I share my personal passwords with others (R)
I use simple, short passwords, with for example only one number or capital letter (R)
I use the same password for different applications, for example, for both social media and online banking and web shops (R)
<i>Backing up important files</i>
I back up important files
I store personal information in an encrypted manner, so that others cannot easily read it
<i>Installing updates</i>
I install operating system updates on my devices as soon as a new update is available
I install updates to the apps or software that I use as soon as a new update is available
I update my security software as soon as a new update is available
<i>Using security software</i>
There is security software installed on my devices to scan for viruses and other malicious software
I use browser extensions <sup>a</sup> to help me to surf safely, such as software to block advertisements or pop-ups
<i>Being alert online</i>
I download software, films, games or music from illegal sources (R)
I use public Wi-fi (for example, in hotels, restaurants, bars, or public transport), without a VPN connection <sup>b</sup> (R)
I check the privacy settings on my devices, apps or social media
<i>Online disclosure of personal information</i>
I share personal information such as my home address, email address or telephone number via social media (R)
I am selective in accepting social media connection requests from others
<i>Handling attachments and hyperlinks in emails</i>
I immediately delete emails that I do not trust
When in doubt about the authenticity of an email, I contact the sender to ask if an email has actually been sent to me
I open attachments in emails, even if the email comes from an unknown sender (R)
R reversed item

<sup>a</sup>A browser extension is software that offers additional functionality to a browser, such as managing cookies or advertisements while surfing the internet

<sup>b</sup>A VPN (Virtual Private Network) connection gives a user secure and anonymous access to a network and thus makes the internet connection safer

## References

- Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information and Computer Security*, 26, 306. <https://doi.org/10.1108/ICS-03-2018-0037>
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312.
- Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837.
- Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1), 400–420.
- Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236.
- 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.
- Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 27(6), 714–731.
- Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, 518, 2–14.
- 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.
- Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 21(2), 343–357.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, 32, 90–101.
- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.
- Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups – 2nd annual eCrime researchers summit* (pp. 37–44). New York, NY: ACM Press.
- 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.
- Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.
- 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.
- Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, 29(4), 420–436.
- Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Doctoral thesis. Enschede: Gildeprint.
- Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *Proceedings – 5th workshop on socio-technical aspects in security and trust, STAST 2015* (pp. 24–31). Piscataway, NJ: IEEE.
- Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.

- Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*, 6(2), 205–228.
- Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, 25(2), 165–180.
- Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, 53(2), 22–30.
- Jong, L., Leukfeldt, R., & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift Voor Veiligheid*, 17(1–2), 66–78.
- Junger, M., Montoya Morales, A. L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75.
- Kaptein, M., Markopoulos, P., De Ruyter, B., & Aarts, E. (2009). Can you be persuaded? Individual differences in susceptibility to persuasion. In *IFIP Conference on Human-Computer Interaction* (pp. 115–118). Berlin: Springer.
- Kaye, J. (2011). Self-reported password sharing strategies. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems – CHI '11* (p. 2619). New York, NY: ACM.
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking*, 17(8), 551–555.
- Leukfeldt, E. R. (Ed.). (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.
- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, 57(3), 704–722.
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280.
- Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims and Offenders*, 15(1), 60–77.
- Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79–100.
- Lusthaus, J. (2018). Honour among (cyber)thieves? *European Journal of Sociology*, 59(2), 191–223.
- Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Retrieved from <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>
- Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2(1), 191.
- Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science: IS*, 6, 42.
- Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The generalizability of survey experiments. *Journal of Experimental Political Science*, 2(2), 109–138.
- Mutz, D. C. (2011). *Population-based survey experiments*. Princeton: Princeton University Press.
- Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 773.
- Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting health behaviour* (pp. 81–127). London: Open University Press.
- Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks. *ACM Transactions on Intelligent Systems and Technology*, 8(4), 1–25.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66, 40–51.

- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security*, 42, 165–176.
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816–826.
- Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, 80(1), 1.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). New York, NY: ACM.
- 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.
- Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behaviour relationship. *British Journal of Social Psychology*, 47(4), 647–666.
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In *ACM Conference on Electronic Commerce* (pp. 1–10). New York, NY: ACM Press.
- Symantec. (2018). *Security center white papers*. Tempe, AZ: Symantec. Retrieved from <https://www.symantec.com/security-center/white-papers>
- Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 – 5th International Conference on Availability, Reliability, and Security* (pp. 196–203).
- Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of Bluetooth security. *Information Management and Computer Security*, 20(5), 364–381.
- Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412.
- Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, 547–559.
- Van Wilsem, J. (2013). “Bought it, but never got it” assessing risk factors for online consumer fraud victimization. *European Sociological Review*, 29(2), 168–178.
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information and Management*, 49(3–4), 190.
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816.