Factors that influence secure behaviour while using mobile digital devices

Marcel Spruit, Deborah Oosting and Céline Kreffer
Center of Expertise Cybersecurity, The Hague University of Applied Sciences, The Hague, The Netherlands

Received 12 February 2024
Revised 18 March 2024
Accepted 4 April 2024

Abstract

Purpose – The use of mobile digital devices requires secure behaviour while using these devices. To influence this behaviour, one should be able to adequately measure the behaviour. The purpose of this study is to establish a model for measuring secure behaviour, and to use this model to measure the secure behaviour of individuals while using mobile digital devices such as smartphones and laptops.

Design/methodology/approach – Based on a wide-ranging questionnaire ($N = 1000$), this study investigates the degree of influence that a relatively large number of factors have on secure behaviour while using mobile digital devices. These factors include knowledge and cognitive attitude, but also affective attitude, as well as several types of bias.

Findings – This study has provided a model for measuring secure behaviour. The results of the measurements show that knowledge, bias, cognitive attitude and affective attitude all have impact on secure behaviour while using mobile digital devices. Moreover, none of these factors is of minor importance.

Practical implications – This study shows that it is important to also consider previously undervalued factors, such as affective attitude and various types of bias, when designing interventions to improve secure behaviour while using mobile digital devices.

Originality/value – Most research on secure behaviour has only looked at a small number of influencing factors, usually limited to knowledge and cognitive attitude. This study shows that one needs a more elaborate model for measuring secure behaviour, and that previously undervalued factors have a clear influence on secure behaviour.

Keywords Information security, Individual behaviour, Personal computing

Paper type Research paper

1. Introduction

Society is becoming increasingly digitised. Many people have mobile digital devices, such as a smartphone or a laptop. This makes it possible to have digital information and support at almost all times and everywhere. Moreover, most devices are connected to the internet, which means that people are linked to a large number of other people and systems.

The fact that the internet connects so many people and systems is useful, but it also has a downside. The internet is a melting pot of all kinds of digital threats (Bitton *et al.*, 2018; Gulshan and Chauhan, 2021). To restrict damage from these threats, it is necessary to

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2024-0035

behave securely while using mobile digital devices. This includes secure execution of actions in the digital environment on the one hand, for example not clicking on suspicious links in an email. On the other hand, it means implementation of the necessary security controls to improve the level of security, for example by using strong passwords and making regular backups. In practice, many people do not do this sufficiently (Allam *et al.*, 2014; CBS, 2022; Hewitt and White, 2021; Livingstone *et al.*, 2011; Witsenboer *et al.*, 2022).

Much research has been conducted into explaining security behaviour. A large part of this research has focused on how situation perception influences the motivation for behaviour. Perception, in turn, is based on knowledge about and interpretation of the situation (Bernstein, 2016). Models with this perspective include protection motivation theory (Rogers, 1975; Sommestad *et al.*, 2015; Verkijika, 2018) and the theory of situation awareness (Endsley, 1995; Ofte and Katsikas, 2023). Furthermore, studies were published in which people's attitude towards security was included as an influence on behaviour. Models with this perspective include the theory of reasoned action (Fishbein and Ajzen, 1980), the theory of planned behaviour (Ajzen, 1985) and the knowledge-attitude-behaviour model (Kruger and Kearney, 2006; Parsons *et al.*, 2017).

It is well-known that attitude is made up of cognitive, affective and behavioural components (Bernstein, 2016; Ostrom, 1969; Robbins and Judge, 2019; Svenningsson *et al.*, 2022). However, in most studies that include attitude, this is especially true for the cognitive component (Bitton *et al.*, 2018; Kruger and Kearney, 2006; Lebek *et al.*, 2014; Parsons *et al.*, 2017; Rahim *et al.*, 2015). Few studies have focused on the influence of affective attitude on security behaviour (Kok *et al.*, 2020; Salameh and Loh, 2022). As a result, there is little data on the influence of affective attitude on security behaviour. This applies even more to the influence of different types of bias (Boysen and Vogel, 2009; Hewitt and White, 2021). Therefore, the available research data does not provide a complete picture of which factors influence security behaviour and to what extent.

We conducted a survey into which factors influence secure behaviour while using mobile digital devices. The factors include knowledge, several types of bias, cognitive attitude and affective attitude. We investigated the extent to which these factors influence behaviour and the relative strength of their influence.

2. Theoretical background

Acting with mobile digital devices requires *secure behaviour*. This behaviour consists of actions and controls that someone performs consciously. From the behavioural science literature, we know that the main predictor for this behaviour is a person's *motivation*, also called *(behavioural) intention*, to perform the behaviour (Ajzen *et al.*, 2009; Bernstein, 2016; Lebek *et al.*, 2014; Michie *et al.*, 2011; Robbins and Judge, 2019; Sheeran, 2002). Obviously, the person must also have the *skills* required for the behaviour (Michie *et al.*, 2011). In this study, we consider only actions and controls that do not require specific difficult skills, the absence of which can be a cause of not behaving securely. Therefore, we do not consider the factor skills in this study. Furthermore, the environment must not make the necessary behaviour too difficult or even impossible, i.e. the environment must offer the person the *opportunity* to perform the required behaviour (Michie *et al.*, 2011; Pollini *et al.*, 2022). In this study, we consider only actions and controls that can be performed relatively easily in the given environment, i.e. the person is given the opportunity to perform the actions and controls. Therefore, we also do not consider the factor opportunity in this study.

Someone's *motivation* to behave securely in a given situation is influenced by the person's *(risk) perception* of that situation (Endsley, 1995; Rogers, 1975; Rundmo and Nordfjaern, 2017; Spruit, 1998). This is somewhat obvious, because a person must first have

an idea of the risks in a given situation before motivation can arise in that person to do something about those risks. Perception, in turn, is strongly influenced by the person's *knowledge* about the situation, i.e. knowledge about the environment, the relevant threats, the potential impact of the threats and the actions and controls that are effective against these threats (Ben-Asher and Gonzalez, 2015; Rasmussen, 1983; Rohrmann and Renn, 2000; Sommestad *et al.*, 2015). To be able to behave securely while using mobile digital devices, it is sufficient to have knowledge as specified by the first three levels in Bloom's taxonomy, i.e. *remembering*, *comprehension* and *application* (Bloom *et al.*, 1956; Krathwohl, 2002). The person then knows which actions are safe in a given situation, which controls are required and how the controls should be implemented. Unfortunately, not everyone has this knowledge to a sufficient degree (CBS, 2022; EC, 2019). As a result, people do not have a good understanding of the risks they run and the behaviour that is necessary, and as a result they may not be sufficiently motivated to behave securely. In this study, we consider knowledge about threats and their impact.

If someone does have the right knowledge about the environment, the relevant threats, their potential impact and the relevant actions and controls, this does not ensure good perception. Kahneman and others have described that through various types of bias a person's *perception* may be distorted (Bernstein, 2016; Kahneman, 2011; Kahneman *et al.*, 1982; Robbins and Judge, 2019). For example, people tend to see risks that they expect to see or that fit well with their opinion (*confirmation bias*) (Klayman, 1995; Knäuper *et al.*, 2016; Nickerson, 1998). Moreover, people overestimate the risks corresponding to threats about which they have a lot of information or that received a lot of media attention (*availability bias*) (Carroll, 1978; Dubé-Rioux and Russo, 1988; Tversky and Kahneman, 1973). Furthermore, people tend to overrate their own knowledge and skills and underrate risks (*optimism bias*) (Bränström *et al.*, 2005; Campbell *et al.*, 2007; DeJoy, 1989; Nandedkar and Midha, 2012; Sharot, 2011). There are other types of bias (Kahneman, 2011), but we assume that in particular the three types of bias mentioned above could have a noticeable influence on secure behaviour while using mobile digital devices. Therefore, we consider these three types of bias in this study.

From the behavioural science literature, we know that even if someone has the right perception of the behaviour that is reasonably appropriate in a given situation, this does not necessarily mean that the person will have a positive attitude about it. The person may know which behaviour is appropriate, but still think or feel that one should behave differently. In this case, the *attitude* of that person towards the given behaviour is negative. This discourages motivation for the behaviour and by extension the behaviour itself (Abdullah *et al.*, 2020; Ajzen, 1991; Bernstein, 2016; Kummeneje and Rundmo, 2020; Robbins and Judge, 2019; Safa *et al.*, 2015; Spruit, 1998).

The *(risk) attitude* someone has towards secure behaviour while using mobile digital devices is made up of three components: *cognitive*, *affective* and *behavioural attitude* (Bernstein, 2016; Ostrom, 1969; Robbins and Judge, 2019; Svenningsson *et al.*, 2022). Usually, these components are in line with each other and reinforce each other. However, sometimes that is not the case, and attitude is mainly determined by only one of the components (Edwards, 1990; Loewenstein *et al.*, 2001).

Cognitive attitude is a reasoning-based attitude. It is based on the extent to which someone believes that the required behaviour is *useful* (effective and proportional), *urgent* and does not involve unreasonable *cost and effort* (Cialdini, 2003; Davis, 1989; Greaves, 2017; Robbins and Judge, 2019).

Affective attitude is a feelings-based attitude. It is based on a combination of feelings (Robbins and Judge, 2019). Firstly, one's *gut feeling* regarding the required behaviour, for

example, fear of computer viruses (Loewenstein *et al.*, 2001; Lupton and Tulloch, 1999). Secondly, *procrastination*, or irrational delaying of tasks, especially those that one considers less pleasant (Harriott and Ferrari, 1996; He, 2017; Solomon and Rothblum, 1984). And lastly, the *subjective norm*, or the pressure to conform to what one thinks others find desirable behaviour (Ajzen, 1991; Winter *et al.*, 2022), especially if this comes from relevant peer groups, such as colleagues, friends, parents and teachers (Asch, 1955; Lawson and Stagner, 1957), important persons, such as managers and police officers (Dobbie *et al.*, 2019; Hu *et al.*, 2012) and influencers, such as politicians and vloggers on the internet (Freberg *et al.*, 2010). In addition, *(emotional) involvement* can play a role, for example because the person has participated in formulating security actions and controls ("invented here") (De Rivera *et al.*, 2002; Hatten and Ruhland, 1995; Senge, 1996). However, the latter is less obvious with mobile digital devices, because secure behaviour while using mobile digital devices consists of standard actions and controls.

Behavioural attitude is based on aligning one's opinion and behaviour to smooth out discrepancies between the two (Festinger, 1957; Robbins and Judge, 2019; Wicker, 1969). This component is normally not the cause of certain behaviour, but rather follows from the behaviour and influences the cognitive and affective attitude in such a way that they align with the behaviour (Festinger, 1957). Since this study focuses on causes of behaviour, we do not consider this component of attitude.

Both cognitive and affective attitude can directly influence behaviour. Both components, as well as its aspects, are therefore included in this study.

If a person has an accurate perception of the behaviour that is reasonably appropriate in a given situation, and also a positive attitude towards that behaviour, then this person will not necessarily be *motivated* to carry out the behaviour in practice. This only happens if the person believes that the given behaviour is normally practicable (*perceived efficacy*) (Ajzen, 1991), and believes that they are capable of practising the behaviour themselves (*self-efficacy*) (Bandura, 1977; Safa *et al.*, 2015). Since in this study we only consider actions and controls that should be feasible for everyone, we do not include the factors perceived efficacy and self-efficacy in this study.

Finally, the expected positive or negative consequences caused by the environment can influence someone's motivation for certain behaviour. For example, the expectation of a positive consequence, such as a reward associated with the behaviour, can strengthen motivation (Bernstein, 2016; Robbins and Judge, 2019). On the other hand, the expectation of a negative consequence, such as a punishment associated with the behaviour, can weaken motivation. Since this study focuses on personal mobile digital devices, where the owner is responsible for the required behaviour, these factors are not relevant to this study.

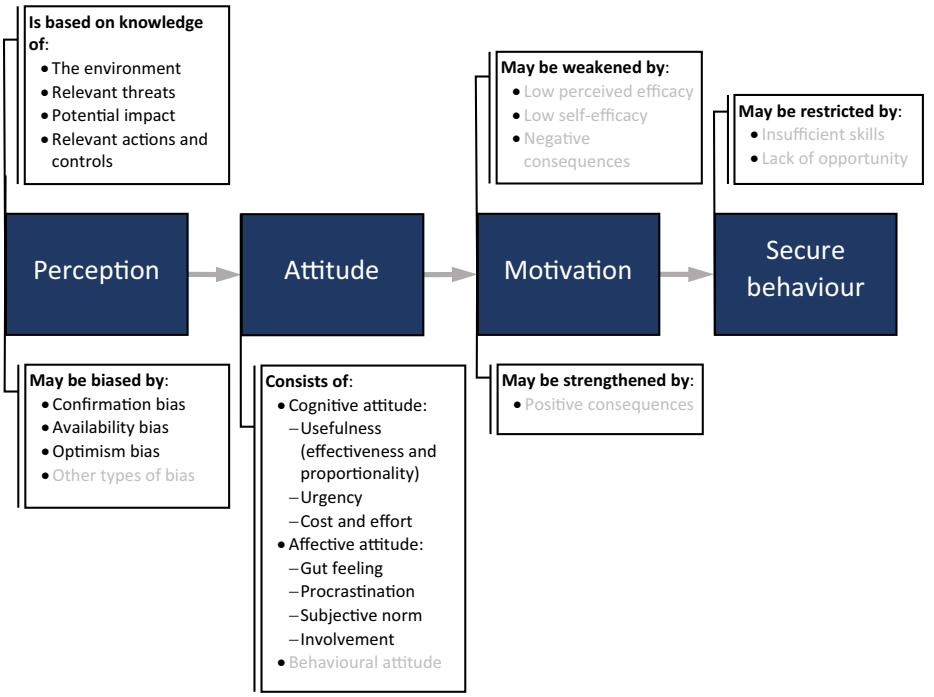
The factors that influence the extent to which someone behaves securely while using mobile digital devices such as smartphones have been summarised in Figure 1.

3. Research methodology

3.1 Participants

The questionnaire was sent out online by a panel organisation with a representative database of Dutch people aged 20 and over. The questionnaire could be filled in anonymously from a smartphone, tablet, laptop or desktop computer. No information was requested that could identify the respondent. Every response was checked for correct completion.

The respondents had to indicate whether they owned at least one smartphone, tablet or laptop. Devices on loan from an employer were not allowed as these devices may have had controls applied to them by a company administrator. The other questions in the questionnaire were solely about self-managed smartphones, tablets and/or laptops.



Notes: Factors that we do not consider relevant in this study are in grey
Source: Created by authors

Figure 1.
Factors that influence secure behaviour while using mobile digital devices

Respondents who did not own a smartphone, tablet or laptop were not included in the analysis.

3.2 Selected security practices

The questionnaire focuses on security behaviour. It looks at whether the respondent has performed certain security behaviour while using mobile digital devices. Based on eight semi-structured interviews with cybersecurity specialists (four assistant professors of computer science, two university cybersecurity researchers and two cybersecurity consultants), a number of security practices have been selected for this study. Each of the practices should be unambiguous and both necessary and common for secure behaviour while using mobile digital devices. Also, the practice should not be realised automatically by default, and both the initiative for the practice and its implementation should lie with the user of the device.

The following seven security practices have been selected:

- Use different passwords for email, online banking, online shopping and social media, with or without the help of a password manager.
- Install security software such as antimalware and a firewall.
- Use Virtual Private Network (VPN) software for a secure connection to and over the Internet.
- Check privacy settings of new apps and software and adjust them if necessary.

- Restrict access to sensitive data on social media so that this data cannot be accessed by everybody.
- Reject unnecessary cookies from websites or adjust them if necessary and possible.
- Turn off the location service on the device when this service is not required.

3.3 Factors

Several factors influence whether security behaviour is carried out. In the theoretical background, it has been argued that both a person's perception (knowledge and bias) and a person's attitude (cognitive and affective attitude) can be relevant to security behaviour in relation to mobile digital devices.

Knowledge means recognising which actions and controls are necessary and how they should be performed, as well as what the consequences may be if they are not performed.

Bias comes in several types. Not all of them are relevant to not performing security behaviour. This study includes the types of bias that could potentially influence secure behaviour while using mobile digital devices. These biases are optimism, availability and confirmation bias. With optimism bias, optimism can relate to both the possible impact of the underlying threats as well as the likelihood of their occurrence.

Cognitive attitude includes several rational aspects, namely the opinion about the usefulness of the behaviour, about the urgency of the behaviour and about the cost and effort it takes to perform the behaviour.

Affective attitude includes a number of aspects that relate to the feelings of the respondent, namely gut feeling, procrastination and subjective norm.

Table 1 summarises the factors and aspects considered in this study that may influence the necessary secure behaviour while using mobile digital devices.

Based on the theoretical background, we could not make reliable statements about the relative importance of the factors and aspects, so they have not been given different weights in advance.

3.4 Questionnaire

The respondents could indicate whether they recognised each selected security practice, and, if so, whether they had performed the practice. The questions aimed at practices for one's own mobile digital devices, so not devices on loan from the employer.

Table 1.
The factors and aspects considered that may influence secure behaviour while using mobile digital devices

Main factor	Factor	Aspect
Perception	Knowledge	Functionality
		Impact
	Optimism bias	Impact
		Probability
	Availability bias	Id.
	Confirmation bias	Id.
Attitude	Cognitive attitude	Usefulness
		Urgency
		Cost and effort
	Affective attitude	Gut feeling
		Procrastination
		Subjective norm

Source: Created by authors

The option "Sometimes" could also be chosen because: The respondents may have several devices that they use in different ways and some security practices, such as rejecting cookies, do not necessarily have to be performed at all times. For a number of practices, such as restricting access to sensitive data on social media, the respondent could also choose the option "Not applicable". Subsequently, the respondent could indicate for each known but not performed security practice which aspects from Table 1, in the respondent's view, had been a decisive cause for not performing the practice.

For each security practice, possible causes for not performing the practice have been formulated for each aspect from Table 1. Table 2 shows possible causes for not performing the practice "Use VPN software for a secure connection to and over the Internet", or in short "Use VPN software". The possible causes for not performing each of the other practices have been formulated analogously.

Respondents who had not performed a certain practice could choose the causes which had been decisive for them for not performing the practice. To prevent minor influences of aspects from being counted too heavily, a respondent could choose a maximum of two causes for each security practice that was not performed. If two aspects have been chosen, each of the two is weighted by a factor of 0.5. No other weights have been applied.

In addition, the questionnaire included some demographic questions about the respondent, as well as some questions about their internet use, the importance of their data and whether the respondent had had one or more incidents involving a mobile digital device or had witnessed an incident elsewhere.

Five people (one cybersecurity researcher and four people with different backgrounds and little knowledge about human behaviour and cybersecurity) were asked to complete the questionnaire in thinking aloud sessions (Boren and Ramey, 2000). In such sessions, the respondent reads each question aloud, while, also aloud, explaining what he or she thinks the question means, what answer he or she chooses and the rationale for the answer. If necessary, the researchers asked control questions to ensure that the answers were well understood and consistent with actual perception, attitude and behaviour. These sessions gave us the opportunity to determine whether the wording of the questions was not unnecessarily difficult and whether the interpretation of the questions was as we intended and was not ambiguous.

Table 2. Possible causes the respondents could choose for not using VPN software

Factor	Aspect	Possible cause for not using VPN software
Knowledge	Functionality	"Because I don't know how to choose/use VPN software"
	Impact	"Because government should be able to see what I'm doing on the Internet"
Optimism bias	Impact	"Because I have nothing to hide"
	Probability	"Because I'm not on the radar of criminals"
Availability bias	Id.	"Because I don't know anyone who has suffered from leaking his Internet address"
Confirmation bias	Id.	"Because it seems strange to me that I would be digitally tapped"
Cognitive attitude	Usefulness	"Because I don't see why I would use a VPN"
	Urgency	"Because I didn't think about it"
	Cost and effort	"Because using a VPN would take me too much effort/time"
Affective attitude	Gut feeling	"Because I just don't feel like it / I'm lazy"
	Procrastination	"I was planning to, but I haven't gotten around to it yet"
	Subjective norm	"Because hardly anyone uses a VPN"
		"Because people in my immediate environment don't use a VPN"

Source: Created by authors

The complete questionnaire will be made available in open access DANS EASY Repository.

4. Results

In total, we received 1,000 correctly completed questionnaires. There were no extreme outliers. The respondents were 49.4% male and 50.6% female. The average age of the respondents was 49.4 years old (SD = 16.8). The youngest respondent was 20 years old, and the oldest respondent was 89 years old. The education level of the respondents was 27.0% low, 42.4% intermediate and 30.6% high. This distribution is close to that for The Netherlands as a whole (CBS, 2023).

The observation that many people behave in a way that is not secure while using mobile digital devices is supported by this study. On average, the respondents performed 4.92 of the 7 selected security practices (SD = 1.68), albeit not always (the option "Sometimes" also counted). Figure 2 shows that only 20.7% of the respondents performed all the selected security practices, always or sometimes. More than 1% of the respondents never performed any of these security practices.

Table 3 shows that the average number of security practices performed by respondents depends on demographic factors, although the differences are small (but statistically significant). Men show a slightly higher score than women. Respondents under 50 years old score slightly higher than those aged 50 and over. Furthermore, a small increase is visible with increasing education level.

Some security practices were performed more often than others. Figure 3 shows that 92.5% of respondents always or sometimes used different passwords for online banking,

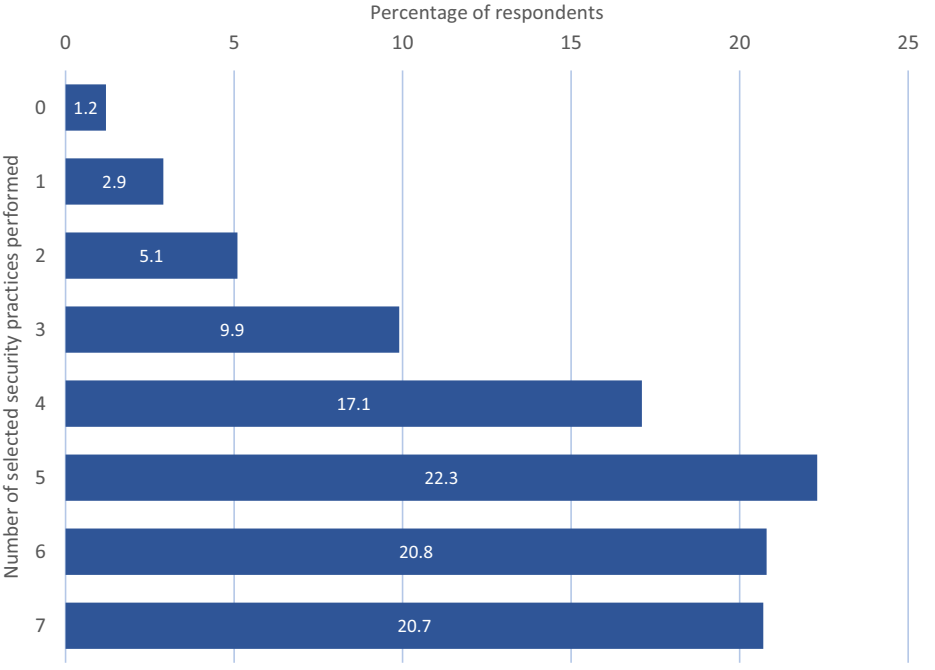


Figure 2.
Percentage of respondents that performed 0 to 7 of the selected security practices

Source: Created by authors

email, online shopping and social media, possibly using a password manager. This means that 7.5% of the respondents never performed this simple practice. At 42.6%, using a VPN to get a secure connection to and over the internet is the least performed security practice.

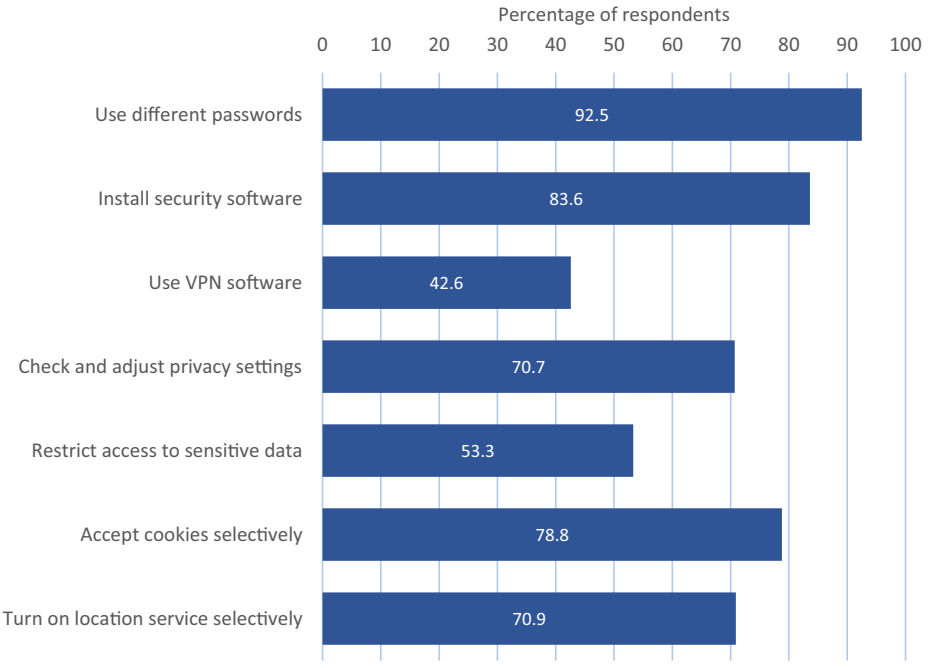
Given the large number of respondents who did not perform one or more of the selected security practices and therefore are less protected against security threats, it is important to see what the causes are for not performing the practices.

If someone does not have the knowledge required for a security practice or does not have it sufficiently, then it is either not possible for the person to perform the practice, or the

Demographic factor	*N*	Average number of practices	SD	*T*-test
All respondents	1,000	4.92	1.679	
Man	494	5.09	1.729	$t\,(998) = 3.159\ p = 0.002$
Woman	506	4.76	1.616	
Age < 50	502	5.13	1.776	$t\,(998) = -3.911\ p < 0.001$
Age ≥ 50	498	4.72	1.552	
Low level of education	270	4.60	1.701	$t_{LH}\,(574) = -3.871\ p < 0.001$
Medium level of education	424	4.96	1.608	
High level of education	306	5.16	1.720	

Source: Created by authors

Table 3.
The average number of security practices performed as a function of demographic factors



Source: Created by authors

Figure 3.
Percentage of respondents that performed a security practice

person does not understand why the practice is necessary and does not perform the practice for that reason. The lack of knowledge may relate to the functionality of the given practice or the impact it may have if the practice is not performed. Figure 4 shows the extent to which the respondents' lack of sufficient knowledge was a decisive cause for not performing each of the selected practices. The lack of sufficient knowledge with regard to both functionality and impact appear to be important causes for not performing practices.

If someone has sufficient knowledge for a security practice, but has a distorted perception due to bias, this may be a cause for not performing the practice. Figure 5 shows to what extent the respondents' distorted perception due to bias was a decisive cause for not performing each of the practices. A distinction has been made between optimism bias, availability bias and confirmation bias. Optimism bias in particular appears to have a significant influence. The availability bias and the confirmation bias have a smaller but still noticeable influence.

If someone has sufficient knowledge for a given security practice and the perception is not distorted by bias, then the person may still rationally believe that it is not necessary to perform the practice. This cognitive attitude is based on the extent to which the person believes that the practice is useful and urgent and that it does not involve unreasonable cost and effort. Figure 6 shows the extent to which the respondents' cognitive attitude was a decisive cause for not performing each of the practices. Opinion about urgency appears to have a significant influence. Cost and effort appear to play an important role for not using different passwords. Opinion about usefulness has a relatively small but still noticeable influence.

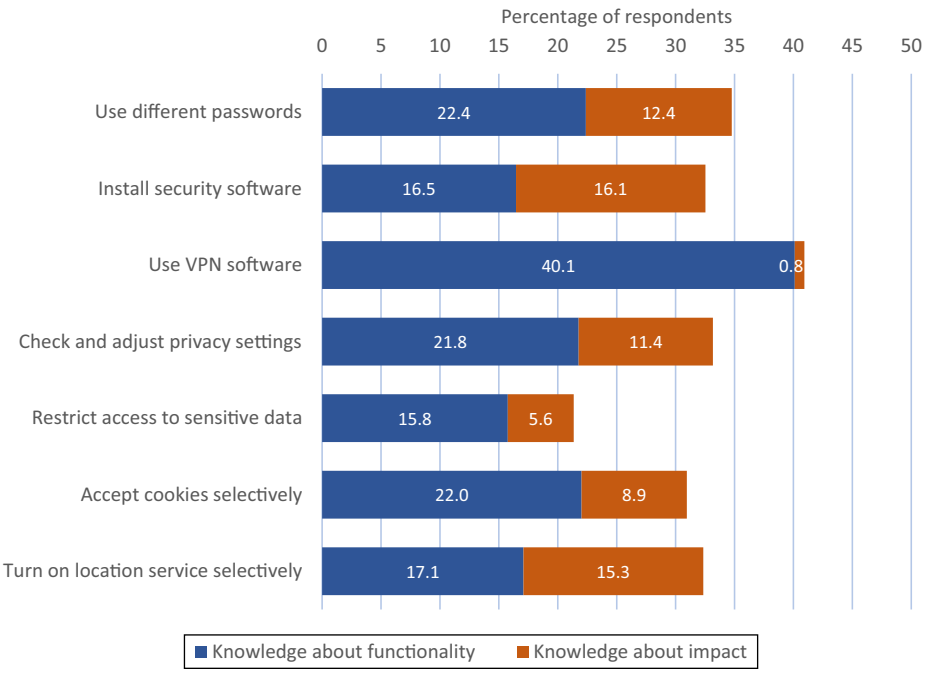
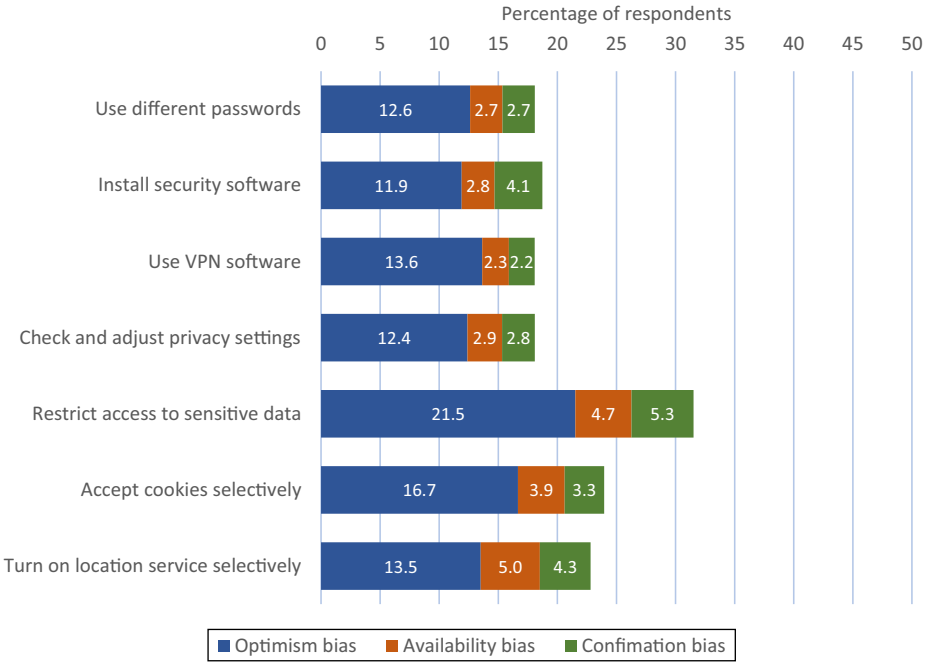


Figure 4.
Percentage of respondents for whom lack of knowledge was a decisive cause for not performing a security practice

Source: Created by authors



Source: Created by authors

Figure 5. Percentage of respondents for whom bias was a decisive cause for not performing a security practice

Affective attitude may also explain the opinion that the selected security practices do not have to be performed. Affective attitude is based on a combination of gut feeling about the practices, procrastination and subjective norm. Figure 7 shows to what extent the respondents' affective attitude was a decisive factor for not performing each of the practices. All three aspects, gut feeling, procrastination and subjective norm, appear to have a clearly noticeable influence.

All factors included in the study appear to have a greater or lesser influence on not performing the selected practices. Some factors or aspects appear to have a somewhat smaller, but noticeable, influence. These include availability bias, confirmation bias and opinion about usefulness. Other factors or aspects, such as knowledge, optimism bias and sense of urgency appear to have a substantial influence.

Figure 8 shows the relative influence of knowledge, bias, cognitive attitude and affective attitude on secure behaviour while using mobile digital devices. The figure shows that the influence of the factors is of the same order of magnitude, but there are some outliers. For example, lack of knowledge is relatively often the cause for not using VPN software. This also applies to not using different passwords, but Figure 3 shows that this only concerns a limited number of respondents. Not restricting access to sensitive data on social media is relatively often caused by bias. Figure 5 shows that it mainly concerns optimism bias.

On average, none of the factors knowledge, bias, cognitive attitude and affective attitude was overshadowed by the others. It therefore seems that previously undervalued factors also influence secure behaviour while using mobile digital devices. This mainly concerns affective attitude and various types of bias.

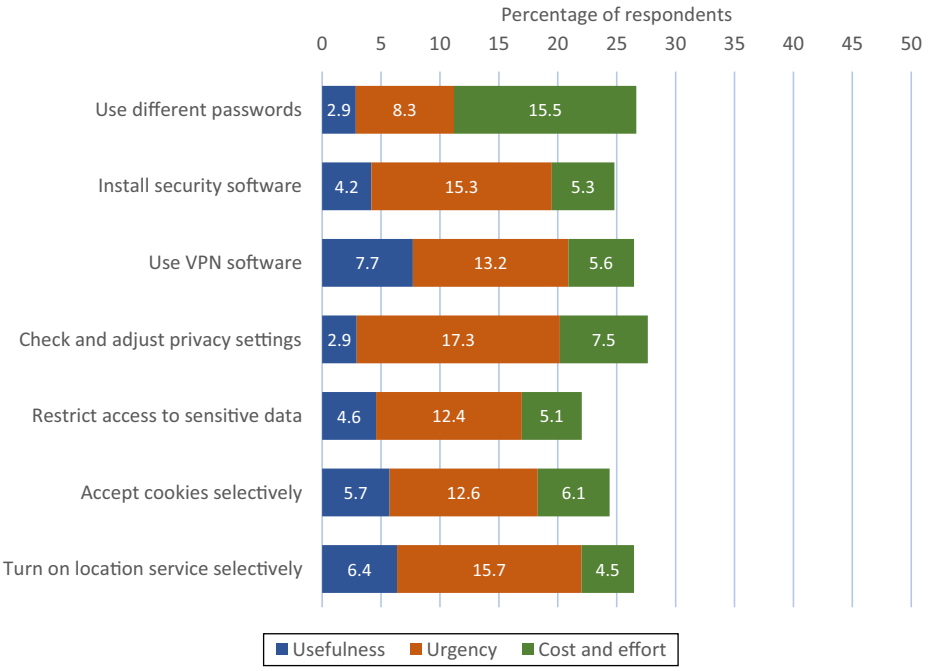


Figure 6.
Percentage of respondents for whom cognitive attitude was a decisive cause for not performing a security practice

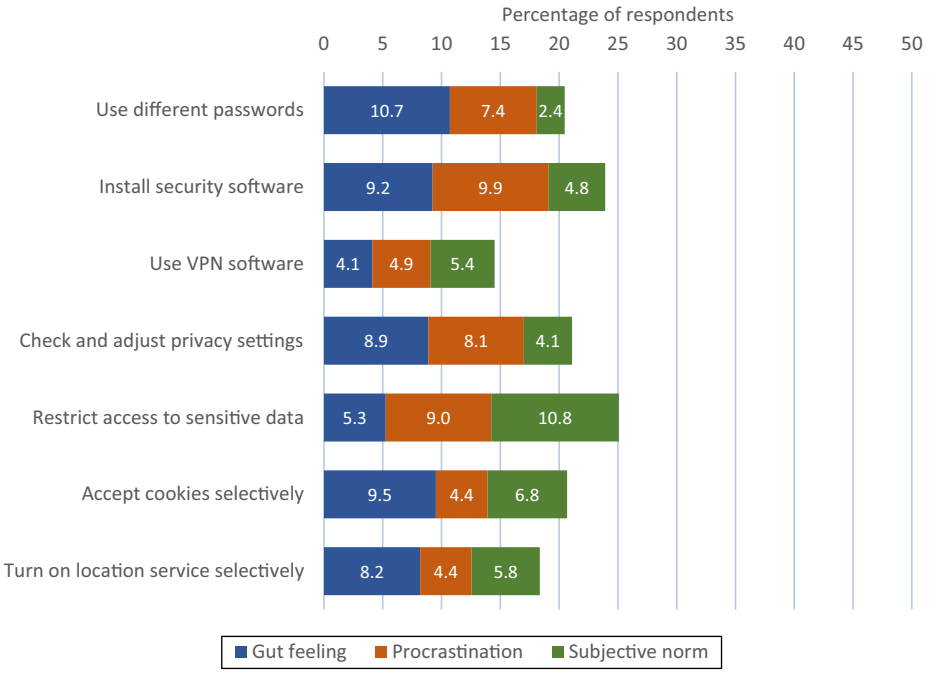
Source: Created by authors

5. Discussion

This study included three types of bias that we suspected could influence the choice of whether to perform a certain security practice. The study has shown that these three types of bias do indeed have an impact, albeit to differing degrees. However, it is possible that other types of bias may also have an influence (Kahneman, 2011; Robbins and Judge, 2019). Further research into the influence of other types of bias could provide more information.

A limitation of the questionnaire is that the influence of each of the factors could only be examined with a limited number of questions in order not to make the questionnaire too extensive and time-consuming. By conducting further research with a smaller group of people, the influence of the factors could be determined more accurately by asking more questions per factor and providing more nuanced answer options. The accuracy could be further increased by using in-depth interviews instead of a questionnaire (Adams and Cox, 2008).

Self-reporting based on a questionnaire is an effective way of finding out about security behaviour and the influence that various factors have on it. However, this kind of self-reporting is less reliable than observing behaviour in practice and then finding out the influence of factors with the help of in-depth interviews (Gollwitzer *et al.*, 2022; Junco, 2013; Kkeli and Michaelides, 2023; Prince *et al.*, 2020; Siponen and Vance, 2010). This said, behavioural observation and in-depth interviews are not feasible with a large group of people, which is why we opted for self-reporting based on a questionnaire. A number of pilot interviews were conducted in preparation for this study. The participants were questioned in an in-depth interview after they had completed the questionnaire. The interviews showed



Source: Created by authors

Figure 7. Percentage of respondents for whom affective attitude was a decisive cause for not performing a security practice

that the perceived influence of the various factors on whether to perform the selected security practices corresponds reasonably well with the outcomes of the questionnaire. In a few interviews, we saw a small deviation in the knowledge factor compared to the questionnaire they had previously completed, but in most interviews, we did not see any significant differences. Nevertheless, it is possible that the results from the questionnaire suffered from some deviation (Sember *et al.*, 2020). In addition, influences that could not be questioned reliably during the interviews may have been somewhat misjudged.

This study shows that previously undervalued factors also influence secure behaviour while using mobile digital devices. It is therefore important to take these factors into account when designing interventions to improve people's behaviour while using their mobile digital devices. Of course, a number of other factors that were not relevant to this study, such as the expected positive or negative consequences from the environment, could be relevant to designing interventions.

6. Conclusions

Although extensive research has been conducted into explaining security behaviour, most of the models that result from this research have only looked into a limited number of influencing factors. Based on a wide-ranging questionnaire ($N = 1{,}000$), this study has investigated the degree of influence for a larger number of factors on secure behaviour while using mobile digital devices such as smartphones and laptops. The results show that perception, based on knowledge and bias, as well as attitude, with a cognitive and an affective component, influence secure behaviour while using mobile digital devices. Moreover, the influence of each of these

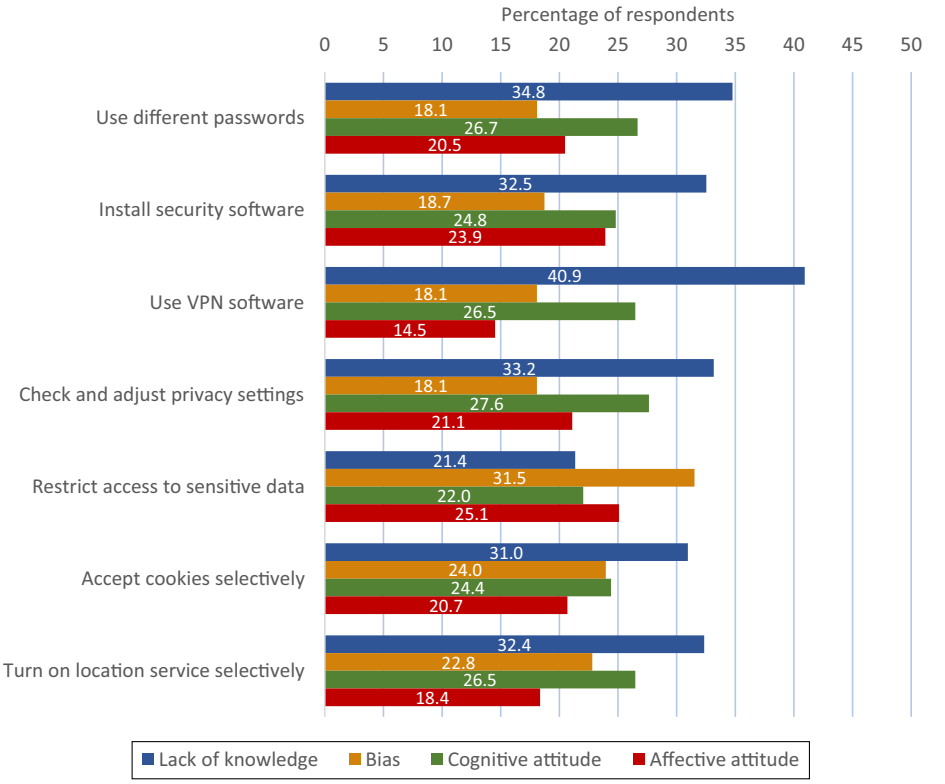


Figure 8.
Percentage of respondents for whom knowledge, bias, cognitive attitude or affective attitude was a decisive cause for not performing a security practice

Source: Created by authors

factors is clearly noticeable. None of the factors is of minor importance. Types of bias not considered in this study may also be of influence, and the influence of some factors, such as subjective norm, may have been somewhat underestimated.

This research shows that it is important to also consider previously undervalued factors, such as affective attitude and various types of bias, in further behavioural research and when designing interventions to improve secure behaviour while using mobile digital devices.

References

Abdullah, S.I.N.W., Samdin, Z., Ho, J.A. and Ng, S.I. (2020), "Sustainability of marine parks: is knowledge-attitude-behaviour still relevant?", *Environment, Development and Sustainability*, Vol. 22 No. 8, pp. 7357-7384.

Adams, A. and Cox, A.L. (2008), "Questionnaires, in-depth interviews and focus groups", in Cairns, P. and Cox, A.L. (Eds), *Research Methods for Human Computer Interaction*, Cambridge University Press, Cambridge, pp. 17-34.

Asch, S.E. (1955), "Opinions and social pressure", *Scientific American*, Vol. 193 No. 5, pp. 31-35.

Ajzen, I. (1985), "From intentions to actions: a theory of planned behavior", in Kuhl, J. and Beckmann, J. (Eds), *Action Control*, Springer, Berlin, pp. 11-39.

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Ajzen, I., Czasch, C. and Flood, M.G. (2009), "From intentions to behavior: implementation intention, commitment, and conscientiousness", *Journal of Applied Social Psychology*, Vol. 39 No. 6, pp. 1356-1372.

Allam, S., Flowerday, S.V. and Flowerday, E. (2014), "Smartphone information security awareness: a victim of operational pressures", *Computers and Security*, Vol. 42, pp. 56-65.

Bandura, A. (1977), "Self-efficacy: toward a unifying theory of behavioral change", *Psychological Review*, Vol. 84 No. 2, pp. 191-215.

Ben-Asher, N. and Gonzalez, C. (2015), "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, Vol. 48, pp. 51-61.

Bernstein, D.A. (2016), *Psychology*, Cengage Learning, Boston.

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. and Shabtai, A. (2018), "Taxonomy of mobile users' security awareness", *Computers and Security*, Vol. 73, pp. 266-293.

Bloom, B.S., Engelhart, M.D., Furst, E.J., Hill, W.H. and Krathwohl, D.R.A. (1956), "Taxonomy of educational objectives", *Book 1: Cognitive Domain*, David McKay, New York, NY.

Boren, M.T. and Ramey, J. (2000), "Thinking aloud: reconciling theory and practice", *IEEE Transactions on Professional Communication*, Vol. 43 No. 3, pp. 261-276.

Boysen, G.A. and Vogel, D.L. (2009), "Bias in the classroom: types, frequencies, and responses", *Teaching of Psychology*, Vol. 36 No. 1, pp. 12-17.

Bränström, R., Kristjansson, S. and Ullén, H. (2005), "Risk perception, optimistic bias, and readiness to change sun related behaviour", *European Journal of Public Health*, Vol. 16 No. 5, pp. 492-497.

Campbell, J., Greenauer, N., Macaluso, K. and End, C. (2007), "Unrealistic optimism in internet events", *Computers in Human Behavior*, Vol. 23 No. 3, pp. 1273-1284.

Carroll, J.S. (1978), "The effect of imagining an event on expectations for the event: an interpretation in terms of the availability heuristic", *Journal of Experimental Social Psychology*, Vol. 14 No. 1, pp. 88-96.

CBS (2022), *Cybersecurity Monitor 2021*, CBS, The Hague.

CBS (2023), "StatLine [Open data]", available at: https://opendata.cbs.nl/statline/#/CBS/nl/

Cialdini, R.B. (2003), "Crafting normative messages to protect the environment", *Current Directions in Psychological Science*, Vol. 12 No. 4, pp. 105-109.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-340.

De Rivera, J., Gerstmann, E. and Maisels, L. (2002), "Acting righteously: the influence of attitude, moral responsibility, and emotional involvement", in Ross, M. and Miller, D.T. (Eds), *The Justice Motive in Everyday Life*, Cambridge University Press, Cambridge, pp. 271-288.

DeJoy, D.M. (1989), "The optimism bias and traffic accident risk perception", *Accident Analysis and Prevention*, Vol. 21 No. 4, pp. 333-340.

Dobbie, F., Purves, R., McKell, J., Dougall, N., Campbell, R., White, J., Amos, A., Moore, L. and Bauld, L. (2019), "Implementation of a peer-led school based smoking prevention programme: a mixed methods process evaluation", BMC Public Health, No. 19:742, pp. 1-9, doi:10.1186/s12889-019-7112-7.

Dubé-Rioux, L. and Russo, J.E. (1988), "An availability bias in professional judgment", *Journal of Behavioral Decision Making*, Vol. 1 No. 4, pp. 223-237.

EC (2019), *Special Eurobarometer 499 "Europeans' Attitudes towards Cyber Security*, European Commission, Luxembourg.

Edwards, K. (1990), "The interplay of affect and cognition in attitude formation and change", *Journal of Personality and Social Psychology*, Vol. 59 No. 2, pp. 202-216.

Endsley, M.R. (1995), "Toward a theory of situation awareness in dynamic systems", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 37 No. 1, pp. 32-64.

Festinger, L. (1957), *A Theory of Cognitive Dissonance*, Stanford University Press, Stanford.

Fishbein, M. and Ajzen, I. (1980), "Predicting and understanding consumer behavior: attitude-behavior correspondence", in Ajzen, I. and Fishbein, M. (Eds), *Understanding Attitudes and Predicting Social Behavior*, Prentice Hall, Englewood Cliffs, pp. 148-172.

Freberg, K., Graham, K., McGaughey, K. and Freberg, L.A. (2010), "Who are the social media influencers? A study of public perceptions of personality", *Public Relations Review*, Vol. 37 No. 1, pp. 90-92.

Gollwitzer, A., McLoughlin, K., Martel, C., Marshall, J., Höhs, J.M. and Bargh, J.A. (2022), "Linking self-reported social distancing to real-world behavior during the COVID-19 pandemic", *Social Psychological and Personality Science*, Vol. 13 No. 2, pp. 656-668.

Greaves, K. (2017), *Messages That Motivate the Adoption of Safe Computing Behaviors*, University of Minnesota, Minneapolis.

Gulshan, and Chauhan, S.S. (2021), "A survey on cyber security threats", *in 2021 International Conference on Technological Advancements and Innovations (ICTAI 2021), IEEE*, pp. 218-223.

Harriott, J. and Ferrari, J.R. (1996), "Prevalence of procrastination among samples of adults", *Psychological Reports*, Vol. 78 No. 2, pp. 611-616.

Hatten, T.S. and Ruhland, S.K. (1995), "Student attitude toward entrepreneurship as affected by participation in an SBI program", *Journal of Education for Business*, Vol. 70 No. 4, pp. 224-227.

He, S.C. (2017), "A multivariate investigation into academic procrastination of university students", *Open Journal of Social Sciences*, Vol. 05 No. 10, pp. 12-24, doi: 10.4236/jss.2017.510002.

Hewitt, B. and White, A. (2021), "Factors influencing security incidents on personal computing devices", *Journal of Organizational and End User Computing*, Vol. 33 No. 4, pp. 185-208.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-659.

Junco, R. (2013), "Comparing actual and self-reported measures of Facebook use", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 626-631.

Kahneman, D. (2011), *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York, NY.

Kahneman, D., Slovic, P. and Tversky, A. (1982), *Judgment under Uncertainty: Heuristics and Biases*, Cambridge University Press, Cambridge.

Kkeli, N. and Michaelides, M.P. (2023), "Differences between self-reports and measurements of weight in a Dutch sample", *European Journal of Environmental and Public Health*, Vol. 7 No. 3, pp. 1-11, doi: 10.29333/ejeph/12781.

Klayman, J. (1995), "Varieties of confirmation bias", *Psychology of Learning and Motivation*, Vol. 32, pp. 385-418.

Knäuper, B., Kornik, R., Atkinson, K., Guberman, C. and Aydin, C. (2016), "Motivation influences the underestimation of cumulative risk", *Personality and Social Psychology Bulletin*, Vol. 31 No. 11, pp. 1511-1523.

Kok, L.C., Oosting, D. and Spruit, M. (2020), "Influence of knowledge and attitude on intention to adopt cybersecure behaviour", *Information and Security: An International Journal*, Vol. 46 No. 3, pp. 251-266.

Krathwohl, D.R. (2002), "A revision of bloom's taxonomy: an overview", *Theory Into Practice*, Vol. 41 No. 4, pp. 212-218.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers and Security*, Vol. 25 No. 4, pp. 289-296.

Kummeneje, A. and Rundmo, T. (2020), "Attitudes, risk perception and risk-taking behaviour among regular cyclists in Norway", *Transportation Research Part F: Traffic Psychology and Behaviour*, Vol. 69 No. 2, pp. 135-150.

Lawson, E.D. and Stagner, R. (1957), "Group pressure, attitude change, and autonomic involvement", *The Journal of Social Psychology*, Vol. 45 No. 2, pp. 299-312.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014), "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092.

Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011), *Risks and Safety on the Internet: The Perspective of European Children*, EU Kids Online, London.

Loewenstein, G.F., Weber, E.U., Hsee, C.K. and Welch, N. (2001), "Risk as feelings", *Psychological Bulletin*, Vol. 127 No. 2, pp. 267-286.

Lupton, D. and Tulloch, J. (1999), "Theorizing fear of crime: beyond the rational/irrational opposition", *The British Journal of Sociology*, Vol. 50 No. 3, pp. 507-523.

Michie, S., Hyder, N., Walia, A. and West, R. (2011), "Development of a taxonomy of behaviour change techniques used in individual behavioural support for smoking cessation", *Addictive Behaviors*, Vol. 36 No. 4, pp. 315-319.

Nandedkar, A. and Midha, V. (2012), "It won't happen to me: an assessment of optimism bias in music piracy", *Computers in Human Behavior*, Vol. 28 No. 1, pp. 41-48.

Nickerson, R.S. (1998), "Confirmation bias: a ubiquitous phenomenon in many guises", *Review of General Psychology*, Vol. 2 No. 2, pp. 175-220.

Ofte, H.J. and Katsikas, S. (2023), "Understanding situation awareness in SOCs, a systematic literature review", *Computers and Security*, Vol. 126, pp. 1-14, doi: 10.1016/j.cose.2022.103069.

Ostrom, T.M. (1969), "The relationship between the affective, behavioral and cognitive components of attitude", *Journal of Experimental Social Psychology*, Vol. 5 No. 1, pp. 12-30.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers and Security*, Vol. 66, pp. 40-51.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. (2022), "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology and Work*, Vol. 24 No. 2, pp. 371-390.

Prince, S.A., Cardilli, L., Reed, J.L., Saunders, T.J., Kite, C., Douillette, K., Fournier, K. and Buckley, J.P. (2020), "A comparison of self-reported and device measured sedentary behaviour in adults: a systematic review and meta-analysis", *International Journal of Behavioral Nutrition and Physical Activity*, Vol. 17 No. 1, pp. 1-17.

Rahim, N.H.A., Hamid, S., Kiah, L.M., Shamshirband, S. and Furnell, S. (2015), "A systematic review of approaches to assessing cybersecurity awareness", *Kybernetes*, Vol. 44 No. 4, pp. 606-622.

Rasmussen, J. (1983), "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models", *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. SMC-13 No. 3, pp. 257-266.

Robbins, S.P. and Judge, T.A. (2019), *Organizational Behavior*, Pearson, London.

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.

Rohrmann, B. and Renn, O. (2000), "Risk perception research", in Renn, O. and Rohrmann, B. (Eds), *Cross-Cultural Risk Perception. Technology, Risk, and Society*, Springer, Boston, Vol. 13, pp. 11-53.

Rundmo, T. and Nordfjaern, T. (2017), "Does risk perception really exist?", *Safety Science*, Vol. 93, pp. 230-240.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers and Security*, Vol. 53, pp. 65-78.

Salameh, R. and Loh, C.S. (2022), "Engagement and players' intended behaviors in a cybersecurity serious game", *International Journal of Gaming and Computer-Mediated Simulations*, Vol. 14 No. 1, pp. 1-21.

Sember, V., Meh, K., Sorić, M., Starc, G., Rocha, P. and Jurak, G. (2020), "Validity and reliability of international physical activity questionnaires for adults across EU countries: systematic review and meta analysis", *International Journal of Environmental Research and Public Health*, Vol. 17 No. 19, pp. 1-23.

Senge, P.M. (1996), "Leading learning organizations: the bold, the powerful, and the invisible", in Hesselbein, F., Goldsmith, M. and Beckhard, R. (Eds), *The Leader of the Future*, Wiley, New York, NY.

Sharot, A. (2011), "The optimism bias", *Current Biology*, Vol. 21 No. 23, pp. R941-R945.

Sheeran, P. (2002), "Intention-behavior relations: a conceptual and empirical review", *European Review of Social Psychology*, Vol. 12 No. 1, pp. 1-36.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Solomon, L. and Rothblum, E. (1984), "Academic procrastination: frequency and cognitive-behavioral correlates", *Journal of Counseling Psychology*, Vol. 31 No. 4, pp. 503-509.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "A meta-analysis of studies on protection motivation theory and information security behaviour", *International Journal of Information Security and Privacy*, Vol. 9 No. 1, pp. 26-46.

Spruit, M. (1998), "Competing against human failing", in Posch, R. and Papp, G. (Eds), *Proceedings of the IFIP TC11 14th International Conference on Information Security (SEC '98), Wenen/Boedapest*, 31 August – 4 September, *Austrian Computer Society, Vienna*, pp. 392-401.

Svenningsson, J., Höst, G., Hultén, M. and Hallström, J. (2022), "Students' attitudes toward technology: exploring the relationship among affective, cognitive and behavioral components of the attitude construct", *International Journal of Technology and Design Education*, Vol. 32 No. 3, pp. 1531-1551.

Tversky, A. and Kahneman, D. (1973), "Availability: a heuristic for judging frequency and probability", *Cognitive Psychology*, Vol. 5 No. 2, pp. 207-232.

Verkijika, S.F. (2018), "Understanding smartphone security bahaviors: an extention of the protection motivation theory with anticipated regret", *Computers and Security*, Vol. 77, pp. 860-870.

Wicker, A.W. (1969), "Attitude versus action: the relationship of verbal and overt behavioral responses to attitude objects", *Journal of Social Issues*, Vol. 25 No. 4, pp. 41-78.

Winter, K., Pummerer, L., Hornsey, M.J. and Sassenberg, K. (2022), "Pro-vaccination subjective norms moderate the relationship between conspiracy mentality and vaccination intentions", *British Journal of Health Psychology*, Vol. 27 No. 2, pp. 390-405.

Witsenboer, J.W.A., Sijtsma, K. and Scheele, F. (2022), "Measuring cyber secure behavior of elementary and high school in The Netherlands", *Computers and Education*, Vol. 186, pp. 1-11, doi: 10.1016/j.compedu.2022.104536.

About the authors

Marcel Spruit, Ph.D., is a Professor in the Center of Expertise Cybersecurity at The Hague University of Applied Sciences, The Netherlands. His research focuses on human behaviour related to cybersecurity, standardisation of cybersecurity education and organising cybersecurity in organisations. Contact details: Prof. Dr. Marcel Spruit, Center of Expertise Cybersecurity, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, The Hague 2521 EN, The Netherlands. Marcel Spruit is the corresponding author and can be contacted at: m.e.m.spruit@hhs.nl

Deborah Oosting, M.Sc., is a Researcher in the Center of Expertise Cybersecurity and Lecturer Safety Management at The Hague University of Applied Sciences in The Hague, The Netherlands. She has a Master's degree in Technical Psychology and a background in UX design. Her interests focus on the human side of cybersecurity. Contact details: Deborah Oosting, M.Sc., Center of Expertise Cybersecurity, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, The Hague 2521 EN, The Netherlands.

Céline Kreffer, M.Sc., is a Researcher in the Center of Expertise Cybersecurity at The Hague University of Applied Sciences, The Netherlands. She has a Master's degree in Social and Organisational Psychology and Forensic Criminology. Her research focuses on human behaviour and organisational aspects in relation to cybersecurity. Contact details: Celine Kreffer, M.Sc., Center of Expertise Cybersecurity, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, The Hague 2521 EN, The Netherlands.