Information & Security

Published since 1998

De Kok, D. Oosting & M. Spruit
vol. 46, no. 3 (2020): 251-266
https://doi.org/10.11610/isij.4618

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour

***Lisa C. de Kok, Deborah Oosting, Marcel Spruit* (✉)**

Department Cybersecurity & Safety, The Hague University of Applied Sciences, The Hague, The Netherlands, https://www.thehagueuniversity.com/research/research-groups/details/cyber-security-safety

ABSTRACT:

In general, people are poorly protected against cyberthreats, with the main reason being user behaviour. For the study described in this paper, a questionnaire was developed in order to understand how people's knowledge of and attitude towards both cyberthreats and cyber security controls affect intention to adopt cybersecure behaviour. The study divides attitude into a cognitive and an affective component. Although only the cognitive component of attitude is usually studied, the results from a questionnaire of 300 respondents show that both the affective and cognitive components of attitude have a clearly positive, albeit varying, influence on behavioural intention, with the affective component having an even greater effect on attitude than the cognitive aspect. No correlation was found between knowledge and behavioural intention. The results indicate that attitude is an important factor to include when developing behavioural interventions, but also that different kinds of attitude should be addressed differently in interventions.

ARTICLE INFO:

RECEIVED: 10 MAY 2020
REVISED: 31 JUL 2020
ONLINE: 03 SEP 2020

KEYWORDS:

information security, cybersecurity awareness, cybersecurity behaviour, cybersecurity questionnaire, cybersecurity knowledge, cybersecurity attitude

Introduction

People are spending more time living and working online. In 2018 there were 3.8 billion internet users worldwide, and this number is only likely to rise.[1] While

✉ E-mail: m.e.m.spruit@hhs.nl

the digital revolution provides us with a lot of benefits, it also carries risks relating to the availability, integrity and confidentiality of online information. As reported by the European Network and Information Security Agency, large numbers of people around the world have been the victim of malware, phishing, spam, identity theft, and other such cyberthreats.[2]

The Dutch public appear to be ill-equipped against these kinds of online threats. In 2018, around 8.5% of the Dutch population fell victim to cybercrime, though the real percentage is likely much higher, as not all cyber incidents are reported. In a survey of major companies in the Netherlands, 64% indicated that they had suffered at least one cyber incident in 2018.[3] Despite these statistics, 69% of the Dutch population said they were not worried about cyberthreats, and 60% stated that their own cyber skills were sufficient. The same study revealed that 52% of the population never backs up their data, and that another 52% never use automatic updates.[4] It is clear then that there is a large gap between how people view their cybersecurity skills how cybersecure their behaviour actually is. The aim of this paper is to understand why people either do or do not engage in cybersecure behaviour.

Knowledge is an important precondition for adopting the correct behaviour in any given situation.[5] Studies undertaken in other fields, such as nutrition[6] and HIV prevention [7] have shown that having the correct knowledge is an important starting point for bringing about behavioural change. With regards to cybersecurity, knowledge is required in order to recognise cyberthreats and to understand the associated risks.[8; 9; 10]

However, as was concluded in an earlier cybersecurity study, knowledge alone is not enough to explain behaviour. [11; 12; 13; 14] Even if a person has a clear understanding of cyberthreats and cybersecurity controls, they must also be able to view such threats as important enough to merit enacting the relevant cybersecurity controls.[15] That is why the behavioural literature states that in addition to knowledge, attitude is also important in explaining behaviour.[16; 17; 18] Previous studies on cybersecurity behaviour have found that attitude has a significant effect on intended behaviour.[19; 20]

Even though knowledge and attitude have been measured both separately and together in explanatory studies on cybersecure behaviour,[21; 22] these aspects are not always properly elaborated. All earlier studies that measured attitude only did so partially. This paper, therefore, includes a more comprehensive approach to cybersecurity related knowledge and attitude. The research question is as follows: *To what extent can intention to adopt cybersecure behaviour be explained by knowledge of and attitude towards cyberthreats and cybersecurity controls?*

Theory

Knowledge is defined as *'remembering specific and general issues, remembering methods or processes or remembering patterns, structures or contexts.'* [23]

Knowledge is a precondition for adopting correct behaviour in a given situation.[24] In the field of cybersecurity this involves recognising and knowing about cyberthreats,[25] understanding their potential impact, and being conscious of the measures that can be taken against them.[26; 27]

There are different types of knowledge, such as factual knowledge, conceptual knowledge and procedural knowledge.[28; 29] Knowledge can be mastered at different levels. According to Bloom's taxonomy, these levels are, 1) remembering, 2) understanding, 3) applying, 4) analysing, 5) evaluating, and 6) creating. In cybersecurity, the first four levels are equivalent to making an inventory of threats and analysing them.[30; 31; 32; 33] The last two levels, evaluating and creating, go further than this. 'Evaluating' is about meta-knowledge, while 'creating' means developing new models and systems. These last two levels are not relevant for the purposes of this study. The measuring of knowledge in earlier cybersecurity related studies were focused on particular target groups, such as children,[34; 35] seniors,[36; 37; 38] or working adults.[39; 40]

Most people do not lack general knowledge about cyberthreats and cybersecurity controls.[41] However, people are generally speaking not sufficiently protected against cyberthreats.[42] It follows then that having knowledge is not enough on its own to ensure proper protection against cyberthreats. Attitude, or opinion about a thing or a person,[43] is also an important factor in explaining behaviour.[44; 45; 46; 47] Attitude can be divided into affective, cognitive and behavioural components.[48] The affective component is formed by a person's gut feelings associated with something or someone. The cognitive component is formed by a characteristics-based evaluation. The behavioural component relates to attitude influenced by earlier behaviour and experience. The behavioural component is not included because people only derive their attitude from their behaviour or experience in exceptional circumstances. This is only the case when their attitude is weak or ambiguous or if they cannot explain their behaviour in any other plausible way.[49]

To measure attitude comprehensively it will be useful to include both its cognitive and affective components, measuring each separately. It seems unlikely that attitude is formed solely on the basis of affect or cognition alone.[50] It may also be the case that people exhibit conflicting attitudes, that is both positive and negative attitudes towards the same object.[51] An ambivalent attitude may consist of conflicting cognitive attitudes or a conflict between a cognitive attitude and an affective attitude. An example of conflicting cognitive attitudes would be someone believing it is useful to have a VPN (virtual private network), but realising that it is not easy to implement. Cognitive and affective components of attitude can be in conflict, for instance, if a person believes it is useful to install updates (cognitive), but has negative, frustrated feelings (affective) when they consider doing it. That is why affect and cognition are measured in this study as two separate factors which together form a person's attitude.

Previous studies on cybersecure behaviour show that the affective and cognitive components are not both included in measurements. [52; 53; 54] Instead, only the cognitive component is assessed.[55; 56] In light of earlier research indicating that the affective component is an important explanatory factor for behaviour,[57] earlier measuring can be said to be incomplete in that regard. This paper also includes the affective component.

Although it seems obvious to measure affective attitude by asking about concrete feelings such as happiness or irritation,[58; 59] a preliminary, small-sample (n = 12) study revealed that these kinds of feelings were not associated with cybersecurity. This preliminary research asked about feelings linked to cybersecurity controls. Even when provided with a list of concrete feelings in the questionnaire, participants were still unable to make connections between cybersecurity controls and concrete feelings. Participants could however indicate whether they had a positive or negative feeling towards these controls. It appears that the affective component of attitude towards cybersecurity controls is more often about general emotions, such as positive and negative feelings, than concrete feelings such as happiness or irritation. The values most often chosen for cognitive attitude in research are usefulness and ease of use. These are also used in this paper.[60; 61]

This paper treats behavioural intention as an outcome variable influenced by knowledge and attitude. Behavioural intention has been chosen instead of self-reported behaviour because people may not accurately remember their own behaviour. Recent research has revealed that actual cybersecure behaviour does not match self-reported cybersecure behaviour.[62] The advantage of relying on behavioural intention is that it lends itself well to questionnaire-based measurements. This requires the use measuring that allows participants to express the extent to which they intend to exhibit a certain behaviour.[63] Earlier research has also shown that behavioural intention explains a substantial part of behaviour, and that intention-behaviour correlations are at around 0.90.[64; 65] Other systematic literature studies on cybersecure behaviour have revealed that behavioural intention is an important predictor of actual behaviour.[66; 67; 68; 69]

Methods

Data Collection

Data was collected through an online questionnaire conducted via a panel company. Measuring was conducted in October 2019. Participants received a small financial compensation for completing the questionnaire via the panel company. Participants were equally distributed by gender and age. Participants were able to complete the questionnaire online from home via their smartphone, tablet or laptop. Participants were informed that the topic of the questionnaire was 'the human side of cybersecurity', that completing the questionnaire would take approximately 30 minutes, and that all data would be processed anonymously. It was also explained that the questionnaire was about the participant's perception and opinion relating to cybersecurity. To discourage people from giving answers based on perceived social desirability, respondents were instructed to choose the option 'I don't know' if they did not know the answer or choose the option 'not applicable' if the participants had never used the control in question. In total 300 respondents completed the questionnaire.

Selected Controls

To determine which cybersecurity controls and associated cyberthreats should be included in the questionnaire, the ISO 27002 standard was chosen.[70] Specific controls were selected according to the following criteria. The control 1) can be implemented at an individual level, 2) is not very context-dependent, and 3) has a clear, unambiguous description. As such, a total of 38 controls were shortlisted. After expert interviews (n = 12), nine controls remained. These nine were broken down into different levels of difficulty.

Measuring Knowledge

In cybersecurity research, knowledge is often measured using a multiple-choice questionnaire. This allows for the option of providing more than two possible answers.[71; 72] A disadvantage of this type of questionnaire is that both the questions and answer options provided must be thoroughly evaluated for possible interpretations. The correct answer should also not be immediately obvious to someone who does not have knowledge of the topic.

Another often used and relatively easy option for questions relating to knowledge is where a statement is given and the respondent has to evaluate whether this statement is correct or not. In this type of question, the answer options are the same for each question, for example 'true/false'.[73; 74; 75] These types of statement were used in the research detailed here. For example, one of the nineteen statements shown was '*A website with 'https' and/or a padlock can be hacked,'* and respondents had to indicate if the statement was true or false.

A possible problem with this type of question is that respondents can easily guess the correct answer, which would skew the actual knowledge score. In order to prevent this as far as possible, the option 'I don't know' was added, and its role highlighted during instructions. Preliminary research (n = 12) and in-depth interviews (n = 5) have shown that this option was positively evaluated by participants and used if necessary. An analysis of the questions relating to knowledge indicated that four questions were wrongly interpreted by the vast majority of the participants. These four questions were removed from the dataset, leaving another 15 knowledge questions that were included in the final analysis.

Measuring Attitude

A fast and user-friendly way to measure attitudes in a larger group is through self-reporting based on a series of statements in a questionnaire. The main problem with self-reporting is that there is a chance that people will provide an answer motivated by social desirability. This could also occur when attitudes are measured through interviews, but in that case the interviewer can ask follow-up questions. However, the questionnaire method is more suitable for the present study, since its aim is to get an indication of attitudes among a larger group.

To prevent respondents from giving socially desirable answers, the instructions emphasise that the study gains most from sincere answers. Nevertheless, it is impossible to prevent all answers motivated by social desirability. To allow for the possibility that people may not have an opinion on a given topic, the option 'not applicable/no opinion' have been added.[76] Despite some objections to measuring attitudes with a questionnaire, it is the best method to measure attitude effectively.[77] In this paper, respondents were asked to self-report attitude using a five-point scale.

In addition, several techniques were applied to improve the validity of attitude measurements. A preliminary study used 'thinking-out-loud' to test if the answers in the questionnaire matched the attitudes found in the in-depth interviews. Based on that, some questions were adapted and retested. The internal reliability of the items that influence attitude were tested using Cronbach's alpha. In addition to this, different scales were used for the three components of attitude. These are explained below.

Affective and cognitive attitude were measured separately through self-reporting, where participants indicated the extent to which a given statement applies to them. Affective attitude was measured in the following form: "*My first feeling when checking if a website address is secure by looking if it contains 'https://' and/or a padlock is shown, is positive.*" When measuring affective attitude, it is important that participants do not express their feeling based on cognition, but truly follow their gut instinct.[78] Prior research relying on thinking-out-loud has revealed that it is more effective to explicitly emphasise this in the instructions and questions. Emphasising this explicitly has led to participants not thinking as long and hard about their answer. Cognitive attitude was measured through two cognitive pairs: ease of use (not easy to use/easy to use) and usefulness (useless/useful). For a statement such as "*Locking a device when I am no longer using it is something I find...,*" participants could indicate how easy and useful they found a control.

Behavioural Intention

In questions about behavioural intention, participants were asked to what extent they intend to take cybersecurity controls in the near future. The question related to reporting an incident, for example, was: "I intend to report a cybersecurity incident if it happens to me, for example ransomware, identity theft and/or a data breach." Answers could be provided along a five-point Likert scale ranging from 'completely disagree' (1) to 'completely agree' (5), and also the options 'I don't know' and 'not applicable'.

Results

Demographics

In total, 300 respondents completed the questionnaire. Data from three respondents was removed from the dataset because of extreme outliers. Of the remaining 297 participants, 49.8% were men. The average age of participants was 48.75 years old (*SD* = 17.39, with the youngest participant aged 18 and the oldest 83). Participants had various levels of education: 11.8% had a lower level of education, 59.9% had an average level of education and 28.3% had a higher level of education.

Reliability

All four factors analysed were measured for internal consistency and reliability using Cronbach's alpha. The knowledge scale of 15 items was below the generally used reliability minimum of 0.70: Cronbach's alpha indicated 0.587. The cognitive attitude scale, however, was found to be reliable (24 items; $\alpha = 0.913$). The affective attitude scale was also found to be reliable (12 items; $\alpha = 0.871$), as was the scale for behavioural intention (12 items; $\alpha = 0.845$).

Average Scores

Initially, averages per component were checked. Participants correctly answered an average 8.9 out of 15 knowledge questions (*SD* = 2.531). The scores for the affective and cognitive components averaged 4.09 out of 12 (*SD* = 0.564) and 4.3 out of 24 (*SD* = 0.545), respectively. For behavioural intention, the participants scored an average of 4.04 out of 12 (*SD* = 0.582).

Effects on Behavioural Intention

Next, each factor was analysed for its effects on behavioural intention. A simple 1000-subsample bootstrapping regression showed that knowledge is not a predictor of behavioural intention ($\beta = 0.027$, $p = 0.069$, 95% CI [5.639^{E-5}, 0.057]). However, both types of attitudes turn out to be medium- to large-value predictors of behavioural intention. This was indicated by a simple 1000-subsample bootstrapping regression model, with $\beta_{affective} = 0.742$ ($p < 0.05$, 95% CI [0.656, 0.822]) and $\beta_{cognitive} = 0.589$ ($p < 0.05$, 95% CI [0,470, 0,715]).

A model with both attitude components combined explains 56% of the variance in behavioural intention, as indicated by a 1000-subsample multiple-regression bootstrapping analysis for both coefficients ($R^2 = 0.559$, $F(2.265) = 169.896$, $p < 0.001$). Of this percentage, affective and cognitive attitude accounted for 66.4% ($\beta = 0.664$, $p < 0.05$, 95% CI [0.538, 0.779]) and 16.6% ($\beta = 0.166$, $p < 0.05$, 95% CI [0.054, 0.296]) of the above result, respectively.

Other Effects

In addition, a simple regression analysis (bootstrapping procedure, 1000 subsamples) was conducted to further research the impact of affective attitude on cognitive attitude. This revealed that affective attitude explains 59% of the variance in cognitive attitude ($\beta = 0.593$, $p < 0.01$,95% CI [0.501, 0.679]). On the other hand, it turned out that cognitive attitude accounted for 61% of the variance in affective attitude *(β* = 0.614, p < 0.05 ,95% CI [0.495, 0.738]).

Although knowledge was not found to have a direct effect on behavioural intention, the relationship between knowledge and the two types of attitude was analysed through two simple regression analyses (bootstrapping procedure, 1000 subsamples). Knowledge was found to have no impact on affective attitude *(β* = 0.021, *p* = 0.165, 95% CI [-0.007, 0.050]) and only explains a very small part (4,3%) of the variance in cognitive attitude *(β* = 0.043*, p* < 0.05, 95% CI [0.013, 0.077]).

Behavioural Model

To research the direction of the relationships found further, a multiple regression analysis was conducted. The model that includes knowledge, affective attitude and cognitive attitude explains 55.8% of the variance in behavioural intention (R^2= .558; *F*(3.264) = 113.58, *p* < 0.001).

Finally, to analyse the individual factors in the model further, a bootstrapping procedure with 1000 subsamples was used again. This revealed that both affective (*β* = 0.663), *p* < 0.01, 95% CI [0.550, 0.780]) and cognitive (*β* = 0.158, *p* < 0.01, 95% CI [0.040, 0.281]) components of attitude have significant positive influence on behavioural intention. An earlier simple regression also indicated that, in the complete model, knowledge had no effect on behavioural intention *(β* = 0.010, *p* = 0.248, 95% CI [-0.07, 0.028]).

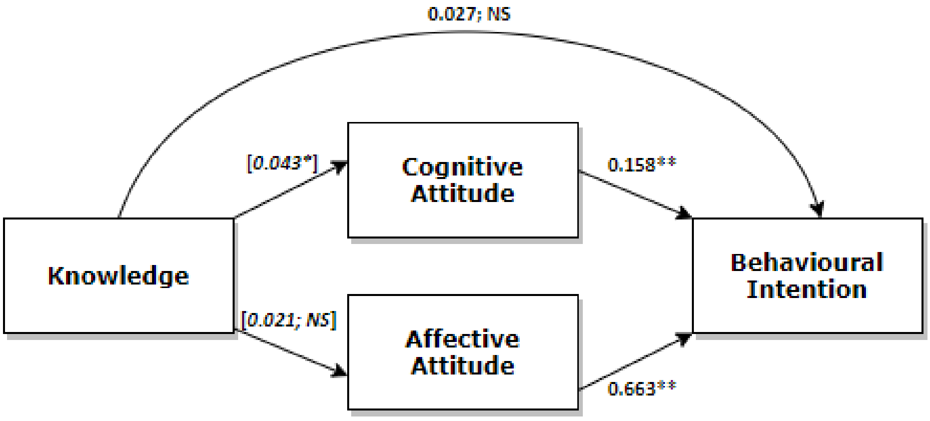

Figure 1: Path coefficients Behavioural Model; Note. [*italic*] = values based on simple linear regressions. * *p* < 0.05, ** *p* < 0.01 NS = Non Significant.

Discussion

The present paper has aimed to address the extent to which knowledge and attitude relating to cyberthreats and cybersecurity controls can explain intention to adopt cybersecure behaviour. Other studies on this topic often fail to consider knowledge and attitude sufficiently in their research.

The results of this study show that on average people answered 8.9 out of 15 knowledge questions correctly (*SD* = 2.531). People also had a positive attitude towards cybersecurity controls. Although cognitive attitude reached a higher score *(μ* = 4.3, *SD* = 0.564) than affective attitude *(μ* = 4.09, *SD* = 0.545), the latter was still high enough to remain a significant factor in explaining a person's intent to adopt cybersecure behaviour. The scales that were developed to measure both types of attitude also demonstrated strong internal consistency, making them suitable for these measurements.

The average score of behavioural intention was high. Finally, the model that includes knowledge, affective attitude and cognitive attitude explains 55.8% of variance in this behavioural intention.

As expected, positive relationships were identified between both types of attitude and behavioural intention. This means that a more positive attitude results in a higher intention to adopt cybersecure behaviour. New to the study described here is the fact that this includes not just cognitive attitude, but also affective attitude. Decisions around behaviour are also made based on associated feelings. A positive relationship between cognitive attitude and behavioural intention was also consistent with earlier studies.[79; 80] No correlation was found between knowledge and affective attitude.

Although multiple studies have found a positive relationship between knowledge and behaviour,[81; 82; 83] the study described here found no relationship between knowledge and behavioural intention. A possible explanation is that the knowledge level of this study was relatively high, with an average of 8.9 correct answers out of 15 questions. That was probably because internet use was a prerequisite for participating in the study. This could mean the basic levels of knowledge were too high to indicate a discerning effect on behavioural intention.

Another possible explanation is that people answered some questions correctly, but based on incorrect knowledge. For example, interviews conducted after the study showed that several participants said they knew that it was better to use 4G on the train than free Wi-Fi. However, the reason provided for this behaviour was not that 4G was safer, but rather that the free Wi-Fi service on the train is so poor that it is useless. Although the questionnaire was tested thoroughly beforehand, these subtleties were not observed during the tests. Finally, it is possible that the use of multiple-choice questions, despite including the option 'I don't know', allowed people to guess, resulting in an inaccurate representation of knowledge level.

Another unexpected finding was the weak relationship between knowledge and cognitive attitude. The literature shows that cognitive attitude is developed based on the characteristics of a certain object, and knowledge plays a role.[84] It is possible that this relationship doesn't exist, or that the differences in knowledge are not sufficiently prominent to result in differences in cognitive attitude.

Theoretical and Practical Implications

Our findings have both theoretical and practical implications. This study shows that attitude is an important factor and that knowledge alone is not enough to change behavioural intention. It also shows that cognitive and affective attitudes are partially complementary, but also partially different from each other. That is why both have to be measured in order to form a complete understanding of attitude. In practice, these insights are relevant for developing effective interventions to change behaviour. Knowledge and attitudes are factors that can be taken into consideration for interventions at an individual level, regardless of the environment. The result variable of this study was behavioural intention. Although this is not a guaranteed predictor of actual behaviour and obstacles may still emerge between intention and actual behaviour, behavioural intention is one of the most important starting points for cybersecure behaviour.[85; 86; 87] To help people progress from being a weak to a strong link in cybersecurity, it is advisable to focus on both the cognitive and affective components of attitude.

Limitations and Further Research

The study is subject to certain limitations, and for this reason possibilities exist for further research on the factors affecting cybersecure behaviour. The sample was not completely representative: half of the respondents were not employed at the time they completed the questionnaire. This means they only had recent experience with cybersecurity issues in their free time or private life.

The results and conclusions in the present study are based on self-reporting. Therefore, although every attempt was made to prevent respondents from giving answers merely because they are socially desirable, there will always be discrepancies between reported and actual knowledge, attitude and behavioural intention. The medium-high to high averages found for all factors seem to indicate that cybersecurity is not a problem, while reality makes it very clear that the number of cyber incidents is still quite high.[88] There are also obstacles between behavioural intention and actual behaviour. Future research could also study which obstacles between behavioural intention and actual cybersecure behaviour are actually relevant. The study could also be enriched by performing observations or experiments in addition to conducting questionnaires.

Acknowledgements

The authors would like to thank The Hague University of Applied Sciences for supporting the research that was the basis for this paper.

References

[1] Statista, "Number of Internet Users Worldwide from 2005 to 2018 (in Millions)," https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/, accessed March 25, 2020.

[2] Andreas Sfakianakis, Christos Douligeris, and Louis Marinos, "ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends," *ENISA*, 2019, https://doi.org/10.2824/622757.

[3] CBS, "Cybersecuritymonitor 2019," https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019, accessed April 19, 2020.

[4] TNS NIPO, "Cybersecurity Awareness en Skills in Nederland," www.alertonline.nl/media/toolkit/onderzoek/Cybersecurity-Awareness-en-Gedrag-2016.pdf, accessed March 25, 2020.

[5] Jens Rasmussen, "Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models," *Systems, Man and Cybernetics, IEEE Transactions On SMC* 13, no. 2 (1983): 257–66, https://doi.org/10.1109/tsmc.1983.6313160.

[6] Anthony Worsley, "Nutrition Knowledge and Food Consumption: Can Nutrition Knowledge Change Food Behaviour?" *Asia Pacific Journal of Clinical Nutrition* 11 Suppl 3 (2002), https://doi.org/10.1046/j.1440-6047.11.supp3.7.x.

[7] Oyewole Durojaiye, "Knowledge, Attitude and Practice of HIV/AIDS: Behavior Change among Tertiary Education Students in Lagos, Nigeria," *Annals of Tropical Medicine and Public Health* 4, no.1 (2011):18–24, https://doi.org/10.4103/1755-6783.80516.

[8] Noam Ben-Asher, and Cleotilde Gonzalez, "Effects of Cyber Security Knowledge on Attack Detection," *Computers in Human Behavior* 48 (2015): 51–61, https://doi.org/10.1016/j.chb.2015.01.039.

[9] Ron Bitton, Kobi Boymgold, Rami Puzis, and Asaf Shabtai, "Evaluating the Information Security Awareness of Smartphone Users," (2019), http://arxiv.org/abs/1906.10229.

[10] Mikko Siponen, "Five Dimensions of Information Security Awareness," *ACM SIGCAS Computers and Society* 31, no. 2 (2001):24–29, https://doi.org/10.1145/503345.503348.

[11] Durojaiye, "Knowledge, attitude and practice," 18–24.

[12] Abdul Rahman Ahlan, Muharman Lubis, and Arif Ridho Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," *Procedia Computer Science* 72 (2015): 361–73, https://doi.org/10.1016/j.procs.2015.12.151.

[13] Maria Bada, Angela Sasse, and Jason Nurse, "Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?" *Proceedings of the International Conference on Cyber Security for Sustainable Society*, (2017): 118–131, https://arxiv.org/abs/1901.02672.

[14] Tracey Caldwell, "Making Security Awareness Training Work," *Computer Fraud and*

Security 6, (2016): 8–14, https://doi.org/10.1016/S1361-3723(15)30046-4.

[15] Mikko Siponen, Adam Mahmood, and Seppo Pahnila, "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information and Management* 51, no. 2 (2014): 217–24, https://doi.org/10.1016/j.im.2013.08.006.

[16] Elliot Aronson and Timothy Wilson, *Sociale Psychologie* (Amsterdam: Pearson Benelux, 2017).

[17] Susan Fiske and Shelley Taylor, *Social cognition: From brains to Culture* (Thousand Oaks, CA: Sage Publications, 2013).

[18] P.G. Schrader and Kimberley Lawless, "The Knowledge, Attitudes, & Behaviors Approach How to Evaluate Performance and Learning in Complex Environments," *Performance Improvement* 43, no. 9 (2004): 8–15, https://doi.org/10.1002/pfi.4140430905.

[19] Benedict Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael Breitner, "Information Security Awareness and Behavior: A Theory-Based Literature Review," *Management Research Review* 37, no. 12 (2014), https://doi.org/10.1108/MRR-04-2013-0085.

[20] Teodor Sommestad, Jonas Hallberg, Kristoffer Lundholm, and Johan Bengtsson, "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management and Computer Security* 22, no. 1 (2014): 42–75, https://doi.org/10.1108/IMCS-08-2012-0045.

[21] Hennie Kruger and Wayne Kearney, "A Prototype for Assessing Information Security Awareness," *Computers and Security* 25, no. 4 (2006): 289–96, https://doi.org/10.1016/j.cose.2006.02.008.

[22] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies," *Computers and Security* 66 (2017): 40–51, https://doi.org/10.1016/j.cose.2017.01.004.

[23] Benjamin Bloom, Max Engelhart, Edward Furst, Walker Hill and David Krathwohl, *Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook 1: Cognitive Domain* (New York: David McKay Company, 1956), 1.

[24] Rasmussen, "Skills, rules, and knowledge," 257–266.

[25] Ben-Asher and Gonzalez, "Effects of cyber security knowledge," 51–61.

[26] Siponen, "Five dimensions," 24–29.

[27] Lindie Du Plessis and Rossouw Von Solms, "Information Security Awareness: Baseline Education and Certification," *Information Technology on the Move* 8, no. 8 (2002): 1–12.

[28] Bloom, Engelhart, Furst, Hill and Krathwohl, *Taxonomy of Educational Objectives,* 1.

[29] David Krathwohl, "A Revision of Bloom's Taxonomy : An Overview," *Theory into Practice* 41, no. 4 (2002): 212–18, https://www.researchgate.net/publication/242400296_A_Revision_of_Bloom's_Taxonomy_An_Overview.

[30] Bitton *et al*., "Evaluating the Information Security Awareness," 266–293.

[31] Anne Blanksma-Çeta and Femke Konings,"Nationaal Cybersecurity Bewustzijnsonderzoek," 2017, accessed January 30 2020, https://www.alertonline.nl/media/

Nationaal-Cybersecurity-Bewustzijnsonderzoek-2017-DEF.pdf.

[32] Russell Glasgow, Edward Lichtenstein, and Alfred Marcus, "Why Don't We See More Translation of Health Promotion Research to Practice? Rethinking the Efficacy-to Effectiveness Transition," *American Journal of Public Health* 93, no. 8 (2003): 1261–67, https://doi.org/10.2105/AJPH.93.8.1261.

[33] Parsons *et al.*, "The Human Aspects," 40–51.

[34] Filippos Giannakas, Georgios Kambourakis, and Stefanos Gritzalis, "CyberAware: A Mobile Game-Based App for Cybersecurity Education and Awareness," *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2015* (2015): 54–58, https://doi.org/10.1109/IMCTL.2015.7359553.

[35] Sreenivas Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang, "A Survey on Internet Usage and Cybersecurity Awareness in Students," *14th Annual Conference on Privacy, Security and Trust,* (2016): 223–28. https://doi.org/10.1109/PST.2016.7906931.

[36] Nabat Arfi and Shalini Agarwal, "A Study on Level of Knowledge Regarding Cybercrime Among Elderly Residing in Homes and Old Age HOMES," *International Journal for Research in Applied Science and Engineering Technology* 2, no. 7, (2014): 30–34.

[37] David Cook, Patryk Szewczyk, and Krishnun Sansurooah, "Seniors Language Paradigms: 21 St Century Jargon and the Impact on Computer Security and Financial Transactions for Senior Citizens," *Proceedings of the 9th Australian Information Security Management Conference*, (2011): 63–68, https://doi.org/10.4225/75/57b52d42cd8b8.

[38] Galen Grimes, Michelle Hough, Elizabeth Mazur, and Margaret Signorella, "Older Adults' Knowledge of Internet Hazards," *Educational Gerontology* 36, no. 3 (2010): 173–92, https://doi.org/10.1080/03601270903183065.

[39] Tejaswini Herath, and Raghav Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* 47, no. 2 (2009): 154–65, https://doi.org/10.1016/j.dss.2009.02.005.

[40] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram, "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers and Security* 42 (2014): 165–76, https://doi.org/10.1016/j.cose.2013.12.003.

[41] Ludwig Slusky and Parviz Partow-Navid, "Students Information Security Practices and Awareness Reproduced with Permission of the Copyright Owner Further Reproduction Prohibited without Permission," *Journal of Information Privacy & Security* 8, no 4. (2012): 3–26, https://doi.org/10.1080/15536548.2012.10845664.

[42] CBS, "Cybersecuritymonitor 2019".

[43] Thomas Ostrom, "The Relationship between the Affective, Behavioral and Cognitive Components of Attitude," *Journal of Experimental Social Psychology* 5, no. 1 (1969): 12–30, https://doi.org/10.1016/0022-1031(69)90003-1.

[44] Icek Ajzen and Martin Fishbein, "The Influence of Attitudes on Behavior," in *The Handbook of Attitudes*, ed. Dolores Albarracín, Blair Johnson and Mark Zanna (Mahway: Lawrence Erlbaum Associates, 2005), 173–221.

[45] Dolores Albarracín, Blair Johnson, and Mark Zanna, ed., *Handbook about Attitudes*

(Mahway, New Jersey: Lawrence Erlbaum Associates Publishers, 2005).

[46] William Crano and Radmila Prislin, *Attitudes and Attitudes Change* (New York: Psychology Press, 2008).

[47] Fiske and Taylor, *Social Cognition: From Brains to Culture*, 232.

[48] Ostrom, "The Relationship," 12–30.

[49] Aronson and Wilson, *Sociale Psychologie*.

[50] Kari Edwards, "The Interplay of Affect and Cognition in Attitude Formation and Change," *Journal of Personality and Social Psychology* 59, no. 2 (1990): 202–216, https://doi.org/10.1037/0022-3514.59.2.202.

[51] Arie Kruglanski and Wolfgang Stroebe, "The Influence of Beliefs and Goals on Attitudes: Issues of Structure, Function, and Dynamics," in *The Handbook of Attitudes*, ed. Dolores Albarracín, Blair Johnson, and Mark Zanna (Mahwah: Lawrence Erlbaum Associates, 2005), 323–368.

[52] Lebek *et al*., "Information Security Awareness and Behavior," 1049–1092.

[53] Noor Hayani Abd Rahim, Suraya Hamid, Laiha Mat Kiah, Shahaboddin Shamshirband, and Steven Furnell, "A Systematic Review of Approaches to Assessing Cybersecurity Awareness," *Kybernetes* 44, no. 4 (2015): 606–22. https://doi.org/10.1108/K-12-2014-0283.

[54] Sommestad *et al*., "Variables Influencing," 42–75.

[55] Kruger and Kearney, "A prototype for assessing," 289–296.

[56] Parsons *et al.*, "The Human Aspects," 40–51.

[57] Stephen Crites, Leandre Fabrigar, and Richard Petty, "Measuring the Affective and Cognitive Properties of Attitudes: Conceptual and Methodological Issues," *Personality and Social Psychology Bulletin* 20, no. 6 (2007): 619–634, https://doi.org/ 10.1177/0146167294206001.

[58] Albarracín *et al*., *Handbook of Attitudes*, 19–40.

[59] Ellen Peters and Paul Slovic, "Affective asynchrony and the measurement of the affective attitude component," *Cognition and Emotion* 21, no. 2 (2007): 300–329, https://doi.org/10.1080/02699930600911440.

[60] Fred Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly: Management Information Systems* 13, no. 3 (1989): 319–339, https://doi.org/10.2307/249008.

[61] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers and Security* 49 (2015), 177–191, https://doi.org/10.1016/j.cose.2015.01.002.

[62] Susanne van 't Hoff-de Goede, Rick van der Kleij, Steve van de Weijer, and Rutger Leukfeldt, "Hoe veilig gedragen wij ons online?" 2019, https://www.wodc.nl/ binaries/2975_Volledige_Tekst_tcm28-421151.pdf.

[63] Martin Fishbein and Icek Ajzen, *Predicting and Changing Behavior: The Reasoned Action Approach*. *Predicting and Changing Behavior: The Reasoned Action Approach* (New York: Psychology Press, 2010), https://doi.org/10.4324/9780203838020.

[64] Fishbein and Ajzen, *Predicting and Changing Behavior,* 518.

[65] Icek Ajzen, Cornelia Czasch, and Michael Flood, "From Intentions to Behavior: Implementation Intention, Commitment, and Conscientiousness," *Journal of Applied Social Psychology* 39, no. 6 (2009): 1356–7, https://doi.org/10.1111/j.155918 16.2009.00485.x.

[66] Martin Fishbein and Icek Ajzen, *Belief, Attitude, Intention, and Behaviour: An introduction to theory and research* (MA: Addison-Wesley, 1975).

[67] Lebek *et al.*, "Information security awareness and behavior," 1049–1092.

[68] Fishbein and Ajzen, "*Belief, Attitude, Intention, and Behaviour*".

[69] Nina Gerber, Paul Gerber, and Melanie Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior," *Computers and Security* 77 (2018), https://doi.org/10.1016/j.cose.2018.04.002.

[70] ISO27002, "NEN-EN-ISO/IEC 27002: Information technology - Security techniques – Code of practice for information security controls," 2017, https://www.nen.nl/NEN-Shop/Norm/NENENISOIEC-270022017-en.htm.

[71] Ben-Asher and Gonzalez, "Effects of cyber security knowledge," 51–61.

[72] Grimes *et al.*,"Older Adults' Knowledge of Internet Hazards," 173–192.

[73] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram, "An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations," *Proceedings of the European Information Security Multi-Conference (EISMC 2013)*, (2013): 34–44.

[74] Tirumala *et al.*, "A survey on Internet Usage," 223–228.

[75] Parsons *et al.*, "An Analysis of Information Security Vulnerabilities," 34–43.

[76] Valerie Sue and Lois Ritter, *Conducting Online Surveys* (Thousand Oaks, CA: Sage Publications, 2012).

[77] Evelyn Dwyer, "Attitude Scale Construction: A Review of the literature," *ERIC Institute of Education Sciences*, no. ED359201 (1993): 1–48, https://eric.ed.gov/?id=ED 359201.

[78] Ostrom, "The Relationship," 12–30.

[79] Shropshire *et al.,* "Personality, attitudes, and intentions," 177–191.

[80] Lebek *et al.*, "Information Security Awareness and Behavior," 1049–1092.

[81] Ben-Asher and Gonzalez, "Effects of Cyber Security Knowledge," 51–61.

[82] Parsons *et al.*, "Determining Employee Awareness," 165–76.

[83] Parsons *et al.*, "The Human Aspects," 40–51.

[84] Ostrom, "The Relationship," 12–30.

[85] Sommestad *et al.*, "Variables Influencing Information Security Policy Compliance," 42–75.

[86] Lebek et al., "Information Security Awareness and Behavior," 1049–1092.

[87] Peter Mayer, Alexandra Kunz, and Melanie Volkamer, "Reliable Behavioural Factors in the Information Security Context," in Proceedings of the 12th International Conference on Availability, Reliability and Security ARES'17, August 2017*,* https://doi.org/10.1145/3098954.3098986.

[88] CBS, "Cybersecuritymonitor 2019."

About the Authors

Lisa de **Kok** is currently a researcher at the Centre of Expertise Cybersecurity at The Hague University of Applied Sciences in The Hague, the Netherlands. She has a Master's degree in Social & Organisational Psychology and a Bachelor's Degree in Public Administration. These are also the subjects where she focuses on in her research: the human & organisational factor of cyber security in (semi)-public organisations.

Deborah **Oosting** is a cybersecurity researcher and a teacher 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 behaviour.

Marcel **Spruit** is professor OF cybersecurity at The Hague University of Applied Sciences in The Hague, the Netherlands. He is responsible for research and the development of new education in the area of cybersecurity. His interests focus on the organization of cybersecurity and the influence of human behaviour.