Optimism bias in susceptibility to phishing attacks: an empirical study

Morné Owen
Department of Information Systems, Rhodes University, Grahamstown, South Africa

Stephen V. Flowerday
Department of Computer Studies, The University of Tulsa, Tulsa, Oklahoma, USA, and

Karl van der Schyff
Department of Information Systems, Rhodes University, Grahamstown, South Africa and School of Design and Informatics, Abertay University, Dundee, UK

Received 19 February 2023
Revised 30 July 2023
7 January 2024
21 April 2024
Accepted 23 April 2024

Abstract

Purpose – Researchers looking for ways to change the insecure behaviour that results in phishing have considered multiple possible reasons for such behaviour. Therefore, the purpose of this paper is to understand the role of optimism bias (OB – defined as a cognitive bias), which characterises overly optimistic or unrealistic individuals, to ensure secure behaviour. Research that focused on issues such as personality traits, trust, attitude and Security, Education, Training and Awareness (SETA) was considered.

Design/methodology/approach – This study built on a recontextualized version of the theory of planned behaviour to evaluate the influence that optimism bias has on phishing susceptibility. To model the data, an analysis was performed on 226 survey responses from a South African financial services organisation using partial least squares (PLS) path modelling.

Findings – This study found that overly optimistic employees were inclined to behave insecurely, while factors such as attitude and trust significantly influenced the intention to behave securely.

Practical implications – Our contribution to practice seeks to enhance the effectiveness of SETA by identifying and addressing the optimism bias weakness to deliver a more successful training outcome.

Originality/value – Our study enriches the Information Systems literature by evaluating the effect of a cognitive bias on phishing susceptibility and offers a contextual explanation of the resultant behaviour.

Keywords Phishing, Cyber security, Optimism bias

Paper type Research paper

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2023-0023

1. Introduction

According to the Cyber Security Breaches Survey (Ell and Gallucci, 2022), 83% of attacks were phishing based. The 2021 State of the Phish report (Proofpoint, 2021) states that more than 75% of organisations experienced a phishing attack in 2020, and 57% of these fell victim to a phishing attack.

This study considers the impact of optimism bias. Unrealistic optimism, or *optimism bias* (OB), is a cognitive bias where a person believes "that negative events are less likely to happen to them than to others, and they believe that positive events are more likely to happen to them than to others" (Weinstein, 1980, p. 807). Individuals characterised by optimism bias underestimate the likelihood of bad events happening (e.g. a car accident, losing their jobs or suffering from a terminal illness) whilst overestimating the likelihood of good events such as individual longevity or job aptitude (Sharot, 2011). It is therefore likely that an individual who is unrealistically optimistic could behave insecurely as they do not think they will be part of a phishing scam.

Prior phishing studies have attempted to understand why certain people are more susceptible to falling victim to a phishing attack (Chen *et al.*, 2020; Parsons *et al.*, 2019; Williams *et al.*, 2017). A logical place to start is by understanding human behaviour, which is the central theme for many studies that focus on persuasion techniques.

Based on the phishing statistics mentioned above, it appears that the implementation of technical security controls and Security, Education, Training and Awareness (SETA) is ineffective in eradicating phishing attacks completely. To make matters worse, some people consider themselves well versed in cyber security awareness and, owing to their confidence or optimistic outlook, do not think a breach will happen to them (Boddy, 2018).

Thus, the following research question was formulated:

RQ1. To what extent does optimism bias influence phishing susceptibility?

Accordingly, the aim of this study was:

- to propose alternative methods for effective SETA specifically considering optimism bias;
- to understand the influence of optimism bias on secure behaviour; and
- to understand how the relationship between attitude, trust and awareness influences the intention to behave securely (i.e. not falling victim to a phishing attack).

The remainder of this paper is structured as follows: We review previous literature on optimism bias, phishing, the *theory of planned behaviour* (TPB) and SETA. These findings are used to develop our research model and hypotheses. The research methodology described and the results presented. To conclude, we discuss how our findings can be used for research and practice, as well as the limitations of this study and future directions for research.

2. Theoretical background

2.1 Optimism bias overview

Optimism bias is a cognitive bias in the social sciences and is referred to in various studies linked to social-reasoning and decision-making (Sweldens *et al.*, 2014). A cognitive bias is defined as "an inaccurate view of the world" that might produce a rational behaviour or result in an outcome bias (Marshall *et al.*, 2013, p. 469). There is evidence that people believe they have a better than average chance of experiencing a variety of desirable future outcomes (Weinstein, 1980). Houston *et al.* (2012, p. 173) define optimism as an "overestimation of the expected gains from future outcomes". People therefore believe that they are at less risk compared to other people.

Unrealistic optimism can be classified into one of two broad categories:

(1) unrealistic absolute optimism; and

(2) unrealistic comparative optimism (Shepperd *et al.*, 2017).

Both types of unrealistic optimism can be applied on both an individual and a group level.

The belief that a personal outcome will be more favourable than it should be according to some quantitative objective standard is referred to as *unrealistic absolute optimism* (Shepperd *et al.*, 2017). Researchers have compared people's predictions about an event to the actual outcomes to assess unrealistic absolute optimism at the individual level (Shepperd *et al.*, 2017). Previous studies using this approach in comparing predictions to actual behaviour have shown that people are unrealistically optimistic about, for example, the time it will take them to complete a task, the starting salary for their first job and their grades for college exams (Buehler *et al.*, 1994). Another method to determine unrealistic absolute optimism at the individual level is to compare an individual's personal risk estimate to a risk calculator, which is defined as a "validated individualised risk-assessment algorithm" (Shepperd *et al.*, 2017). An example would be when a woman rates herself as having a 5% chance of getting breast cancer when the risk calculator suggests 21%.

The tendency for people to report that they are less likely to experience a negative event compared to others is known as *unrealistic comparative optimism* (Baek *et al.*, 2014). Previous studies that explained comparative optimism have included risk rejection, which is the belief that people disregard the likelihood of experiencing negative events (Arnett, 2000); ego safety, which is the belief that people want to defend themselves against a negative self-image (Helweg-Larsen *et al.*, 2002); and a sense of control, which is the belief that people are overconfident in their ability to control future events (Weinstein, 1980). Researchers contend that a group of people exhibits unrealistic comparative optimism if the group's mean comparative risk estimate for an unfavourable outcome is less than "average". The logic is that if a group of people accurately estimate their risk, their estimates should balance out overall by taking the accurate below and above average into account (Shepperd *et al.*, 2017).

2.1.1 The influence of optimism bias on attitude. Optimism bias could lead to a careless attitude of "it won"t happen to me', thus placing the responsibility for secure behaviour on other people or on technology. Not paying attention to possible cyberthreats owing to a lack of conscious awareness can result in risky behaviour. For example, a phishing email may be seen as merely another request to be complied with, motivated either through fear or reward.

The current findings indicate that optimism bias and the illusion of control are widespread phenomena (Rhee *et al.*, 2011). A person's attitude (belief) towards an object influences the overall pattern of their responses to the object, as demonstrated in numerous studies that tested the contention of strong attitude (belief) and subsequent behaviour relations (Ajzen and Fishbein, 1977). As a result of this strong inclination to underestimate their own risk and overrate their controllability observed in the domain of cyber security, we may argue that people may see little point in changing their current behaviour and have little motivation to be attentive to potential threats (Rhee *et al.*, 2011).

2.1.2 The influence of optimism bias on trust. Since trust is based on the positive expectations of others this can increase the outlook for trust in the good disposition of others (Andersson, 2012). Marsh (1994) argues that an optimist is likely to be one whose trust in others is high and who is inflexible in a downward direction. Thus, even though an optimist is abused by another, their trust in that other will not reduce by much. In contrast, the amount of trust a pessimist has in others will be relatively uncompromising in an upward direction, and a small manipulation by another will result in an extreme loss of trust (Marsh, 1994). Hence, if an unrealistic optimist's trust is not reduced by a previous security breach it could lead to further insecure behaviour.

2.2 Theory of planned behaviour

TPB posits that behaviour is influenced by *attitude*, *subjective norms,* and *perceived behavioural control* (Ajzen, 1991). Attitude is described as a taught inclination to judge things in a certain way and refers to positive or negative feelings about a specific behaviour. If the inclination changes, then attitude will change, leading to changed behaviour. A positive feeling about a certain behaviour will result in more motivation to perform the behaviour in question. 'Subjective norms' refers to the assumed social burden involved in performing a specific behaviour. Perceived behavioural control is one's perception of the effort, considering one's skills and abilities, required to implement the behaviour of interest. Undertaking a specific behaviour may favour perceptions that are related to either a desirable or an undesirable outcome. An individual's intention to undertake a certain behaviour is a key aspect of the TPB, as intentions are thought to capture the motivating variables that influence behaviour; these are indicators of how hard someone is willing to try and how much work they intend to put in to complete the behaviour. In general, the stronger the desire to engage in a behaviour, the more likely it is that it will be carried out.

According to the TPB, behaviour is a function of salient beliefs about the behaviour in question. People may have various beliefs about an activity, but they can only concentrate on a few of them at a time. These salient beliefs may have an impact on a person's intentions and actions. By tying each idea to a specific outcome, behavioural beliefs influence attitude. We develop favourable attitudes towards beliefs that lead to desirable results and negative attitudes towards activities that lead to negative consequences. *Normative beliefs* are linked to *social norms,* as they are concerned with the approval or disapproval of a specific behaviour shown by influential persons. *Control beliefs* are linked to perceived behavioural control, as people believe they have more control over a behaviour when they possess the skills or confidence to perform it.

Other studies using the TPB to understand secure behaviour when using information systems include the evaluation of the rank order of employees, addressing careless cyber security behaviour, how to create training and awareness methods for better SETA, and investigating why SETA campaigns fail (Aurigemma and Mattson, 2017; Bada and Sasse, 2014; Safa *et al.*, 2015).

The TPB was deemed suitable in the context of our study to guide the development of the research model and the associated hypotheses. As salient beliefs play a crucial role in the intention to perform a certain behaviour, and unrealistically optimistic people believe bad things will not happen to them, we are of the opinion that TPB is more suitable than any other theory examined.

3. Research model and hypotheses

3.1 Attitude towards secure behaviour

Attitude has been defined as a way of thinking, feeling or acting that represents a mental or emotional condition (McLeod, 2018). In the context of this study, attitude is defined in relation to secure employee behaviour and thus not falling for phishing attacks.

Attitude is used in many studies relating to cyber security. Herath *et al.* (2014) found that attitude had a significant effect on the use of email identification services in behaving securely, and Lowry and Moody (2015) found that attitude influenced the behaviour to comply with organisational cyber security policies. Other examples include the study of

Turkanović and Polančič (2013) which explained that attitude towards privacy and security is moving from an unaware state to greater awareness where people try to protect themselves as best they can. In addition, a study done by Tsohou *et al.* (2015) confirms that biases affecting personal beliefs and attitudes influence the intention to behave securely.

We therefore hypothesise that:

H1. An employee's attitude towards cyber security is positively associated with the intention to behave securely. In other words, the more the employee values cyber security the more they intend to behave securely.

3.2 The behavioural influence of trust

Trust in the context of this study is more accurately described as "benevolent trust"; the employees are placing significant trust in the security systems provided by the employer to protect their mutual interests (Mayer *et al.*, 1995).

Musuva *et al.* (2019) found that a person's perception of trustworthiness was a strong predictor of their behaviour. People who are trusting are more susceptible to becoming victims of social engineering than those who distrust.

Trust spans multiple areas, for example the use of systems, trusting that electronic communications received are authentic and, specifically in our study, the trust placed in the security controls implemented by the organisation's IT department. We adapted the TPB by replacing subjective norms with "trust", because our population consists of employees from one organisation, thus creating a semi-controlled environment. In the context of our study, we did not perceive social pressure in relation to the performance or non-performance of a certain behaviour as significant. The employees trust that the security controls implemented by the IT department would protect them regardless of what other employees were doing (Butavicius *et al.*, 2020). This attitude could, however, lead to insecure behaviour.

Therefore, SETA must clearly state that the security tools that have been implemented only serve as a first line of defence and should not be trusted blindly. Employees need to understand that the tools cannot cater for all threats, especially zero-day vulnerabilities (Butavicius *et al.*, 2020). Accountability for system use, whether that use is secure or insecure, cannot be abdicated. SETA should provide examples of scenarios where the security tools could fail to prevent a breach. We accordingly hypothesise that:

H2. An employee's trust is positively associated with the use of technical cyber security controls creating the intention to behave securely. In other words, the more the employee values cyber security the more they intend to behave securely

3.3 The behavioural influence of awareness

Awareness is another factor influencing decision-making. Several studies have focused on computer users' inability to identify cyber security threats as a result of their lack of technical skills. Although SETA is believed to be the best solution for combating security attacks involving people, the desired outcome is not always achieved. Aloul's (2012) phishing audit resulted in 9% of users falling victim to the attack. SETA was subsequently conducted, and a second audit revealed a decrease from 9 to 2% of users. Abbasi *et al.* (2012) found that 15% of users ignored browser security toolbars warning them of phishing sites. Therefore, awareness is not the only factor that needs to be considered when dealing with people and cyber security, as optimism bias should be considered as well.

A study by Li *et al.* (2019) showed that employees who are more aware of their company's information security policy and procedures were better equipped to behave securely. Tschakert and Ngamsuriyaroj (2019) performed SETA using various techniques, from instructor-led to gamification, video and text-based material, and found them all to be effective in raising awareness and changing behaviour.

As discussed, although SETA does not completely mitigate insecure behaviour for all employees, it does reduce the risk of insecure behaviour. We therefore hypothesise that:

H3. An employee's awareness of cyber security is positively associated with the intention to behave securely

3.4 The behavioural influence of optimism bias

Importantly, empirical evidence links optimism bias to behaviour. For example, White *et al.* (2011) found that young drivers with optimism bias rated themselves as "somewhat more" skilled than a typical young driver in terms of perceived overall and specific driving skills, while rating themselves as "somewhat less" likely to be in an accident, even though road accidents are the leading cause of death and injury among those under the age of 25 in First World countries. optimism bias therefore has a direct influence on decision-making.

Previous research has found that some forms of optimism and self-enhancement can be reduced or at least controlled by providing people with more information (awareness) and making them more accountable for the accuracy of their predictions (Barberia *et al.*, 2013).

A study performed by Cho *et al.* (2010) considered the influence of optimism bias on online privacy risks and found that unrealistically optimistic people do not respond to mere warning messages about privacy concerns, nor do they personalise the risk, seeing it rather as a risk to "others". Min and Kim (2015) also studied the effect of optimism bias on online privacy concerns and came to the same conclusion; that is, that unrealistically optimistic people engage in risky behaviour. People underestimate the risk because they believe they are immune to cyberattacks, even when others have been shown to be vulnerable.

In the TPB, *perceived behavioural control* refers to "people's perception of the ease or difficulty of performing the behaviour of interest" (Ajzen, 1991). In this study, we replaced perceived behavioural control with awareness as our control for secure behaviour. Furthermore, we believe that there is a significant difference in behaviour between the optimism bias group and the average group. Optimism bias people frequently believe that behaving securely requires no effort on their part, since they will not be placed in a threat situation. Thus, we hypothesise that:

H4a. Employees' attitudes towards cyber security differ significantly between the unrealistic optimistic group and the average group

H4b. Employees' trust is positively associated with cyber security and differs significantly between the unrealistic optimistic group and the average group

H4c. Employees' awareness of cyber security is positively associated with the intention to behave securely and differs significantly between the unrealistic optimistic group and the average group

4. Methodology

We used a cross-sectional survey to inform this study (Saunders *et al.*, 2016). Ethical clearance was obtained from both the university ethical standards committee and the financial services organisation where the primary data was collected. Respondents were informed that their results would be used in a research study and that they could opt-out at any stage.

4.1 Respondent population and sample

The respondents were representative of the general population of employees ($n = 775$) in the financial services sector. This company was selected as an audit finding found it had insufficient SETA placing the company at risk. The company's IT is managed as an internal function consisting of infrastructure maintenance, end-user computing, custom software development and BI, network and security functions. SETA is offered through the company learner management system (LMS) and weekly topical security emails remind staff to remain vigilant. Respondents' qualifications and experience differs significantly from each other as the roles included call centre agents, accountants, IT professionals, attorneys and general admin staff. Since this is a financial company the risk resulting from a security breach will be significant as it could impact millions of customers.

Systematic random sampling based on employee email addresses was used in the selection process. The email addresses were sorted alphabetically and every third employee was selected. Respondents included employees from all levels within the organisation, such as call centre consultants, administration clerks, staff employed in the legal, IT and human capital departments and senior management.

4.2 Data collection and screening

The questionnaire was distributed using the organisation's web-based learning management system (LMS) and completion of the questionnaire was voluntary. Data was collected from 257 respondents. Employees were encouraged by management to complete the survey due to a previous audit finding highlighting the importance of SETA. Owing to a combination of incomplete data input and validity concerns, 31 responses were dropped. Subsequently, the data obtained from the remaining 226 respondents was used for further analysis. Our research instrument was largely adapted from previous research. We used certain items from the Human Aspects of Information Security Questionnaire (HAIS-Q). HAIS-Q was developed to measure information security threats triggered by employees. The questionnaire focuses on individuals' knowledge and attitudes towards policies and procedures relating to their behaviour when using a work computer (Parsons *et al.*, 2017). See Appendix Table A1 provides a complete outline of the items and the associated descriptive statistics that comprised the research instrument for this study.

4.3 Classifying employees as unrealistic optimistic or average

We used 11 optimism bias items (refer See Appendix Table A2) to determine which respondents were unrealistic optimists and which were average based on the study performed by Weinstein (1980). The life events that were included, both positive and negative, had to be relevant to all respondents. Respondents were asked to rate themselves in comparison to their peers in terms of the optimism bias questions. When it comes to positive events, *optimism* is defined as believing that one's odds are better than average, whereas *pessimism* is defined as believing that one's chances are worse than average. These definitions of optimistic and pessimistic responses are swapped for negative events (Weinstein, 1980). Accordingly, respondents had to complete all the optimism bias questions to categorise themselves as either unrealistic optimists or average. In our sample, 49% of respondents were classified as unrealistic optimists.

4.4 Data analysis and results

The primary data was analysed by way of PLS path modelling, which is a suitable approach when the data violates distributional assumptions (Hair *et al.*, 2019). All the items with outer loadings in excess of 0.7 were kept and formed part of the resultant multivariate analysis.

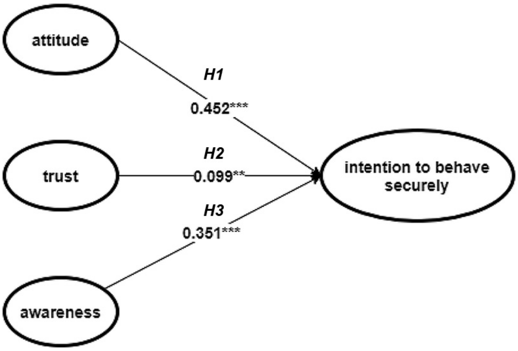
4.4.1 Evaluating the measurement model. As part of this evaluation, we assessed both convergent and discriminant validity. To assess convergent validity, all the constructs and their respective items were investigated to establish whether their factor loadings exceeded 0.5. We also inspected the significance of the outer loadings of the items using their associated t-statistic values. Accordingly, the outer loading of each item was found to be in excess of 0.5. Additionally, all the constructs exhibited AVE values in excess of 0.5. Together, these findings satisfy the criteria for convergent validity.

Discriminant validity was assessed in three ways. First, we used the Fornell-Larcker criterion to evaluate whether the square root of the AVE value of each construct was greater than all the correlation coefficients among the measurement model constructs (Fornell and Larcker, 1981). See Appendix Table A3 presents these square root values on the diagonal. We also inspected the cross loadings to ensure that the items of each construct loaded highest on itself. As a third means of assessing discriminant validity, we inspected the mean heterotrait-monotrait (HTMT) ratio values which were all below the theoretical threshold of 0.9 (Henseler *et al.*, 2014; Kline, 2011). Together, these tests confirm that the measurement model is valid from both a convergent and a discriminant perspective. Because we performed a PLS-based analysis, we also assessed the measurement model for any signs of multicollinearity (Hair *et al.*, 2019; Lowry and Gaskin, 2014). All the variance inflation factor (VIF) values were below 3, thus eliminating the presence of multicollinearity (Craney and Surles, 2002; García *et al.*, 2015; Hair *et al.*, 2010). See Appendix Table A1 for a complete outline of these VIF values. As a final means of evaluating the measurement model, we also assessed the reliability of the questionnaire by calculating values for both composite reliability (CR) and Cronbach's alpha (CA). In general, the reliability of a questionnaire attests to whether it would produce the same results if it were to be administered again (Cronbach, 1951). Both the CA and CR values were in excess of the accepted threshold of 0.7 (Tavakol and Dennick, 2011), as presented in See Appendix Table A3.

4.4.2 Evaluating the structural models. To evaluate the models from a structural perspective, we made use of PLS path modelling, in particular the path coefficients, predictive power (R^2), effect sizes (f^2), and the out-of-sample predictive relevance (Stone-Geisser's Q^2). A summarised version of the values relating to the global model is illustrated in Figure 1. From the results illustrated in Figure 1, it is clear that there is support for *H1, 2* and *H3*. Additionally, the global model (both the unrealistically optimistic and the average individuals) accounts for 67.7% (adjusted $R^2 = 0.677$) of the variance in the target construct (*intention to behave securely*). The out-of-sample predictive relevance equals 56.8% ($Q^2 = 0.568$) (Geisser and Eddy, 1979; Hair *et al.*, 2017; Stone, 1974). In the bootstrapped significance testing (with 100 subsamples), *attitude* was shown to exert a significant influence on intention to behave securely ($\beta = 0.452$, $p < 0.01$), which supports the first hypothesis (*H1*). The results also indicate that *trust* significantly influences *intention to behave securely* ($\beta = 0.099$, $p < 0.05$), which provides support for the second hypothesis (*H2*).

Similarly, *awareness* significantly influences *intention to behave securely* ($\beta = 0.351$, $p < 0.01$), which provides support for the third hypothesis (*H3*).

In addition to the significance testing that was conducted, we also assessed the relative impact of each independent variable by inspecting its effect size using Cohen's guidelines for f^2 (Cohen, 1988). Of all the latent constructs in the global model, *attitude* exhibited the largest effect size (0.363 – a large effect) on intention to behave securely. This was followed by



Source: Created by the authors'

Figure 1. Quantitative research model (global), ***at $p < 0.01$; **at $p < 0.05$

awareness (0.103 – a small effect), and finally *trust* (0.023 – the smallest effect). This indicates that an individual's attitude towards cyber security is pivotal when explaining their intentions to act securely within the workplace.

4.4.3 PLS multigroup analysis (unrealistically optimistic vs average group). Because the results of the global model did not allow us to infer that a significant difference exists between those individuals who are optimistically biased as opposed to those who are not, we also conducted a PLS-based multigroup analysis. Although we could have employed a repeated application of unpaired t-tests (or a permutation test for that matter), it is important to note the shortcomings of these techniques. First, these tests do not take the whole model into account (Klesel *et al.*, 2019). This is especially pertinent within exploratory contexts, where researchers are not just interested in significant differences between path coefficients. Second, unpaired t-tests are particularly sensitive to the distribution of the sample – something that does not hamper PLS path modelling.

As with the significance tests conducted for the global model, we also performed a bootstrapped significance test. Note that PLS-based multigroup analyses are non-parametric and are largely based on specific group parameter estimates. These include model aspects such as outer weights and loadings, as well as path coefficients (Sarstedt *et al.*, 2011). From the results presented in Table 1 below, it is apparent that all the relationships illustrated in Figure 1 show significant differences when the quantitative "unrealistic optimists" model is compared with the "average" model. In other words, there are significant differences in attitude, trust and level of awareness when comparing those individuals classified as unrealistic optimists with those classified as average. Importantly, these multigroup results provide support for the fourth hypothesis (H4a, b and c). Refer to See Appendix Table A4 for a summary of all models that comprise this study.

Table 1. Results of the multigroup analysis

Hypothesis	Path	Diff (abs)	*p*-value	t-statistic	Support
H4a	Attitude → intention to behave securely	0.427	0.000	3.841***	Yes
H4b	Trust → intention to behave securely	0.255	0.085	1.731*	Yes
H4c	Awareness → intention to behave securely	0.298	0.059	1.900*	Yes

Notes: *** at $p < 0.01$, *at $p < 0.10$ (unrealistic optimists vs. average)
Source: Created by the authors'

5. Discussion

The focus of this study was to gain a better understanding of why certain employees are more susceptible to phishing than others. Specifically, we examined (1) how attitude, trust and awareness influenced the intention to behave securely, and (2) the effect of unrealistic optimism on attitude, trust, awareness and secure behaviour. From the results, the following key findings are noteworthy. First, attitude had a significant influence on the intention to behave securely in the workplace. Second, trust plays a significant role in how employees behave in the workplace, as they rely on the security controls implemented to protect them. Third, awareness leads to more secure behaviour but does not completely eradicate insecure behaviour. These findings give us a better understanding of which employees are more likely to behave insecurely.

5.1 Contributions

Our contribution enhances secure behaviour by considering a cognitive bias called optimism bias when confronted with phishing attacks. Our model (Figure 2) proposes that optimism bias influences the intention to behave securely. Our model contributes to the IS literature, providing a better understanding of why certain employees are more susceptible to insecure behaviour.

Our contribution to practice is that SETA programmes need to be adapted to cater for unrealistically optimistic people. SETA should contain a section intended to make employees aware of whether they are unrealistically optimistic and therefore what the likely outcome of their behaviour could look like.

The effectiveness of a SETA programme is influenced by how it is presented. The use of interactive methods to engage participation during training and being able to test the subject matter after the training are critical. SETA is not a once-off event but an ongoing programme, focusing on current threats and scenarios so that employees can relate to and correctly respond to these threats (Bauer *et al.*, 2017).

A false sense of security is created in organisations with a dedicated IT department that manages the end-user environment by implementing restrictive administration controls and

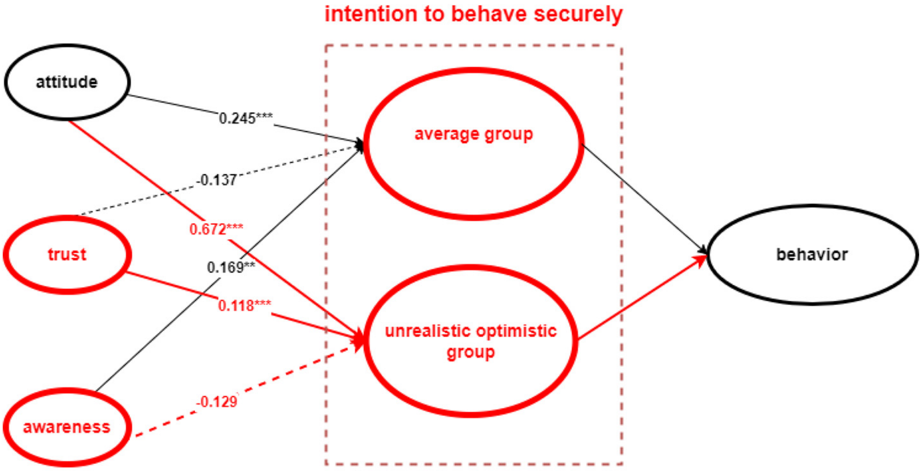


Figure 2. Intention to behave securely

Source: Created by the authors’

demonstrating to users that "big brother" is watching. This approach encourages employees to blindly trust that these controls will protect them regardless of their behaviour (Butavicius *et al.*, 2020). Instead, there is a need to educate employees through SETA programmes, so that they will understand that the controls which have been implemented could fail, and that the responsibility for behaving securely can never be placed solely on systems.

We compared the unrealistically optimistic group with the average group and found that attitude had the largest effect on the intention to behave securely. The attitude of "it won"t happen to me' among the unrealistic optimists significantly influenced their trust and ultimately their behaviour (see Appendix Table A4). This discrepancy sheds light on the psychological underpinnings of secure behaviour. Unrealistically optimistic individuals, driven by the belief that security incidents won't affect them personally, exhibit a distinct attitude. These individuals' perception that they are immune to threats influence their intention to behave securely. It is important to recognise that this is not a linear statistical observation but a robust indication that the attitude–intention relationship differs significantly between the two groups. For cyber security practitioners, addressing this attitude gap is imperative. Security awareness programs should be tailored to challenge this overly optimistic outlook, emphasising that anyone (regardless of perceived invulnerability) is susceptible to threats. These results underscore the need for interventions that reshape the optimistic group's attitude by debunking the notion that security breaches are an improbability for them.

As indicated in Table 1, our multigroup analysis also found a significant difference in trust towards the intention to behave securely between the two groups. This outcome implies that trust in security controls varies between unrealistically optimistic and average individuals. Unrealistically optimistic individuals may disproportionately rely on security measures, fostering a (potentially) misguided trust in their effectiveness. The nuanced statistical significance emphasises that this distinction is not arbitrary but indicative of a meaningful disparity in how trust influences the intention to behave securely. For security practitioners, clarifying the limitations of such security controls is therefore paramount. While trust is generally positive, an unwarranted trust that disregards personal responsibility (e.g. to act securely) might lead to negligent security practices. For this reason, we argue that education efforts should emphasise that security controls are part of a broader strategy where individuals need to actively contribute to safeguarding sensitive company information.

Our multigroup results also indicate that there is a significant difference between these groups when it comes to the relationship between awareness and their intention to behave securely. This highlights that awareness plays a role in shaping intentions differently for unrealistically optimistic and average individuals. While both groups benefit from awareness, the optimistic bias might influence how effectively security knowledge is integrated into behaviour. This result underscores the need for nuanced interventions in awareness programs. Unrealistically optimistic individuals may benefit from tailored content that not only imparts security knowledge but also addresses their specific cognitive biases. Fostering a realistic understanding of security threats is essential for translating awareness into proactive and secure behaviour.

5.2 Limitations and future research

Since data was collected from a single organisation, the effect of different cultures on optimism bias needs to be studied further. Chang *et al* (2001) compared optimism bias in American and Japanese people, finding that while both groups had an optimistic bias towards negative life experiences, the Japanese had a pessimistic bias for favourable life occurrences. In addition, variances in organisational culture influence the behaviour of users as they follow the example of top management (Hu *et al.*, 2012). Culture plays a significant role in human behaviour and future research is needed to address this vital theme.

The organisation in which the data was collected has implemented strong security controls. Employees are aware of these controls and have seen in the past how they have successfully stopped certain threats. However, this could lead to a false sense of benevolence trust, creating a careless attitude towards behaving securely. Future research should be done in an organisation with fewer internal controls to see if this would alter the behaviour of unrealistic optimists.

6. Conclusion

The objective of this study was to understand how a cognitive bias called optimism bias makes certain individuals more susceptible to phishing attacks. Humans remain vulnerable to cyber security breaches, which is clearly seen in the increasing number of successful phishing attacks. We found that one's attitude, security awareness and trust are critical in terms of the intention to behave securely.

Interestingly, there was a significant difference between the average and unrealistically optimistic employee groups in relation to attitude, awareness and trust in terms of the intention to behave securely (Figure 2). A crucial difference in the attitude of an unrealistically optimistic employee is the perception that a security breach won't happen to them. As a result, we have found that unrealistic optimists are more susceptible to security threats. These employees need to be reminded that they cannot blindly trust systems, that not all requests are legitimate, and above all, that they are not immune to security threats.

References

Abbasi, A., Zahedi, F. and Chen, Y. (2012), "Impact of anti-phishing tool performance on attack success rates", ISI 2012 - 2012 IEEE International Conference on Intelligence and Security Informatics: Cyberspace, Border, and Immigration Securities, pp. 12-17, doi: 10.1109/ISI.2012.6282648.

Ajzen, I. (1991), "The theory of planned behaviour", *Organizational Behaviour and Human Decision Processes*, Vol. 50, pp. 179-211, doi: 10.4135/9781446249215.n22.

Ajzen, I. and Fishbein, M. (1977), "Attitude-behaviour relations", : *A Theoretical Analysis and Review of Empirical Research*, Vol. 84 No. 5, pp. 888-918.

Aloul, F.A. (2012), "The need for effective information security awareness", *Journal of Advances in Information Technology*, Vol. 3 No. 3, pp. 176-183, doi: 10.4304/jait.3.3.176-183.

Andersson, M.A. (2012), "Dispositional optimism and the emergence of social network diversity", *The Sociological Quarterly*, Vol. 53 No. 1, pp. 92-115.

Arnett, J.J. (2000), "Optimistic bias in adolescent and adult smokers and nonsmokers", *Addictive Behaviours*, Vol. 25 No. 4, pp. 625-632.

Aurigemma, S. and Mattson, T. (2017), "Privilege or procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls", *Computers and Security*, Vol. 66, pp. 218-234, doi: 10.1016/j.cose.2017.02.006.

Bada, M. and Sasse, A. (2014), "Security awareness campaigns: why do they fail to change behaviour?", [Draft Working Paper]. Global Cyber Security Capacity Centre, July, 1-38. http://discovery.ucl.ac.uk/1468954/1/AwarenessCampaignsDraftWorkingPaper.pdf

Baek, Y.M., Kim, E. and Bae, Y. (2014), "My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns", *Computers in Human Behavior*, Vol. 31, pp. 48-56, doi: 10.1016/j.chb.2013.10.010.

Barberia, I., Blanco, F., Cubillas, C.P. and Matute, H. (2013), "Implementation and assessment of an intervention to debias adolescents against causal illusions", *PLoS ONE*, Vol. 8 No. 8, p. e71303.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017), "Prevention is better than cure! designing information security awareness programs to overcome users' non-compliance with information security policies in banks", *Computers and Security*, Vol. 68, pp. 145-159, doi: 10.1016/j.cose.2017.04.009.

Boddy, M. (2018), "Phishing 2.0: the new evolution in cybercrime", *Computer Fraud and Security*, Vol. 2018 No. 11, pp. 8-10, doi: 10.1016/S1361-3723(18)30108-8.

Buehler, R., Griffin, D. and Ross, M. (1994), "Exploring the 'planning fallacy': why people underestimate their task completion times", *Journal of Personality and Social Psychology*, Vol. 67 No. 3, pp. 366-381, doi: 10.1037/0022-3514.67.3.366.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M. and Calic, D. (2020), "When believing in technology leads to poor cyber security: development of a trust in technical controls scale", *Computers and Security*, Vol. 98, p. 102020, doi: 10.1016/j.cose.2020.102020.

Chang, E.C., Asakawa, K. and Sanna, L.J. (2001), "Cultural variations in optimistic and pessimistic bias: do easterners really expect the worst and westerners really expect the best when predicting future life events? ", *Journal of Personality and Social Psychology*, Vol. 81 No. 3, pp. 476-491, doi: 10.1037/0022-3514.81.3.476.

Chen, R., Gaia, J. and Rao, H.R. (2020), "An examination of the effect of recent phishing encounters on phishing susceptibility", *Decision Support Systems*, Vol. 133 No. 2019, p. 113287, doi: 10.1016/j.dss.2020.113287.

Cho, H., Lee, J. and Chung, S. (2010), "Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience", *Computers in Human Behavior*, Vol. 26 No. 5, pp. 987-995, doi: 10.1016/j.chb.2010.02.012.

Cohen, J. (1988), *Statistical Power Analysis for the Behavioural Sciences*, Lawrence Erlbaum Associates.

Craney, T.A. and Surles, J.G. (2002), "Model-dependent variance inflation factor cutoff values", *Quality Engineering*, Vol. 14 No. 3, pp. 391-403.

Cronbach, L.J. (1951), "Coefficient alpha and the internal structure of tests", *Psychometrika*, Vol. 16 No. 3, pp. 297-334.

Ell, M. and Gallucci, R. (2022), "Cyber security breaches survey 2022", available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-5-incidence-and-impact-of-breaches-or-attacks

Ferres, N. and Travaglione, A. (2003), "The development and validation of the workplace trust survey (WTS): combining qualitative and quantitative methodologies", APROS, Emotions, Attitudes, and Culture Stream, pp. 1-22, available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+development+and+validation+of+the+workplace+trust+survey+(WTS):+Combining+qualitative+and+quantitative+methodologies#0

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

García, C.B., García, J., López Martín, M.M. and Salmerón, R. (2015), "Collinearity: revisiting the variance inflation factor in ridge regression", *Journal of Applied Statistics*, Vol. 42 No. 3, pp. 648-661.

Geisser, S. and Eddy, W.F. (1979), "A predictive approach to model selection", *Journal of the American Statistical Association*, Vol. 74 No. 365, pp. 153-160, doi: 10.1080/01621459.1979.10481632.

Hair, J., Hult, T., Ringle, C. and Sarstedt, M. (2017), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (2nd ed.) Sage, London.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/EBR-11-2018-0203.

Hair, J.F., Black, W., Babin, B.Y.A., Anderson, R. and Tatham, R. (2010), *Multivariate Data Analysis: A Global Perspective*, Pearson Higher Education.

Helweg-Larsen, M., Sadeghian, P. and Webb, M.S. (2002), “The stigma of being pessimistically biaseid”, *Journal of Social and Clinical Psychology*, Vol. 21 No. 1, pp. 92-107.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2014), “A new criterion for assessing discriminant validity in variance-based structural equation modeling”, *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135, doi: 10.1007/s11747-014-0403-8.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H.R. (2014), “Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service”, *Information Systems Journal*, Vol. 24 No. 1, pp. 61-84, doi: 10.1111/j.1365-2575.2012.00420.x.

Houston, A.I., Trimmer, P.C., Fawcett, T.W., Higginson, A.D., Marshall, J.A.R. and McNamara, J.M. (2012), “Is optimism optimal? Functional causes of apparent behavioural biases”, *Behavioural Processes*, Vol. 89 No. 2, pp. 172-178, doi: 10.1016/j.beproc.2011.10.015.

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.

Klesel, M., Schuberth, F., Henseler, J. and Niehaves, B. (2019), “A test for multigroup comparison using partial least squares path modeling”, *Internet Research*, Vol. 29 No. 3, pp. 464-477, doi: 10.1108/IntR-11-2017-0418.

Kline, R.B. (2011), “Principles and practice of structural equation modeling”, *Structural Equation Modeling*, (3rd ed.). Guilford.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behaviour”, *International Journal of Information Management*, Vol. 45 No. 2018, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Lowry, P.B. and Gaskin, J. (2014), “Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioural causal theory: When to choose it and how to use it”, *IEEE Transactions on Professional Communication*, Vol. 57 No. 2, pp. 123-146, doi: 10.1109/TPC.2014.2312452.

Lowry, P.B. and Moody, G.D. (2015), “Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies”, *Information Systems Journal*, Vol. 25 No. 5, pp. 433-463, doi: 10.1111/isj.12043.

McLeod, S.A. (2018), “Attitudes and behaviour”, Simply Psychology, available at: www.simplypsychology.org/attitudes.html

Marsh, S. (1994), “Optimism and pessimism in trust”, *Proceedings of the Ibero-American Conference on Artificial Intelligence (IBERAMIA’94)*.

Marshall, J.A.R., Trimmer, P.C., Houston, A.I. and McNamara, J.M. (2013), “On evolutionary explanations of cognitive biases”, *Trends in Ecology and Evolution*, Vol. 28 No. 8, pp. 469-473, doi: 10.1016/j.tree.2013.05.013.

Mayer, R.C., Davis, J.H. and David Schoorman, F. (1995), “An integrative model of organizational trust”, *The Academy of Management Review*, Vol. 20 No. 3, pp. 709-734.

Min, J. and Kim, B. (2015), “How are people enticed to disclose personal information despite privacy concerns in social network sites? the calculus between benefit and cost”, *Journal of the Association for Information Science and Technology*, Vol. 66 No. 4, pp. 839-857, doi: 10.1002/asi.23206.

Mittal, S. (2015), “Understanding the human dimension of cyber security”, *Indian Journal of Criminology and Criminalistics*.

Musuva, P.M.W., Getao, K.W. and Chepken, C.K. (2019), “A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility”, *Computers in Human Behavior*, Vol. 94 No. 2018, pp. 154-175, doi: 10.1016/j.chb.2018.12.036.

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, doi: 10.1016/j.cose.2017.01.004.

Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M. (2019), "Predicting susceptibility to social influence in phishing emails", *International Journal of Human-Computer Studies*, Vol. 128, pp. 17-26, doi: 10.1016/j.ijhcs.2019.02.007.

Proofpoint (2021), "2021 State of the phish", available at: www.proofpoint.com/us/resources/threat-reports/state-of-phish

Rhee, H., Ryu, Y.U. and Kim, C. (2011), "Unrealistic optimism on information security management", *Computers and Security*, Vol. 31 No. 2, pp. 221-232, doi: 10.1016/j.cose.2011.12.001.

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, doi: 10.1016/j.cose.2015.05.012.

Sarstedt, M., Henseler, J. and Ringle, C.M. (2011), "Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical results", in Sarstedt, M., M. Schwaiger and C. Taylor (Eds), *Measurement and Research Methods in International Marketing (Advances in International Marketing*; Emerald Group, Bingley.

Saunders, M., Lewis, P. and Thornhill, A. (2016), *Research Methods for Business Students*, (7th ed.) Pearson Education, London.

Sharot, T. (2011), "The optimism bias", *Current Biology*, Vol. 21 No. 23, pp. 941-945, doi: 10.1016/j.cub.2011.10.030.

Shepperd, J.A., Pogge, G. and Howell, J.L. (2017), "Assessing the consequences of unrealistic optimism: challenges and recommendations", *Consciousness and Cognition*, Vol. 50, pp. 69-78.

Stone, M. (1974), "Cross-validatory choice and assessment of statistical predictions", *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*.

Sweldens, S., Puntoni, S., Paolacci, G. and Vissers, M. (2014), "The bias in the bias: Comparative optimism as a function of event social undesirability", *Organizational Behavior and Human Decision Processes*, Vol. 124 No. 2, pp. 229-244, doi: 10.1016/j.obhdp.2014.03.007.

Tavakol, M. and Dennick, R. (2011), "Making sense of Cronbach's alpha", *International Journal of Medical Education*, Vol. 2, pp. 53-55.

Tschakert, K.F. and Ngamsuriyaroj, S. (2019), "Effectiveness of and user preferences for security awareness training methodologies", *Heliyon*, Vol. 5 No. 6, p. e02010, doi: 10.1016/j.heliyon.2019.e02010.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015), "Managing the introduction of information security awareness programmes in organisations", *European Journal of Information Systems*, Vol. 24 No. 1, pp. 38-58, doi: 10.1057/ejis.2013.27.

Turkanović, M. and Polančič, G. (2013), "On the security of certain e-communication types: risks, user awareness and recommendations", *Journal of Information Security and Applications*, Vol. 18 No. 4, pp. 193-205, doi: 10.1016/j.jisa.2013.07.003.

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

White, M.J., Cunningham, L.C. and Titchener, K. (2011), "Young drivers' optimism bias for accident risk and driving skill: Accountability and insight experience manipulations", *Accident Analysis and Prevention*, Vol. 43 No. 4, pp. 1309-1315, doi: 10.1016/j.aap.2011.01.013.

Williams, E.J., Beardmore, A. and Joinson, A.N. (2017), "Individual differences in susceptibility to online influence: a theoretical review", *Computers in Human Behavior*, Vol. 72, pp. 412-421, doi: 10.1016/j.chb.2017.03.002Abbasi.

Further reading

Blythe, J.M. and Coventry, L. (2018), "Costly but effective: comparing the factors that influence employee anti-malware behaviours", *Computers in Human behavior*, Vol. 87 No. 2017, pp. 87-97, doi: 10.1016/j.chb.2018.05.023.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014), "Information security awareness and behaviour: a theory-based literature review", *Management Research Review*, Vol. 37 No. 12, pp. 1049-1092, doi: 10.1108/MRR-04-2013-0085.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T. and Ebner, N. (2017), "Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. Proceedings of the 2017 conference on human factors in computing systems", pp. 6412-6424, 10.1145/3025453.3025831

Sedikides, C., Campbell, W.K., Reeder, G.D. and Elliot, A.J. (2002), "The self in relationships: Whether, how, and when close others put the self 'in its place", *European Review of Social Psychology*, Vol. 12 No. 1, pp. 237-265.

Shepperd, J.A., Ouellette, J.A. and Fernandez, J.K. (1996), "Abandoning unrealistic optimism: performance estimates and the temporal proximity of self-relevant feedback", *Journal of Personality and Social Psychology*, Vol. 70 No. 4, pp. 844-855, doi: 10.1037/0022-3514.70.4.844.

Vinzi, V., Chin, W., Henseler, J. and Wang, H. (2010), *Handbook of Partial Least Squares*, Springer, Cham.

Appendix

Table A1. Questionnaire items, descriptive statistics and multicollinearity values (full model)

Construct	Item	Item description	Source	M	SD	Loading	t-statistic	VIF
Intention to behave securely	Q23	I believe my system is secure and will protect me from cyberthreats	New item	2.498	1.163	0.916	2.147893**	1.011
	Q24	My attitude positively changed towards information security (security behaviour) over the past Two years		2.208	1.154	0.910	1.913345*	1.014
Attitude	Q18	It's risky to open an email attachment from an unknown sender	HAIS-Q Parsons *et al.* (2017)	1.973	1.063	0.790	1.856068*	2.100
	Q21	It's risky to send sensitive work files using a public Wi-Fi network		2.004	1.119	0.838	1.790885*	2.108
	Q25	My work environment is positive and provides for satisfactory work conditions	(Mittal, 2015)	2.195	1.152	0.817	1.905382*	1.989
Awareness	Q26	It's acceptable to use my social media passwords on my work accounts	Hais-q Parsons *et al.* (2017)	3.815	1.170	0.746	3.260684**	1.101
	Q27	I am not permitted to click on a link in an email from an unknown sender		1.968	1.099	0.836	1.790719*	1.077
	Q29	I can't be fired for something I post on social media		3.333	1.347	0.713	2.474388**	1.077
	Q31	If I see someone acting suspiciously in my workplace, it is my duty to report it		1.953	1.022	0.852	1.910959*	1.064
Trust	Q45	Most people at my workplace are basically honest	Ferres and Travaglione (2003)	2.759	0.952	0.519	2.898109**	1.113
	Q46	I tend to trust the people I work with		2.909	1.031	0.813	2.821532**	1.027
	Q47	Most of the people I work with are basically good and kind		2.837	1.044	0.800	2.717433**	2.078
	Q48	Most of the people I work with trust others		3.116	0.848	0.796	3.674528**	2.128
	Q49	Most of the people I work with can be trusted		3.012	0.915	0.826	3.291803**	2.018
	Q50	I tend to see the best in the people I work with		2.665	1.117	0.628	2.385855**	2.065

Source: Created by the author

Question	Source	Question type	Response anchors
	Weinstein (1980)	Multiple choice	100% less (no chance), 80% less, 60% less, 40% less, 20% less, 10% less, average, 10% more, 20% more, 40% more, 60% more, 80% more, 100% more, 3 times average, 5 times average
1. Compared to otder employees, what do you think are the chances tdat the following events will happen to you? Your work will be recognized with an award.			
2. Compared to other employees, what do you think are the chances that the following events will happen to you? You expect to live past the age of 80 years old			
3. Compared to other employees, what do you think are the chances that the following events will happen to you? You may have contemplated suicide			
4. Compared to other employees, what do you think are the chances that the following events will happen to you? You expect to read about your achievements in the newspaper			
5. Compared to other employees, what do you think are the chances that the following events will happen to you? You don't expect to spend a night in hospital in the next 5 years			
6. Compared to other employees, what do you think are the chances that the following events will happen to you? You are likely to contract a venereal disease			
7. Compared to other employees, what do you think are the chances that the following events will happen to you? Your weight will remain constant for the next five years			
8. Compared to other employees, what do you think are the chances that the following events will happen to you? You will probably have a heart attack before the age of 60 years old			
9. Compared to other employees, what do you think are the chances that the following events will happen to you? You won't fall ill next winter			
10. Compared to other employees, what do you think are the chances that the following events will happen to you? You are likely to take an unattractive job			
11. Compared to other employees, what do you think are the chances that the following events will happen to you? You are likely to be fired from a job			

Source: Created by the author

Table A2.
Optimism bias instrument

Construct	CR	CA	AVE	1	2	3	4
Trust (1)	0.875	0.827	0.547	*0.740*			
Attitude (2)	0.858	0.748	0.665	0.324	*0.816*		
Awareness (3)	0.859	0.797	0.622	0.278	0.490	*0.789*	
Intention to behave securely (4)	0.909	0.800	0.834	0.307	0.622	0.500	*0.913*

Source: Created by the author

Table A3.
Measurement model statistics

Table A4. Summary of all models

	Global	t-statistic	p-value	f^2	Optimistic	t-statistic	p-value	f^2	Average	t-statistic	p-value	f^2	Diff(abs)	t-statistic	p-value
Attitude → intention to behave securely	0.452	7.001***	0.000	0.363	0.672	7.514***	0.000	0.509	0.245	2.624***	0.010	0.064	0.427	3.841***	0.000
Awareness → intention to behave securely	0.351	5.456***	0.000	0.103	−0.129	1.092	0.277	0.011	0.169	2.202**	0.030	0.045	0.298	1.900*	0.059
Trust → intention to behave securely	0.099	2.107**	0.036	0.023	0.118	3.007***	0.003	0.081	−0.137	1.527	0.130	0.023	0.255	1.731*	0.085
Sample size		226				111				115					
R^2		0.681				0.522				0.139					
Adjusted R^2		0.677				0.514				0.124					
Q^2		0.568				0.357				0.087					

Notes: *** at $p < 0.01$; ** at $p < 0.05$; * at $p < 0.10$
Source: Created by the author

About the authors

Morné Owen holds a N.Dip: IT, B.Tech: IT, Master’s in Business Information Systems and PhD degree. His research interests lie in behavioural cyber security. Morné is the Chief Information Officer for a financial services company. Morné Owen is corresponding author and can be contacted at: morne.owen@gmail.com

Stephen V. Flowerday is a Professor in the School of Cyber Studies at the University of Tulsa. His research interests lie in cybersecurity, behavioural information security, and information security management. Over the last sixteen years, he has authored and co-authored more than 120 refereed publications. His work has been funded by IBM, THRIP, NRF, SASUF, ERASMUS, GMRDC, and others.

Karl van der Schyff holds a BSc, MSc, and PhD degree. His field of interest lie in behavioural information security, information privacy, and cyberpsychology. He has authored and co-authored several refereed publications in addition to reviewing publications within the senior scholars basket of IS journals, such as the Journal of the Association for Information Systems (JAIS).