RHODES UNIVERSITY

Where leaders learn

THE ROLE OF OPTIMISM BIAS IN SUSCEPTIBILITY TO PHISHING ATTACKS IN A FINANCIAL SERVICES ORGANISATION

By

Morné Owen

THE ROLE OF OPTIMISM BIAS IN SUSCEPTIBILITY TO PHISHING ATTACKS IN A FINANCIAL SERVICES ORGANISATION

By

Morné Owen

18O9781

THESIS

submitted in fulfilment of the requirements for the degree

DOCTOR OF PHILOSOPHY

in

INFORMATION SYSTEMS

in the

FACULTY OF COMMERCE

of

RHODES UNIVERSITY

Supervisor: Prof. Stephen Flowerday

30 SEPTEMBER 2022

ABSTRACT

Researchers looking for ways to change the insecure behaviour that results in successful phishing have considered multiple possible reasons for such behaviour. Therefore, the purpose of this study is to understand the role of optimism bias (OB – defined as a cognitive bias), which characterises overly optimistic or unrealistic individuals, in order to ensure secure behaviour. Research is considered that has focused on issues such as personality traits, trust, attitude and information security awareness training (ISAT). We used a mixed methods design to investigate OB behaviour, building on a recontextualised version of the theory of planned behaviour to evaluate the influence that OB has on phishing susceptibility. To model the data, an analysis was performed on 226 survey responses (systematic random sampling method) from the employees of a financial services organisation using partial least squares (PLS) path modelling. To evaluate OB behaviour, we conducted an experiment consisting of three ISAT sessions and three simulated phishing attacks. After each phishing experiment, we conducted interviews to gain a better understanding of why people succumbed to the attacks. It was subsequently found that overly optimistic individuals are inclined to behave insecurely, while factors such as attitude and trust significantly influence the intention to behave securely. Our contribution to practice is to enhance the effectiveness of ISAT by identifying and addressing the OB weakness to deliver a more successful training outcome. Our contribution to theory enriches the Information Systems literature by evaluating the effect of a cognitive bias on phishing susceptibility and, through research, offering a contextual explanation of the resultant behaviour.

UITTREKSEL

The home language of the researcher is Afrikaans and therefore the abstract was translated.

Navorsers op soek na ‘n antwoord om onveilige gedrag te verander wat lei na uitvissing het verskeie moontlike redes oorweeg vir sulke gedrag. Daarom is die doel van hierdie verhandeling om die rol van optimistiese vooroordeel (*OB* - gedefinieer as 'n kognitiewe vooroordeel) te verstaan, wat te optimistiese of onrealistiese individue kenmerk om veilige gedrag te verseker. Navorsing was oorweeg wat gefokus het op kwessies soos persoonlikheidseienskappe, vertroue, gesindheid en inligtingsekuriteitsbewustheidsopleiding (*ISAT*). Die navorser het gemengde metodes gebruik om *OB*-gedrag te ondersoek. Daar was voortgebou op 'n gerekontekstualiseerde weergawe van die *theory of planned behaviour* om die invloed wat *OB* op uitvissing-vatbaarheid het, te evalueer. Om die data te modelleer, is 'n analise gedoen waar 226 opname antwoorde verkry is van 'n finansiële dienste organisasie en is *partial least squares (PLS) path modelling* gebruik. Om *OB*-gedrag te evalueer, het ons 'n eksperiment uitgevoer wat bestaan uit drie *ISAT*-sessies en drie gesimuleerde uitvissing-aanvalle. Na elke uitvissing-eksperiment het ons onderhoude gevoer om 'n beter begrip te kry waarom mense aan die aanvalle geswig het. Te optimistiese individue is geneig om onveilig op te tree, terwyl faktore soos gesindheid en vertroue die voorneme om veilig op te tree, aansienlik beïnvloed het. Die studie se bydrae tot die praktyk is om die doeltreffendheid van *ISAT* te verbeter deur die *OB*-swakheid te identifiseer en aan te spreek om 'n meer suksesvolle opleidingsuitkoms te lewer. Verder verryk die studie die Inligtingstelsels-literatuur deur die effek van 'n kognitiewe vooroordeel op uitvissing-vatbaarheid te evalueer en deur navorsing bied dit 'n kontekstuele verduideliking van die gevolglike gedrag.

DECLARATION

I, Morné Owen, hereby declare that:

- The work presented in this thesis is my own work.
- All sources used or referred to have been documented and acknowledged.
- This thesis has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification.
- I am fully aware of the Rhodes University's policy on plagiarism and have taken every precaution to adhere to this regulation.
- Ethical approval for this study was obtained from the university's Ethics Committee with certificate reference number: CIS18-11

Date: September 2022

ACKNOWLEDGEMENTS

All praise be to the Creator God (Yahweh) who sustains me daily. To my family, for their encouragement to complete this work and their patience to allow me to do so. To my supervisor, Prof. Flowerday, for his guidance and support throughout this journey. To Prof. Syden Mishi from Nelson Mandela University (NMMU) and Dr Karl van der Schyff from Rhodes University for their assistance with the statistical data analysis.

GLOSSARY

Term	Definition
Attitude	Attitude has been defined as a way of thinking, feeling or acting that represents a mental or emotional condition (McLeod, 2018). The characteristic property of attitude, according to Peterson and Thurstone (1932), is an evaluative or emotional inclination toward an object, concept or issue.
Information security awareness training (ISAT)	In an organisational setting, security awareness refers to employees' understanding of and attitude toward the protection of their company's physical and information assets (Pattinson et al., 2016). Security awareness is a critical link in an organisation's security chain, as even the most effective security procedures are useless in an environment where there is no security culture.
Optimism bias (OB), unrealistic comparative optimism	Optimism bias occurs when people believe “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). Houston et al. (2012) define optimism as an “overestimation of the expected gains from future outcomes”. People therefore believe that they have less risk compared to other people. Optimism bias is also known as unrealistic comparative optimism (Baek, Kim and Bae, 2014).
Phishing	Hadnagy (2014, p.24) defines social engineering as “any act that influences someone to take an action that may or may not be in his or her best interest”. Phishing falls into the category of social engineering and is defined as a deceptive action in which the phisher/attacker attempts to entice internet users into revealing their personal information/credentials in order to profit financially (Kirda & Kruegel, 2005; Leukfeldt & Holt, 2019).

PLS-SEM	Partial least squares (PLS) path modelling is a variance-based structural equation modelling (SEM) technique that is widely used in corporate and social sciences (Henseler, Hubona and Ray, 2016). Because of its ability to model composites and factors, it is a powerful statistical tool for new technology research.
Trust	Trust is defined as the inclination to “accept risk und vulnerability based upon positive expectations of the intentions or behaviours of another” (Rousseau et al., 1998) and might be considered the thread that binds our social universe together (Weiss et al., 2021). When our personal results are dependent on others, our expectations of their benevolent versus malevolent intentions toward us have a significant impact on our behaviour and, as a result, on our interpersonal interactions (Rotter, 1967; Weiss et al., 2021).

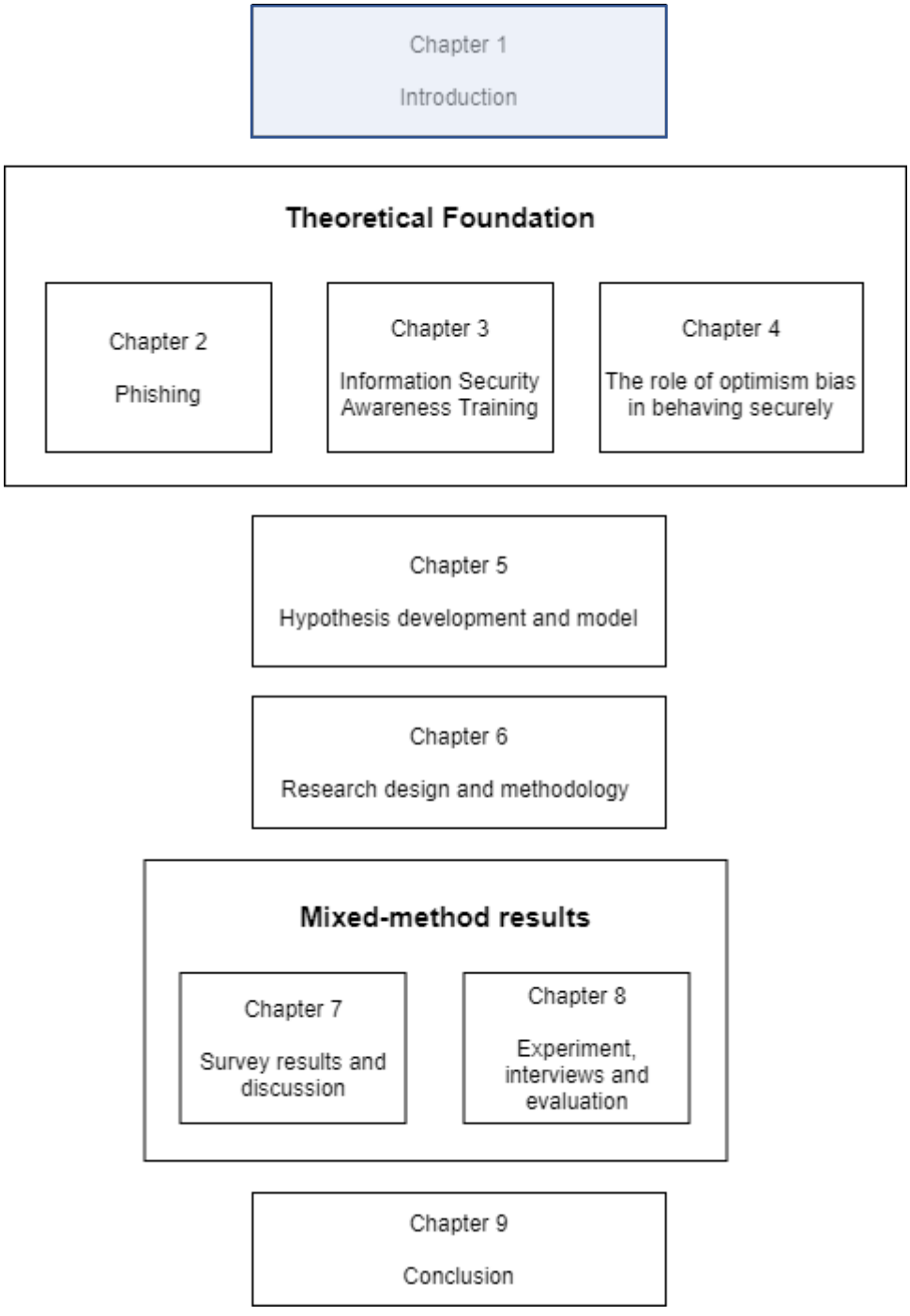
TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION



1. INTRODUCTION

1.1 Introduction

The continued increase in internet and data usage is closely followed by increased cybercrime. An estimated 58% of the world's population (4.5 billion people) is connected to the internet, an increase of more than 1157% compared to a decade ago (Neto et al., 2021). Button and Cross (2017) estimate that 29 billion spam emails are sent daily, with one in 196 emails containing a virus and one in 392 being classified as a phishing email. As more people become reliant on the internet, this trend is likely to increase. People are deceived by these phishing emails and fall victim to these attacks (Proofpoint, 2021; Petrič and Roer, 2022). Although phishing is not a new concept, as it has been around for more than two decades, there is currently no solution to completely eradicate this risk (Petrič and Roer, 2022). Phishing is another form of fraud. There is no solution to stop fraud from happening. Why people still succumb to phishing attacks warrants further exploration which presents the main underlying problem of this study. Researchers have taken different approaches in phishing studies. This chapter provides the background to the problem, explains the main objective and research questions of the study, as well as the methodological approach that was followed.

1.2 Background

The internet has become pervasive in everything we do (Wei et al., 2021). It comprises various systems that are interconnected to form an ecosystem or platform, allowing for voice, video and text communication, online shopping and learning, as well as recently allowing the work-from-home phenomenon to explode (Chadee et al., 2021; Garrote Sanchez et al., 2021; Noura et al., 2019; Purwanto & Tannady, 2020; Zhghenti & Gedenidze, 2022). For the 4.5 billion people connected to the internet (Section 1.1), not a day goes by without checking their email and accessing instant messages or websites; some even suffer from "internet addiction" (Roberts et al., 2022). Behaviour is driven by the fear of missing out (FOMO) so that people feel they need to stay up to date at all times (Akbari et al., 2021). It would therefore appear that one cannot be part of society

today without being connected to the internet. Unfortunately, everything created can be used for its intended purpose or abused for another purpose. This also applies to the internet. Owing to the lucrative gains to be made from cybercrime, such crime is a thriving and growing business. In fact, cybercrime services are offered on the dark web basically to assist anyone to join this “business” (Van Wegberg et al., 2018).

One of the methods used in cybercrime is known as social engineering. Hadnagy (2014, p.24) defines social engineering as “any act that influences someone to take an action that may or may not be in his or her best interest”. Phishing falls into this category and is defined as a deceptive action in which the phisher/attacker attempts to entice internet users into revealing their personal information/credentials in order to profit financially (Kirda & Kruegel, 2005; Leukfeldt & Holt, 2019). Unfortunately, many think phishing is a technical issue and thus corporations focus on technical controls. Researchers have also investigated many technical controls, hoping to find a solution to mitigate the risk of phishing. These technical controls include the blacklisting of sites, warning messages when browsing a malicious site or when a suspicious email is received, browser controls, endpoint protection to determine malware and, lately, the implementation of Artificial Intelligence (AI) / Machine Learning (ML) to determine suspicious activity (Baadel & Lu, 2019; Kirda & Kruegel, 2005; Y. Lin et al., 2021; Qabajeh et al., 2018). Sadly, these controls merely reduce the risk of phishing, as the current stats indicate that phishing is still the number one reason for security breaches. This is according to Verizon’s (2022) data breach investigations report which states that 82% of all breaches are due to human error. Chapter 2 is dedicated to describing phishing in detail.

Since technical controls do not eradicate the risk of phishing entirely, the focus needs to turn to human behaviour. The second mitigating control for the risk of phishing is information security awareness and training (ISAT). If people have the knowledge to identify a phishing attack they should be in a position to protect themselves (Mittal, 2015). However, the current phishing statistics indicate that awareness also does not completely mitigate the risk (Verizon, 2022). Ultimately, there is no simple solution to eradicate the risk of phishing. ISAT is described further in Chapter 3.

The current body of knowledge on phishing susceptibility focuses on personality traits, ISAT and demographics (Tornblad et al., 2021). Personality traits include the following:

- *Conscientiousness.* People with higher conscientiousness tend to succumb more to phishing attacks as they are normally hard working and goal

orientated (Halevi, Memon & Nov, 2015). However, Frauenstein and Flowerday (2020) found this not to be true for social networking sites owing to lower reliance on heuristic processing.

- *Agreeableness.* People with this trait are normally friendly, polite and trusting of others and are therefore more susceptible to the phishing risk (Anawar et al., 2019).
- *Neuroticism.* This trait refers to people who tend to be more emotional. They often experience negative feelings such as pessimism or guilt and therefore experience low emotional stability. Such people have been found to be susceptible to phishing (Ge et al., 2021).
- *Openness to experience.* When people are open-minded and eager to try new things, they expose themselves to risk and are therefore susceptible to phishing (Alseadoon, 2014).
- *Extraversion.* This is a significant predictor of phishing susceptibility as these people experience positive emotions and are more sociable and open to new ideas (Lawson et al., 2020).
- *Impulsivity.* Impulsive people make decisions quickly without understanding the consequences and therefore tend to behave insecurely by clicking on email links (Coutlee et al., 2014). In addition, lack of planning has been found to be a significant negative predictor (Hadlington, 2017).
- *Sensation seeking.* Those who pursue new experiences or feelings are more susceptible to phishing as they are not able to distinguish between phishing and legitimate emails (Hoyle et al., 2002; Jones et al., 2019).
- *Curiosity.* Moody et al. (2017) found that the need to obtain new knowledge and experiences is a positive predictor of phishing susceptibility.
- *Risk propensity.* People who are willing to take risks are more susceptible to phishing attacks (Moody, Galletta and Dunn, 2017)
- *Dispositional trust and distrust.* Dispositional trust is the tendency to trust in other people's positive characteristics and is a significant positive predictor of phishing (Alseadoon, 2014). Hong et al. (2013) discovered that less trusting people were more likely to delete legitimate emails, a behaviour that could potentially reduce the risk of falling victim to an attack.
- *Submissiveness.* Submissiveness is associated with obedience to and compliance with authority and has been shown to be a significant positive predictor of phishing susceptibility (Alseadoon, 2014).

Previous studies have included the educational background of the participants. For example, Gavett et al. (2017) predicted that those with higher levels of education should be more suspicious and therefore less likely to be phished. Parsons et al. (2013) also found that the more educated person was in a better position to deal with a phishing email, but only if they were not told that they were part of a phishing study. In addition, others have shown less susceptibility to phishing owing to internet experience (Lin et al., 2019; Sheng et al., 2010). However, some studies have failed to show that education predicts susceptibility (Moody, Galletta and Dunn, 2017). Interestingly, people in technical jobs do not have an advantage over non-technical people, as they are equally able to distinguish a phishing email from a legitimate email (Kumaraguru et al., 2008).

Demographics used in phishing studies include age and gender. Some studies have found that younger people (18–25) are more susceptible to phishing attacks than older people (Jagatic et al., 2007; Parsons et al., 2019). Others have not found any difference based on age (Zielinska et al., 2014; Moody, Galletta and Dunn, 2017). Certain studies that include gender have reported that women are more susceptible to phishing than men (Hong 2013, Jagatic 2007), while others have not found any differences (Gavett 2017, Moody 2017, Parsons 2019).

From what has been discussed in the previous section, it would appear that there are contradictory findings:

- Halevi et al. (2015) found c*onscientious* people to be more susceptible to phishing, but Frauenstein and Flowerday (2020) found this not to be true for social networking sites.
- Coutlee et al. (2014) found *impulsive* people more susceptible to phishing, but Hadlington (2017) found that non-planning, a factor of *impulsiveness,* was not a significant predictor of susceptibility to phishing.
- Gavett et al. (2017) and Parsons et al. (2013) found that people with a higher level of education should be in a better position to deal correctly with phishing, but Moody et al. (2017) failed to see that education level had a significant influence on susceptibility.
- Jagatic et al. (2007) and Parsons et al. (2019) found that younger age groups are more susceptible to phishing than older groups but Moody et al. (2017) and Zielinska et al. (2014) did not find age to be a predictor of phishing susceptibility.

- Hong (2013) and Jagatic (2007) found women to be more susceptible to phishing but Gavett (2017), Moody (2017) and Parsons (2019) did not find gender to be a predictor of phishing susceptibility.

Thus, personality, demographics and education all play a role in phishing susceptibility, but merely looking at these factors alone do not create a clear pattern of who is susceptible to phishing. Individuals' decisions regarding phishing attempts are not always entirely sensible (Metzger and Suh, 2017). Behaviour is also influenced by cognitive bias (Marshall et al., 2013). There are many different types of cognitive bias, but this study will focus on optimism bias (OB), as there is scant research linking OB to phishing and on the influence OB has on attitude and trust (Kisak, 2015). OB is discussed in Chapter 4 in more detail. In this study, the expressions ‘optimism bias’ and ‘unrealistic optimism’ will be used interchangeably. Positive illusions in general, and unrealistic optimism in particular, are sometimes claimed to be systematic tendencies to form beliefs that are biased, and frequently false, but have significant benefits (Jefferson, Bortolotti and Kuzmanovic, 2017).

There are many forms of positive illusions, such as:

- *Self-serving bias* and *wishful thinking* where a person hopes for the best but does not influence the target outcome, for example a soon-to-be bride and groom who are hoping for good weather on their wedding day (Krizan and Windschitl, 2009)
- The *illusion of control*, which is an overestimation of one's ability to control independent, external events (Langer and Roth, 1975);
- The *better-than-average effect*, also known as the superiority illusion, which is a more positive perception of oneself, one's past behaviour and one's lasting characteristics than is actually the case, for example "I have more abilities than the average person" (Brown, 2012).

In the context of this study, OB (Section 4.1) occurs when one 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). In terms of OB, the likelihood of bad events happening is underestimated, for example a car accident, losing a job or suffering from a terminal illness (Cherry, 2020) whilst overestimating good events such as individual longevity or job aptitude (Sharot, 2011). OB has also been observed in online environments, for example, Campbell et al. (2007) investigated OB in a variety of internet activities (e.g. cyberbullying, installing

malware, selling personal information and financial fraud). Their findings suggest that such people perceive themselves to be less vulnerable to adverse internet events than others but more likely to encounter good internet events. Furthermore, Rhee, Ryu and Kim (2005) discovered that users had an optimistic bias when it came to risk assessments about information security. Other studies found that OB was also prominent in the context of online privacy (Cho, Lee and Chung, 2010; Baek, Kim and Bae, 2014). OB was even found in the way people perceive privacy threats, with the bias being determined by perceived control and previous experience (Metzger and Suh, 2017).

The result of looking at the world too favourably could result in poor decision-making since people's preference leans towards positive outcomes (Bracha and Brown, 2012). In addition, overconfidence – when people believe that outcomes are under their control – could result in incorrect decision-making (Acquisti and Leon, 2017). Overconfidence can lead to OB as people mistakenly believe that they will not fall prey to a security attack based on their cognitive ability, knowledge and experience in relation to ISAT. Knowledge alone does not result in the correct action being taken, since it is a combination of knowledge and one's attitude that results in behaviour (Pattinson et al., 2016; Rhee et al., 2005; Safa et al., 2015). However, it may be deduced that individuals may optimistically regard themselves to be less likely than others to be the victim of phishing, which can have a significant impact on their attitude toward taking preventive steps against such attacks. Thus, understanding OB in relation to phishing is critical and will be the focus of this study, as this bias may interfere with one's decision about whether to take protective measures to prevent phishing attempts.

The preceding section debated whether the susceptibility to phishing was influenced by

- higher levels of awareness
- trusting in technology controls
- understanding various personality types
- demographics, such as age and gender, or
- positive illusions, such as OB.

All these factors seem to have some influence on phishing susceptibility. It is therefore important to understand the effect of unrealistic optimism towards phishing susceptibility, taking the two phishing mitigation strategies, namely technology controls, or more specifically the trust people place in these controls, and ISAT into account.

This study is firstly informed by the *theory of planned behaviour* (TPB) which attempts to explain human behaviour in certain situations and secondly by the cognitive bias referred to as optimism bias (Weinstein, 1980; Ajzen, 1991). The TPB (see Figure 1.1) concludes that behaviour is influenced by attitude, subjective norms and perceived behavioural control. 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 the said behaviour will result in more motivation to perform the behaviour in question. Subjective norms refer to the assumed social burden regarding whether to perform a certain behaviour. Perceived behavioural control is one's perception of the effort, considering one's skills and abilities, required to implement the behaviour of interest, while perception is "the way in which something is regarded, understood, or interpreted" (Dictionary.com, 2021). Undertaking a specific behaviour can 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 element of the TPB, as intentions are thought to capture the motivating variables that impact a behaviour; they 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 will be carried out.

According to the TPB, behaviour is a function of salient beliefs about the behaviour. People may have many 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 toward beliefs that lead to desirable results and negative attitudes toward activities that lead to negative consequences. *Normative beliefs* are linked to *social norms* as they are concerned with influential persons' approval or disapproval of a specific behaviour. *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 the behaviour.

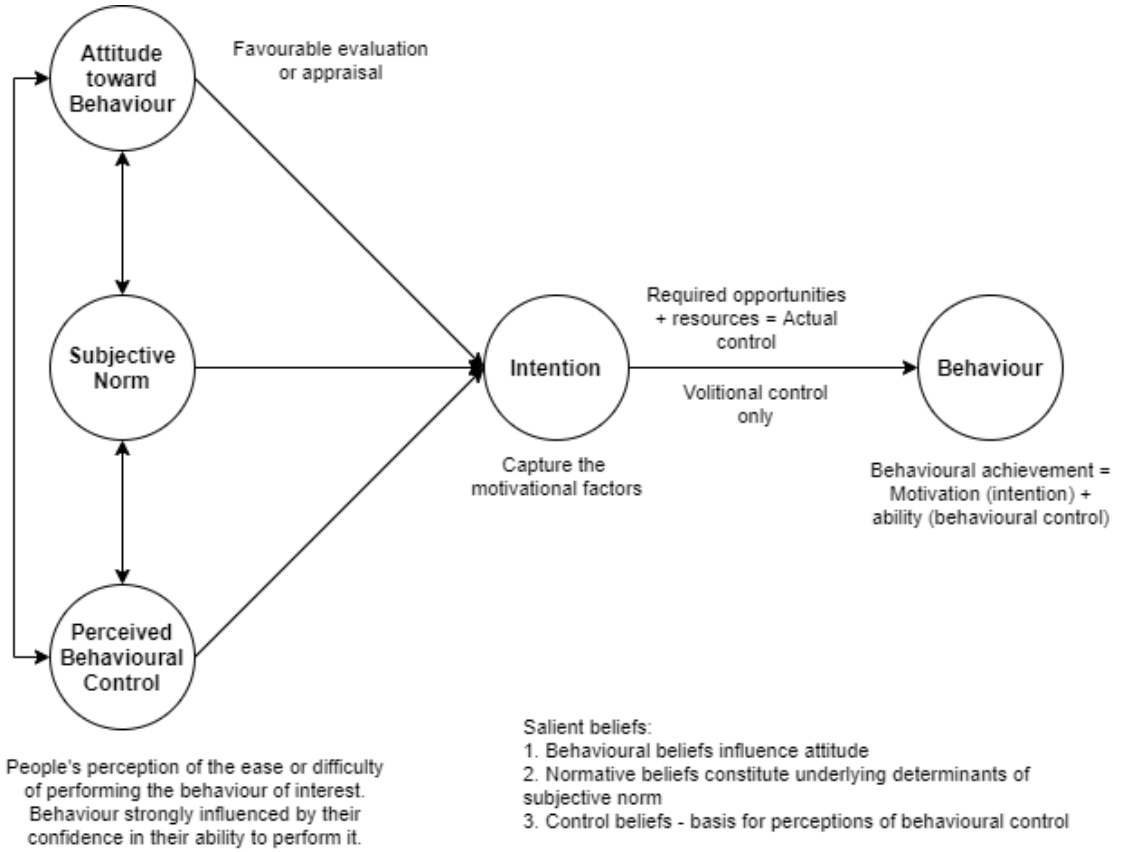


Figure 1.1 The theory of planned behaviour (adapted from Azjen, 1991)

Weinstein (1980) conducted a study to determine the inclination of people to be unrealistically optimistic about upcoming life events. He found that college students rated their own chances as above average for positive events and below average for negative events. Thus, unrealistically optimistic people could be under the false impression that they will not succumb to a phishing attack.

1.3 Problem statement

There is a dearth of research on the effect of OB on ISAT. Therefore, this study poses the following problem statement:

Certain dispositional factors such as attitude, trust, awareness and optimism bias (OB) influence employees' ability to detect phishing emails in the work environment, thus putting the organisation and other employees at risk.

1.4 Research questions

Based on the problem statement, this study implies that current ISAT is not sufficient to address the risk of phishing for certain susceptible employees.

Main question: *How should information security awareness training initiatives improve to overcome phishing in susceptible individuals employed by a mid-size financial services company?*

The following sub-questions were derived to answer the main question:

- **Sub-question one.** *Why is information security awareness training not always effective in changing human behaviour?*

  Knowledge can set the correct intention but not result in the correct behaviour. The relationship between knowledge and behaviour needs to be understood to create the desired outcome.

- **Sub-question two.** *What effect does optimism bias have on secure behaviour?*

  If a person is under the impression that nothing bad will happen to them, for example falling victim to a phishing attack, then awareness training might not have a positive effect. Hence, could OB cloud a person's judgement?

- **Sub-question three**. *How does attitude affect secure behaviour?*

  The wrong attitude results in insecure behaviour because one thinks everything is under control. The correct balance must be created between attitude and behaviour so that one will not fall victim to a security breach.

- **Sub-question four.** *How does trust in technology security controls affect secure behaviour?*

  People might succumb to a phishing attack if they blindly trust that technology will safeguard them regardless of their behaviour.

Therefore, the aims of this study are to

- understand that knowledge obtained through ISAT can set the correct intentions but ultimately leads to incorrect security behaviour
- understand the effect of OB in relation to secure behaviour relating to phishing
- study the effect of one's attitude in relation to security behaviour, and
- question the trust placed in the technical controls implemented by the IT department.

1.5 Research objective

The main goal of this study was to address the aforementioned research questions by:

Developing a model that identifies users who are susceptible to phishing, taking into account the role of optimism bias when creating an ISAT initiative.

This model was subsequently used to evaluate the influence of attitude, trust and awareness on the intention to behave securely. To investigate the role of OB, the survey participants were split into two groups, based on the OB survey questions: (1) the unrealistically optimistic group and (2) the average group. The final model will depict the differences between the two groups in relation to their intention to behave securely. Furthermore, actual behaviour was measured through the use of an experiment in a real work environment. The research done by Parsons et al. (2013) found that people responded differently to phishing emails if they were told that they were participating in a phishing study. Thus, the objective of this study was to test actual behaviour to phishing susceptibility in such a way that it was not seen as a research exercise but as part of a normal workday for an employee, in other words, real world conditions.

1.6 Overview of the methodological approach

Since this study used mixed methods research, a pragmatic paradigm was used as it works well when quantitative and qualitative research are implemented. From a theoretical perspective, this study followed an abductive approach. Since both the intention to behave securely and actual behaviour was researched, the study alternated between induction and deduction. Hypothesis development was supported by the collection of secondary data using a literature study.

This study adopted a survey strategy to collect primary data. Data was collected using the learner management system (LMS) of the financial organisation involved. A pilot survey was conducted to remove any question ambiguity. The questionnaire consisted of 39 items, with most of the items taken from other sources or adapted as required. The distribution of these items in relation to each construct is displayed in Table 1.1.

Table 1.1 Constructs used in this study

Construct	**Items**	**Source**
Optimism bias (OB)	11	Weinstein (1980)
Attitude	8	HAIS-Q adapted from Parsons et al. (2017).
Trust	6	Ferres and Travaglione (2003)
Awareness	6	HAIS-Q adapted from Parsons et al. (2017).
Intention to behave securely	2	New items

Additionally, the questionnaire captured data related to

- the respondent's email address
- demographics: age and gender
- job role
- number of formal computer courses completed, and
- number of years' work experience using computers.

Systematic random sampling was used by sorting the employees' email addresses and selecting every third person to participate. Since an audit finding from an international audit firm required that more awareness training be conducted, the employees were willing and encouraged to participate. The total population of the organisation is 775. A total of 257 responses were collected of which 226 were deemed usable.

Validity and reliability testing was conducted once the data was collected. This resulted in the elimination of several items as a result of low factor loadings (Table 1.2). The hypotheses were statistically evaluated by using a multivariate analysis technique referred to as partial least squares structural equation modelling (PLS-SEM). This approach was deemed suitable for conducting the analysis for this study, given that this study was largely exploratory and considering the complexity of the relationships required to form a single structural model.

Table 1.2 Items dropped

Construct	**Item**	**Item Description**
Attitude	19	If it helps me to do my job, it doesn't matter what information I put on a website.
	20	It doesn't matter if I post things on social media that I would not normally say in public.
	22	Nothing bad can happen if I ignore poor security behaviour.
	23	I believe my system is secure and will protect me from cyber threats.
	24	My attitude positively changed towards information security (security behaviour) over the past 2 years.
Awareness	28	I am allowed to download any files onto my work computer if they help me do my job.
	30	Sensitive printouts can be disposed of in the same way as non-sensitive ones.

The quantitative analysis in this study measured the *intention to behave securely* for the global group, as well as for the unrealistically optimistic and average groups separately. *Actual behaviour* was analysed using an experiment. The phishing experiment was repeated three times every third month to allow for ISAT to be conducted, debriefing and interviews to be concluded. The experiment consisted of the following steps:

- ISAT was conducted using the LMS of the organisation.
- A simulated phishing exercise was performed by emailing participants a phishing email that allowed them to enter their credentials into a website once they had clicked on the link.
- Debriefing was done after the simulated attack to explain that this was a phishing email and how participants should have identified it as such.
- Interviews were conducted to better understand why participants succumbed to the phishing attack.

Finally, the study was evaluated using triangulation (see Section 8.5).

1.7 Ethical considerations

Permission to conduct the research was obtained from the CEO of the financial services company. The ISAT training formed part of the training requirements for the company, as this had been highlighted as necessary by an international audit firm. Participating staff members were informed that their results would be used in a research study and that they could opt-out at any stage. In addition to these considerations, the researcher obtained ethical clearance from Rhodes University before conducting interviews or soliciting survey responses.

Ethics is concerned with how information is gathered and how results are communicated (Collis and Hussey, 2014, p.30). Phishing experiments that simulate real-world scenarios present significant ethical considerations because they include participants in research without their permission and involve trickery (Resnik and Finn, 2018). In this study, the data collection process included a survey and three simulated phishing attacks against the participants, using their email addresses to determine who succumbed to the attacks. Resnik and Finn (2018) argue that it is ethically permissible to include human subjects in a study without their permission, firstly, if the research cannot be carried out unless the subjects provide consent, and secondly, if involving subjects in the research without their permission does not significantly jeopardise their autonomy. In line with these requirements, since the aim of this study was to perform a real-world phishing attack, participants could not give consent for the experiment; in addition, their autonomy was not jeopardised.

Debriefing is widely accepted as a technique for reducing the harms associated with deception and holding researchers accountable to subjects (Oczak and Niedźwieńska, 2007; Miller, Gluck Jr and Wendler, 2008). Debriefing should inform subjects about the nature and significance of the research, as well as the reasoning behind the deception (Miller, Gluck Jr and Wendler, 2008). Accordingly, debriefing was done to inform the participants that the intervention was a phishing exercise and that only their email address was stored.

The university and the participants faced no financial, emotional, or physical risk or loss. A more detailed discussion on the ethical process can be found in Section 6.11 and the informed consent form can be found in Appendix B.

1.8 Contribution

Researchers have studied various phenomena to understand why people still succumb to phishing attacks, with some focusing only on the intention to behave securely through the use of a survey and statistical analysis, and not measuring actual behaviour (Chen, Gaia and Rao, 2020; Williams and Joinson, 2020; Shahbaznezhad, Kolini and Rashidirad, 2021). Unfortunately, there is often a difference between intention and actual behaviour, known as the intention–behaviour gap (Jenkins, Durcikova and Nunamaker, 2021). Other researchers have presented a list of emails to participants, asking them to distinguish between phishing and authentic emails or showing them a series of websites and asking them to identify the phishing websites (Alsharnouby, Alaca and Chiasson, 2015; Wang, Li and Rao, 2016). Parsons et al. (2015) state that informing participants that they are part of phishing research makes them more alert and thus more able to correctly identify a phishing email. Furthermore, phishing is more successful when it is aligned with an employee's work context (Steves, Greene and Theofanos, 2020).

The study's practical contribution is a better understanding of who is vulnerable to phishing attempts in the workplace. Moreover, a cognitive bias, called OB, was introduced to determine the effect it has on behaving securely. This study concludes that ISAT needs to be adapted to address unrealistically optimistic people by clearly communicating to them that a security breach could happen to them. Thus, ISAT should contain a section to determine these warning signs and make the participant aware that they are unrealistically optimistic.

This study's contribution to theory is an adapted model of the TPB, better enabling the identification of employees who are susceptible to phishing. The results indicate that there is a significant difference between the unrealistically optimistic and average groups and therefore they should be treated differently when applying mitigating controls for information security. Optimistic bias has a significant influence on both intention and actual behaviour.

1.9 Thesis structure

This study consists of nine chapters (Figure 1.2). Chapter 1 provided an overview of the study by describing what led to this research by giving the background, the problem statement and the study objectives. The research process, the research design and the methodology were briefly discussed.

Chapter 2 explains phishing in detail. It not only describes the theoretical nature of phishing, but also covers some of the practical phishing implementation techniques. This is the first chapter, together with chapters 3 and 4, that forms the theoretical foundation.

Chapter 3 focuses on ISAT and gives a detailed overview of the various cybersecurity frameworks. This is important, since one of the objectives of this study is to improve ISAT, specifically taking OB into account. As people have different learning styles and might be learning differently in the workplace (on-the-job training) this is also discussed.

Chapter 4 discusses OB and the influence it has on behaviour. Attitude determines one's outlook on life and therefore could relate to OB. Trust could also be influenced by attitude as it is influenced by the behaviour of others and is therefore also discussed in this chapter.

Chapter 5 details the way in which the hypotheses were formulated and explains the TPB. In addition, the suitability of the TPB for this study is justified.

Chapter 6 defines the research design and methodology. Since this is a mixed method study, it includes both the quantitative and experimental components of the study.

Chapter 7 presents the reader with the results of the quantitative analysis. The evaluation of both the measurement model and structural model is discussed, as are the results of the global model (all participants). Subsequently, the results for the multigroup are shown. Importantly, a significant difference was found between the unrealistically optimistic and average group in the *intention to behave securely*.

Chapter 8 discusses the results of the experiment, detailing the process that was followed. Importantly to note that there is a significant difference in *actual behaviour* between the unrealistically optimistic and average group. Lastly, the evaluation of the study is discussed with the use of triangulation.

Chapter 9 provides a complete review of the entire thesis. Emphasis is placed on how the research questions were answered as well as the contribution made by this study.

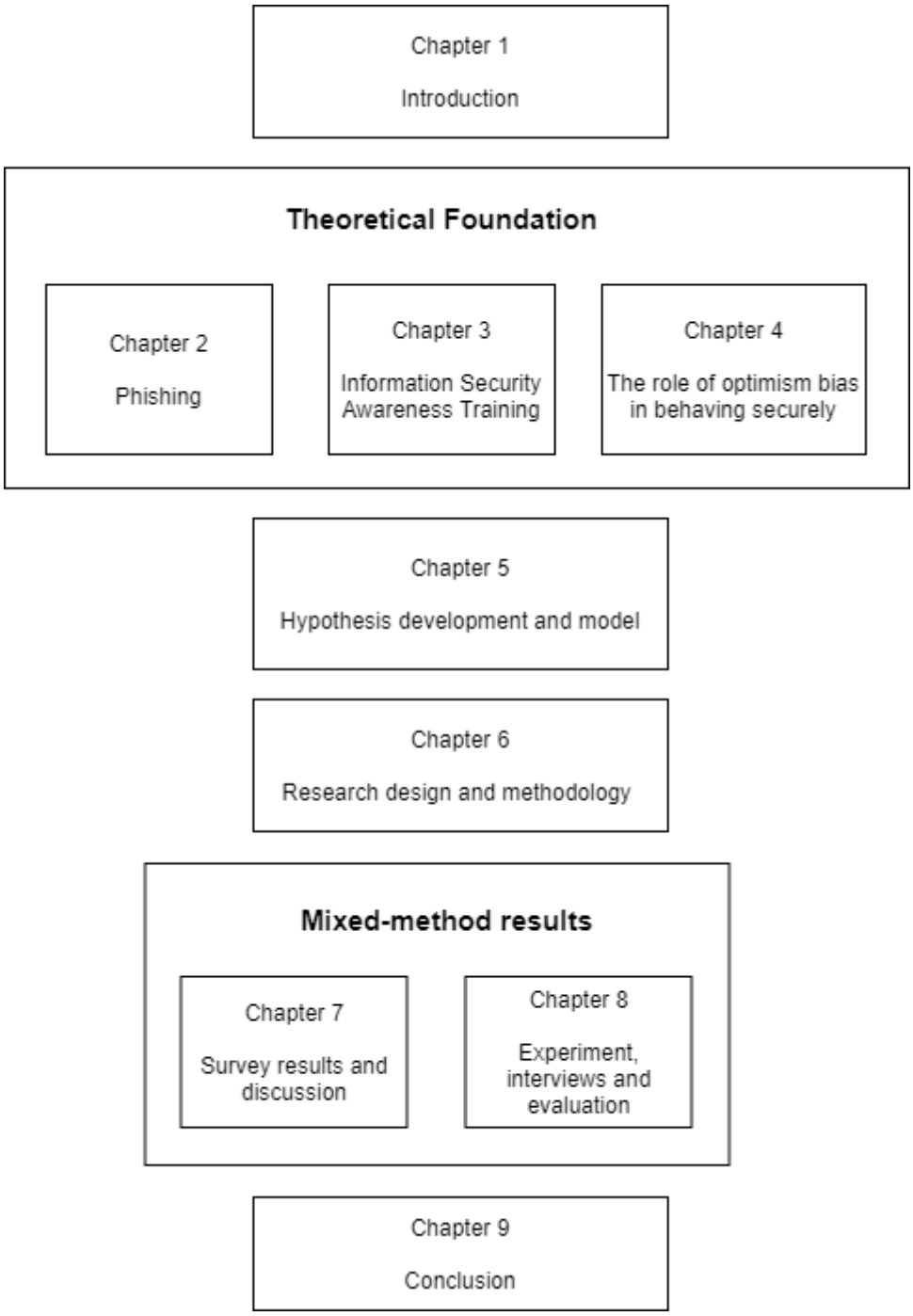
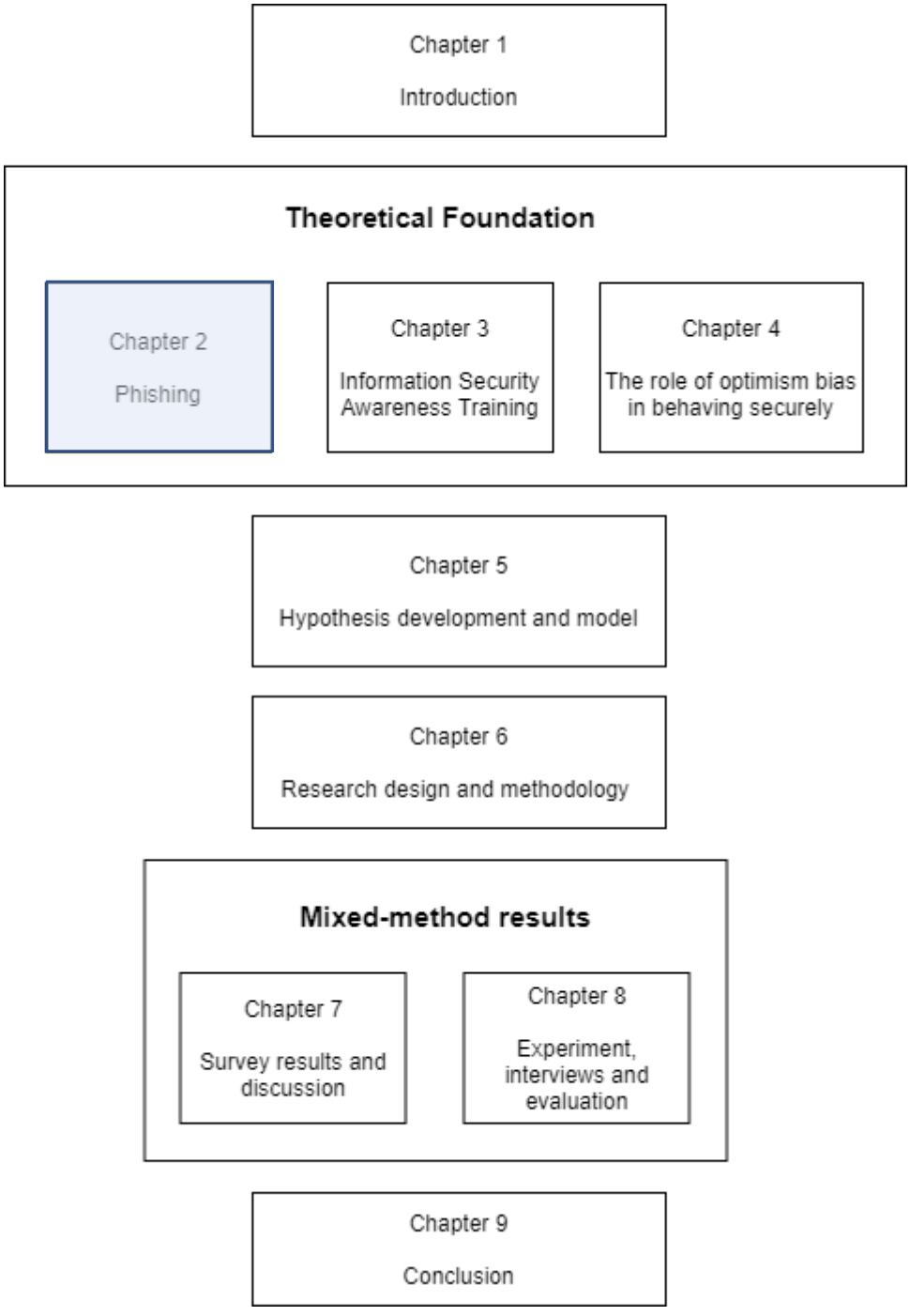


Figure 1.2 Chapter layout of the study

CHAPTER 2

PHISHING



2. PHISHING

2.1 Introduction

Humans can be manipulated by fear or reward (Franchina et al., 2018; Moody, Siponen and Pahnila, 2018; Chowdhury, Adam and Teubner, 2020). With the advent of the digital age social engineering has grown exponentially, assisted by the use of technology (Ögütçü, Testik and Chouseinoglou, 2016; Williams, Beardmore and Joinson, 2017). Frank Abagnale, a cheque fraudster in the 1960s, claims that hypothetically it is now about 4000 times easier to socially engineer people using digital tools (Sachs, 2017).

Computer users often lack the technical skills to determine an information security threat and therefore need to be made continuously aware of what these threats look like by raising awareness of information security (Downs, Holbrook and Cranor, 2007; Arachchilage and Love, 2014; Arachchilage, Love and Beznosov, 2016; McCormac et al., 2017). However, some people consider themselves knowledgeable in this area and as a result of their confidence or optimistic outlook that it will 'not happen to them', they fall victim to the next phishing attack (Boddy, 2018).

This chapter will explain and define phishing as understood in this study. Social engineering is as relevant today as it was 60 years ago when the cheque fraudster named Abagnale, posing to be a pilot, illegally ordered flight uniforms over the phone (Sachs, 2017).

2.2 Phishing overview

In the online age we live in, deception takes an electronic form which is relatively easy to create and has the added ability to be mass marketed. Enhancing its success is the speed at which we need to complete tasks to remain relevant and competitive in our respective market segments. We are bombarded with multiple different tasks during a working day, often switching between them, not completing one before starting another. This has resulted in a diminished concentration span, resulting in tick-box actioning where we need to complete tasks as soon as possible (Sweller, 1994; Levine, Waite and

Bowman, 2007; Junco and Cotten, 2012; Feng et al., 2019). Electronic communication tools such as email, instant messaging and social networking are fighting for our attention through notifications via websites and mobile phones, which is a major distraction, further stretching our ability to concentrate (Fox, Rosen and Crawford, 2009).

The conditions described above could lead to clicking without thinking. We have become processing robots, pursuing rewards for completing tasks as quickly and efficiently as possible. In this race to be successful we often do not fully understand the content we are provided with nor do we investigate its truthfulness (Schneider, Slaughter and Dux, 2017).

The speed at which tasks need to be completed combined with the effectiveness of persuasive communication could result in insecure behaviour (Dhamija, Tygar and Hearst, 2006). The elaboration likelihood model developed by Petty and Cacioppo (1986) defines the relationship between persuasive communication and attitude change. The theory argues that people process communication with different levels of thought, known as elaboration, ranging from low to high. Based on the level of elaboration, one of two routes will be followed to process communication: (1) a low level requires little thought such as conventional conditioning and mere experience, and (2) a high level requires significantly more thought such as *expectancy-value* and *cognitive-response processes*. The two routes are known as the (1) *peripheral route* when lower elaboration processes predominate and (2) the *central route* for high elaboration processes. Central-route processes tend to persist over time and resist persuasion, whereas peripheral-route processes do not. Any given variable can play multiple roles in persuasion, including the action of a certain judgement, as well as influencing the thought process about a message. The extent of the elaboration determines the specific role that a variable plays. There is a strong correlation between the degree of thought used in the persuasion context and the resultant attitude. Attitudes have been a key topic in research on persuasion, because they enable important social and psychological functions which could influence decisions and behaviours as they *summarise one's beliefs, emotions and preferences regarding issues, objects and people* (Cacioppo et al., 2018).

Research conducted to understand human behaviour relating to persuasion has not yielded a robust and stable model. Modic and Lea (2014) developed the Susceptibility to Persuasion (StP) scale to understand the individual differences in scam compliance. Factors they included that can influence one's ability to react rationally were (1) liking and similarity, (2) trust and authority, (3) social influence, (4) risky behaviour (sensation

seeking), (5) lack of self-control, (6) illusions of superiority and control, (7) the scarcity and uniqueness of the scam offer and (8) consistency and commitment. Although their models have shown acceptable construct validity, a deeper understanding of 'why' people succumb to online fraud is required (Norris, Brookes and Dowell, 2019).

Fischer, Lea and Evans (2013) confirm the factors to consider when trying to ascertain why people might respond to the persuasion of a phishing communication. These factors include substantial gain through reward, trust that the request is legitimate, social influence to be compliant or to promote liking and reciprocation and the scarcity or urgency of the request. Although Fischer et al. found some support for these factors in predicting victimisation, they also added personality, with a focus on 'self-confidence', which could be interpreted as one's belief in the ability to detect scams. Furthermore, feelings or emotions could play a role in decision-making. Various studies indicate that a negative mood results in lower risk taking while people in a neutral or positive mood are more inclined to take risks (Yuen and Lee, 2003; Chou, Lee and Ho, 2007).

In the online era, deception or phishing is not new. Multiple studies have been done over several years to understand why people succumb to deception and to create a robust and stable model that could be used to prevent people from falling victim to phishing. Today, it is still not clear why some people succumb to certain deceptive message requests while others do not. A deeper understanding is required about how individuals process message requests.

Phishing is a combination of fraudulent social engineering techniques and technical trickery used by an attacker to obtain sensitive information in order to perpetrate identity theft for financial gain. The phishing process starts with a spoofed email or instant message convincing a victim to act by clicking on a URL or to open an attachment. The phishing URL opens a website that represents a legitimate site, using the same look and feel, hoping that the victim will part with their credentials i.e. username and password (Alsharnouby, Alaca and Chiasson, 2015; Aleroud and Zhou, 2017; Zhao et al., 2017; APWG, 2020).

Hadnagy (2018) describes the goals of phishing as follows:

- To provide a mechanism for the installation of malicious software thereby granting an attacker remote access
- To gather sensitive information, i.e. the victim's credentials
- To gather additional information that could be used in additional attacks.

Without realising it, the victim compromises their security, allowing an attacker to assume their identity. Malicious software installed through a phishing attack often remains undetected for months, allowing an attacker to gain access to many of the victim's accounts (Abraham and Chengalur-Smith, 2010; Al-rimy et al., 2018).

2.2.1 Characteristics and elements of a phishing attack

Ramzan (2010) defines the following characteristics of a phishing attack: (1) a well-known entity or organisation could be spoofed, (2) the victim must be directed to a fraudulent website and (3) the victim's credentials must be captured on the website. These three steps form the basis of any phishing attack. The email message should be convincing so that the employee wants to comply with the request. A typical phishing email consists of several elements.

KnowBe4 (2017) defines the following elements of phishing emails:

- Unusual urgency – emails containing inappropriate urgent messages are used to entice the victim to respond quickly. This results in emotional decision-making, bypassing any logic to check if the message is in fact legitimate.
- Poor design – legitimate organisations will ensure all their communications are done professionally. Phishing emails are often badly formatted.
- Misspellings – poor spelling and grammar use could indicate that the message was not created by a professional company.
- Too good to be true – the victim is enticed to click on a link or open an attachment in order to receive a reward.
- Hyperlinks – links are often disguised and do not open the site referred to in the text.
- Attachments – often used to hide payloads for malware.
- Unusual sender – if it looks suspicious or out of character do not click any links.

Figure 2.1 illustrates what you need to check if you received an unusual or unwanted email. Reviewing these elements or ‘red flags’ could result in more secure behaviour.

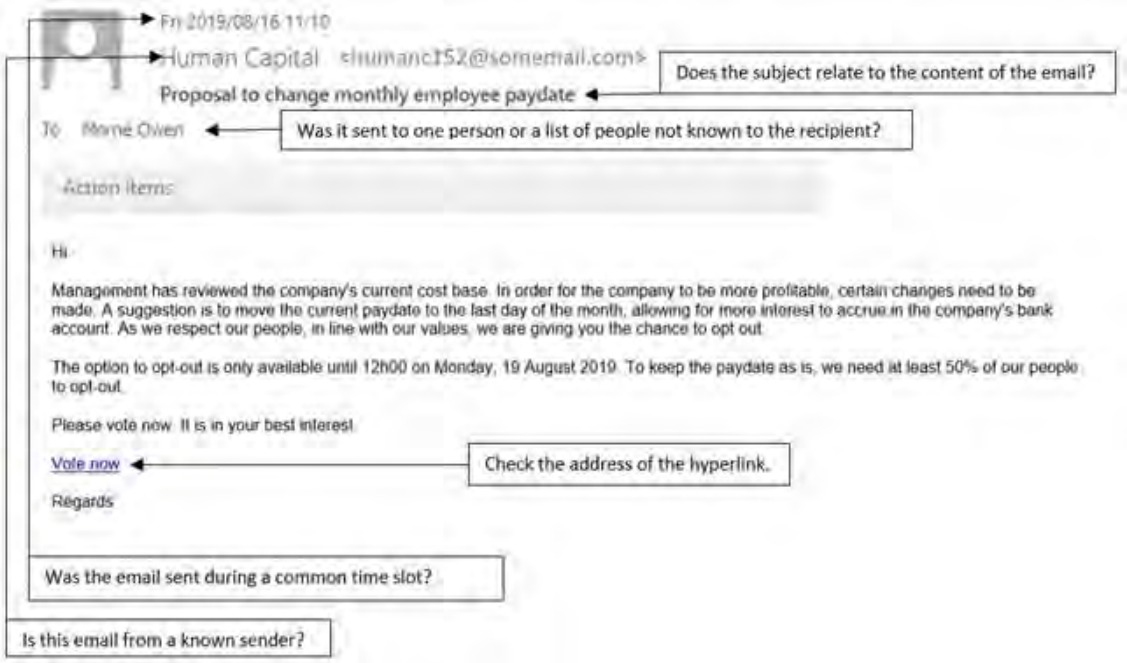


Figure 2.1 Social engineering red flags adapted (KnowBe4, 2017)

Computer users will be able to recognise a phishing email if they take the time to carefully consider the following:

- The “From” address – is the sender known to the recipient? Does the email address seem legitimate? If the email is from a known sender, does it seem strange or different from emails received before? Was this email expected?
- The “To” address – was it sent to one participant or a list of people not known to the recipient? Was the email sent based on some illogical grouping, for example to everyone with a surname starting with “A”?
- Hyperlinks – verify the URL by hovering over the link. If the address seems suspicious, this is reason for caution. Emails with no text containing only a hyperlink or a hyperlinked that is misspelled should not be trusted.
- Date – emails sent during uncommon time slots need to be investigated.
- Subject – if the subject does not relate to the contents of the email body, it could indicate a security issue.
- Attachments – executable type attachments not having any bearing on the contents of the email should be deleted.

- Content – what is the action that is requested in the email? Does it drive unwarranted fear or reward? If actions are required that do not make logical sense, it would be safer to delete the attachment.

This section explained the elements making up a phishing attack. The next section will focus on how people are specifically targeted. Certain phishing strategies place an emphasis on specific groups of people and therefore adjust the message to lure the victim to comply.

2.2.2 Types of phishing

Spear phishing

This phishing type entails an attack that targets a specific organisation to collect the credentials of its users as well as financial and other sensitive information. In order for spear phishing to succeed, the attackers need to have a good understanding of the organisation (Parmar, 2012; Aleroud and Zhou, 2017). Symantec (2019) reports that targets include various types of organisation. The victim is tricked into thinking that the attack is from a known or trusted source. Often, executives in financial departments are the targets, making spear phishing lucrative. Another type of spear phishing, referred to as social phishing (Jagatic et al., 2007), uses friendship information from social networks. This type of phishing has been found to obtain a success rate of 70%.

Whaling

Whaling or business email compromise refers to spear phishing attacks aimed specifically at senior executives, otherwise known as the “big fish or whale” (Giandomenico, 2017; Trend Micro, 2019). As executives typically have access to confidential company data, the intention of the whaling email is to get the executive to part with such confidential or private data (Moul, 2019). The attack email could contain an attachment containing malware, which infects the executive’s computer in order to create a backdoor for the attacker (Gil, 2020). To get the attention of the executive, the content of a whaling attack email will be relevant to them, such as a subpoena or customer complaint (Goodin, 2008).

Catfishing and catphishing

Catfishing (spelled with an ‘f’) is a type of online trickery where an attacker creates a presence in social networks as a sock puppet or creates a fictional online identity with

the purpose of forming a relationship with the objective of obtaining money, gifts or attention. Using the fake nature of the sock puppet identity allows the attacker to make controversial and offensive comments, masquerading as a real person with no ulterior agenda. Catphishing (spelled with a 'ph') is similar but the focus is on befriending the target to gain access to information and/or the resources they have (Jouriles and Sargent, 2017).

> Simply put, the former is out to break hearts (and bank accounts), while the latter is out to compromise individuals, organisations, and quite possibly even countries (Malwarebytes, 2018).

Clone phishing

An attacker will clone a legitimate and often previously delivered email by replacing the links or attachments with a malicious version. To complicate matters, the email is sent from a spoofed address appearing to be the original sender. The target believes it is an update of the previous email sent and processes it accordingly (Certnz, 2018; NZ Herald, 2018; ZD Net, 2020).

Vishing (voice phishing)

This attack is similar to email phishing but does not require a fake website as the attacker uses a voice call to trick a victim in giving away their account credentials. Vishing attacks increased with the SARS-CoV-2 coronavirus (commonly referred to as Covid-19) as more people worked from home using a corporate VPN. A compromised VPN allows an attacker to impersonate a legitimate entity using their telephony systems (Moul, 2019; Musuva, Getao and Chepken, 2019; Johnson, 2020; Social-Engineer, 2020). Voice over IP technologies such as automatic dialling and telemarketing calls are exploited for vulnerabilities, guiding victims to fake services to compromise their accounts (Aleroud and Zhou, 2017). Caller ID spoofing is also used to trick the victim into believing that the call is from a legitimate entity (Reuters, 2005). The increased use of mobile phones fuels these attacks.

SMiShing

SMS phishing or smishing uses mobile text messages as the attack surface to trick a victim into parting with account credentials. Users tend to be warier of phishing emails, but in general trust an SMS (Norton, 2018). The SMS could contain a URL to a malicious website or a number to phone so that the attacker can obtain the victim's credentials

(Keyworth, 2016). Mobile browsers make it difficult to spot a fake website as the URL is not always fully displayed (Mishra and Soni, 2019). The increased use of mobile phones with good internet connectivity have made these devices more vulnerable (Mishra and Soni, 2020).

eFax

eFax, also known as internet fax, allows users to send and receive faxes via email, thus eliminating the need for a traditional fax machine (J2 Global, 2020). The online capabilities of eFax are similar to email and therefore an attacker can exploit it in the same fashion as email (Chiew, Yong and Tan, 2018).

Instant messaging

The use of instant messaging has soared over the last few years especially during the Covid-19 pandemic with more people working from home (Gartner, 2020; McKinsey and Company, 2020). Messages may include voice notes, photos, maps, hyperlinks, files, and the like, which makes instant messaging an ideal platform for an attacker to launch a phishing attack (Wright and Marett, 2010).

Social network

People love to interact with other people who share the same interests and values. Social media makes this possible by creating a platform for people to opt in to groups or become friends. However, affiliation often creates trust and therefore allows the attacker to exploit this environment (Ögütçü, Testik and Chouseinoglou, 2016).

The mass adoption of any new communication platform creates a new attack surface that could be exploited. Table 2.1 briefly summarises the various phishing types targeting different user groups and technical platforms.

Table 2.1 Summary of phishing types.

Phishing type	**Description**
Spear phishing	The victim is tricked into thinking the email is from a known trusted source.
Whaling	Spear phishing attack specifically aimed at senior executives.
Catfishing and catphishing	An attacker creates a fake social network persona to befriend the victim.
Clone phishing	A legitimate email is modified to contain links to malicious sites or contain a malicious attachment.
Vishing	An attacker uses a voice call to lure the victim to comply.
SMiShing	The attack is delivered using mobile text messages.
eFax	Uses internet fax which is similar to email.
Instant messaging	The wide adoption of instant messaging across multiple devices makes it an ideal attack platform.
Social network	By using affiliation trust is created, allowing an attacker to exploit the human relationships.

Phishing attacks follow a similar process, starting with the selection of the target audience and carefully considering the elements of the phishing message, while selecting the most appropriate technology platform to deliver the attack. In the next section, we will discuss these steps in more detail.

2.2.3 The steps in or phases of a phishing attack

A planned spear phishing attack yields better results than sending a random email hoping to trick a potential victim. Wetzel (2005) defines the phishing attack process as comprising five phases: the *attack planning*, *attack setup*, *attack execution*, *fraud* and *post-attack phases*. A more elaborate process is defined by Jakobsson and Myers

(2007) who define the information flow in the attack as attack preparation, delivering the malicious payload via email, luring the potential victim to engage, asking for confidential information, capturing the information and using the credentials obtained for monetary gain. The phases (see Figure 2.2) proposed by Aslaner (2018) follow a similar approach: (1) targeting employee(s) using a phishing campaign, (2) employee(s) opening the email which activates the malicious payload, (3) compromising the workstation to gather credentials, (4) using the stolen credentials to gain unlawful access, and finally, (5) extracting sensitive business information.

Figure 2.2 Stages of a phishing attack (Aslaner, 2018)

Owing to the similarities in these phishing attack phases, Aleroud and Zhou (2017) condensed the phases into three: *preparation, execution* and *results from exploitation* (Figure 2.3).

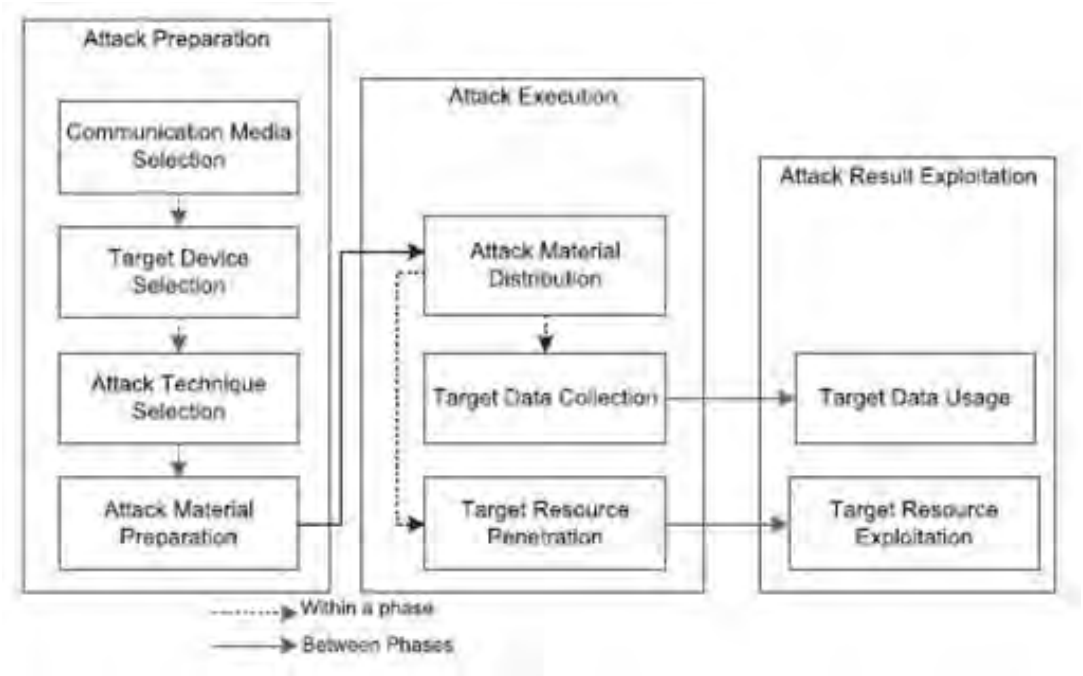


Figure 2.3 Phishing process phases (Aleroud and Zhou, 2017).

Attack preparation: The first step is for the attacker to determine the *communication media* to use. Email is used predominantly, but the attack surface has grown with the popularity of mobile devices to include instant messaging, apps, social media and

vishing (voice). The attacker needs to consider *target devices* to ensure the successful delivery of the malicious payload. The *attacking technique* applied is the site where the potential victim will provide their personal information, for example a spoofed website. Once the attacker understands these steps, the *attack material preparation* process will create the malicious artifact for distribution which could take place via email.

Attack execution: This is the heart of the process and consists of three processes. *Attack material distribution* is the mechanism chosen to deliver malicious content to a potential victim. The attack material and target device will influence the selection of a distribution mechanism. To illustrate, if the attack material is in text and the target device is mobile then using a wireless network would be the preferred attack surface. *Target data collection* starts when the victim responds to the material sent. To enhance the process of collecting user information, the attackers could inject a client-side script into a webpage.

Attack results exploitation: Once the data collection process has been completed successfully, the confidential information or credentials are used to impersonate the victim.

2.3 Practical phishing implementation

As explained in the previous sections, multiple transport layers or *mediums* exist that could be used by an attacker in conjunction with a *vector* to deliver the malicious content. The successful implementation of a phishing attack could be done with the use of various technical methods or *approaches*. Chiew, Yong and Tan (2018) summarise the relationships (see Figure 2.4) between the medium, vector and technical approach of phishing techniques.

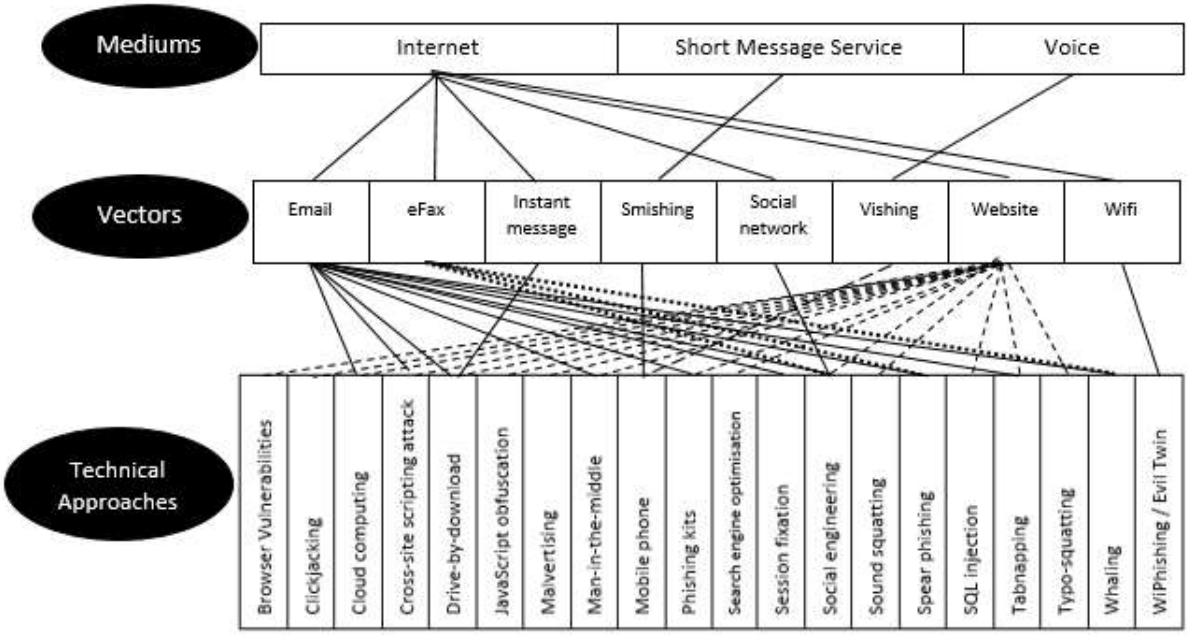


Figure 2.4 The interlink between the medium, vector and technical approach of the phishing techniques (Chiew et al., 2018)

Browser vulnerabilities refer to browser software vulnerabilities that could be exploited by an attacker to launch a phishing attack. New vulnerabilities are often introduced into software by ongoing improvement efforts that have not been properly tested (Ollmann, 2004). One such improvement is to allow a third party to create an add-in that can be installed in the browser. This creates an opportunity for an attacker to create an add-in containing malicious code that compromises the user's confidential information. It is harder to detect this type of phishing attack as the user would not be aware that the add-in contains malicious code and it could go unnoticed for a long period. Vulnerabilities resulting from plug-ins have doubled in recent years with Adobe Flash Player being the most vulnerable (Bilge, Han and Dell'Amico, 2017). Users need to ensure that they regularly patch add-ins to keep them up to date or find an alternative add-in. Another helpful browser function, the auto-fill function, which allows a user to quickly complete a form based on previous information saved in the browser, is another vulnerability that a phisher could use to obtain confidential information from a user without their consent. The form could contain hidden fields not visible to the user and when the auto-filled function is used, these fields are populated (Loeb, 2018).

Clickjacking is the manipulation of the user interface (UI) of a webpage that seems legitimate but unknowingly to the user has been compromised. This could be done in various ways such as overlaying the target website with a div container (HTML component), thus hiding the target website and displaying the correct information in the

fake div container. The user will think it seems correct but not realise that any clicks performed on the fake page are done with the data from the obfuscated target site (Sood and Enbody, 2011a).

Cloud computing is an online service that provides three service models, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). There has been an increase in the adoption of these services as they have improved. Security, however, remains one of the top concerns for cloud users. Symantec (2019) predicted that phishers would target cloud computing services owing to the abundance of information stored in one location. An email address is required to create a cloud computing account thus making it an ideal target for a phishing attack. A successful phishing attack would yield the cloud service credentials, enabling the attacker to control all services running on the cloud service and possibly allow them to obtain the credentials of other users thereby increasing their attack surface.

Cross-site scripting (XSS) is an exploited vulnerability in a web application that allows an attacker to inject malicious code into form data fields using client-side scripts. The use of XSS attacks is increasing yearly as they are relatively easy to construct and difficult to alleviate completely (Rodríguez et al., 2020). Before using any supplied data web developers have to sanitise user input to eliminate any vulnerabilities created by malicious scripts (Gundy and Chen, 2012). Attackers often exploit the vulnerability on websites where users are allowed to make comments. The malicious code is injected into the comment field and then automatically executed when the victim loads the web page (Rader and Rahman, 2013).

Drive-by-download occurs when a user visits an infected website or views an HTML email that installs malware, a virus or a shell code on his computer. This is often done by executing JavaScript targeting the vulnerability of a browser or plug-in (Sood and Enbody, 2011b; McAfee, 2013; RSA, 2016). The malware could be in the form of a Trojan. The word ‘Trojan’ comes from the Greeks who used a wooden horse as a disguise to infiltrate their enemy’s base (Christensson, 2006). A Trojan is a malicious program that seems legitimate and therefore tricks the user into installing it. Once installed, it has full access to the user’s machine via a backdoor program and could record the victim’s personal information or report back to a command-and-control server to perform malicious activities (Mäkitalo, 2017; Symantec, 2019).

Javascript obfuscation is used to alter the chrome area of the browser window which includes the address bar, status bar, toolbar and menu area. The phisher spoofs the

address bar or status bar to make the URL appear legitimate. To make things worse, the phisher could also create the perception that a site is secure by spoofing the 'lock' icon or pretending to use 'https' protocol. The victim will be unaware that the website is not legitimate (Chiew, Yong and Tan, 2018).

Malvertising infects user machines using online advertisement hosting services when a phisher creates an advertisement containing malicious code. The victim's machine is infected when he clicks on the advertisement (Sanders, 2018).

Man-in-the-middle attacks occur when the phisher inserts himself into the communication between the victim and the website, often using free or unsecured Wi-Fi. The phisher can then receive copies of all the data communicated between the website and the victim. The user will perceive his experience as normal and the attack will remain undetected (Chivers, 2020).

Mobile phone phishing attacks are growing in popularity as the number of mobile users increases (Drolet, 2018). The form factor of the device limits the amount of information that can be displayed, therefore making it difficult to distinguish legitimate applications from malicious ones. For example, Facebook Messenger was used to send a video of a recipient with their name, photo and view count together with a link allowing them to login to a fake Facebook site (Umawing, 2019).

Phishing kits allow users without knowledge of programming to create their own phishing websites. Often these kits have backdoors leaking the personal information obtained back to their creators. Cybercriminals have copied cloud computing to create Malware-as-a-Service (MaaS). This service includes the development of the kit, deploying the kit and managing the financial aspect of the phishing attack (Moreno-Fernández et al., 2017).

Search engine optimisation, also known as spamdexing, can be used to deliver phishing sites in search results by deliberately manipulating search engine indexes (Gyongyi and Garcia, 2005; Chakraborty et al., 2016; Jeong et al., 2017). The phisher creates a website and applies the correct indexing to ensure it is returned in the results. Adding popular words to a site increases the search score. In addition, products are advertised at unbelievable prices to attract traffic to the website.

Session fixation occurs when a phisher is able to hijack a user's current session as a result of poor state management implementation in a website. The internet protocols HTTP and HTTPS used in websites are stateless and therefore cannot store values. As

a user moves between different pages on a website, it is important to store certain data such as username, items in the cart for a shopping site, and suchlike. In order to store these values, the webserver creates a session with a unique session ID (SID). For this phishing attack to work, the phisher creates a SID that the user needs to authenticate, usually via a phishing email. The phisher then uses this authenticated SID to hijack the session and impersonate the user (Chiew, Yong and Tan, 2018).

Social engineering is the use of emotion to get the victim to respond to a request without making rational decisions. Emotions exploited include fear, greed, excitement, curiosity, anger, self-importance, philanthropy, a sense of community belonging or a sense of duty and authority, especially in the work environment (Abraham and Chengalur-Smith, 2010; Chiew, Yong and Tan, 2018). Hyping up emotion, such as creating the opportunity to gain or lose something of value, could result in the victim thinking irrationally and providing his or her personal information (Boss et al., 2015). This behaviour is driven by self-protection to take instant preventative action (Leventhal, 1970).

Sound-squatting is a method used by phishers to register domain names sounding similar to legitimate websites. Similar sounding words are called homonyms, for example air and heir, ascent and assent, and whether.com and weather.com (Trend Micro, 2019). Phishers also use the number in place of the word, for example www.tencent.com and www.10cent.com. This directs the user to the phishing site where their credentials are compromised.

Structured Query Language (SQL) injection is the exploitation of database vulnerabilities, allowing SQL commands to be added to the text captured in form fields, giving the attacker database access in order to retrieve information (OWASP, 2017). The injected code results in a new SQL statement being executed and returning the data to the phisher.

Tabnapping occurs when an attacker can open a spoofed website in a browser tab. Tabnapping comes from the words “tab” and “kidnapping”, indicating that the tab has been kidnapped. The phisher emails a phishing site link to the victim and once the victim clicks it, an ordinary website is opened. Embedded JavaScript monitors the user’s behaviour to determine whether they have browsed to other tabs. If the script determines that the phishing tab has lost focus, it loads a phishing site which looks like Gmail and waits for the user to login. When the user returns, they are under the impression that the

session has expired and they need to login again. When they login, they provide their credentials to the phisher (Chiew, Yong and Tan, 2018).

Typo-squatting takes place when phishers register multiple domains (squatting) with minimal differences in the spelling of a legitimate website, usually by changing the order of certain letters. If a user mistypes the URL of a domain they could end up on the phishing site which is not identified as such as it looks similar to the legitimate site (Waziri, 2016).

Wiphishing/evil twin occurs when a phisher places himself in between a user and a legitimate wireless access point (AP) by using a rogue AP. This technique involves the creation of a rogue AP with the same service set identifier (SSID) or network name as a legitimate AP in the area (Nakhila et al., 2018). Software is available to enable a laptop to become an AP (Huculak, 2016). The laptop is then moved closer to the victim in order for them to connect to this rogue AP, allowing the phisher to intercept all communications. This is usually done in public areas where free Wi-Fi is available.

The phishing taxonomy proposed by Aleroud and Zhou (2017) and displayed in Figure 2.5 summarises the discussion in the previous sections. Various communication media running on different target devices are used in phishing attacks. To increase the chances of success it makes sense to launch an attack where there is a large user base. The shortcomings of some target devices allow the attacker to exploit these features, for example when using a mobile device it could be more difficult to determine whether a link is legitimate owing to the screen real estate on mobile phones. As discussed previously, the phishing attack process is summarised in the following steps: *attack initialisation, data collection* ultimately leading to *system penetration.* Any *countermeasures* used should have a positive effect on secure human behaviour by identifying cyberthreats. In the next chapter we will focus on the role of ISAT as such a countermeasure.

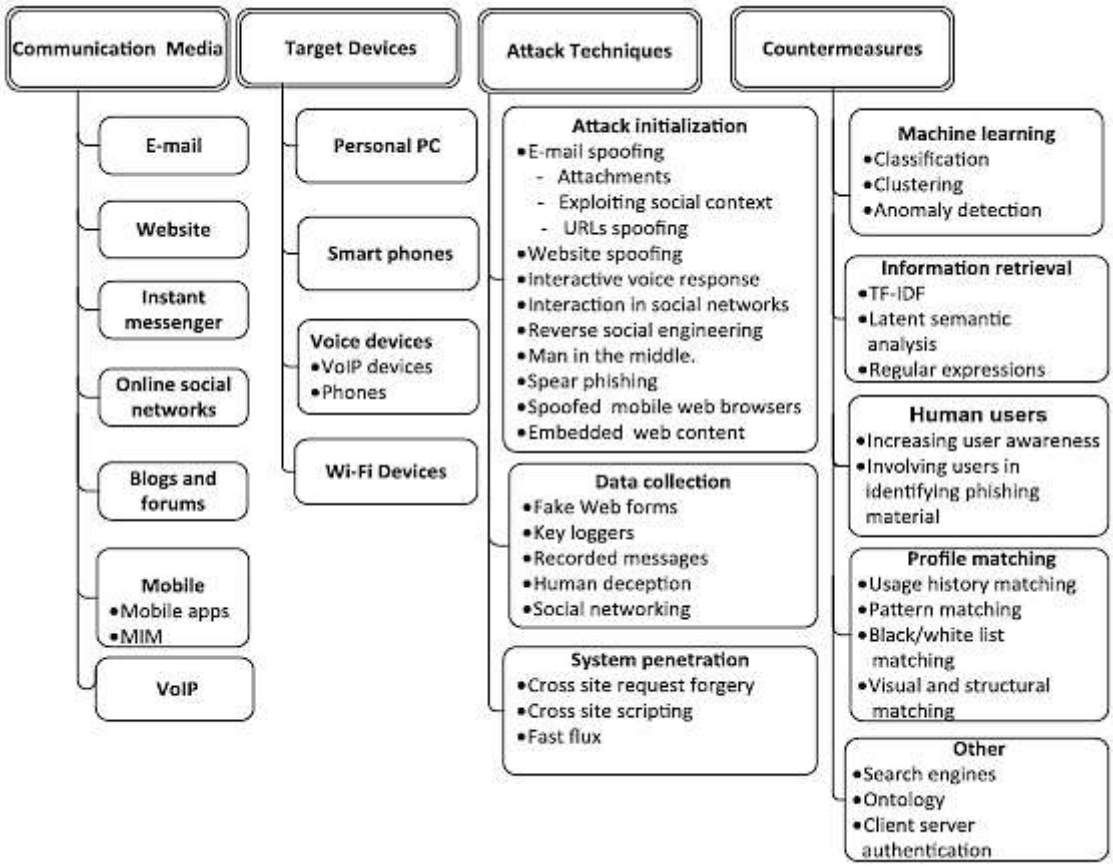


Figure 2.5 Proposed phishing taxonomy (Aleroud and Zhou, 2017)

2.4 Intention vs behaviour

Generally, people have good intentions; they want to do the right thing. This includes behaving securely and using information systems responsibly. Nevertheless, some of the worst security breaches were caused by unintentional human error (Alhogail, Mirza and Bakry, 2015). To understand some of the possible reasons for this disconnect, one needs to look at the psychological aspects of human decision-making.

2.4.1 Fear and reward phishing approaches

The goal of phishing is to encourage the victim to perform an action, primarily using one of the following persuasive tactics to influence emotions such as curiosity, fear, greed or reward (Hasle et al., 2005; Workman, 2008). To exploit these emotions, an attacker will create an email subject line that will 'hook' victims, leading to their emotions getting the better of them. They then open the email and either click on a URL or open an unsafe attachment. Fear-based phishing sets out to scare users into believing that they will lose something of value and therefore need to act, for example fake pop-up warnings of disk corruption. Although the user's intention is to behave securely, the fake warning could lead them to download and install malware perceived as legitimate security updates.

Greed or reward-based phishing plays to the fact that people love free things. Attackers capitalise on this by luring the victim into thinking that they will receive a free item by clicking on a URL or opening an attachment (Abraham and Chengalur-Smith, 2010).

2.4.2 Habits and the role of influence in persuasion

Humans are creatures of habit. Out of habit, we follow routine, perform habitual behaviour or make a decision without thinking about it (James, 1890). Habits assist us in making our behaviour more efficient, reducing our daily decision load and freeing up psychological energy for more challenging tasks (Mendelsohn, 2019). Therefore, certain habits could lead one to make faulty decisions, resulting in insecure behaviour. Cialdini

(2006) further developed the theme of human habits by stating that humans have fixed behavioural patterns that are triggered during certain events. He calls these events that trigger behavioural patterns *psychological principles of influence.* These principles include *authority, commitment, liking, reciprocation, scarcity* and *social proof*.

Authority refers to people's behaviour in generally complying with requests made by those in a position of authority, which could include their employer, the government or police. Creating phishing emails from someone in authority could therefore yield the desired result, that is, of compromising the victim's account, since people follow commands to avoid a negative outcome such as losing a privilege or something valuable (Milgram, 1983).

Humans often take a stand on an ethical issue resulting in a *commitment* and feel obligated to act accordingly (McCaul, Hinsz and McCaul, 1995). For example, Jane has witnessed gender violence and when asked to sign a petition against it, she will support it. An attacker who is aware of this could exploit this scenario.

People take a *liking* to other people who think like them or with whom they can associate. It would, for example, be easier to accept a request from someone who volunteers at the same charity as you rather than a request from someone out of town with whom you share no interest (Giles and Wiemann, 1987).

The principle of repaying like for like is known as *reciprocation* and occurs when people make indirect commitments to others (Allen and Meyer, 1990). An attacker could leverage this principle giving a gift, albeit it with malware installed.

Scarcity has to do with the apparent value of an item, opportunity or life-changing event when it is deemed to be a limited commodity (Brehm, 1966). An attacker could create urgency to act quickly and therefore be successful in the phishing attempt.

The *social proof* principle refers to the 'sheep' mentality which holds that the majority (peer group, role models, important others) must be correct and is therefore to be trusted (Asch, 1946). For example, 90% of people who purchased a limited product said it was good value for money and since it was not to be repeated, considered a chance of a lifetime, thereby creating trust for others to purchase it.

Habits steer us to act without thinking through the possible consequences of the decisions we make. This blinds us to seeing possible security vulnerabilities.

2.4.3 Disinformation techniques

Hernon (1995) states that wrong and deceptive information causes bad behaviour regardless of whether the source made an honest mistake (misinformation) or consciously planned to deceive (disinformation). Disinformation is similar to fake news, as it comprises incorrect information supplied with the intention of deceiving people (Allcott and Gentzkow, 2017). It was used in “Operation Bodyguard” during the Second World War to hide the intended location of the D-Day invasion. Disinformation was sent using fake radio transmissions to convince the Germans that there was a large force in East Anglia ready to attack Calais rather than Normandy (Farquhar, 2005).

In the internet age we live in, specifically the ease with which information is shared, disinformation poses a significant threat to information quality. This situation has created the ideal opportunity for phishing attacks to use this information as bait. If users were exposed to the disinformation and did not recognise it as fake, a phishing email with the same information might convince them to act. Carpenter (2020) defines the following disinformation techniques:

- *Astrosurfing:* the term derives from a product of artificial grass that is made to look real. A number of comments, that appear to be uncoordinated, are made by well-meaning private citizens on social media, blogs and websites. However, they are orchestrated by an adversary to achieve a certain outcome.
- *Gaslighting* stems from the proverbial ‘adding fuel to the fire’ which uses psychological manipulation on a victim to distort their sense of truth. A s*ock puppet* is someone who creates a false identity on a social media platform, making controversial and offensive comments on divisive issues, while seeming to be a legitimate person with no hidden agenda.
- *Clickbait* uses an enticing but false post to lure a victim to click on a link to read the full article, with malware being downloaded in the process.
- *Microtargeting* focuses on dividing voters into small groups based on demographics, interests, biases or affiliations to deliver specific messages that appeal to those groups.

The sophistication level of disinformation or deception increases with the use of modern technology. People often believe what they see, failing to take into account the visual manipulation that technology provides today (Stenberg, 2006; Newman et al.,

2015). Deepfakes are often difficult to recognise and as the technology matures they will become more real and therefore more convincing (Ahmed, 2021).

The techniques mentioned can be used to set the scene for a phishing attack as the victim has been conditioned subconsciously to believe a lie. Several phishing email campaigns were created during the Covid-19 pandemic, confusing people and enticing them to take action. Disinformation creates the ideal environment for successful phishing campaigns.

2.5 Current statistics

The FBI Internet Crime Complaint Center (IC3) in the USA reports annually on internet crime based on the complaints it receives. Between 2015 and 2019 it received 1.7 million complaints resulting in a $10.2 billion loss. The losses reported in 2015 ($1.1 billion) more than tripled in 2019 ($3.5 billion). On average, the IC3 receives 1200 complaints per day (FBI Internet Crime Complaint Center, 2019). The most frequent complaints relate to social engineering attacks (phishing/vishing/smishing/pharming) which affected 114 702 victims in 2019. Of these, business email compromise resulted in the highest reported financial loss at $1.7 billion. 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. A key finding of the report is that the impact of phishing varies widely per region, for example Japan had an onslaught of fraudulent Amazon messages leading to higher-than-average account compromise compared to 69% of Spanish respondents and 47% of Australians experiencing data loss. The global impact of phishing attacks is summarised in Figure 2.6. The number of breaches reported via the media has recently increased significantly. Using links in a phishing email to solicit account credentials remains the preferred phishing email type compared to data entry sites or attachments.

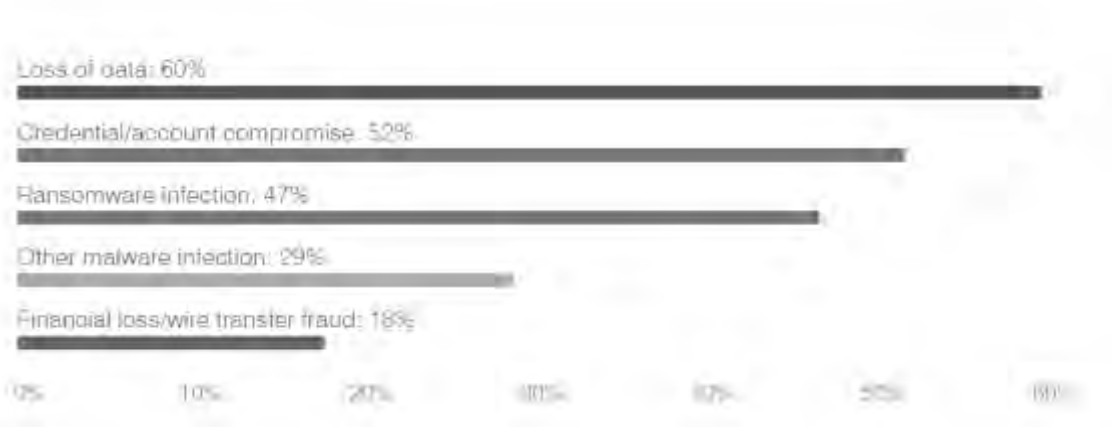


Figure 2.6 Effects of phishing (adapted from Proofpoint, 2021).

Attackers ensure that their phishing emails are topical, thus ensuring that phishing remains one of the preferred social engineering techniques. For example, Covid-19 was used to create millions of phishing emails, ranging from information on the spread of the virus to conspiracy theories and news relating to a vaccine (Proofpoint, 2021). Since these emails seem authentic, users struggle to identify phishing attacks.

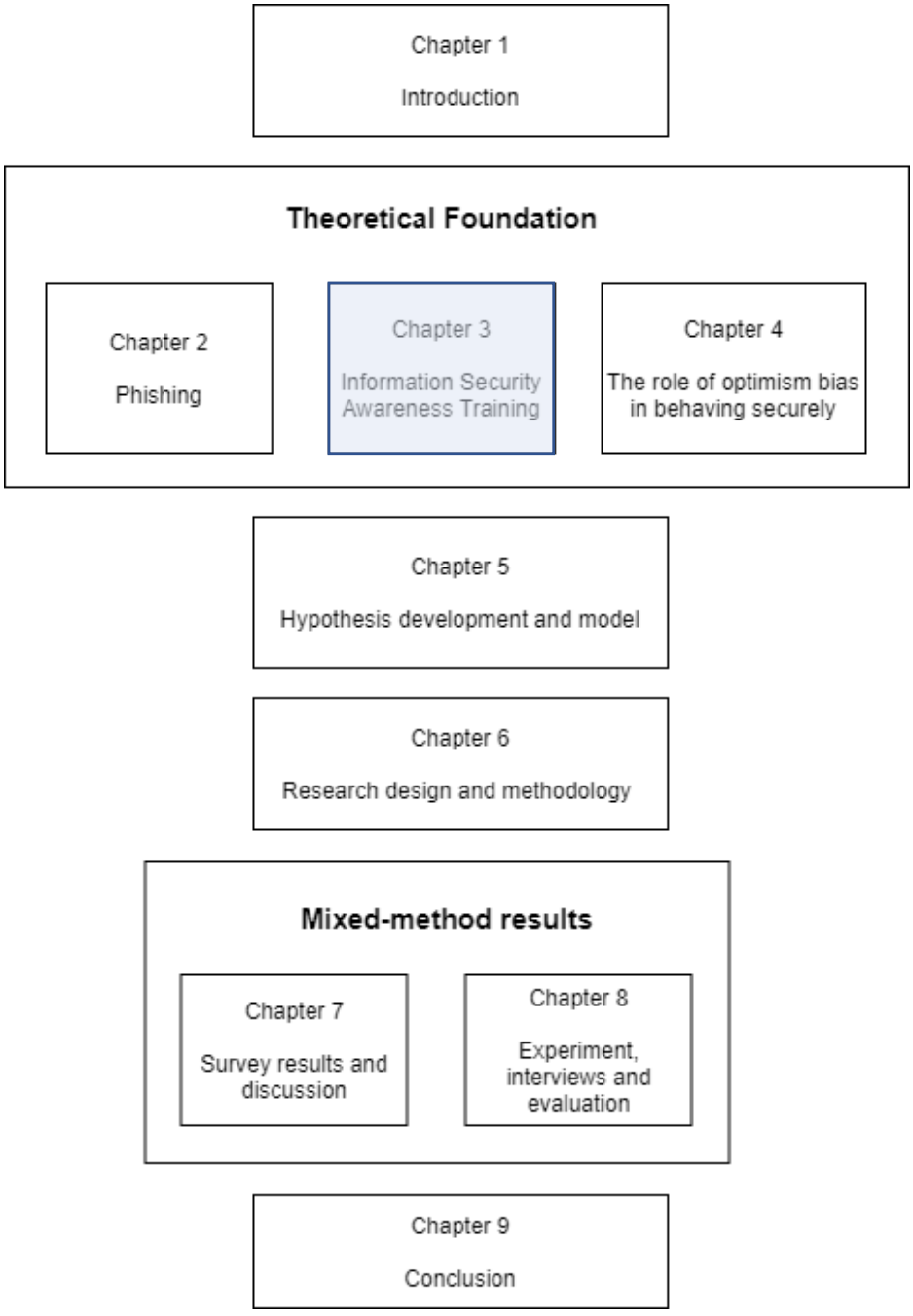
2.6 Summary

This chapter explained phishing in detail by discussing the context to better understand the research sub-questions. The chapter began by explaining the theory of phishing and how it is used to deceive humans into behaving insecurely. The literature review emphasised that people are motivated by fear or reward. It was also indicated that persuasion is not the only motivating factor that influences behaviour. Certain personality traits seem to be more susceptible to succumbing to phishing attacks. The literature also pointed out that there are a host of different phishing types, although they contain similar elements and characteristics. Therefore, any internet-based communication platform or device could be used for a phishing attack. This large attack surface means that users need to be consciously aware of possible cybersecurity threats when engaging with these platforms. Unfortunately, people are creatures of habit, which often results in decisions being made ‘unconsciously’. This happens especially in the work environment, where people are driven to produce results and want to comply with requests from a superior, known as the *authority* principle. Although people have good intentions to

behave securely, literature reveals that this is not always the case as phishing attacks continue to be successful. Attackers ensure that their phishing emails are topical thereby creating the impression that their requests are legitimate. Previous studies suggest that if people can identify what a phishing attack looks like, they should be in a better position not to succumb to it. Therefore, the next chapter will focus on the effectiveness of ISAT.

CHAPTER 3

INFORMATION SECURITY AWARENESS TRAINING



3. INFORMATION SECURITY AWARENESS TRAINING (ISAT)

3.1 Introduction

In the context of an organisational setting, security awareness refers to employees' understanding of and attitude toward the protection of their company's physical and information assets (Pattinson et al., 2016). Security awareness is a critical link in an organisation's security chain, as even the most effective security procedures are useless in an environment where there is no security culture.

The terms ‘security culture’, ‘information security culture’ and ‘cybersecurity culture’ will be used interchangeably in this study. A security culture consists of the following: top management support, policy and procedures, and information security awareness (ISA). Many of the cybersecurity frameworks share a common core set of components, with organisational culture fulfilling a crucial role in creating the appropriate cybersecurity culture models (Ruhwanya and Ophoff, 2019; Uchendu et al., 2021).

Information security has been defined as more than just a “technical problem” (Alhogail, Mirza and Bakry, 2015). People are often regarded as the weakest link in the security chain and therefore human behaviour must be addressed to improve overall information security behaviour (Parsons et al., 2014; Bélanger et al., 2017; Fagade and Tryfonas, 2017). The perceived solution to this problem is the use of ISAT (information security awareness training) as it has been shown to have a positive impact on creating more secure behaviour.

Bulgurcu, Cavusoglu and Benbasat (2010) state that in employees, ISA comprises both a general knowledge of information security and an awareness of the organisation’s information security policy. This policy stipulates what is allowed and not allowed when using the organisation’s ICT infrastructure and systems. It is vital that employees understand the possible threats and consequences relating to any breach of information security in order to behave securely.

The objective of this chapter is to define at a high level the various information security threats and therefore what the goal of ISAT is. The literature review will show that a

successful ISAT programme contains the right content for overcoming these threats and takes into account the desired behaviour that the training needs to enforce. To gain a better understanding of the content required, several cybersecurity frameworks will be discussed. Once the content requirements are understood, the design recommendations for ISAT must be taken into account whilst understanding how people learn to maximise the effectiveness of the training.

3.2 Brief overview of security threats

Multiple types of security threat exist, but they are usually in the form of malicious code known as malware. Malware, short for malicious (or malevolent) software, includes viruses, Trojans, worms, bots, backdoors, spyware and ransomware to name a few (Han et al., 2019). The purpose of malware is to disrupt, damage or gain unauthorised access to computer systems, often for financial gain (Parmar, 2012). Malware may be delivered by visiting illicit websites, downloading rogue applications or falling victim to a phishing attack (Ifinedo, 2018).

To be effective ISAT must be relevant and practical. It is therefore important to understand the current security threats, by reviewing the notifications from security companies and software vendors, to ensure that the ISA material remains relevant in addressing the risks. One of these risks can be classified as malware.

3.2.1 Types of malware

There is a variety of different malware types, allowing an attacker to choose the best method to achieve their goal. Malware can be classified into (1) spying applications for leaking or stealing information that aim to be unobtrusive and exist for a long time, and (2) destructive applications that cause damage to information or computer systems. The outcome could include the destruction of systems either for or without financial gain (Bahtiyar, 2016). The following section briefly describes various malware types.

Viruses are the oldest form of malware. A virus is a piece of code that (1) has the capability to automatically reproduce, and (2) attaches itself to other computer objects

such as programs, disks and USB storage devices. A virus cannot execute by itself; for the code to execute it needs a host program to run on.

A worm is a program that actively replicates to other computers in a network, usually by exploiting vulnerabilities in operating systems. A worm can execute on its own as it is a complete program (Bahtiyar, 2016).

A Trojan Horse is malicious code pretending to be something else. It is frequently found in pirated software downloaded from unauthorised sources. It can also download and install additional programs to achieve its goal of stealing information or damaging the system (Pandya, 2013).

A rootkit is software designed to gain administrator or 'root' permissions on a computer without being detected. Rootkits are difficult to detect as they are able to cover their tracks. Once installed they can be used to access the computer remotely or steal information (Shafiee Hasanabadi, Habibi Lashkari and Ghorbani, 2020).

Spyware is an application that aims to gather information about a person or organisation without their knowledge (Alghamdi, 2021).

Adware is often installed alongside other applications of dubious reputation and will insert unsolicited advertising into a user's browser (Singh and Singh, 2021).

Ransomware has become very common in recent years. This software is designed to exploit a known Windows vulnerability and consequently bypasses traditional anti-virus protection (Kara and Aydos, 2022). This grants the malware full administrative rights over the victim's computer. Once it has full access, it encrypts all the files and locks the victim out of their computer. A ransom is subsequently demanded to obtain the key to unlocking it.

Phishing was discussed in detail in the previous chapter. Generally, a successful phishing attack results in malware being deployed on the victim's computer. In order to behave securely, employees need to understand the different cybersecurity risks and, at a high-level, the different mechanisms used to initiate these attacks.

3.3 The goal of information security awareness training (ISAT)

ISAT should encourage people to play an active role in securing their environment by knowing what to protect and why (Beyer et al., 2015). One of the aspects of a good security culture is that people take responsibility for their online behaviour.

A security awareness programme ensures that everyone in the organisation has an appropriate level of know-how about security along with an appropriate sense of responsibility. Such programmes are important because they reinforce the notion that security is everyone's responsibility. When employees understand their responsibility and the consequences of insecure behaviour, the resultant behaviour should indicate that security is taken seriously. Responsibility refers to the duty a person has to process a task and how accountable they are for its results (Musuva, Getao and Chepken, 2019). The more accountable someone is, the greater the motivation to complete a task correctly or more securely. An employee who takes accountability for their actions will endeavour to do what is in the best interests of the organisation.

Technology is always evolving and therefore attack strategies keep on changing. Employees need to be aware of new attacks and how to circumvent them (Bauer, Bernroider and Chudzikowski, 2017). This is achieved through ongoing awareness training programmes which take the latest cyberthreats into account.

The goal of ISAT is to stress the importance of secure behaviour and the possible negative outcomes of a security breach. The training should result in more than just a compliance check-box exercise; it should consider how people interact with processes and technology to solve business problems (Ki-Aries and Faily, 2017). Awareness programmes should trigger security behaviours, helping employees to discern security concerns in order to respond securely to threats (Tsohou, Karyda and Kokolakis, 2015). The result should be a reduction in security breaches.

3.4 An overview of cybersecurity frameworks

Cybersecurity frameworks were created to assist organisations to create effective ISAT programmes. The frameworks consist of processes, practices and technologies that an organisation may implement to secure their systems. In addition, regulatory privacy acts, for example the General Data Protection Regulation (GDPR) (Anon., 2018) and the Protection of Personal Information Act (POPIA) Act 4 of 2013, demand the safekeeping and protection of personally identifiable information. In the following section we will discuss a number of these frameworks.

3.4.1 INTERNATIONAL STANDARDS ORGANISATION 27001/ISO 27002

The ISO 27001 cybersecurity framework is an international standard that makes recommendations for managing information security management systems (ISMS). ISO 27001 uses a risk-based process to guide organisations in creating controls to safeguard them against cybersecurity threats (ISO/IEC, 2013). The security controls consist of the following:

- *Organisational context:* the information security needs and expectations to scope and create the ISMS are identified.
- *Leadership:* management is committed to the process, signs off on the information security policy and delegates responsibilities.
- *Planning:* information security risk assessments and treatments are performed.
- *Support*: suitably qualified people are employed for the project and awareness and project documentation are kept up to date.
- *Operation:* the risk treatment plan is implemented and constantly refined.
- *Monitoring, measuring, analysis and evaluation:* the overall effectiveness of the ISMS is determined and future changes recommended.
- *Continuous improvements:* these are critical to ensure the continued efficiency and relevancy of the ISMS.

ISO 27001 states that ongoing awareness training must be done but does not stipulate how it should be done.

3.4.2 National Institute for Standards and Technology Cybersecurity Framework

In 2013, the National Institute for Standards and Technology (NIST) in the USA created the National Initiative for Cybersecurity Education (NICE) framework to address various security topics, specifically to manage the risks to data and information security (Petersen et al., 2020). The NICE framework is comprised of the following components: (1) categories that describe a high-level grouping of common cybersecurity functions, (2) specialty areas of cybersecurity work, and (3) work roles that form part of cybersecurity work, comprising the specific knowledge, skills and abilities (KSAs) required to perform tasks in a work role.

The NICE framework defines the following functions for managing the risks to data and information security:

- *Identify:* helps organisations to detect security risks using comprehensive risk assessment and management processes.
- *Detect:* defines security controls, including access control, training and awareness, data security, information protection procedures and maintaining protective technologies.
- *Response:* makes recommendations for responding to a security incident, as well as for mitigation procedures, communication processes and activities for improving security resiliency.
- *Recovery:* gives guidelines for recovering from an attack.

The NIST 800-53 publication (Security and privacy controls for information systems and organisations) was specifically created to enable federal agencies to secure their information systems, but is suitable for any organisation (NIST, 2020). This publication contains more than 900 security requirements, making it one of the most complicated frameworks to implement. Controls included in the framework consist in enhancing physical security, penetration testing, guidelines for implementing security assessments and authorisation policies and procedures.

3.4.3 Information Assurance for Small to Medium-sized Enterprises Governance (IASME)

This standard assists small and medium-size organisations to implement adequate cybersecurity controls (IASME Consortium Limited, 2018). It is used to accredit the cybersecurity posture of an organisation and is far more affordable than ISO 27001 certification. The standard uses a framework to determine the risk profile for the organisation by understanding (1) how information systems are used, (2) how outsourced services are used, (3) whether the organisation allows employees to bring their own device (BYOD), (4) the use of mobile and remote systems, (5) awareness of and attitude to the threat environment and (6) the value of the organisation's business assets and information technology.

3.4.4 System and Organisation Controls 2 (SOC 2) and System and Organisation Controls for Cybersecurity (SOC-C)

The SOC 2 and SOC-C frameworks were developed by the American Institute of Certified Public Accountants (AICPA) and form part of the System and Organisation Controls (SOC) suite of services (AICPA, 2022). SOC 2 was developed for service organisations to maintain proper security where personal customer information is stored using cloud services. The objective of SOC 2 is to provide information about controls related to the security, availability, integrity, confidentiality and privacy of information. The framework also includes rules and requirements for software as a service (SaaS) companies to follow, in order to mitigate data breach risks and boost their cybersecurity postures. The framework gives guidance on conducting an external and internal threat assessment in order to identify possible cybersecurity threats. SOC 2 contains 61 compliance requirements, including guidelines for the destruction of confidential information, alert systems for security anomalies, procedures for responding to security incidents and internal communication guidelines, among others.

SOC-C is a framework for non-service businesses, providing users with information on the organisation's Cyber Risk Management Policy (CRMP). A CRMP is defined by the SOC-C as the policies, procedures and controls implemented by an organisation to

protect their information from a security breach and to be able to respond to, mitigate and recover from a security incident (Al-Moshaigeh, Dickins and Higgs, 2019). The objective of the framework is to allow organisations to communicate information about their cybersecurity risk-management programmes and the criteria for assessing their effectiveness. Reporting is done on three levels: (1) organisation – includes board, management, investors and regulators, (2) service providers – any vendor providing a service to effectively manage cybersecurity risk, and (3) supply chain – all suppliers and processes are adequately documented to mitigate any cybersecurity risks.

3.4.5 Center for Internet Security (CIS)

The CIS framework is maintained by the Center for Information Security. CIS lists 18 actionable cybersecurity controls meant for enhancing the security standards of all organisations (CIS, 2022). The framework categorises the information security controls into three implementation groups: group 1 is for businesses that have limited cybersecurity expertise and resources; group 2 is for all organisations with moderate technical experience and resources in implementing the sub-controls, and group 3 targets companies with vast cybersecurity expertise and resources. CIS stands out because it enables businesses to develop cost-effective cybersecurity initiatives. An additional benefit is the ability to prioritise cybersecurity activities. Some of the CIS critical security controls include an inventory of software assets, data protection, account management, access control, data recovery, security awareness and skills training.

3.4.6 Control Objectives for Information Technologies (COBIT)

In 2019, the Information Systems Audit and Control Association (ISACA) updated its COBIT framework to create a governance system and governance framework (ISACA, 2018). Rather than relying on individual security controls to ensure compliance, COBIT 2019 starts with the demands of stakeholders, assigns job-related governance responsibilities to each category, and then maps the responsibility back to technology. The goal of COBIT is to ensure appropriate oversight of the organisation’s security posture.

The COBIT core model groups governance and management objectives into five domains:

- Governance objectives:
    - EDM: evaluate, direct and monitor
- Management objectives:
    - APO: align, plan and organise
    - BAI: build, acquire and implement
    - DSS: deliver, service and support
    - MEA: monitor, evaluate and assess

COBIT's design principles include

- understanding the enterprise strategy
- scoping the governance system
- refining the scope, and
- completing the design.

The COBIT framework considers and caters for humans in the security chain by taking culture, ethics and behaviour, as well as skills and competencies, into account (see Figure 3.1).

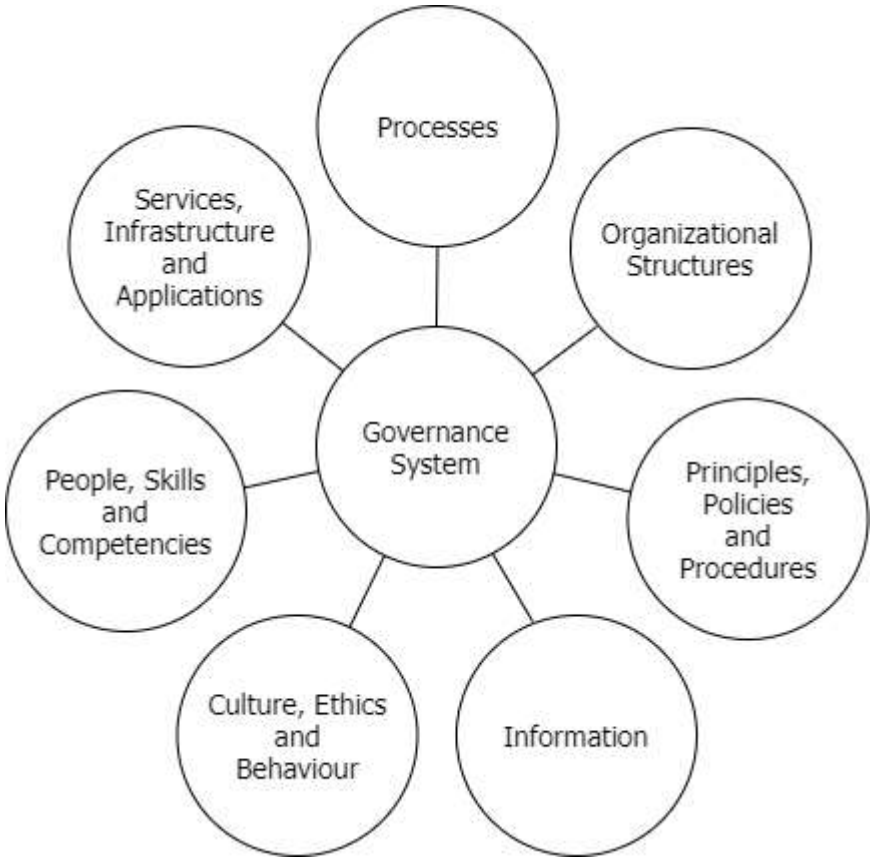


Figure 3.1. COBIT 2019 Framework: Basic Concepts: Governance Systems and Components

COBIT's main output is to create a security framework that streamlines audits and incorporates continuous improvement to enhance outcomes.

3.4.7 Privacy: General Data Protection Regulation (GDPR) and the Protection of Personal Information Act (POPIA)

GDPR is a framework enacted to secure personally identifiable information belonging to European citizens (Anon., 2018). The framework provides a set of compulsory security requirements that organisations across the world must implement. It is treated as a global framework that protects the data of all EU citizens. Non-compliance could result in huge penalties, leading most companies to comply with the requirements. GDPR requirements include implementing appropriate controls for restricting unauthorised access to stored data. These controls include access control measures, for example least privilege and role-based access controls and multifactor authentication schemes. Organisations or websites must acquire a data owner's consent before using the data for purposes such as marketing or advertising. Personally identifiable data breaches that result from a company's inability to implement security controls lead to non-compliance with the GDPR.

The POPIA is applicable to all South African public and private organisations (No 4 of 2013: Protection of Personal Information Act). The Act is similar to the GDPR and forces South African organisations to take cybersecurity seriously, with non-compliance leading to fines and/or imprisonment. The requirements of the Act highlight the importance of continued security awareness and training.

3.4.8 Summary of frameworks discussed

The frameworks discussed share common themes, starting with understanding what information assets need to be protected by creating an information asset register that describes the value of these assets. Policies and procedures provide guidelines for the use of such assets by employees. These frameworks indicate that technology security controls do not provide a fool proof environment and that employees need consistent training and monitoring.

3.5 The role of information security policies and procedures

A policy is a set of principles created with the intention of guiding actions and achieving sensible outcomes. It is a declaration of intent that is executed through a procedure or protocol. Policies are generally adopted by a governing body of an organisation (Philips, Sander and Govers, 1994).

Creating an information security policy is the first step to protecting an organisation's data against cybersecurity threats (Moody, Siponen and Pahnila, 2018). Although this is a good starting point for a strong security posture, several studies have found that employees do not pay attention to the contents of the policy and therefore behave insecurely (Ifinedo, 2012; 2014; Han, Kim and Kim, 2017). This problem must be addressed through ISAT that includes the contents of the security policy. Safa, Von Solms and Furnell (2016) found that commitment and personal norms had a significant effect on attitude and the intention to behave securely. An employee's attitude towards secure behaviour can be changed if they understand the risks and consequences of insecure behaviour. Employees who are aware of their company's information security policy and procedures are more competent to manage cybersecurity risks than those who are ignorant of the policy (Li et al., 2019). In addition, the organisational information security environment positively influences employees' threat assessment and coping assessment abilities, resulting in secure behaviour (Li et al., 2019).

The information security policy and procedures must become living documents. To mitigate cybersecurity threats, employees need to have a practical understanding of the contents.

3.6 Frequency and approach of ISAT

ISAT should be done on an ongoing basis to reinforce awareness, putting security practices into normal daily routine and using mock tests to foster a security-focused culture (Beyer et al., 2015). The training programme should focus on building a strong security culture.

3.6.1 Frequency of ISAT

Initial ISAT should be done when new employees are hired and should include essential education on the organisation's information security policies and procedures. Employees should confirm either electronically or in writing that they have received the training and that they understand what is required from them. This can be used later as proof that the employee was warned about what is allowed using the organisation's systems (Sadowsky et al., 2003).

ISAT is forever evolving owing to a changing technology landscape. This makes it difficult for employees to stay up to date with cybersecurity threats. ISAT programmes should be structured in such a way that employees are constantly updated on the latest threats (Bauer, Bernroider and Chudzikowski, 2017). Li et al. (2019) found that digital transformation has an impact on long-term cybersecurity plans, methods and practices. This highlights the need to update ISAT material regularly.

3.6.2 Elements of a successful security awareness programme

Manke and Winkler (2012) identified several elements required for a successful security awareness programme:

(1) Obtain senior management support

With executive buy-in, budgets are increased, and other departments are more ready to assist the programme. ISAT is a legal necessity that, in the end, should save the company money by preventing security breaches.

(2) Partner with all departments

Departments, such as legal, compliance and human resources, may be able to provide income to support the training if they are involved. Their support will guarantee that the training is made mandatory within their teams, and it may even be incorporated into the induction process for new hires. Including the demands of other departments in security training could be advantageous, for example compliance could be added to the training materials.

(3) Be relevant

The ISAT programme should not be a check-box activity. Using an out-of-date selection of computer-based training movies may also be ineffective. Based on current threats, content must be timely and relevant. The utilisation of contemporary cases will demonstrate the potential for undesirable consequences.

(4) Measure success

Before any training is conducted, a baseline should be created to measure programme success. This should be measured again once the training is completed (Fertig and Schütz, 2020). Surveys of security attitudes, a mock phishing test, monitoring web content for malicious activity, or the use of a social engineering attack are all possible tests and may include, for example, a USB stick containing malware (Silva, Feitosa and Garcia, 2020). Any progress that can be measured will make it easier to justify the continued support and funding of the awareness programme (Khando et al., 2021).

(5) Set the example of how to securely behave

It is more important to tell employees how to use technology than to prohibit them from using it. Telling employees not to use social media, for example, will result in them finding ways to use it. Successful awareness training teaches employees how to accomplish tasks safely.

(6) Incentivise awareness

Employees should be rewarded for secure behaviour, for example when security incidents are reported.

(7) Use several awareness tools

Training should not be limited to the use of one type of tool; it should encourage participation from employees to demonstrate that they relate to the training. Training material should be personalised for the intended audience.

The implementation of these elements should result in a successful ISAT programme. It is understood that participation from everyone in the organisation is required for a successful ISAT programme. The content should be relevant and therefore updated on a regular basis. The organisation should also administer

practical tests after each training session to monitor the effectiveness of the employee training. In the next section we will focus on the design elements of effective ISAT.

3.6.3 Design recommendations for ISAT

Effective ISAT should target a company's risks and focus on specific employee groups (Beyer et al., 2015). It is important that companies define their own security culture to demonstrate the seriousness thereof to all employees. Not only is it important to select the appropriate topics for training, but attention must also be paid to how these security topics are addressed. To do this effectively, the target audience must be categorised (González-Manzano and de Fuentes, 2019). Therefore, the training must be relevant to the work context and must address defined security requirements.

The delivery mechanism plays a vital role in how well the material is internalised and understood by the employee (Al-Daeef, Basir and Saudi, 2017). Online e-learning platforms allow employees to register for a course and to complete it in their own time. Management can track progress by reviewing the stats created by the system. Such stats could include who has successfully completed the course by correctly answering the test questions and how many attempts were required to complete a course. In addition, if multiple attempts are required to complete a course it could be an indication that either the course has too much material to cover or the material is difficult and/or boring (González-Manzano and de Fuentes, 2019).

Design recommendations for ISAT include the following:

- Training material should be interesting so as to keep the employee's attention and to retain the acquired knowledge.
- Training activities should be embedded in an employee's normal workday where feasible and not seen as a once-off exercise.
- A variety of mechanisms should be used to master the material, for example e-learning courses, emails, messages when logging in and gamification could be used.
- The information security risks and the possible consequences of a security breach should be clearly explained. If employees are emotionally involved, they will have a better chance of retaining the knowledge acquired.

- Training material should be customised and be specific where feasible.
- The contents of the information security policy should be explained as well as the punitive measures for non-compliance.
- Employees should be able to review the material multiple times at their leisure.
- Check for understanding by asking questions or requiring employees to do a short test based on the contents of the training material. The employee should receive immediate feedback so that corrective action can be taken if required. Repeat training until the material has been successfully mastered.
- Make the training practical, for example conduct simulated phishing attacks to demonstrate what these could look like. Make users aware of the phishing emails that the organisation receives.

Implementing these design recommendations will ensure that the training material covers the organisational risks and that the awareness training is embedded in the employees' daily work activities. Since people have different learning preferences, the next section will address those, as they could have an influence on how well employees internationalise the material.

3.7 How do people learn?

People have different preferences when it comes to learning, which could influence how knowledge is acquired and retained. Of particular interest to this study is how people learn in the workplace. Understanding how people learn could help shape ISAT to enhance its effectiveness.

3.7.1 Learning styles or methods

People prefer either words, pictures or speech and/or the kind of intellectual activity they find most stimulating, for example analysis versus listening (Pashler et al., 2008). There is ample research to support this notion (Pashler et al., 2008; Dekker et al., 2012; Howard-Jones, 2014). Learning styles are classified as visual, auditory or tactile.

Visual learners prefer to learn by seeing images, reading books or watching content. They prefer to look at the written words on a blackboard or presentation than to only listen to the educator. They convey understanding by using expressions such as “I get the picture” and “I see”. The visual learner performs well on tests as they are able to read and translate the words into images (Bueno, 2005; Xu, 2011; Zhang et al., 2020)

Auditory learners or verbal learners prefer to learn by listening. This student is the most verbal of the three types of learner. They leam by listening and love class dialogues (Vincent and Ross, 2001). They may not be fond of reading books, a they prefer to hear more and see less. The auditory learner conveys understanding by discussing the issue; their speech patterns indicate how they think (McVay Lynch, 2012).

Kinaesthetic or tactile learners do not respond to verbal instruction, preferring to express their feelings physically, and are socially outgoing (Vincent and Ross, 2001; Syofyan and Siwi, 2018). A kinaesthetic learner will leam by doing. They remember and develop understanding by touching and feeling, performing hands-on activities (McVay Lynch, 2012). Owing to their restlessness, kinaesthetic learners will find it difficult to learn in an online environment. Accordingly, the instructor should encourage them to make notes and discuss the material with others in the group.

The meshing hypothesis posits that if people are given instruction in their preferred modality (visual, auditory, kinaesthetic) they will experience enhanced learning results (Pashler et al., 2008). However, Aslaksen and Lorås (2018) found that there is no statistical evidence to confirm that using a person’s preferred modality will result in an enhanced learning outcome. Furthermore, Pashler et al. (2008) confirm that the majority of the research on learning styles lacks the “experimental methodology capable of testing the validity of learning styles applied to education”.

It would therefore appear that learning style is more a preference than a recipe for success. However, it could create an emotional connection that allows the learner to feel more comfortable with the material and therefore provide a more engaging experience resulting in good learning outcomes (Pessoa, 2008).

3.7.2 How do people learn in the workplace?

Some of the characteristics of workplace learning include the effect of work assignments and the work environment on what and how people learn, as well as their former work experience (Collin, 2006; Lemmetty and Collin, 2020). Learning can take different forms depending on the nature of the job. These may include formal learning through training courses and informal learning like on-the-job training where one colleague assists another to master an activity (Twidale, 2005; Vasanthi and Basariya, 2019). In a fast-paced, changing world, to remain competent adults need to take responsibility for their own learning. In their work people can learn on their own by experimenting and using information. This is known as self-directed learning or non-formal learning (Livingstone, 2001; Lemmetty and Collin, 2020). Non-formal learning lacks the following formal learning characteristics: (1) a prescribed learning framework, (2) an organised learning event or package, (3) the presence of a designated instructor and (4) the award of a qualification or credit (Kooken, Ley and de Hoog, 2007; Seemann, Stofkova and Binasova, 2019). Learning in this study is seen as what people do with the knowledge they acquire and their resulting behaviour.

3.7.3 The effect of awareness (cybersecurity learning) on secure behaviour

Figure 3.2 (Beyer et al., 2015) indicates that secure behaviour is influenced by both the knowledge and skills of employees. Secure behaviour requires consistent communication of relevant information via a multitude of channels. These channels should include electronic messages, posters and newsletters to name a few. Intervention is required from the organisation in every step in the process to ensure that awareness maturity is achieved. The awareness raised through this communication process should result in unconscious competence for the employees, meaning that they are adequately equipped to handle security risks and tasks. On the flip side, conscious incompetence leaves the employee vulnerable to security risks owing to a lack of awareness.

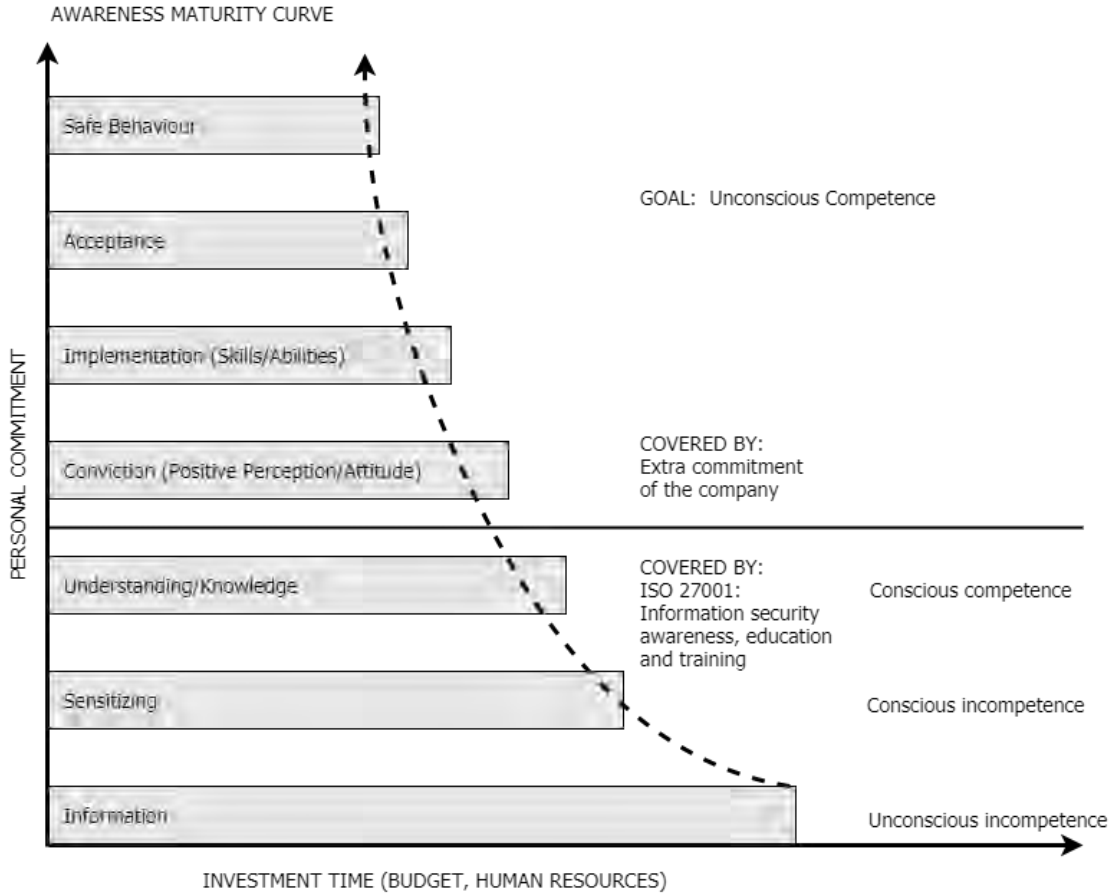


Figure 3.2. Hewlett Packard Enterprise Awareness Maturity Curve

In Figure 3.2, The Understanding and Conviction stages require management buy-in. Management needs to lead by example by displaying secure behaviour, as this motivates employees to do the same. In the Implementation stage, employees need to take personal responsibility for protecting the organisation's information assets; they need to know what is expected of them. The Acceptance and Safe Behaviour phases require commitment from the employees to implement the awareness knowledge they have acquired. Secure behaviour should become self-sustaining over time. This is done by continuously reviewing the lived security culture and identifying any behavioural changes that are required. Management needs to give recognition for secure behaviour and so motivate employees to stay security compliant. Ongoing engagement is required to foster social capability and to develop discourse around security.

3.8 Previous ISAT studies and outcomes

Previous studies have shown that increased ISAT has a positive impact on secure behaviour (McCormac et al., 2017; Khando et al., 2021). When people know what to look for, they are able to identify security threats (Mittal, 2015). However, Dodge et al. (2007) question how well ISAT mitigates insecure behaviour. Users may complete the training successfully, but without taking measures to check that they apply this knowledge there is a possibility that the ISAT could fail to change insecure behaviour. Counting the number of successful attacks is one such measure. However, this approach may be inadequate, because fewer successful attacks may be the result of fewer attempts, and more successful attacks may reflect new vulnerabilities or other variables unrelated to user behaviour (Egelman and Peer, 2015). In addition, phishing attacks increased during such events as the Covid-19 pandemic and the US elections (Bhardwaj et al., 2020). Because the number of attacks varies greatly from month to month, this approach is not a reliable measure for determining the effectiveness of ISAT.

To make matters worse, traditional ISAT programmes are often unsuccessful because they are seen as dull and lack user contact and participation (Mansfield-Devine, 2013; Abraham and Chengalur-Smith, 2019). Using posters and flyers alone to create awareness is completely ineffective (Bada and Sasse, 2014); instead, a different approach is required. Wash and Cooper (2018) considered both the traditional “facts-and-advice” and the use of “story telling” to convey the same message. Interestingly, they found the facts-and-advice approach to be effective when presented by a security expert, while the use of storytelling was effective when done by a peer. It therefore seems that the perceived origin of training materials can influence the behavioural outcome. To create an interactive training experience that will yield better results, the use of various online tools, such as discussion groups, animation and multimedia in websites or gamification, should be used (Shaw et al., 2009; Clarke, 2013; Gjertsen et al., 2017). Web-based training has become very popular in delivering content and managing learners’ progress.

A study by Li et al. (2019) showed that employees who were more aware of their company’s information security policy and procedures were better equipped to behave securely. A phishing audit performed by Aloul (2012) resulted in a reduction from 9% to 2% of people succumbing to phishing attacks after ISAT was done. Tschakert and Ngamsuriyaroj (2019) performed ISAT 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.

3.9 Summary

As discussed in this chapter, although ISAT does not completely mitigate insecure behaviour for all users, it does reduce the risk of insecure behaviour. A successful ISAT programme will enable employees to recognise a cybersecurity threat and act accordingly. Various frameworks have been created to assist organisations to create an efficient ISAT programme. It was also indicated that ISAT must be relevant to the organisation and be a good cultural fit.

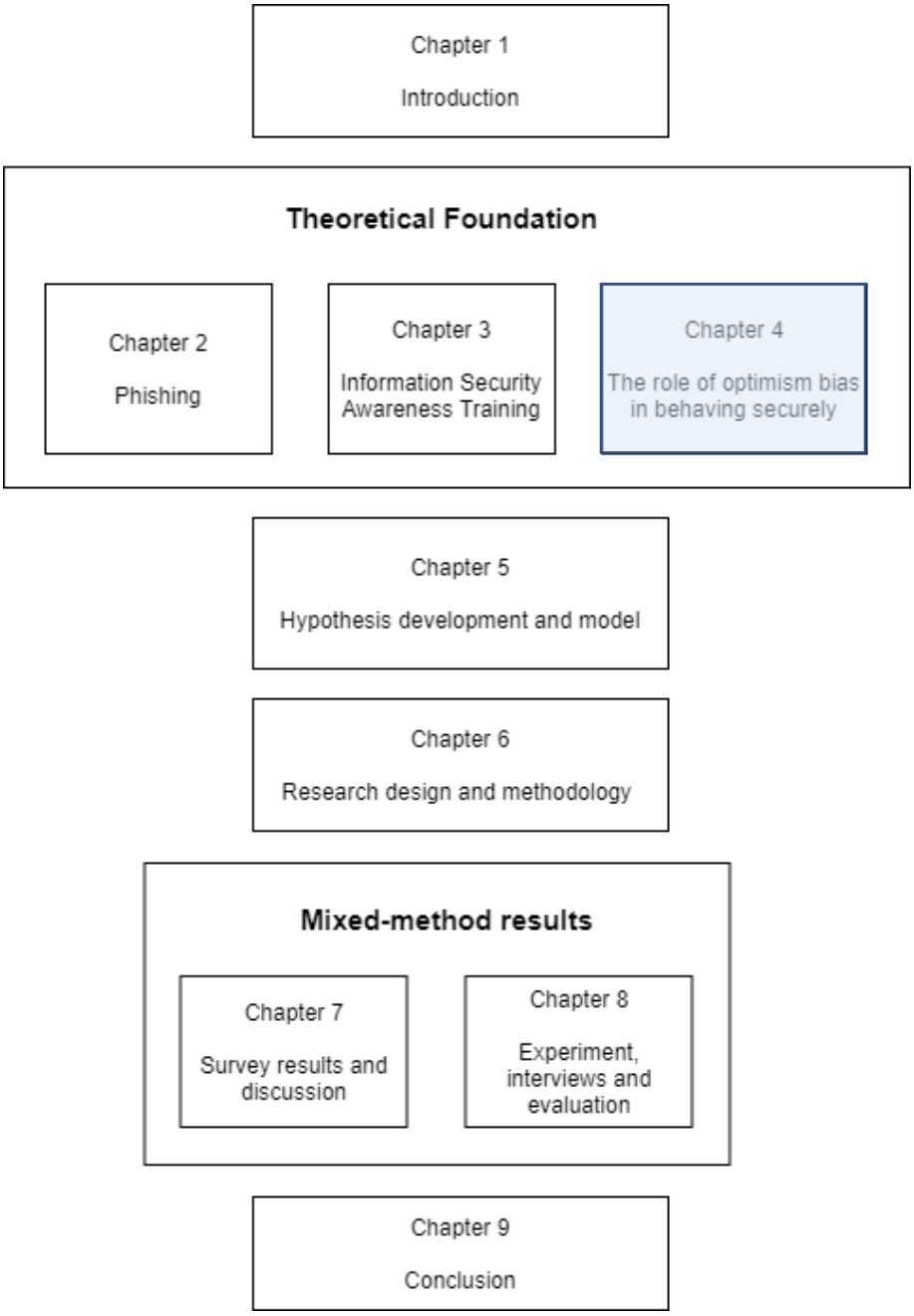
Although there is no statistical proof that certain learning styles yield better results, it is important for employees to make an emotional connection to the material. Therefore, training programmes need to cater for all learning styles in order to foster a connection with the employee so that knowledge can be acquired and retained.

Most of the learning that employees do is self-directed, as they need to take responsibility for their own learning. However, to protect the organisation's information assets, organisations have a responsibility to ensure that their employees are adequately trained in information security. ISAT is not a once-off exercise. It needs to be adapted as technology changes. Management should strive to create more dialogue around cybersecurity and praise good security behaviour.

Many countries expect their organisations and citizens to comply with privacy regulations, for example through laws such as the GDPR and POPIA. The implementation of cybersecurity frameworks could assist the organisation in assessing its compliance with such regulations, as the implementation of cybersecurity frameworks will result in a better security culture.

CHAPTER 4

THE ROLE OF OPTIMISM BIAS IN BEHAVING SECURELY



4. THE ROLE OF OPTIMISM BIAS IN BEHAVING SECURELY

4.1 Introduction

Phishing was discussed in detail in Chapter 2 where it was established that phishing is still a relevant information security risk today. Although the intention of employees is to behave securely, they often do not. In the previous chapter, we discussed the effect of ISAT on secure behaviour. Although it has a positive effect in reducing insecure behaviour, it does not eradicate it completely. Various information security frameworks were reviewed which should be used to ensure that the content of ISAT is relevant. The different learning styles people prefer were discussed to ensure that all employees are able to understand and internalise the content. However, the decision to behave in a certain way consists of many elements.

In answering the research question about how ISAT needs to improve ("How should information security awareness training initiatives improve to overcome phishing in susceptible individuals employed by a mid-size financial services company?"), it is vital to understand which employees are deemed more susceptible to phishing attacks. To better understand human behaviour, this study will consider the effect of certain human traits and cognitive biases. Therefore, this chapter will describe additional factors that could influence behaviour. One such factor that influences decision-making is *optimism bias (OB)*. When people do not expect bad things to happen to them, they believe their behaviour will not have negative consequences. They may, therefore, behave insecurely, not understanding the risk they are taking or the consequences for themselves or the organisation.

Different people have different outlooks on life. This results in their *attitude* being positively or negatively associated with a certain behaviour. People often do not see their own vulnerabilities and therefore need to be made aware of their negative attitudes towards certain behaviours in order to change.

Trust goes together with attitude in influencing behaviour. Trust will be studied from a human-to-human relationship and a human-to-systems perspective. Focus will be

placed on the influence trust has on secure behaviour and specifically the effect of trust in the workplace where employees place their trust in security controls implemented by the IT department.

In the context of this study, attitude, trust, awareness and OB will be tested as constructs of the theory of planned behaviour (TPB). These constructs have an influence on the intention to behave in a certain way, which results in actual behaviour.

4.2 Optimism bias

4.2.1 Definition

OB is a well-known cognitive bias in the social sciences and is one of the most reported findings influencing results in social-reasoning and decision-making studies (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). There is evidence that people believe they have a better than average chance of experiencing a variety of desirable future outcomes, whether good or negative (Weinstein, 1980). This phenomenon is known as “unrealistic” optimism or “optimistic bias” (Weinstein, 1980). Houston et al. (2012) 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.

Examples of OB can be found with regard to driving skills, where drivers have been found to be optimistically biased. Optimistic people have a tendency to believe that they are better and safer drivers than other people (Svenson, 1981). Furthermore, in a study by Svenson, Fischhoff and MacGregor (1985), the majority of their participants stated that their risk of being involved in a traffic accident was lower than that of others. Both expert and novice drivers believed they had superior driving ability, indicating that professionals had a tendency to overestimate their own abilities (De Craen et al., 2011). Other studies included the likelihood of developing skin cancer or lung cancer from smoking and found that people showed OB in rating their own risk (Brown and Imber, 2003; Weinstein, Marcus and Moser, 2005). In short, the results show that people with an OB tend to believe that their future looks much brighter than for people in general.

It is important at this point to clarify the difference between unrealistic optimism and optimism, also known as dispositional optimism. Dispositional optimism is viewed as a personality trait that people exhibit to varying degrees (Jefferson, Bortolotti and Kuzmanovic, 2017). Roughly defined, it is a universal inclination to expect positive outcomes (Carver, Scheier and Segerstrom, 2010). This expectation does not have to be unrealistic. The Life Orientation Test is used to measure a general positive outlook rather than expectations about certain life events (Scheier, Carver and Bridges, 1994). However, people may be unrealistically optimistic about certain potential circumstances in the future and not optimistic about others (Shepperd, Ouellette and Fernandez, 1996). Thus, optimism generally refers to a positive outlook on one's personal life whereas unrealistic optimism has a uniquely comparative nature.

Unrealistic optimism can be classified into one of two broad categories: (1) *unrealistic absolute optimism* and (2) *unrealistic comparative optimism* (Shepperd, Pogge and Howell, 2017). Both types of unrealistic optimism can be applied both on 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, Pogge and Howell, 2017). Researchers have compared people's predictions about an event to the actual outcomes to assess unrealistic absolute optimism at the individual level (Shepperd, Pogge and Howell, 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 on college exams (Buehler, Griffin and Ross, 1994; Shepperd, Ouellette and Fernandez, 1996). 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, Pogge and Howell, 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%. Risk calculators could contain errors, for example when they are based on non-representative samples or fail to assess crucial variables (Allan, Garrison and McCormack, 2014; Bonner et al., 2014). When assessing unrealistic absolute optimism at the group level, it is impossible to tell whether a given person exhibits this trait. Nonetheless, researchers can argue that a group of people is unrealistically optimistic if the mean of their risk estimations is lower than the group's

actual risk as defined by some objective measure, such as base-rate data (Shepperd, Pogge and Howell, 2017).

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, Kim and Bae, 2014). Previous studies that explained comparative optimism 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, Sadeghian and Webb, 2002); and a sense of control, which is the belief that people are overconfident in their ability to control future events (Weinstein, 1980). Since comparative optimism results comes from comparing one's own risk with that of others, it is based on personal and target risk estimates (Helweg-Larsen and Shepperd, 2001). It is impossible to determine whether a given person is displaying unrealistic comparative optimism at the group level. 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, Pogge and Howell, 2017).

Blanco (2017) defines cognitive bias as "a systematic (that is, non-random and, thus, predictable) deviation from the rationality in judgment or decision making". Context, motivation, anticipation and experience all influence people's perceptions and cognitions, according to previous psychological studies (Robertson and Kesselheim, 2016; Blanco, 2017). People's perceptions and judgements have been proven to be influenced by factors unrelated to the information they have available. Nevertheless, our limited information processing capacity performs excellently, but it also contributes persistent flaws in decision-making (Simons and Chabris, 1999). Even so-called experts suffer from these "bias blind spots" (Pronin, Lin and Ross, 2002). People selectively focus on what they consider worthy of their attention and process it in a manner that matches any pre-existing knowledge or experience. This information processing is generally automatic and goes unnoticed by the individual. While such automaticity and efficiency are the foundations of competence, they have also been discovered to be a major source of bias (Robertson and Kesselheim, 2016). A good example to demonstrate this is the Müller-Lyer stimulus (see Figure 4.2). This is a simple visual illusion that shows how irrelevant information (the adornments – the arrows at the ends of the lines) can fool people's inferences, leading to systemic errors in perception (Howe

and Purves, 2005; Blanco, 2017). Line A appears to be shorter than line B, but in reality they are the same length. A comparable scenario may arise in a variety of domains and tasks, revealing cognitive biases not only in perception but also in reasoning, decision-making and memory. Cognitive bias usually manifests itself in the form of predictable irrational behaviour (because it is systematic). Many risky or problematic beliefs and behaviours, such as superstitions, pseudoscience, discrimination and poor consumer choices, have been linked to cognitive biases (Blanco, 2017).

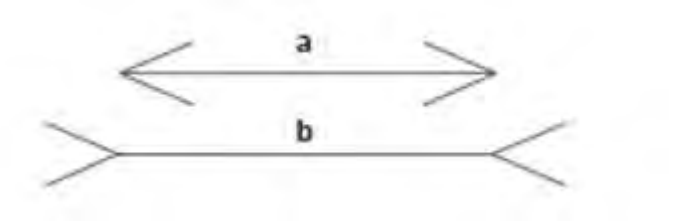


Figure 4.1 Müller-Lyer stimuli (adapted from Howe and Purves, 2005)

Although cognitive biases were conceptualised in 1974, little information security research has been linked to this topic (Tversky and Kahneman, 1986; Kießling, Hanka and Merli, 2021). The number of known cognitive biases is deemed to be between 150 and 180 with some overlap between the individual biases (Kisak, 2015). A study by Fleischmann et al. (2014) reviewed cognitive bias-related research, specifically in information systems, over a period of 20 years. They found that it would be worthwhile to further study information security in relation to cognitive biases. They were also concerned that the articles they reviewed merely defined cognitive biases and did not offer any solution to mitigate the associated risks or changed behaviour. According to Keet (2021), in information systems research, cognitive biases are classified according to the dimension of interest. Examples of these dimensions include type of task (estimation, decision, recall, etc.) for information visualisation, software engineering knowledge area (e.g. design, testing, management) and cognitive styles in ontology building. Lately, there has been a lot of interest in bias in IT systems, especially with the building of models using machine learning (Keet, 2021).

Kießling, Hanka and Merli (2021) reviewed current publications to form an opinion on which cognitive biases should be studied in conjunction with information security. They identified the following biases that should be overcome:

(1) *Affect bias*. When it comes to risks and expense, people tend to underestimate these when they are linked to things they enjoy and overestimate them when they are associated with things they dislike.

(2) *Anchoring bias*. What people notice first becomes a powerful anchor, which has an impact on future thoughts.
(3) *Confirmation bias*. People are more likely to believe information that confirms their pre-existing beliefs; therefore, they go out of their way to find it. Humans dislike being proven wrong because the brain interprets this as physical discomfort.
(4) *Optimism bias (OB)*. The OB causes a human to think that they are less at risk of suffering a negative occurrence compared to others.
(5) *Status quo bias*. As a starting point, the current status quo is used. Any deviation from the status quo is regarded as a loss. Only when there is a strong enough motivation to act can human behaviour change.

Kießling, Hanka and Merli (2021) also defined a set of cognitive biases that should be used to change behaviour through the use of ISAT. These include the following:

(1) *Anthropomorphism bias*. The assignment of human characteristics, emotions or intentions to nonhuman entities has the potential to influence behaviour. Anthropomorphised objects are rated higher by humans.
(2) *Availability bias*. In every decision-making process, information that is easily recalled is given more weight; for example, recent occurrences and vivid recollections are simpler to recall. That's why people pay more attention to recent threats, especially when they are linked to emotional stories, and ignore data.
(3) *Bandwagon effect*. Individual adoption of a behaviour is more likely when the proportion of people who have previously done so increases.
(4) *Humour effect*. Items that are funny are easier to recall than those that are not.
(5) *Picture superiority effect*. When information is given visually rather than in writing, it is significantly more likely to be recalled. Interestingly, Kießling, Hanka and Merli (2021) mention the need to overcome OB via the creation of workshops and simulation exercises to demonstrate to the overly optimistic that security threats could also happen to them.

Other studies have considered phishing attacks that take advantage of cognitive biases such as *priming* and *confirmation bias* (Thomas and Mantri, 2015). Priming creates conscious and subconscious trust associations that can be leveraged, such as the look and feel of a business website. Confirmation bias is more conceptual and subjective and refers to the idea that ‘if all you have is a hammer, everything looks like a nail’; for example a socially designed Trojan sent by a compromised but trusted acquaintance. Thus, patterns of security, or the lack thereof, are ultimately a mental

state; to address this fundamentally, it must be reduced to patterns recognisable in human cognitive biases (Thomas and Mantri, 2015). Schwind and Buder (2012) investigated how learners using computer systems experienced the effects of (1) *confirmation bias* when people prefer to select information that agrees with their previous perspectives, and (2) *evaluation bias*, when people think the previous knowledge they have gained is better than the information they are presented with. Schwind and Buder (2012) found that confirmation bias deters people from taking opposing information into consideration. Hale and Gamble (2019) found the extent to which confirmation bias was prevalent among security experts surprising. This behaviour could also be linked to overconfidence, especially when someone considers themselves an expert in a field. Park and Oh (2016) researched the following cognitive biases:

- *Affect heuristic*. Occurs when people take a mental shortcut to make judgements and decisions hesitantly based on affective impressions; in other words, the decision is based on affect rather than rational judgement.
- *Goal framing*. Arises when alternative framing of contextually similar information produces different decisions. People may see an outcome as a gain or a loss, which leads to different reactions.
- *Optimism bias*. This bias influences the intention to behave securely.

Anderson et al. (2015) focused on *repetition suppression bias* where users ignore security warning messages. They observed how habituation is developed in response to security warnings. After seeing a warning once there was a drop in visual processing, and after seeing the same warning 13 times there was a significant drop. People therefore easily form the habit of clicking on warning messages without reading them.

From the previous research mentioned above, it is clear that cognitive biases influence the way people use IT systems and therefore behaviour. The focus of this study therefore is on OB, as people are generally seen as hopeful and optimistic (Dolinski et al., 2022), and do not expect to experience a security incident. Since most people are deemed to be optimistic, this type of bias would yield a larger population than studying other cognitive biases (Weinstein, 1980).

4.2.2 Measurement of unrealistic optimism

Optimism bias can be measured in two ways: directly and indirectly (Fromm, 2005, p.11). When the direct method is used, the respondent is asked to rate their own risk: is it lower, higher, or equal to that of their peers or the general population? The indirect method, on the other hand, requires separate estimates of personal and general risk.

The use of a peer group as a comparison target is a common approach in optimism bias research. For example, a sample of college students may be asked to compare their own risk to that of an average student of their age and gender at their college (Weinstein, 1980). According to research, comparison targets that are psychologically close to the respondent reduce the level of optimism bias (Hoorens, 1994). When compared to friends or family or a specific person within a group, the level of optimism bias is reduced (Klein and Weinstein, 1997). The reason given for this is that when the target is known or when one's own risk is assessed it is based on unique and personal information, whereas judgment made on other people's risk will be based on base rates and statistical information (Fromm, 2005).

The significance of the risk specificity has also been emphasised (Armor and Taylor, 2002). In their study on environmental risks, Hatfield and Job (2001) hypothesised that the level of optimism would increase when the risks were phrased in more specific and personally relevant terms. They asked respondents a general question, that is, to rate the risk of noise pollution, versus a specific question, that is, to rate the risk of suffering from psychological issues as a result of noise pollution. While no optimism bias was found for general environmental questions, risk decisions relating to specific consequences were optimistically biased.

Using the direct method to ensure that respondents rate their own risk compared to a known peer group might yield better results than using the indirect method where both personal and general risk estimates are required. In addition, general questions and ambiguous questions should be avoided. Questions should be specific and relevant to the respondent.

4.2.3 The influence of OB on behaviour

Although OB may improve self-esteem and motivation (Aue et al., 2021), the most prominent potential negative result is that it may lead to a less attractive individual future should people take unwarranted risks or fail to prepare for possible problems (Shepperd, Pogge and Howell, 2017). Previous research has found that people are less likely to take health precautions such as health check-ups or stopping risky health behaviours if they believe their risk is low (Janz and Becker, 1984; Floyd, Prentice-Dunn and Rogers, 2000). Thus, unrealistic optimism may result in less health-encouraging behaviours or more risky behaviours to the extent that they reflect the view that one is not at risk (Shepperd, Pogge and Howell, 2017).

In general, people are more optimistic about future events or events for which no formal date has been set (Kinari, 2016). Overconfidence is a separate human trait that is closely linked to OB. Moore and Healy (2008) divide overconfidence into three categories: (1) *overestimation* of one's own successes, (2) *overplacing* one's execution compared to others (assuming better-than-average execution where in fact it is not), and (3) *overprecision*, which refers to extreme confidence in the correctness of one's perceptions as displayed in one's attitudes. According to Plous (1993), overconfidence is the most common and potentially catastrophic issue in judgement and decision-making. Bracha and Brown (2012) consider two systems of reasoning: the *rational* process, which chooses a course of action, and the *emotional* process, which shapes risk perception and is usually optimistically skewed. To arrive at a conclusion, the two processes interact.

Furthermore, Reisberg (2001) refers to different brain functions that specialise in various activities. The amygdala, for example, is linked to feelings, while the prefrontal cortex is linked to higher-order, deliberate thought. Psychological research distinguishes between analytical versus intuitive processing, and between deliberate versus emotional processing (Chaiken and Trope, 1999). Gray et al. (2002) state that “at some point of processing, functional specialisation is lost, and emotion and cognition conjointly and equally contribute to the control of thought and behaviour”. Pessoa (2008) confirms that “emotions and cognition not only strongly interact in the brain, but [that] they are often integrated so that they jointly contribute to behaviour”. Under risk and uncertainty, decision-making may be modelled as a deliberate mechanism that selects the best course of action, as well as an emotional cognitive process that shapes risk perception

(Kahneman, 2003). The emotional mechanism shapes risk perception by balancing two opposing impulses: (1) affective motivation, which is the urge to maintain a favourable personal risk perception, i.e. optimism; and (2) a desire for precision or correctness in doing the right thing. This suggests that motivated reasoning is a psychological mechanism in terms of which one's beliefs are motivated by emotional goals, resulting in psychological biases such as OB (Kunda, 1990).

Importantly, empirical evidence links OB to behaviour. For example, White et al. (2011) found that young drivers with OB 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; this despite the fact that road accidents are the leading cause of death and injury among those younger than 25 in First World countries. Interestingly, 68% of new business owners believe their venture is more likely to succeed than that of their competitors, despite the fact that only 50% of new businesses survive for more than three years (Baker, Ruback and Wurgler, 2006). OB therefore has a direct influence on decision-making.

4.2.4 The influence of OB on secure behaviour

While there are many studies about OB in the context of psychology, there is very little research linking OB to ISAT and secure behaviour. A study performed by Cho et al. (2010) considered the influence of OB 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 et al. (2014) also studied the effect of OB 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. They may disregard preventative care measures such as patching because they believe they will not be affected (Pfleeger and Caputo, 2012). Interestingly, this is not only true for the general population; unrealistically optimistic information security executives also believe that they are less vulnerable than others and have better skills to control threats to information security (Rhee, Ryu and Kim, 2011).

Optimistic beliefs are, to a certain point, susceptible to evidence (Jefferson, Bortolotti and Kuzmanovic, 2017). 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 and making them more accountable for the accuracy of their predictions (Sedikides et al., 2002; Barberia et al., 2013). Chapter 3 discussed the positive effect of ISAT on increasing secure behaviour. It was noted that awareness alone is not enough to eradicate insecure behaviour. It seems that those who succumb to phishing attacks should be held accountable for their actions by making them aware that they hold inaccurate predictions and therefore are susceptible to phishing attacks.

4.2.5 The influence of OB on attitude

As discussed, OB 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. A phishing email may be seen as merely another request to be complied with, either through fear or reward. As we have seen, emotional decisions often yield incorrect results (Norris and Brookes, 2021). Logical or rational thinking is often replaced in the moment by the belief that complying with the phishing email is in one's best interests.

The current findings indicate that optimism bias (OB) and the illusion of control are widespread phenomena (Rhee, Ryu and Kim, 2011). Perceptions, whether true and sensible or not, are critical aspects in managing risk realities (Baron, Hershey and Kunreuther, 2000). A person's attitude (belief) toward an object influences the overall pattern of his 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 information security, we may argue that people may see little point in changing their current behaviour and have less motivation to be attentive to potential threats (Rhee, Ryu and Kim, 2011).

4.2.6 The influence of OB on trust

Since trust is based on positive expectations of others (see Section 4.4.1) this can increase the outlook for trust in the good disposition of others (Andersson, 2012). In addition, an optimist is generally more forgiving. Marsh (1994) argues that an optimist is likely to be one whose trust in others is high, and is inflexible in a downward direction (see Figure 4.2). Thus, following his being abused by another, his trust in that other will not reduce by too much. In contrast, the amount of trust a pessimist has in others will be relatively uncompromising in an upwards direction, and a small manipulation by another will result in extreme loss of trust (Marsh, 1994). Hence, if an unrealistic optimist's trust is not reduced through a previous security breach it could lead to further insecure behaviour.

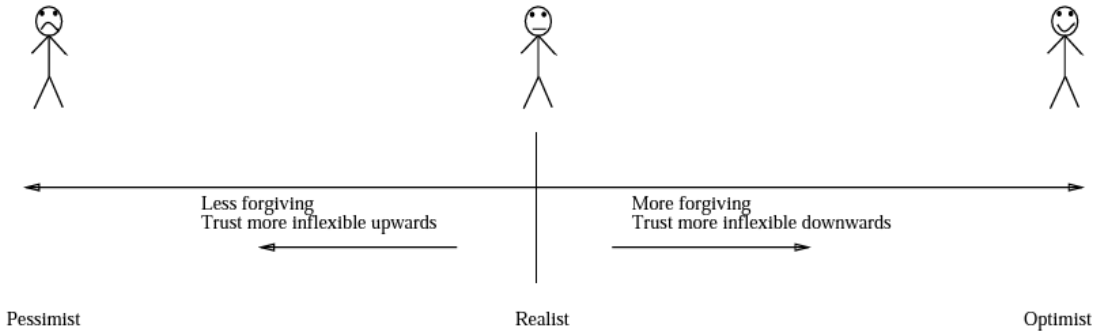


Figure 4.2 Spectrum of realism (Marsh, 1994)

4.3 Attitude

4.3.1 Definition

The psychologist Herbert Spencer first used the term ‘attitude’ in 1862 (Spencer, 1867). Attitude has been defined as a way of thinking, feeling or acting that represents a mental or emotional condition (McLeod, 2018). The characteristic property of attitude, according to Peterson and Thurstone (1932), is an evaluative or emotional inclination toward an object, concept or issue. Someone is said to have a bad attitude if they have a negative attitude towards ISAT or information security, while a positive attitude could create a perfect platform for secure behaviour. Attitude can be seen as a catalyst driving behaviour; a mental filter through which people experience the world. Some people perceive the world through an optimistic lens (the glass is half full), while others experience life through a pessimistic lens (the glass is half empty) (Keller, 2001).

4.3.2 Theories of attitude

Attitude is incorporated in several theories. The value-belief-norm theory states that the role of individuals’ influence on their own behaviour is crucial and includes employees’ beliefs, attitudes and awareness (Stern et al., 1999). The theory provides a framework for investigating normative factors that promote sustainable attitudes and behaviour. Ajzen’s (1991) theory of planned behaviour (TPB) states that the intention to perform a specific behaviour is strongly influenced by attitude, subjective norms (trust placed in the IT department) and perceived behavioural control (OB and ISAT). He states that attitude is an independent element of intention referring to the degree that an individual has a favourable or unfavourable assessment or view of the behaviour in question. The theories indicate that attitude influences behaviour. In the context of this study, attitude is defined as the willingness to comply with all security requirements.

4.3.3 Attitude in the context of secure behaviour

An individual's attitude towards information security could result in them behaving securely or insecurely. If they are of the opinion that nothing bad will happen to them regardless of the online actions they take and the websites they visit, the chances are good that they will fall victim to an attack. A positive attitude towards information security should result in more secure behaviour as the individual should have a better understanding of the risk.

Attitude is used in many studies relating to information security. For example, Guhr et al. (2019) suggest that attitude should be investigated specifically for leaders as it plays a role in secure behaviour. Unfortunately, their study did not consider the attitudes, motivations and intentions of employees. To fully understand the effect of leadership style on information security it is necessary to contrast leadership findings in this regard with those relating to employees. Herath et al. (2014) found that attitude had a significant effect on the use of an email identification service to behave securely, while Lowry and Moody (2015) found that attitude influenced the behaviour to comply with organisational information security policies. When individuals 'buy into' and take ownership of the security tools, policies and procedures, they generally comply and behave more securely. In information security research, links between attitude and intentions have been studied extensively; whereas some researchers have focused on positive attitudes and positive compliance (e.g. Bulgurcu et al., 2010), others have focused on negative attitudes and noncompliance (e.g. Hu et al., 2011). A study done by Nunes, Antunes and Silva (2021) in a healthcare organisation confirmed that there is a correlation between attitude and risky cybersecurity behaviour among employees, while Sas et al.'s (2021) study on the relationship between attitude and physical security came to the same conclusion.

Other examples include the study of Turkanović and Polančič (2013) which explains that attitude towards privacy and security entails moving from an unaware state to greater awareness where people try to protect themselves as best as they can. The aware category consists of people who are aware of the security and privacy risks and who have a positive attitude towards information security. In addition, a study done by Tsohou et al. (2015) confirms that biases affecting personal beliefs and attitudes influence the intention to behave securely and, therefore, ISAT needs to be adapted to address these attitudes.

Understanding how to change and influence attitude positively, especially through awareness, could lead to more secure behaviour.

4.3.4 Changes in and influences on attitude

Attitudes form and change within three contexts: (1) the person (i.e. attitude can change in connection to values, general goals and emotions); (2) social relationships (i.e. when attitude is changed based on persuasive messages, social media and culture); and (3) sociohistorical (i.e. when unique economic and climatic occurrences influence attitude) (Albarracin and Shavitt, 2018). A person's attitude may be influenced internally, by themselves, if they come to a new realisation about a concept or object. It could also be influenced through peer pressure in a social environment or in a work situation by a superior where the employee feels the need to comply with authority. Weber (1978) relates authority to institutionalised command and discipline as a source of power. Normal employee behaviour would be to comply with instructions, thus not opening themselves to a disciplinary procedure. Some people learn from history and form their attitude based on influential past events. Despite considering these factors, some employees keep behaving insecurely. Something motivates them to behave in this manner.

In the fast-paced, results-driven world we live in, an employee's attitude is driven by the *benefit of compliance*, the *cost of compliance* and the *cost of noncompliance* (Bulgurcu, Cavusoglu and Benbasat, 2010). An employee will take all of these 'costs' into account when making a decision. Sometimes it might even seem of value to them to follow the road of noncompliance just to complete a task. Since employees are often measured by predefined key performance indicators (KPIs) that are linked to their remuneration, they might be willing to take a risk. KPIs have a strong influence on behaviour but are often focused on generating revenue rather than mitigating risk (Hristov and Chirico, 2019).

Brannon et al. (2019) found that attitude towards "focal objects" was supplemented by equivalent changes in attitude towards "proximally related objects". Accordingly, this should be considered when considering how to change attitudes. Similar objects or topics should be grouped together to maximise the effectiveness of attitude change. For example, employees have to comply with all the policies of an organisation. Thus,

changing their attitude towards policies could also change their attitude towards the information security policy. In turn, this could lead to a change in behaviour, for example not taking risks and behaving more securely.

4.3.5 Previous attitude studies and outcomes

Previous research found that user job attitudes, namely job involvement and intrinsic involvement, affected user behaviour (Liberman et al., 2011). *Job involvement* is the degree to which one is cognitively preoccupied with, interested in, and obsessed with one's current work. *Intrinsic involvement* is the conviction that the user's work is valuable and that his or her efforts are making a significant contribution to the organisation. High degrees of job and intrinsic involvement may lead to goal-oriented conduct to complete work at all costs. Therefore, results-driven employees are more prone to falling victim to phishing attacks since they are likely to comply with incoming requests by making hasty decisions (Mamonov and Benbunan-Fich, 2018). Studies also confirm that employee attitudes are influenced by intrinsic motivation (Cho and Perry, 2012). People are intrinsically driven when they seek pleasure, interest, fulfilment of curiosity, self-expression, or a new challenge in their work (Cho and Perry, 2012).

Furthermore, disengaged employees, as a result of a bad attitude, often display counterproductive behaviour. For example, an ’I don’t care’ attitude resulting from an employee feeling undervalued and possibly resentful could result in insecure behaviour (Liberman et al., 2011). A deeper understanding is therefore required to address the root cause of employee disengagement or bad attitude, as failure to resolve this could lead to employment termination and/or damage to the organisation. In addition, lack of awareness, carelessness and apathy create a negative attitude towards information security making an employee vulnerable to a phishing attack (Safa, Von Solms and Furnell, 2016). Safa et al. (2018) conducted a study on insider threat behaviour and found that employees who accepted the organisational policies and procedures and had a positive attitude towards information security were less likely to behave insecurely. A happy, inspired and motivated employee (positive attitude) will realise that behaving securely is in the best interests of all stakeholders (Lee et al., 2016).

Another factor influencing users’ attitudes to information security is their reliance on the IT department to protect them through the implementation of security tools in the

organisation. This can lead to a careless attitude, resulting in users who do not take ownership of their own actions. Moreover, unrealistic optimists often assume that bad things will not happen to them and therefore do not expect to be part of, or the cause of, a security breach.

In the next section we will discuss trust in more detail, as the reliance placed on the security tools in the organisation could lead to insecure behaviour.

4.4 Trust

4.4.1 Definition

Trust is defined as the inclination to “accept risk und vulnerability based upon positive expectations of the intentions or behaviours of another” (Rousseau et al., 1998) and might be considered the thread that binds our social universe together (Weiss et al., 2021). When our personal results are dependent on others, our expectations of their benevolent versus malevolent intentions toward us have a significant impact on our behaviour and, as a result, on our interpersonal interactions (Rotter, 1967; Weiss et al., 2021). Thus, trust is necessary for the functioning of social ties, from close friendships to interactions with strangers (Rempel, Holmes and Zanna, 1985). Trust appears to be especially important in interdependent circumstances when there is a conflict of interest. Because disagreement between preferred outcomes entails additional risk and vulnerability, trusting the other's good intentions is more important in such circumstances (Weiss et al., 2021).

Trustworthiness is a prerequisite for trust. Scholars see trust as a managerial resource and have highlighted the components of trustworthiness as competence, consistency, fairness, integrity, loyalty, openness, receptivity, compassion, and value congruence, as they have grown to see trust as a managerial resource (Butler, 1991; Sitkin and Roth, 1993; Cho and Perry, 2012; Jiang and Probst, 2015). Since trust guides our relationships, it has a strong influence on behaviour.

In the context of this study, the concept of trust can be defined as the trust that employees, in an organisation, place in the technical security controls implemented by their IT department. This could result in an attitude of false security, believing they are

fully protected when they are not. Blindly trusting security controls that could fail could lead to a successful phishing attack (Blythe and Coventry, 2018).

4.4.2 The influence of trust on behaviour

Trust is conceptualised in terms of three approaches: (1) a focus on trustee characteristics (i.e. whether or not the other person can be trusted); (2) a focus on the relevant aspects of the trustor–trustee relationship (i.e. how well do the parties know each other and will they meet again?); and (3) a focus on the individual characteristics of the trustor (i.e. how stable do they seem and do they have a willingness to trust others) (Weiss et al., 2021). Figure 4.3 conceptualises the relationships between the three approaches and the effect they have on behaviour.

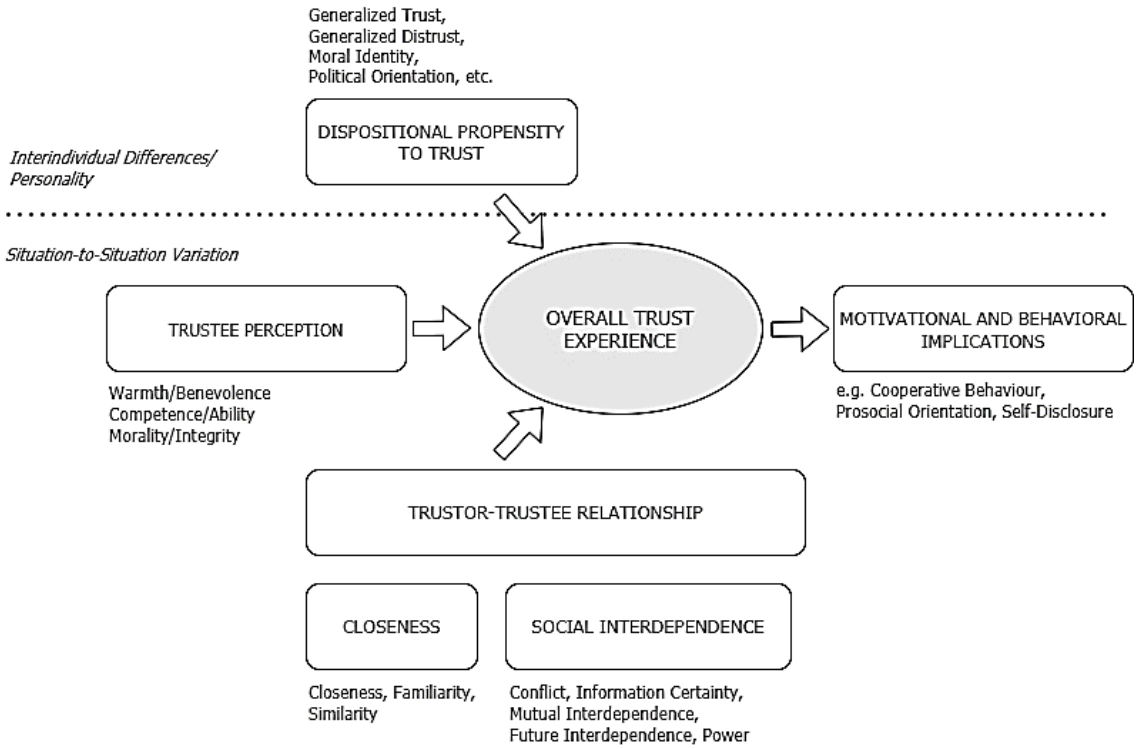


Figure 4.3 Overview of the variables potentially influencing the experience of trust (Weiss et al., 2021)

The *trustee perception approach* to trust is based on the notion that trustors condition their trust on their view of the other person's trustworthiness. The assumption is that

trustors form an opinion of trustworthiness based on personal cues and previous interaction (Weiss et al., 2021). Although these opinions could be wrong, the trustee will act based on their intuition.

The *relational approach* (trustor and trustee) attempts to discover the core aspects of the trustor–trustee relationship, as well as the larger context that may influence trust experiences. This relates to social closeness and suggests that trust develops over time (Weiss et al., 2021). It is easier for people to trust if there is a strong relationship between the various parties. This study was conducted in a financial services organisation where the IT department had implemented various technical security controls. The relationship between trustor and trustee in this case was of such a nature that the employees believed they were protected. For example, employees often found that firewalls prevented them from accessing certain folders or websites, or were reminded that an email was from an external source and should be treated with caution. In addition, endpoint protection (e.g. anti-malware and anti-virus products) prohibited the use of suspicious files. Such interventions create the illusion that employees are in a fully protected environment. However, trust in this instance is misguided.

The *dispositional approach* to trust focuses on the trustor's predisposition to trust as a personality trait (Weiss et al., 2021). It can be described as “a belief in the benevolence of human nature in general and thus is not limited to particular objects” (Yamagishi et al., 2015). Overly optimistic people see only the best in others and have a natural inclination to trust (*optimistic trust effect*) (Wilson and Darke, 2012).

Thus, trust between people relies on human behaviour and traits to gauge whether someone can be trusted. People often use intuition to decide whether to trust someone or not and this is mostly based on previous experience (Weiss et al., 2021). However, trust in the context of information security, when dealing with systems, excludes some of the human interaction and therefore behavioural decisions are made differently.

4.4.3 Trust in the context of information systems and security

Trust in systems spans multiple areas; for example, the use of systems to do calculations, the integrity of a blockchain, trusting that electronic communications received are authentic, and finding a new business partner or a new dating partner online (Riegelsberger, Sasse and McCarthy, 2005; Lankton, Mcknight and Tripp, 2015; Beck

et al., 2017). Trust in technology refers to the trust placed in a technological object and differs from trust in people as it refers to a human-to-technology relationship rather than a ahuman-to-human relationship (Lankton, Mcknight and Tripp, 2015). Lankton, Mcknight and Tripp (2015) compared human-like trusting beliefs with system-like trusting beliefs (see Table 4.1). They found that if the technology was low in humanness, system-like trust constructs (reliability, functionality, helpfulness) had a stronger influence on outcomes, whereas human-like trust constructs (integrity, ability, competence, benevolence) had a stronger influence if the technology was high in humanness. People therefore try to ascribe humanness to systems in order to trust them or not. The employees trust the IT department's integrity, ability, competence and benevolence. Therefore, they trust the security controls the department implements as they believe in their reliability, functionality and helpfulness.

Table 4.1 Major trust in technology constructs used (Lankton, Mcknight and Tripp, 2015)

Human-like trusting beliefs	**Corresponding system-like trusting beliefs**
Integrity: the belief that a trustee adheres to a set of principles that the trustor finds acceptable.	**Reliability**: the belief that the specific technology will consistently operate properly.
Ability: the belief that the trustee has a group of skills, competencies and characteristics that enable them to have influence within some specific domain. **Competence**: the belief that the trustee has the ability to do what the trustor needs to have done.	**Functionality**: the belief that the specific technology has the capability, functions or features to do for one what one needs to be done.
Benevolence: the belief that the trustee will want to do good by the trustor, aside from an egocentric profit motive.	**Helpfulness**: the belief that the specific technology provides adequate and responsive help for users.

Many studies indicate that trust has a significant influence on secure behaviour (Komiak and Benbasat, 2006; Shropshire, Warkentin and Sharma, 2015; Kearney and Kruger, 2016; Sultan et al., 2020). Hong et al. (2013) found that less trusting individuals deleted not only phishing emails but also legitimate emails, thus indicating the significance effect trust has on secure behaviour. 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. Therefore, phishers who are skilled at instilling a sense of trust through the use of aesthetic cues are generally successful in their attacks. To create trust they use techniques such as personalisation or familiarisation, for example by mentioning the victim's name and/or contact details (Blythe et al., 2011).

This discussion was about how people trust systems. In the context of this study, it is important to understand whether there is a difference in the way employees trust work systems versus the trust they place in their home systems. They might not trust their home system security controls as they set them up and do not consider themselves experts, whereas they implicitly trust the security controls implemented by their IT department.

4.4.4 The influence of trust in the workplace on information security

Most organisations create policies and procedures to guide employees to behave in a certain way. The information security policy is normally one of these (Hu et al., 2012). Employees trust that skilled people are employed to create these policies and procedures. They also believe that a proper risk assessment has been done to implement mitigating controls (Lowry and Moody, 2015; D'Arcy and Lowry, 2019).

Some of these mitigating controls could be the security controls implemented by the IT department. Employees seem to trust these security controls and believe they will protect them regardless of their behaviour (Butavicius et al., 2020). This attitude could, however, lead to a security incident. Security tools cannot cater for all threats, especially zero-day vulnerabilities (Blythe and Coventry, 2018; Butavicius et al., 2020). Accountability for system use, whether that use is secure or insecure, cannot be abdicated. ISAT should provide examples of scenarios where the security tools might fail to prevent a breach. This would give users a better understanding of what is meant

by insecure or risky behaviour. User perceptions regarding the risks involved in using the organisation's IT systems should be calibrated to minimise the overconfidence typically placed in the security controls that have been implemented.

Employees generally trust their managers and believe that the controls and measures implemented in the organisation are for the greater good. Hu et al. (2012) found that there is a direct relationship between the behaviour of management and that of the employees. If a manager ignores the information security policy and behaves insecurely, their subordinates will behave in the same way. It is therefore vital to stress that information security is everyone's responsibility. Subordinates should feel safe in correcting anyone's insecure behaviour, even their manager's.

Owing to the mitigating controls put in place in the work environment, and the governance implemented through the use of policies and procedures, employees may easily believe that it is not possible for them to behave insecurely. Therefore, they could have an overly optimistic outlook.

4.5 Summary

Since human behaviour plays a critical role in mitigating phishing susceptibility, this chapter focused on additional factors that could influence secure behaviour. The three factors discussed were OB, attitude and trust.

OB is known as a cognitive bias. It is found in people who are overly optimistic, believing that bad things will not happen to them. Because of this belief, they may act insecurely, not expecting any negative consequences for their actions. OB has a direct influence on behaviour. To combat OB, systems may be designed to convey threat impact and likelihood in ways that are relevant to people's real-world experiences (Pfleeger and Caputo, 2012). Although behaviour may be affected by various factors (as discussed above), this study sought to understand how the intention to behave securely is affected by the influence of ISAT and OB.

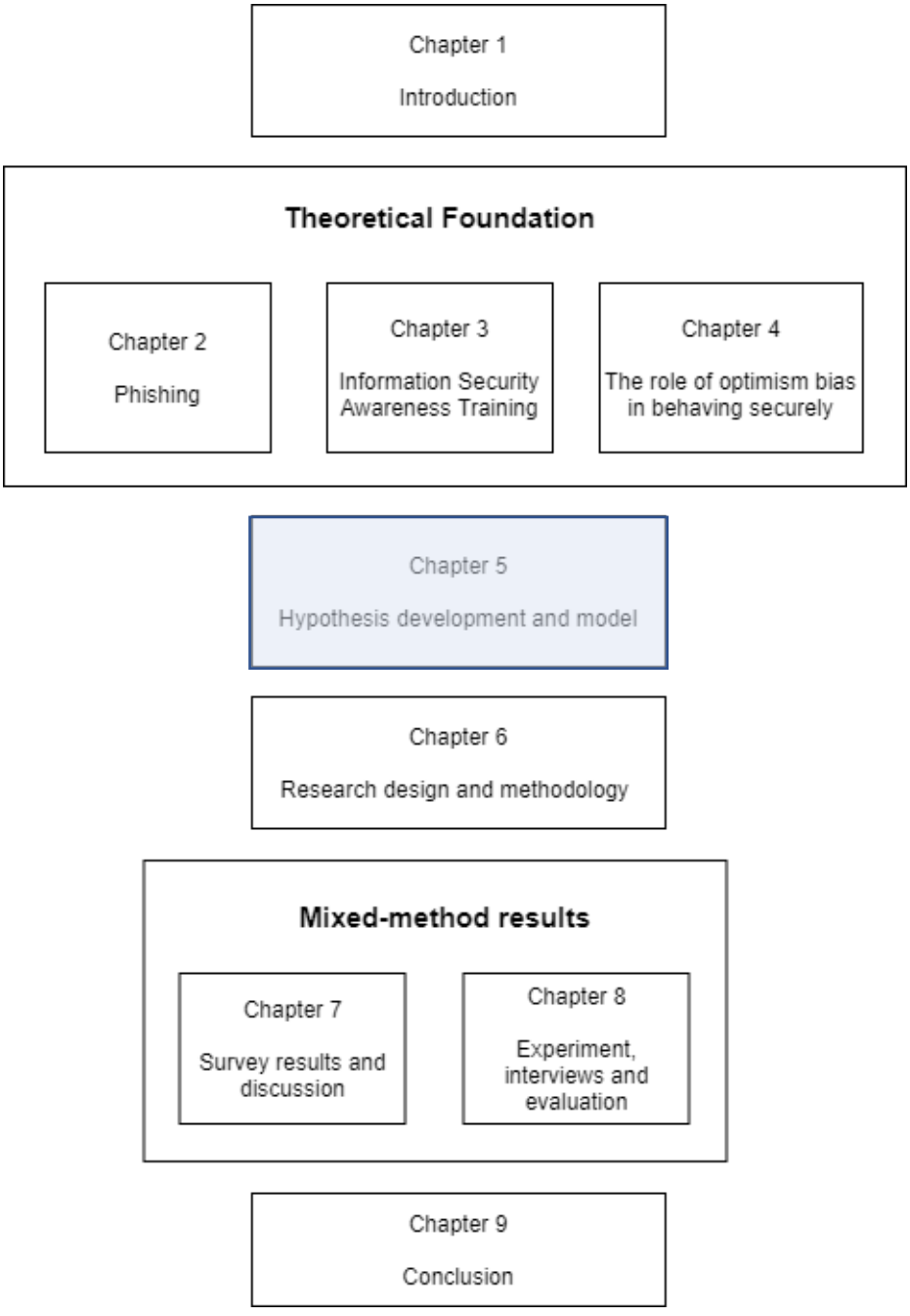
Attitude was described as a way of thinking that represents a mental or emotional condition. When a person makes emotional decisions, there is no room for logic. A positive attitude towards information security policies and procedures therefore results in more secure behaviour.

Trust was reviewed to understand when and how people decide to trust. At some point we all need to trust and often we are led by intuition to do so. The trust triangle consisting of the trustor, the trustee–trustor relationship and the characteristics of the trustor were discussed. There is a difference between trust in human relationships and trust in human-to-system relationships. These were contrasted and discussed in terms of integrity, ability, competence, benevolence versus reliability, functionality and helpfulness and it was found that people apply human attributes to systems to develop trust in using them.

This chapter concludes the literature chapters that established the theoretical foundation for the study. This theoretical foundation forms the starting point for investigating phishing susceptibility, considering factors such as attitude, awareness, trust and OB. The objective of this study is to create a model to identify employees at risk to phishing. The following chapter puts the aforementioned factors together and offers the theoretical model and hypotheses that accompany it.

CHAPTER 5

HYPOTHESIS DEVELOPMENT AND MODEL



5. HYPOTHESIS DEVELOPMENT AND MODEL

5.1 Introduction

This chapter explains the primary research question ("How should information security awareness training initiatives improve to overcome phishing in susceptible individuals employed by a mid-size financial services company?") and hypotheses that were developed to meet the research objective of the study. It presents the theoretical model for the study, which was derived from the literature review. The hypotheses for the research model, as well as their justifications, are formulated. As a result, the research questions are answered, and theoretical contribution of the proposed model is highlighted. The theory of planned behaviour (TPB) was used to better understand both the intention to behave securely and actual behaviour with regard to phishing, while considering the role of optimism bias (OB).

5.2 Theory development and hypothesis

The research process identified the behavioural factors related to phishing susceptibility. This assisted in defining the research question and led to the development of the model constructs. From the literature study the relationships between the constructs became clear thus assisting in formulating the hypotheses. A hypothesis may be defined as a supposition, a surmise, a presumption, a tentative explanation, or a likely cause (Runes, 1984). A hypothesis, according to Walker (1988), is a prediction based on theory, an informed estimate drawn from many assumptions that can be tested in a variety of ways, but is most typically connected with an experimental process. It may also be regarded as a suggestion put forward for evidence or discussion.

5.2.1 The theory of planned behaviour

The TPB was introduced in Chapter 1. According to the theory, various motivating factors influence the intention to behave in a certain way. From the literature study in Chapter 4, it was found that *attitude* influences the intention to behave securely, with a positive attitude towards information security in general resulting in more secure behaviour. This study proposes retaining this construct, as previous literature has confirmed that attitude plays a role in the workplace when it comes to secure behaviour.

The subjective norm construct was replaced with *trust,* since the survey participant population consists of employees from one organisation, thus creating a semi-controlled environment. Therefore, social pressure in relation to the performance or non-performance of a certain behaviour was not perceived as significant. Employees seem to trust that the security controls implemented by the IT department will protect them, regardless of what other employees intend to do or are actually doing. According to Butavicius et al. (2020), this way of thinking could lead to insecure behaviour.

Perceived behavioural control relates to the perception of difficulty in performing a certain behaviour and relies on one's confidence and skills in being able to perform this behaviour (Ajzen, 1991). This control was replaced with *awareness* as it is more relevant to this study. Employees who are more aware of cyberthreats, that is, those who can identify them, have more confidence in their abilities and skills. Accordingly, they should be in a position to correctly identify a phishing attack. The literature discussed in Chapter 3 made it clear that although awareness reduces the risk of being phished, it does not completely eradicate it. The level of awareness is therefore perceived as a control; the more aware someone is of cyberthreats, the more they should behave securely.

Table 5.1 Definitions of constructs adapted from the theory of planned behaviour

Construct	**Definition**
Attitude	The willingness to behave securely (Bulgurcu, Cavusoglu and Benbasat, 2010; Lowry and Moody, 2015)
Trust	Defined as benevolent trust where employees implicitly trust the security controls implemented by the IT department (D'Arcy and Lowry, 2019)
Awareness	The ability to discern security concerns in order to respond securely to threats (Tsohou, Karyda and Kokolakis, 2015; Parker and Flowerday, 2021)

Other studies using the TPB to understand secure behaviour when using information systems include the evaluation of the rank order of employees (Aurigemma and Mattson, 2017), addressing careless information security behaviour (Safa et al., 2015), how to create training and awareness methods for better ISA (Lebek et al., 2014) and investigating why ISA campaigns fail (Bada and Sasse, 2014). Shahbaznezhad et al. (2021) used the TPB to understand the factors that result in employees clicking on a phishing email.

Although *protection motivation theory* (PMT) is applied in many studies linked to secure behaviour, the primary purpose of the theory is to explain the impact of fear requests on attitudes and behaviours (Rogers, 1983). Fear can be triggered in response to a situation that is deemed dangerous and thus necessitates protective measures (Sikolia, Twitchell and Sagers, 2016). PMT posits that protective behaviour is achieved through threat and coping appraisals. Threat appraisals are influenced by perceived vulnerability and sensitivity to hazards, as well as the benefits associated with risky activities. Coping appraisals consist of the coping self-efficacy, response efficacy and response costs related to safe or adaptive activities. Coping self-efficacy is the belief that people can enact the protective behaviour because they have the skills and means to do so. Response efficacy refers to how well the protections work and response cost refers the cost associated with using the protection. PMT stresses interactions with the goal of changing people's minds, feelings, or behaviours, or persuading them (Sikolia, Twitchell and Sagers, 2016).

Previous studies using PMT and phishing have considered maladaptive behaviours based on fear and threats (Bax, McGill and Hobbs, 2021). Jansen and Van Schaik (2018) used PMT to determine the extent to which fear appeals can convince users to behave securely. Moody et al. (2018) found that fear in the context of health threats should be investigated to determine whether cybersecurity threats evoke the same fear. Phishing attacks are not only fear based, but often reward based (Fischer, Lea and Evans, 2013). Thus, in this study it was decided against the use of PMT, as unrealistically optimistic people do not think that bad things will happen to them and therefore do not focus on threats but rewards.

Another theory considered was cognitive evaluation theory (CET). CET is a sub-theory of self-determination theory. The theory emphasises competence and autonomy especially when investigating how external pressures affect self-rewards (Deci and Ryan, 1985; Christenson, Reschly and Wylie, 2012; Sikolia, Twitchell and Sagers, 2016). CET was developed to predict the negative effects of rewards on intrinsic motivation, particularly when the rewards were tangible (e.g. prizes or awards). According to CET, when rewards are interpreted as a tool for controlling behaviour, the recipients feel controlled, and their feelings of self-determination and autonomy decline (Siponen, Adam Mahmood and Pahnila, 2014). CET also predicts that rewards, particularly verbal rewards, will have a positive effect on intrinsic motivation. However, in order to increase employees' beliefs that they are skilled in completing a task, verbal rewards must be administered in a non-coercive manner (Siponen, Adam Mahmood and Pahnila, 2014). CET has been used in previous research to determine the adherence of employees to information security policies (Siponen, Adam Mahmood and Pahnila, 2014; Sikolia, Twitchell and Sagers, 2016). Since phishing is delivered via email and is therefore non-verbal and the tone normally not one of control, it was decided not to use CET in this study.

The TPB is suitable in the context of this 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, the TPB was considered to be more suitable than any other theory for the purposes of this study, which considers both the intention to behave securely and actual behaviour. Ultimately, it would appear that few in-depth studies have considered the effect of OB using the TPB in the context of secure behaviour.

5.3 Hypotheses

5.3.1 Attitude towards secure behaviour

The TPB, as discussed previously, makes it clear that attitude significantly influences the intention to behave in a certain manner. Within the context of information security, attitude refers to employees' beliefs about whether the behaviour is safe, unsafe, risky or not risky (Ameen et al., 2021). These beliefs about what is safe or unsafe are often shaped on the basis of their information security knowledge. This is demonstrated by the Knowledge-Attitude-Behaviour (KAB) model. The KAB model is used in the context of ISA and proposes that through improved knowledge of how to behave securely an employee's attitude improves, resulting in improved information security behaviour (Parsons et al., 2014; 2017). A study by Grassegger and Nedbal (2021) found that employees can resist social engineering attacks if they have a positive attitude towards ISA, thus resulting in the intention to behave more securely. Various studies have found that a positive attitude towards policies and procedures resulted in more secure behaviour as employees make the transition from an unaware state to a more aware state in respect of information security (Hu et al., 2012; Siponen, Adam Mahmood and Pahnila, 2014; Bélanger et al., 2017; D'Arcy and Lowry, 2019). Employees buy in to the security policies and procedures when they understand that these were created to help them protect themselves. This is usually achieved through ISAT, which helps the employee to understand the various security threats and consequences (Alshaikh, Maynard and Ahmad, 2021; Chowdhury, Katsikas and Gkioulos, 2022). Furthermore, employee attitudes are driven by the benefit of compliance, the cost of compliance and the cost of noncompliance. The amount of effort required to comply with policies is compared with the successful execution of daily tasks (Bulgurcu, Cavusoglu and Benbasat, 2010). Goal-oriented employees could be so focused on outcomes that they rush to complete a task and behave insecurely as they have a negative attitude towards information security.

In the context of this study, attitude is defined in relation to secure employee behaviour. The study proposes:

Hypothesis 1. *An employee's attitude towards information security is positively associated with the intention to behave securely.*

5.3.2 The behavioural influence of trust

People use various systems every day to perform tasks ranging from business to leisure. Accordingly, significant trust is placed in the accuracy and correctness of these systems. For example, people trust systems to run and manage their bank accounts, to protect their personal information, including their medical history, and to efficiently run their local infrastructure such as the water and electricity supply (Lowry et al., 2010; Lankton, Mcknight and Tripp, 2015; Dupont and Karpoff, 2020). The use of systems has become so pervasive in everyday life that often no thought is given to the accuracy or integrity provided by these systems, with people blatantly trusting their outcomes. However, not all people trust equally (Cha and Lee, 2021; Weiss et al., 2021); some are more sceptical than others. Previous studies found that those who are more sceptical not only deleted phishing emails but also legitimate ones (Gopavaram et al., 2021). The aim of this study is to understand how employees behave when knowing that security controls are implemented by their IT department. If employees blindly trust the controls implemented, this could lead to insecure behaviour as they falsely think they are fully protected against cyberthreats, regardless of their behaviour. Employees need to be trained, through the use of ISAT, to understand the capabilities of the controls implemented (Arduin, 2021). This should guide them to understand that their actions will have consequences. They cannot blindly trust these controls as they often do not identify zero-day vulnerabilities or the next new phishing attack (Botacin et al., 2020). Employees should be reminded that cybersecurity is a primary concern, especially in the workplace. Hence, they cannot devolve their responsibility to technical interventions or senior management (Hadlington, 2018). Therefore, ISAT should clearly state that the security tools that have been implemented only serve as a first line of defence. Employee perceptions regarding the risks involved in using the organisation's IT systems should be calibrated to minimise the overconfidence typically placed in the security controls that have been implemented. Accordingly, the study proposes:

Hypothesis 2. *An employee's trust is positively associated with the intention to behave securely.*

5.3.3 The behavioural influence of awareness

The aim of ISAT is to empower employees to know what to look for when it comes to cyberthreats. If they can identify a phishing email successfully this will enable them to behave more securely (Aldawood and Skinner, 2019). ISAT should be practical and not a mere theoretical exercise. Thus, employees need to understand what is written in the company information security policy and how to implement it (Hina, Panneer Selvam and Lowry, 2019). People learn by doing and the more they practise the better they will become at recognising a phishing attack. Therefore, ISAT is an ongoing activity and, in order to implement it successfully, companies should create a documented security training strategy (Al-Daeef, Basir and Saudi, 2017; Stefaniuk, 2020). Chapter 3 discussed the fact that people have different learning styles and ISAT should be adapted to ensure that the material is understood and memorised by all. In addition, fostering a strong information security culture within an organisation will improve the overall security posture. Da Veiga et al. (2020) define a security culture as "an aware and knowledgeable workforce implementing conscientious, caring behaviour to comply with policies as guided by management". Such an information security culture needs to be driven by top management downwards to ensure that all levels of staff adhere to the security requirements. Various studies have found that subordinates follow the example set by their managers (Grassegger and Nedbal, 2021; Khando et al., 2021). Consequently, top management needs to show it participation in behaving securely by adhering to the security policy and communicating to subordinates to do the same (Jalali et al., 2020). Hwang et al. (2021) state in this regard: "Interestingly, managerial security participation has the strongest relationship to employees' awareness."

A difference of opinion exists as to how well ISAT works in combatting phishing attacks (Qabajeh, Thabtah and Chiclana, 2018). Delivering the training and sharing the material are only the beginning. If employees do not put the knowledge gained into practice, they will end up behaving insecurely. In contrast, overtraining could also lead to overconfidence where an employee thinks they are an expert in cybersecurity and therefore their actual behaviour is less secure (Zwilling et al., 2022). Through the training it should be made clear that attackers are constantly trying new things or new attack vectors. Therefore, employees are required to remain vigilant at all times.

As discussed, although ISAT does not completely mitigate insecure behaviour for all employees, it does reduce the risk of insecure behaviour for certain employees. The study proposes:

Hypothesis 3. *An employee's awareness of information security is positively associated with the intention to behave securely.*

5.3.4 The behavioural influence of optimism bias

In Chapter 4, OB was explained in detail with a particular focus on secure behaviour. OB is seen as a weakness with regard to information security because unrealistically optimistic people believe bad things, such as phishing attacks, will not happen to them. Therefore, they are under the illusion that their behaviour, safe or risky, will not lead to a security breach (Baek, Kim and Bae, 2014). They tend to see the good in everything and therefore trust that their actions will only yield positive results. OB is a cognitive bias that leads to error in judgment; the unrealistically optimistic person's risk perception is therefore incorrect (Shepperd, Pogge and Howell, 2017). Unrealistically optimistic people's beliefs lead them to act and behave in a certain way as they are convinced the behaviour is correct (Jefferson, Bortolotti and Kuzmanovic, 2017).

Since OB has a direct relationship with behaviour, it stands to reason that it will also influence the intention to behave in a certain way. To test for intention, this study uses a survey to classify participants into two groups: unrealistically optimistic (OB group) and average. The survey was adapted from Weinstein's (1980) survey*,* "Unrealistic optimism for future life events". In addition, the survey used in this study contained questions on information security and behaviour. This allows for the comparison of intention to behave securely between the two groups. Furthermore, the study tests actual behaviour with a phishing experiment and uses the results to compare the two groups.

Unrealistic optimists frequently believe that no effort is required on their part in order to behave securely since they will not be placed in a threat situation. Thus, the study proposes:

Hypothesis 4a. *Employees' attitudes towards information security differ significantly between the OB group and the average group.*

Hypothesis 4b. *Employees' trust is positively associated with information security and differs significantly between the OB group and the average group.*

Hypothesis 4c. *Employees' awareness of information security is positively associated with the practice of information security and differs significantly between the OB group and the average group.*

5.3.5 Measuring intention and behaviour

The three constructs used in this study – attitude, trust and awareness – play a critical role in the intention to behave securely. In some areas they overlap, for example attitude and trust, where attitude is influenced because employees place trust in the technical controls to protect them. Awareness leads to overconfidence which could negatively influence attitude towards information security. Figure 5.1 shows the changes made to the constructs and introduces OB together with the TPB. OB should not be seen as a construct but is used to classify the individual into a group, as well as to define the two groups, as previously explained: the unrealistically optimistic group and the average group. The three constructs will be tested for intention and actual behaviour for both groups. Intention to behave securely will be tested with a survey and evaluated using PLS-SEM statistical analysis. Actual behaviour will be tested with a phishing experiment followed by interviews to gain a better understanding why employees succumbed to the attacks.

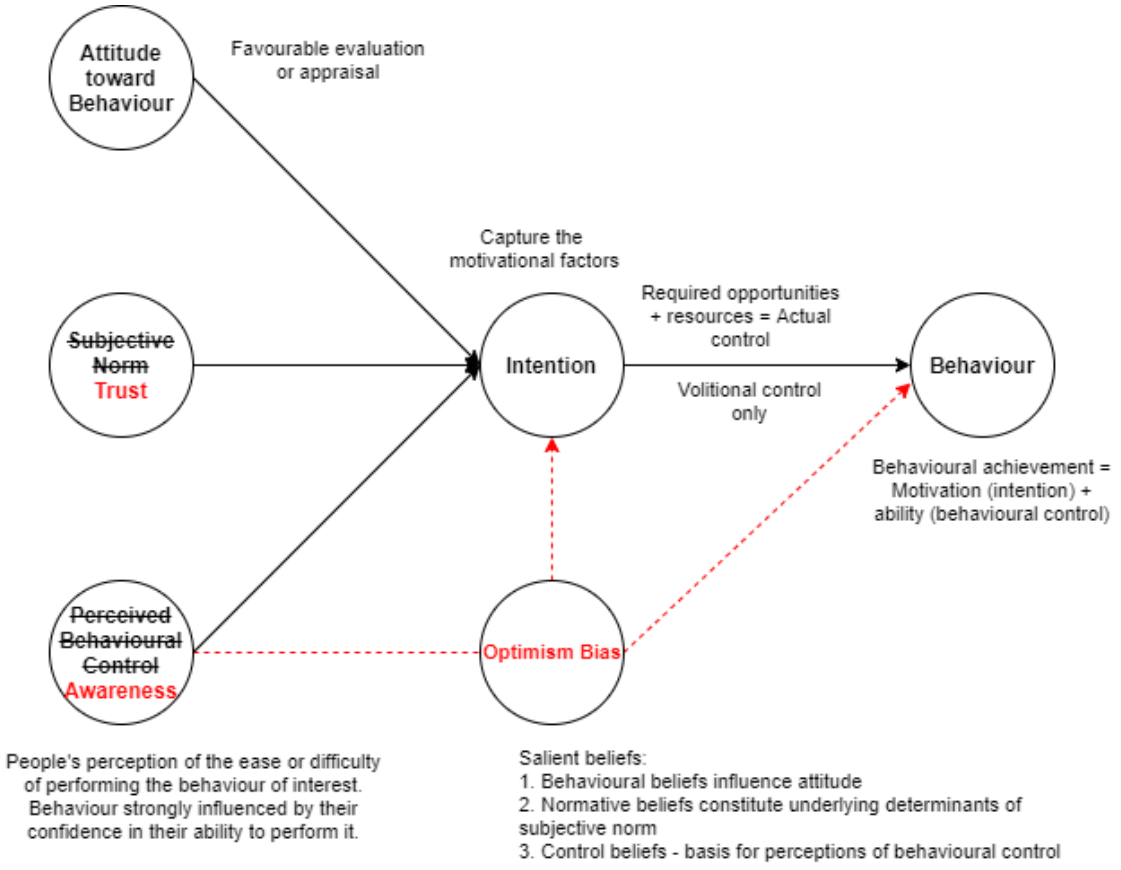


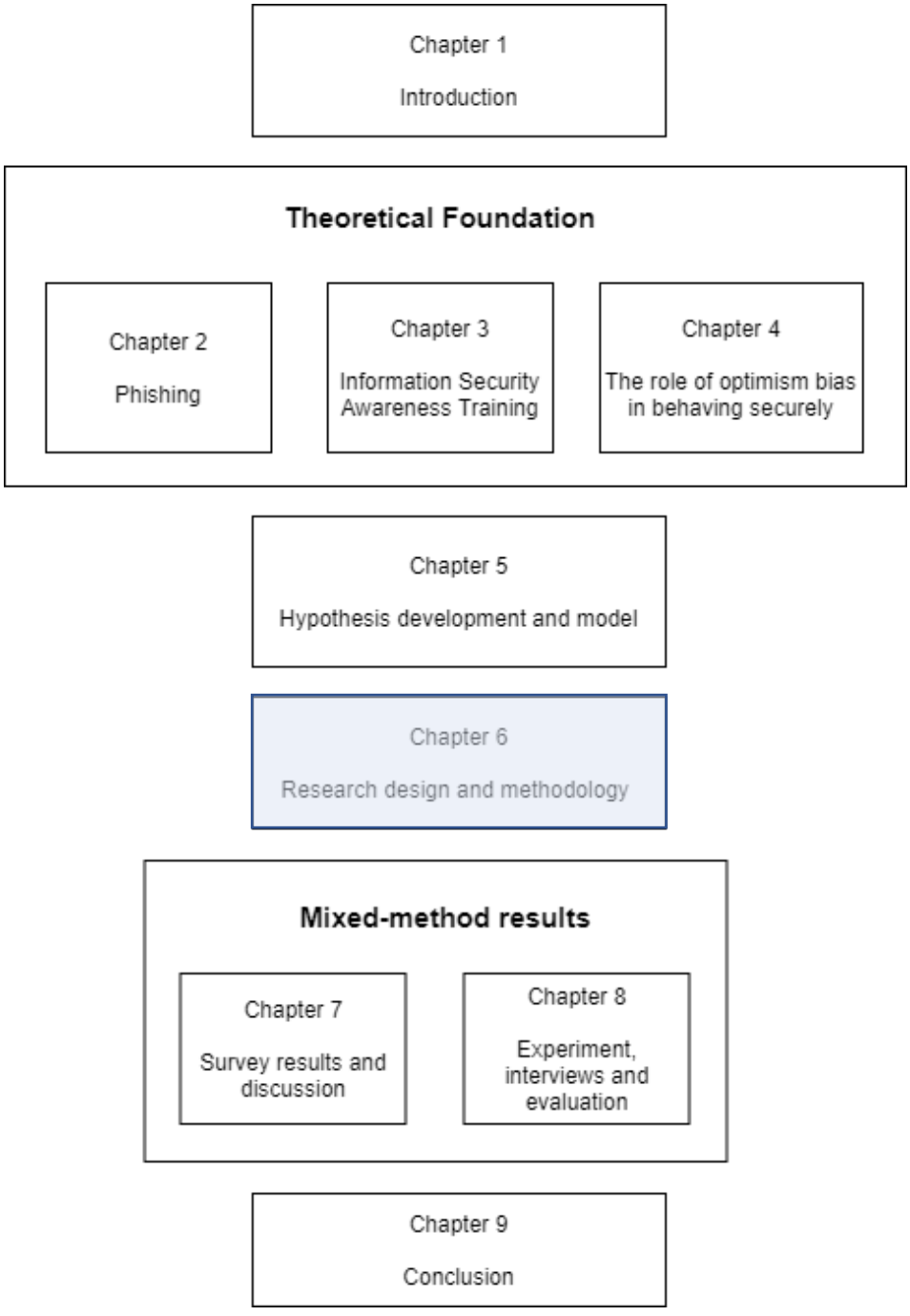
Figure 5.1 Adapted TPB

5.4 Summary

Hypotheses one, two and three are evaluated in Chapter 7, while hypothesis 4 is evaluated and discussed in Chapter 8. The next chapter describes the procedures and approaches used to ensure that the research process was carried out scientifically, using a mixed methods design that combined qualitative and quantitative data collection techniques. This included a quantitative survey, email phishing experiments and interviews. Particular attention is paid to how the data analysis techniques and procedures were conducted to ensure that the constructs were valid and reliable.

CHAPTER 6

RESEARCH DESIGN AND METHODOLOGY



6. RESEARCH DESIGN AND METHODOLOGY

6.1 Introduction

The literature reviewed in the previous chapters resulted in establishing the relevance of the research problem and its theoretical underpinnings. The theoretical model and its associated hypotheses were also discussed. The purpose of this chapter is to detail the techniques and approaches utilised to ensure that the research process was conducted scientifically throughout the duration of the study. As a result, this chapter emphasises the philosophical viewpoint of the study and examines the research paradigm, research method and research strategy, as well as the data collection and analysis tools that accompany them. Furthermore, this chapter explains why a certain research methodology was chosen, as well as how these methodologies were used to find solutions to the research problem. The statistical approaches implemented to ensure the validity and reliability of the variables in this study are also discussed.

6.2 Design overview

Research is frequently confused with gathering information, documenting facts and sifting information (Leedy and Ormrod, 2001). A more correct definition for research would be the process of gathering, analysing and interpreting data in order to comprehend a phenomenon (Leedy and Ormrod, 2001). The research process is pragmatic in the sense that defining the goal, managing the relevant information, and conveying the findings all take place within well-known frameworks and in agreement with established guidelines (Williams, 2007). The frameworks and guidelines inform researchers about what to include in their research, how to conduct the research, and what types of conclusion are likely based on the data collected (Williams, 2007). According to Saunders, Lewis and Thornhill (2016), the research design is the general plan of how one will go about answering one's research questions. The research design includes a clear goal obtained from the research questions, as well

as a description of the data sources and methods used to collect and analyse it. Figure 6.1 illustrates the “research onion” (Saunders, Lewis and Thornhill, 2016, p.124), which is frequently used to describe research methodology when considering how it supports the philosophies, approach to theory development, strategies and data collection methods for a specific study. In this study the items that are circled in red in Figure 6.1 represent the areas applied.

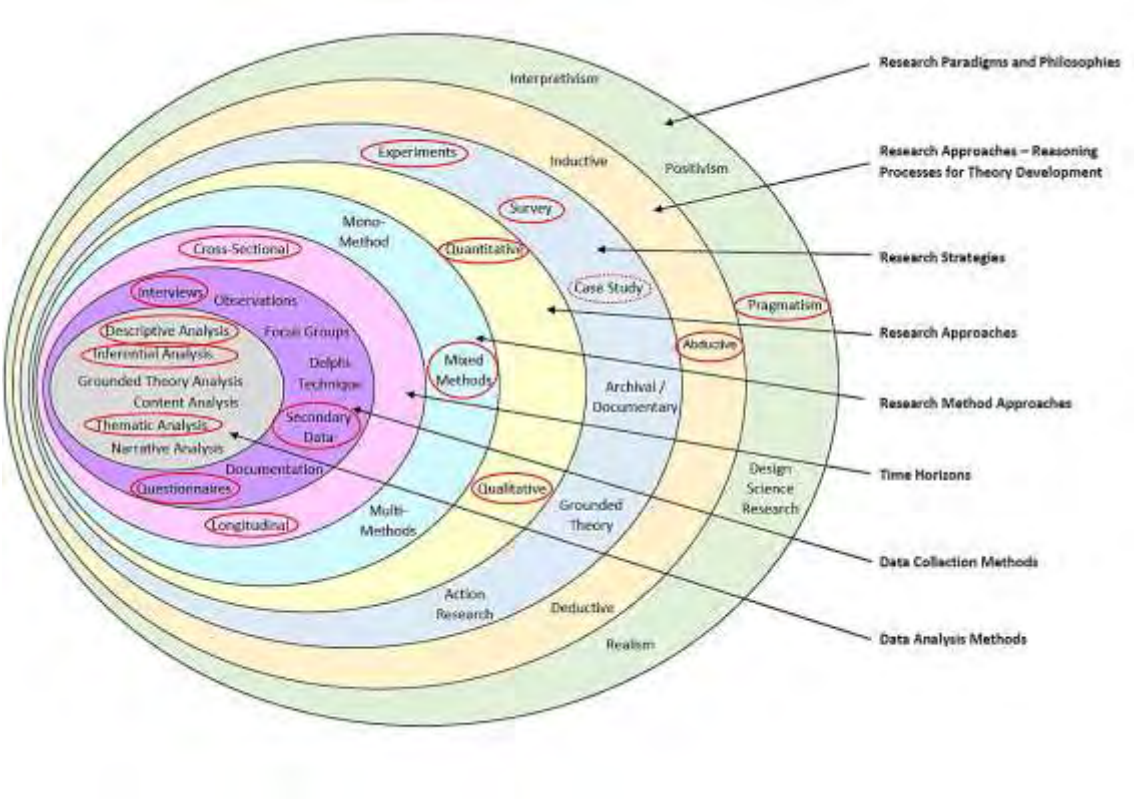


Figure 6.1 The research onion (adapted from Saunders, Lewis and Thornhill, 2016, p.124)

Figure 6.2 depicts the process flow followed in this study. Mixed methods research entails a study that combines a quantitative methods paradigm (the use and analysis of numerical data using statistical techniques) as well as a qualitative methods paradigm (that uses narrative data collected from interviews, focus groups, archival materials and opinion surveys) (Saunders, Lewis and Thornhill, 2016).

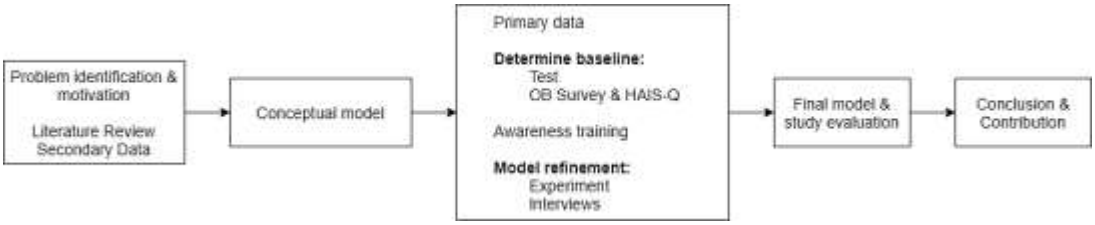


Figure 6.2 Process flow of research design followed

This study commenced with the identification of the problem using a problem statement and research questions. To better understand the problem, a literature review was conducted which formed the basis of the conceptual model. The next step was to collect the primary data which was done quantitatively with the use of a survey and an experiment, and qualitatively through interviews and observations, which assisted in the refining the model. Once the model refinement was completed, the final model and study evaluation were done to produce the study's contribution.

'Mixed methods' is distinct from 'multi-methods' research, as the latter uses multiple data collection methods from a single paradigm (either quantitative or qualitative) (see Figure 6.3). Mixed methods research has been heralded as a solution to the long-running, circular and remarkably ineffective debates over the benefits and drawbacks of quantitative versus qualitative research as a result of the paradigm "wars" (Feilzer, 2010). The study was designed as a multi-phase mixed methods (complex) research project (Saunders, Lewis and Thornhill, 2016) consisting of (1) collecting quantitative primary data from a survey, (2) running an experiment and quantifying the result, and (3) obtaining qualitative data through the use of interviews and observations, as explained in Figure 6.2.

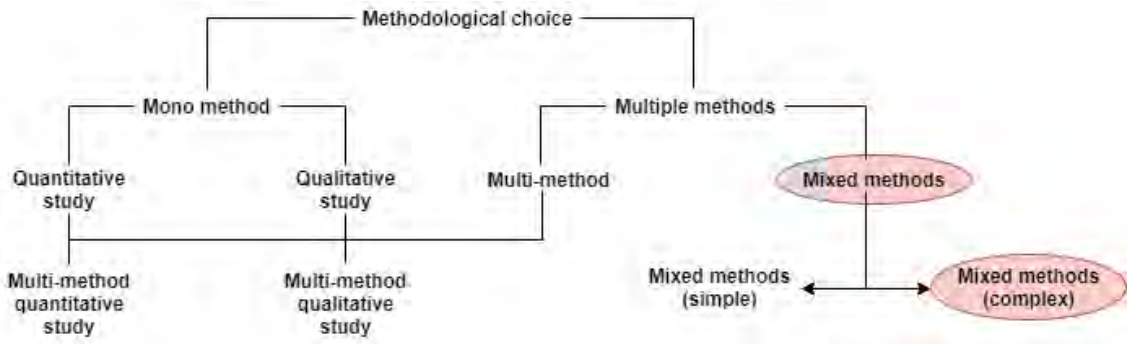


Figure 6.3 Methodological choice (adapted from Saunders, Lewis and Thornhill, 2016, p.167)

6.3 Philosophical perspective (research paradigm)

According to Saunders, Lewis and Thornhill (2016, p.124), the term *research philosophy* refers to a system of beliefs and assumptions about the development of knowledge. The researcher brings their own set of worldviews, theories and paradigms to the research project (Creswell and Poth, 2016). A paradigm can be defined as a "set of interrelated assumptions about the social world which provides a philosophical and conceptual framework" (Filstead, 1979). Choosing a research paradigm should be one of the first steps in defining the research design in order to: (1) describe the purpose of the research to be conducted, (2) provide a clear indication of underlying motivations as well as additional methodological choices, and (3) allow other researchers to understand what type of results to expect and conclusions to be made (Mackenzie and Knipe, 2006). Ultimately, the paradigm choice allows researchers to question their worldviews. These worldviews impact not only how data is obtained but also which data is considered important to collect. These are mostly philosophical questions, with questions varying greatly from one researcher to the next (Van der Schyff, 2019).

Figure 6.4 depicts that the *positivistic* and *phenomenological* approaches are the two extremes on the research paradigm continuum. The traits and assumptions of one paradigm are gradually reduced and replaced by those of the other as one continues along the scale. According to Collis and Hussey (2003), few people would conduct research in the pure form of each. Figure 6.4 contains six stages indicating that different research paradigms contain traits from both extreme paradigms. Research methods do not have to be used in isolation and may be mixed and matched. Collis and Hussey (2003) emphasise that mixing methods provides a more comprehensive and often complementary picture of the research problem. When research methods are combined, it is referred to as triangulation. Collis and Hussey (2003) claim that triangulation can overcome the bias and sterility of a single-method approach. Saunders, Lewis and Thornhill, (2016) agree that through triangulation, the different methods used can corroborate the results.

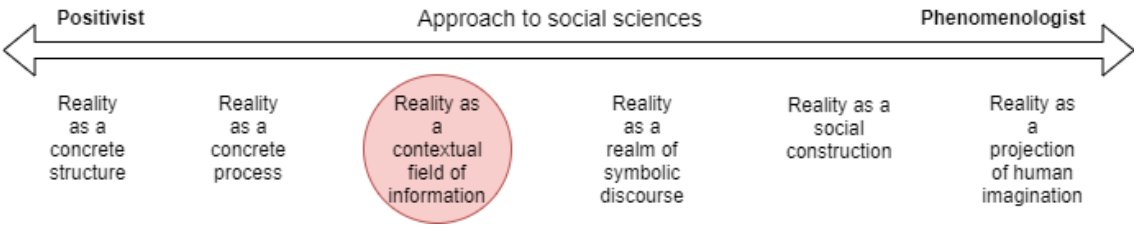


Figure 6.4 Continuum of core ontological assumptions (Morgan and Smircich, 1980, p.492 in Collis and Hussey, 2003, p.51)

Since this study is based on a financial services organisation and half of the respondents are unrealistically optimistic, it is concrete within the context. The study is predominantly quantitative (systematic random sampling and a survey and experiment) rather than qualitative (interviews). It is consequently assumed that if another researcher conducted a similar study they would be likely to obtain similar results.

In the next section the different paradigms are discussed in more detail.

6.3.1 Positivism

According to Park, Konge and Artino (2020, p.690), positivism relies on the hypothetico-deductive method to verify a priori hypotheses that are often stated quantitatively, where functional relationships can be derived between causal and explanatory factors (independent variables) and outcomes (dependent variables). These researchers claim that positivism is aligned with the hypothetico-deductive model of science. They (Park, Konge and Artino, 2020) further state that the hypothetico-deductive method is a repetitive process that begins with theory from the literature to (1) create testable hypotheses, (2) create an experiment by operationalising variables (i.e. identifying variables to manipulate and measure via group projects), and (3) carry out an experiment-based empirical study. Finally, the results of such a study are used to help inform theory and contribute to the literature, completing the process (theory → hypothesis → operationalising variables → experimentation → theory) (Park, Konge and Artino, 2020). The results of an empirical study can support or enhance theory. According to Collis and Hussey (2014, p.44), positivism is based on the belief that reality is independent of us, and the goal is to identify theories based on empirical research conducted by means of scientific methods, in particular observations and experiments. ‘Positive information’ becomes knowledge because it can be scientifically verified by

means of justification or proof. As a result, positivists would benefit from pure data and facts that are not influenced by human interpretation or subjective bias (Saunders, Lewis and Thornhill, 2016, p.137). Saunders et al. (2016, p.137) elaborate further that positivists attempt to remain neutral and detached from the research and the data in order to avoid influencing their findings. Since the results could be used to support or enhance current theory and then be tested again later, positivism aligns with deductive reasoning.

Positivism has been criticised for dismissing various sources of understanding of the world, including those derived from human experiences, reasoning or interpretation, as unsuitable for scientific investigation (Fox, 2008). Fox (2008) states the following criticisms:

- In the social sciences, these alternative understandings (e.g. qualitative interview data) are critical as foundations for learning development, and many areas of social scientific inquiry would be impoverished if such sources were not available, because this interpretative work is itself of interest.
- A second criticism is that positivism ignores context in order to establish generalisations that are independent of setting. Setting is frequently an integral component of activity in social science, and as such, it cannot be overlooked; indeed, claims to knowledge require full contextualisation.
- A third criticism is that, as social order emerges from human sense-making, it will be dependent largely on value perspectives, making it difficult to define a single truth about the characteristics of the social world.
- Finally, positivism is dedicated to eliminating the subjective nature of knowledge development, and thus rejects any function that requires reflexivity among researchers.

For these reasons, positivism has been heavily criticised since the beginning of social science, and has gradually been replaced, particularly in qualitative research, by post-positivist epistemologies (theories of knowledge) and ontologies (theories of the nature of reality) (Patomaki and Wight, 2000; Fox, 2008).

6.3.2 Post-positivism

While the pursuit of knowledge remains a goal of social scientific inquiry, the concept of an absolute truth may be viewed as an aspiration rather than something that can be discovered once and for all (Fox, 2008). Understanding, rather than interpretation, is sometimes regarded as the goal of post-positivist inquiry, but this is frequently limited by perceptions regarding the setting as well as contingencies (Panhwar, Ansari and Shah, 2017). Furthermore, the role of the researcher as data interpreter is openly recognised in post-positivism, as is the importance of introspection in research practice.

6.3.3 Interpretivism

Interpretivism contends that humans and their social worlds cannot be studied in the same way as physical phenomena and that, as a result, social science research must be distinct from natural science research rather than the former attempting to mimic the latter (Saunders, Lewis and Thornhill, 2016, p.116). Therefore, interpretive methods of research adopt the position that our knowledge of reality is a social construction by human actors (Walsham, 1995, p.376). According to this viewpoint, value-free data cannot be obtained because the researcher uses their preconceived ideas to guide the process of enquiry, and then interacts with the human subjects of the enquiry, changing both parties' perceptions (Walsham, 1995). Interpretivism is underpinned by the belief that social reality is subjective because it is influenced by our perceptions (Collis and Hussey, 2014, p.45). Interpretivism differs from positivism in that it is assumed that the researcher's ‘objective’ data can be used to test prior hypotheses or theories (Walsham, 1995). Lincoln and Guba (1985, in Oates, 2006) highlight a set of criteria for interpretivist research that is an alternative to, but parallel to, those for the positivist approach (see Figure 6.5).

Positivism	Interpretivism
Validity	Trustworthiness
Objectivity	Conformability
Reliability	Dependability
Internal validity	Credibility
External validity	Transferability

Figure 6.5 Quality in positivist and interpretivist research (Lincoln and Guba,1985, in Oates, 2006, p.294)

In contrast to positivists, who seek to quantify the occurrence of a phenomenon, interpretivists use qualitative methods to define, translate and find value. As a result, the conclusions are generic because they are not based on any statistical analysis (Frauenstein, 2021). Saunders, Lewis and Thornhill et al. (2016, p.140) generalise that interpretivism emphasises that humans differ because they are born into different cultural backgrounds, under different circumstances and at different times; as a result, they will create (i.e. interpret) their own subjective meanings from physical phenomena. Interpretivism does not start the research process with a theory, but rather develops it as the research evolves. Both qualitative and quantitative research methods (mixed methods) apply to this paradigm and were adopted in this study (Mackenzie and Knipe, 2006).

6.3.4 Critical realism

Critical realism seeks to explain what we see and encounter in terms of the underlying reality structures that form observable events (Saunders, Lewis and Thornhill, 2016, p.138). For critical realists, reality is the most important philosophical reflection, with a formal and layered ontology (the way we think the world is) being crucial (Fleetwood, 2005). Critical realists consider reality to be external and distinct, but not readily accessible through inspection and understanding. Saunders, Lewis and Thornhill et al. (2016) define critical realism as “the philosophical stance that what we experience are some of the manifestations of the things in the real world, rather than the actual things”. Critical realists emphasise how frequently our senses delude us (Saunders, Lewis and Thornhill, 2016, p.139). Similarly, Patomaki and Wight (2000) argue that in critical

realism, the world consists of underlying structures, authority and inclinations that exist whether or not they are recognised or known through one's experience and/or discussion and debate.

6.3.5 Pragmatism

Pragmatism is not committed to any single philosophy or reality system; rather, it affirms that the research question should determine the research philosophy and that methods from multiple paradigms can be used in the same study (Collis and Hussey, 2014). Pragmatism strives to reconcile objectivism and subjectivism, factual information and values, precise and stringent knowledge, and various contextualised experiences. This is accomplished by considering theories, ideas, thoughts, hypotheses and research results not in an abstract way, but in terms of the roles they play as tools of thought and action, as well as their practical implications in specific contexts. Pragmatists value reality as the practical effects of concepts and understanding to carry out actions successfully (Saunders, Lewis and Thornhill, 2016, p.143). Morgan (2014) agrees, arguing that pragmatism can be used as a paradigm for social research regardless of whether it employs qualitative, quantitative or mixed methods. As a result, a pragmatic researcher is more concerned with the research outcome and less concerned with the specific methods used to achieve the outcome. Pragmatism is commonly used to answer both what and how questions (Creswell, 2014) and opposes the idea of a single objective reality. The problem statement is attributed the utmost importance as the underlying philosophical perspective of mixed methods research, and all manner of methods are used to address it (Creswell, 2014).

6.4 Paradigm adopted in this study

The paradigm used in this study is pragmatism since it fits well with mixed methods research where quantitative and qualitative research are considered (Feilzer, 2010; Hall, 2013). The focus of this study is to find a practical solution to enhance the outcome of ISAT, resulting in people behaving more securely specifically towards phishing attacks,

thus protecting themselves and the organisations they work for. Therefore, the main goal of the study is more focused on the outcome of the research than the specific methods used to achieve the outcome.

6.5 Approach to theory development

The degree to which a researcher understands the theory at the outset of their research raises an important question about the design of their research project (Saunders, Lewis and Thornhill, 2016). Saunders, Lewis and Thornhill (2016, p.166) state that a research design can use deductive, inductive or abductive reasoning to develop theory.

Deductive reasoning starts with the general and then moves to the particular. The process starts with a theory, deriving hypotheses from it, then testing the hypotheses and ultimately revising the theory (Locke, 2007; Woiceshyn and Daellenbach, 2018). Inductive reasoning involves moving from the particular to the general; empirical observations are made about a phenomenon of interest and then concepts and theories are based on them (Locke, 2007). An abductive approach, as opposed to moving from theory to data (deduction) or data to theory (induction), moves back and forth, effectively combining deduction and induction (Suddaby, 2006). Abduction begins with the discovery of a ‘surprising fact’, followed by the development of a plausible theory as to how this could have happened. According to Van Maanen et al. (2007), some plausible theories can account for what is observed better than others, and it is these theories that will assist in the discovery of more 'surprising facts'. They argue that these surprises can occur at any point in the research process, even at the very end when the findings are written up.

This study followed an abductive approach. The surprising fact is that people still succumb to phishing attacks regardless of the amount of ISAT done or technical controls implemented. This, then, creates the focus on the further study of human behaviour from a theory (in this case, TPB) perspective to better understand the ‘surprising facts’.

6.6 Secondary data collection

According to Levy and Ellis (2006), a good literature review should (1) establish a firm foundation for a research topic, (2) establish a firm foundation for research methodology selection, and (3) demonstrate that the proposed research adds to the cumulative body of knowledge.

Secondary data analysis is the examination of information gathered by someone else for a prime reason. For researchers with limited time and resources, using someone else's existing data is a viable choice (Johnston, 2014). Secondary data analysis is a versatile method that may be utilised in a variety of ways but remains an empirical exercise and a systematic method with procedural and evaluative processes, similar to gathering and assessing primary data (Johnston, 2014).

This section will explain the sources and processes used to create a relevant body of literature to better understand and define the research problem while at the same time, as previous literature is better understood, looking for possible solutions.

6.6.1 Sources of secondary data

Technological advancements have resulted in large volumes of data being collected, organised and archived, most of which are now readily accessible for research (Johnston, 2014). The use of search engines on the internet has made the process of finding literature relatively easy. Specifically, Google Scholar was used to find relevant articles from peer-reviewed sources. Search keywords used included 'phishing', 'attitude', 'trust', 'awareness', 'ISAT' and 'optimism bias' (OB) or 'unrealistically optimistic', to mention a few. Articles found were taken from sources such as the *Information Systems Journal*, *MIS Quarterly* and *Conference on Human Factors in Computing Systems.* In addition, through the online library at Rhodes University, access was obtained to Elsevier's ScienceDirect academic database and journals such as *Computers & Security, Computers in Human Behaviour, Information & Management, International Journal of Human-Computer Studies* and *Computers and Education* provided relevant articles for this study. Not all articles found in the search results were suitable as they did not meet the quality criteria, for example articles from Wikipedia

were not used as they are not peer reviewed. Literature was sourced from both the disciplines of information systems and psychology since the study focused on the relationship between people and the secure use of information systems.

6.6.2 Process of secondary data analysis

Relevant articles found online were downloaded and saved to the Mendeley Reference Manager application. Articles were sorted into groups or focus areas (Table 6.1) for example attitude, trust, awareness or a topic of interest such as OB. The application provides a search function for all items loaded into the database. Articles can be tagged to further group them based on relevance or importance. The literature review should be viewed as a funnel that begins with a wide opening and narrows to a small, finite end (Denney and Tewksbury, 2013) . In other words, the literature evaluation must progress from broad to specialised. The broad beginning initiates the process with a general research question, allowing each theme to narrow the focus to a specific research question in the study.

Table 6.1 Number of articles by focus area

Focus group	No. of articles	No. of articles after screening
Attitude	69	26
Awareness	88	49
Information Security	175	61
Learning	50	20
Optimism Bias	93	30
Phishing	154	68
Trust	58	26
Total	**687**	**280**

6.7 Research instrument

The research instrument went through a process of refinement. Primary data collection was done with the employees of the organisation using systematic random sampling. The purpose of the research instrument was to group employees as either unrealistic optimistic or average and to gain a better understanding of their perceived behaviour towards information security.

6.7.1 Pilot questionnaire

A pilot study was conducted to test the reliability and validity of the construct items and to identify potential problem areas and deficiencies in the research instrument. A survey was created using Google Forms to collect the data. Twelve respondents (colleagues) completed the questionnaire which is sufficient for a pilot study (Bradburn, Sudman and Wansink, 2004). The answers were reviewed and minor changes made to refine the instrument so as to avoid ambiguity in certain questions.

6.7.2 Final questionnaire

The questionnaire covered the disciplines of both social psychology (OB) and behavioural information security. Questionnaires allow for relatively easy data collection from a large sample, especially those administered electronically (Saunders, Lewis and Thornhill, 2016, p.439). In addition, they offer a convenient way for respondents to complete them in their own time and can be done in complete privacy. Multiple sources (prior studies) were used in certain cases, as shown in the Source column of the tables listing the elements of the research instrument (see Appendix A).

The questionnaire included the model constructs and addressed the research question. Respondents had to choose answers from a Likert scale, allowing for a uniform response and easier data analysis; all questions were close ended. Sequencing of the questions started with the demographics, which could be considered the easier questions, and then progressed to the various construct questions. To create a suitable questionnaire, Acharya (2010) suggests the following:

- Use simple language so that the respondents will interpret the questions correctly.
- Questions should be clear, avoiding ambiguous concepts.
- Questions that are leading or embarrassing should be rephrased. Answering these questions offends people.
- The answer options should be sufficient. At the data collection stage, the questions should not be constructed in such a way that several options are mashed together. The real value of data is lost when answer options are merged.
- Every question should be brief, preferably in one phrase, and tailored to the respondent's cognitive abilities.

Punch (2003, pp. 49-50) suggests the following:

- The items should correspond to the research questions. This was achieved by aligning the literature review with the model constructs and the research questions.
- The theoretical framework should be aligned to the knowledge that is needed. Because the focus of this study is behavioural, it employs a behaviour-centric theoretical framework, the TPB.
- It should be determined whether these constructions will be measured using a single item or several items (a scale).
- The questionnaire should be piloted.
- The pilot results should be used to correct or enhance the final questionnaire.

6.7.3 Addressing measurement errors

The statistical technique of partial least squares (PLS) path modelling was used for the analysis of the quantitative data. The measurement of the results is discussed in detail in Section 7.2.5.

6.8 Methods used in this study

It is widely understood that research methodologies can be classified as either quantitative or qualitative (Saunders, Lewis and Thornhill, 2016). In qualitative studies researchers hope to gain a comprehensive grasp of the phenomena at hand. On the other hand, quantitative research aims to predict or evaluate hypotheses or propositions (Sechrest and Sidani, 1995). This study used mixed methods, as discussed in Section 6.2. Since this study evaluates hypotheses (intention to behave securely), quantitative research, using a survey, was used to test them (Morgan, 2015). In addition, qualitative research was used to measure actual secure behaviour using an experiment, interviews and observations. Model evaluation will be done by means of triangulation, taking all methods used into account (Saunders, Lewis and Thornhill, 2016).

6.9 Primary data collection

6.9.1 Sources of primary data

This study was performed at a financial services organisation based in South Africa. The organisation specialises in offering unsecured loans and debt collection through a contact centre. South Africa in general is seen as an attractive target for cybercrime, owing to inadequate funds being made available by businesses for cybersecurity, government's lack of cybercrime regulation and law enforcement training, and an uninformed public that does not clearly understand cyberthreats (Mcanyana, Brindley and Seedat, 2020). A security audit performed by an international audit firm at the organisation where this study took place emphasised the need for ISAT. The organisation's information technology (IT) is internally managed by a team of 50 people who have implemented best practice security safeguards. The organisation is subjected to many phishing attacks on an ongoing basis, for example fraudulent invoices to be paid or bank statements containing malware to be processed.

6.9.2 Sampling strategy

Systematic random sampling was used to select a sample representative of the population from which it was selected, allowing statistical generalisations about the population to be established based on an analysis of the data gathered from the sample (Rowley, 2014). Using systematic random sampling based on a sampling frame or a list

of the people in the population, every instance in the population has a high probability of being included in the sample, which increases the chances of selecting instances that represent the overall population (Rowley, 2014). The respondents in this study are representative of the general population of users in the financial services sector. Email addresses were used in the selection process by sorting them alphabetically and selecting every third employee. Respondents included users from all levels of the organisation, including call centre consultants, administration clerks, staff employed in the legal, IT and human capital departments and senior management. The total population (number of employees) in the organisation is 775, and one out of every three employees was asked to participate in the study.

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, i.e. one-third of the organisation's employees. Owing to a combination of incomplete data input and validity concerns, 31 responses were excluded. Data obtained from the remaining 226 respondents was used for further analysis.

6.9.3 Process of primary data analysis

The survey data was analysed by way of PLS path modelling, which is a suitable approach when the data violates distributional assumptions (Hair et al., 2019). In addition, structural equation modelling (SEM) was applied as it is suitable for a wide range of research problems because of its capacity to represent latent variables, account for various types of measurement error, and evaluate complete hypotheses (Henseler, Hubona and Ray, 2016). As a result, SEM is a useful analysis framework for examining real-world (therefore applied) processes and their interconnections. Although SEM is sometimes misinterpreted as a technique for confirming a priori causal hypotheses, it is frequently used to create a best fit structural model taking causal pathways into account (Kelloway, 1995). PLS path modelling is extensively used in information system research (Henseler, Hubona and Ray, 2016), as it largely avoids factor indeterminacy, making it suitable to both exploratory and confirmatory studies (Lowry and Gaskin, 2014). As this study is largely exploratory in developing an unestablished model, PLS is a suitable approach. The quantitative results are discussed in detail in Chapter 7.

6.10 Experiment and interviews

6.10.1 ISA and simulated phishing experiment

The experiment consisted of two parts: (1) ISA online training sessions were conducted using the company's LMS and (2) after each training session a simulated phishing attack was conducted. This process was repeated three times as this was deemed sufficient to collect adequate data in determining a trend. The training focused on the following themes: the importance of cybersecurity, that it is everyone's responsibility, and practical tips for behaving securely. The various cyberthreats were explained, including phishing and ransomware. The practical tips covered secure email usage, controls to mitigate ransomware, how to create a complex password applying secure password recommendations, how to report a breach, how to process sensitive information and what to do in the case of a lost or stolen device. To keep the employees engaged, the amount of material was limited to four slides and was visually attractive (see Figure 6.6, Appendix A). The training included short videos to practically demonstrate the concepts covered in the material and a few questions (see Table A1) to test the employees' understanding. The estimated length of time for each training session was less than 25 minutes. The employees received immediate feedback on their answers as either correct or incorrect, and no limit was placed on how many times they could repeat the training, since learning improves with repetition (Reddy et al., 2016). Once all the data was collected, it was analysed with descriptive stats and t-tests; in addition, the associated probability (p-value) was provided to determine significance.

Figure 6.6 Sample training slide.

Shortly after each training session, a simulated phishing attack was launched. The phishing emails were sent to those who were part of the population sample and the attacks were themed as either fear-based or reward-based (Johnston and Warkentin, 2010; Boss et al., 2015; Furnell and Vasileiou, 2017; Jansen and Van Schaik, 2018). One of the most important motivational factors in OB is the expectation of earning a reward. Therefore, it was decided to make two of the phishing emails reward based (Sharot, 2011). The company logo was obtained from the internet to make the emails look legitimate and every email contained a unique link that, when clicked, recorded a response in a database. See Figure 6.7 for an example of a phishing email. Feedback was given to the employees who succumbed to the attack via email. During this feedback, it was made clear to them that they should carefully review the clickable link address in any email, as well as how to check the 'from' address used in the email.

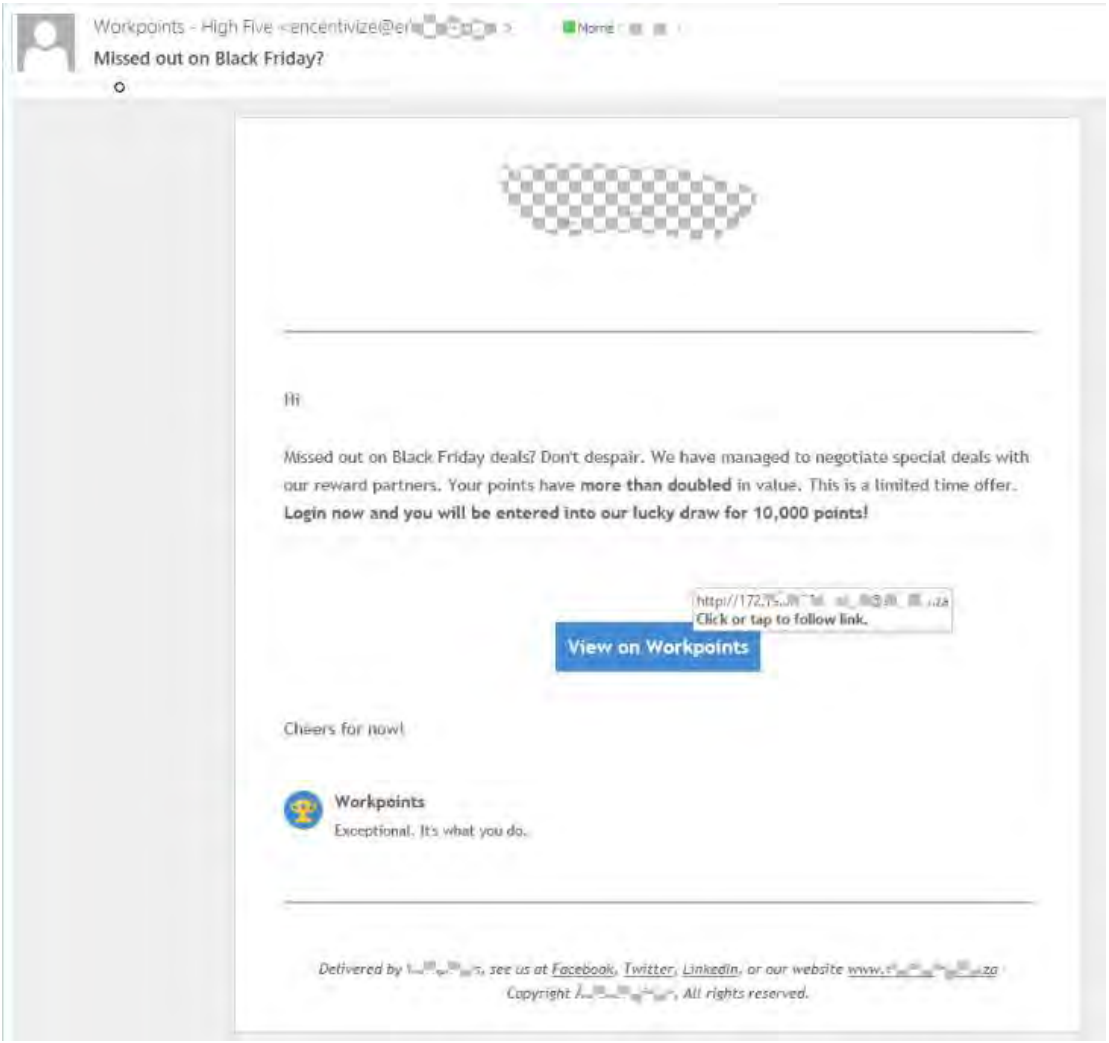


Figure 6.7 Example phishing email

6.10.2 Interviews

To determine why employees succumbed to the attacks, interviews were conducted until data saturation was reached (no new ideas or answers) (Saunders, Lewis and Thornhill, 2016). Semi-structured interviews, also known as qualitative research interviews, make use of a list of questions or themes not always asked in the same order and allow for comments to further the discussion (Saunders, Lewis and Thornhill, 2016). These qualitative interviews should provide an in-depth understanding of the reasoning applied by those who succumbed to the attacks. According to Saunders et al. (2016), a semi-structured interview

- is used to collect data which is usually analysed qualitatively
- the data from the interview is likely to be used to better comprehend not only the 'what' and 'how' but also to emphasise the 'why'
- gives essential background or metadata for the research performed
- in an explanatory study may be used to understand the relationships between variables, similar to those discovered in a descriptive study
- creates an understanding of the reasons for the decisions that the participants have taken, or to understand the reasons for their attitudes and beliefs
- creates an opportunity to explore answers, allowing interviewees to clarify or build on their answers.

As part of the interview results, a mind map showing the common themes was created. According to Fearnley (2022), transcribing using a mind map enables creative thinking between themes and assists in spotting emerging common themes. She also argues that using this simple method of description and analysis provides a way to quickly collect data in a format that can be analysed. Burgess-Allen and Owen-Smith (2010) define the following advantages of using mind mapping in qualitative data analysis:

- Efficiency and cost-effectiveness
- A visually appealing summary of the themes/findings
- Results in larger themes comparable to conventional qualitative techniques

The qualitative findings of this study are discussed in detail in Chapter 8.

6.11 Ethical considerations

Saunders, Lewis and Thornhill (2016, p.239) refer to the ethical norms that guide a researcher's behaviour in relation to the rights of individuals who become the focus of their research or are affected by it. Ethics is more than merely requesting permission and obtaining approval from an ethics board or committee; ethical concerns should be addressed throughout the research process, beginning with the formulation of the research problem (Crowe and Sheppard, 2012). Furthermore, ethical issues include ethical behaviour toward participants as well as ethical behaviour by the researcher (see Figure 6.8). To ensure that this study was conducted ethically, the following steps were taken:

- University requirements. Approval was obtained from the university's Ethics Committee for the collection of the primary data. Ethical clearance was granted with reference CIS18-11 (see Appendix C).
- Financial services organisation. Permission was obtained from the CEO to perform the study within the organisation.
- Informed consent. Before collecting the primary data, all respondents were given sufficient information about the purpose of the study, and were also provided with the researcher's contact information. On the homepage of the survey instrument, the terms and conditions of the research study were displayed, requiring respondents to consent before they could begin the questionnaire (see Appendix D).
- Confidentiality and anonymity. The information gathered from the participants was kept private (Oates, Griffiths and McLean, 2022). In order to conduct the experiment, interviews and create the two groups (average and unrealistically optimistic) it was necessary to record the participants' full names.
- Honesty and transparency. The respondents were fully informed about the study goal and were told that the findings would be used for academic purposes and for enhancing ISAT (see Appendix D).
- Dignity. Respondents could discontinue their participation at any moment during the questionnaire if they were uncomfortable in any way (Oates, Griffiths and McLean, 2022). They could also contact the researcher by email, as the address was listed on the homepage of the questionnaire (see Appendix D).

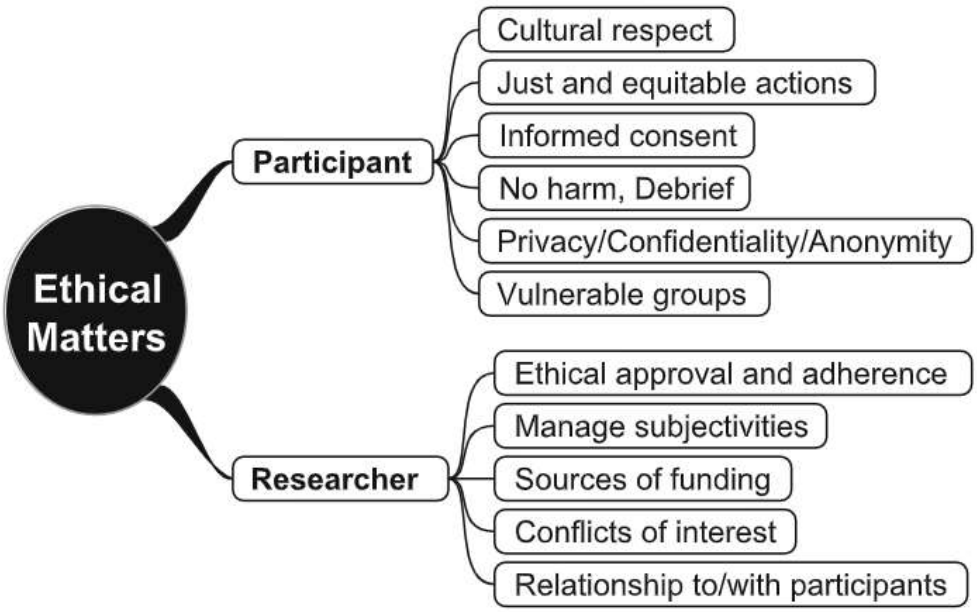


Figure 6.8 Ethical matters (Crowe and Sheppard, 2012)

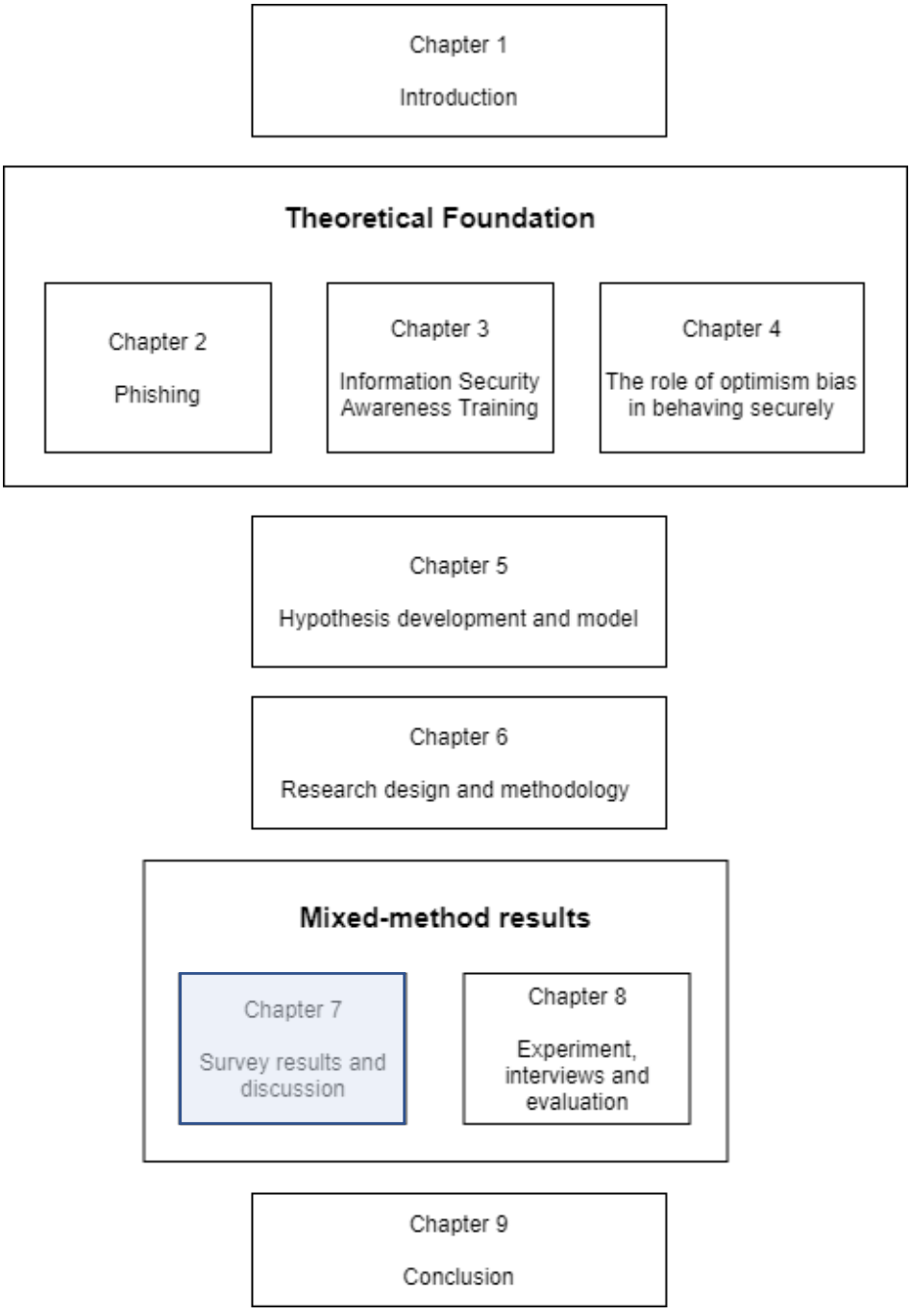
No sources of funding were obtained for this study. The researcher has no conflict of interest to declare.

6.12 Summary

This chapter provided an overview of the way in which the research was conducted. The *research onion* introduced in Section 6.2 created the framework for the research design process followed. The paradigm used in this study was pragmatism as it is well suited to mixed methods research. In addition, the study adopted an abductive approach as it effectively combines both inductive and deductive approaches and is also well suited to such research. Thus, the study consisted of deductive reasoning that started with a theory, created and tested hypotheses, to finally revise the theory. An inductive reasoning approach was used in the qualitative research where empirical observations were made about secure behaviour which led to beliefs and theories about the behaviour. The relevant theory was selected based on the literature reviewed and was used to create the research questions. The various literature sources were discussed in detail. The primary data (quantitative data) was collected using a cross-sectional survey and analysed using PLS-SEM techniques followed by an experiment. The qualitative data was collected using semi-structured interviews and observations. The quantitative results are discussed in Chapter 7 and the qualitative results in Chapter 8.

CHAPTER 7

SURVEY RESULTS AND DISCUSSION



7. SURVEY RESULTS AND DISCUSSION

7.1 Introduction

This chapter is a continuation of the previous chapters, presenting the statistical analyses of the survey results. The results pertaining to the tests of questionnaire validity and reliability are presented as well as the results of the data collection process. In addition, the descriptive statistics (univariate analyses) relating to the study are presented together with additional inferential results pertaining to the multivariate analysis. These results were subsequently used to create a measurement and structural model. The chapter concludes by discussing the results of the structural model within the context of the hypotheses of this study. The results discussed in this chapter emanate from the survey only and were obtained by means of the formal research instrument used.

7.2 Results of the pilot study

Data collection for the pilot study took place from 3 January 2019 to 14 January 2019. The pilot study was conducted using Google Forms, with twelve respondents (colleagues) completing the survey. The results were analysed and any ambiguity in the wording of the questions was addressed. Cronbach's alpha was used to test the survey questions for suitable reliability, which helped to refine the research instrument.

7.3 Results of the study

7.3.1 Respondent population and sample

The sampling frame consisted of the employees of a financial services organisation in South Africa. The respondents are representative of the general population of users in

the financial services sector. Systematic random sampling, based on user email addresses, was used in the selection process. Respondents included users from all levels of the organisation, including call centre consultants, administration clerks, staff employed in the legal, information technology and human capital departments and senior management. Every employee had an equal chance of being selected to participate in this study. The total population (number of employees) of the organisation is 775, and one out of every three employees was asked to participate in the study.

7.3.2 Data collection and screening

Data collection for the final study took place from 29 May 2019 to 3 July 2019. 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, i.e. one third of the organisation's employees. Owing to a combination of incomplete data input and validity concerns, 31 questionnaires were excluded. Data obtained from the remaining 226 respondents was used for further analysis. Demographics were not considered as there was no significant differences between the two groups with regard to age and gender. Table 7.1 provides a complete outline of the items and the associated descriptive statistics that comprised the research instrument.

Table 7.1 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 has positively changed towards information security (security behaviour) over the past 2 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 satisfactory work conditions.	(Mittal, 2015)	2.195	1.152	0.817	1.905382*	1.989
Awareness	Q26	It's acceptable to use my		3.815	1.170	0.746	3.260684**	1.101

		social media passwords on my work accounts.	HAIS-Q (Parsons et al., 2017)					
	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		3.012	0.915	0.826	3.291803**	2.018

		can be trusted.						
	Q50	I tend to see the best in the people I work with.		2.665	1.117	0.628	2.385855**	2.065

The research instrument was largely adapted from previous research. Items were measured using the OB scale introduced by Weinstein (1980) and a five-point Likert scale, ranging from ‘strongly disagree’ to ‘strongly agree’. We used eleven OB items to determine which respondents were unrealistic optimists and which were average. 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 OB questions. When it comes to positive events, *optimism* is defined as believing that one's own odds are better than average, whereas *pessimism* is defined as believing that one's own chances are worse than average. These definitions of optimistic and pessimistic responses are swapped for negative events (Weinstein, 1980). Respondents had to complete all the OB questions to categorise themselves as either unrealistic optimists or average.

In addition, we used 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., 2014).

The information security awareness model (Figure 7.1) emphasises the relationship between knowledge, attitude and behaviour, with the outer circle focusing on personality (Individual), security culture (Organisational) and training (Intervention) (Parsons et al., 2017). Used in conjunction with HAIS-Q, it provides an authentic measure for measuring ISA.

Figure 7.1 Information security awareness model (Parsons et al., 2017)

7.3.3 Univariate analysis

As part of the univariate (descriptive) analysis of the final study, the means of the constructs (and distributions) were analysed.

7.3.3.1 Attitude

The results in Table 7.2 show that 93.27% of employees agreed that they should not open an email from an unknown sender and 83.11% agreed that using public Wi-Fi is risky. Most of the employees (79.71%) had a positive attitude towards their work environment. This indicates that the majority of employees had a positive attitude towards information security.

Table 7.2 Distribution of items related to the construct *Attitude*

	%				
Item	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**
It's risky to open an email from an unknown sender.	61.43	31.84	4.04	1.79	0.90
It's risky to send sensitive work files using a public Wi-Fi network.	47.11	36.00	10.22	3.56	3.11
My work environment is positive and provides satisfactory work conditions.	19.20	60.71	7.14	11.16	1.79

7.3.3.2 Awareness

As depicted in Table 7.3, employees were mostly aware of good password use (80%) and phishing (88%), while 89.7% of employees also felt morally obliged to report suspicious activity. However, there seems to be a grey area (20.89%) when it comes to the use of social media, with 55.11% being of the opinion that social media could impact their career. as opposed to 24% who believe that it should be decoupled from their working life.

Table 7.3 Distribution of items related to the construct *awareness*

	%				
Item	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**
It's acceptable to use my social media passwords on my work accounts.	1.33	7.56	11.11	48.00	32.00
I am not permitted to click on a link in an email from an unknown sender.	44.44	43.56	5.33	5.78	0.89
I can't be fired for something I post on social media.	4.00	20.00	20.89	33.33	21.78
If I see someone acting suspiciously in my workplace, it is my duty to report it.	33.33	56.44	5.33	4.89	0

7.3.3.3 Trust

From the results of Table 7.4 it is clear that respondents trusted their own judgement more than that of others, with 58.4% trusting the people they work with, 62.83% rating their colleagues as good and seeing the best in other employees, and 81.86% seeing the best in other employees. However, only 36.72% agreed that their colleagues were honest, 31.42% agreed that there was mutual trust between people and only 42.92% trusted their colleagues.

Table 7.4 Distribution of items related to the construct *trust*

	%				
Item	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**
Most people at my workplace are basically honest.	4.42	32.30	37.61	16.37	9.29
I tend to trust the people I work with.	3.98	54.42	12.39	25.22	3.98
Most of the people I work with are basically good and kind.	5.75	57.08	19.91	15.49	1.77
Most of the people I work with trust others.	3.10	28.32	46.46	19.47	2.65
Most of the people I work with can be trusted.	3.98	38.94	34.07	19.03	3.98
I tend to see the best in the people I work with.	16.37	65.49	11.06	7.08	0

7.3.3.4 Optimism bias (OB)

Table 7.5 depicts the results obtained from the OB questions. Four questions were asked relating to positive life events and seven questions relating to negative ones. The results of the questions pertaining to positive life events were as follows:

1. Chances that one's work will be recognised with an award: 46.22% more than the average
2. Expect to live past the age of 80: 53.83% more than the average
3. Expect to read about one's achievements in the newspaper: 31.39% more than the average
4. One's weight will remain constant for the next five years: 39.9% less than the average

While the results of the questions relating to negative life events were as follows:

1. Chances that one may have contemplated suicide: 80.81% less than the average
2. Do not expect to spend a night in hospital in the next five years: 43.31% less than the average
3. Contract a venereal disease: 82.36% less than the average
4. Have a heart attack before the age of 60: 64.55% less than the average
5. Won't fall ill next winter: 45.21% less than the average
6. Likely to take an unattractive job: 60.54% less than the average
7. Likely to be fired from a job: 75.79% less than the average

The respondents were confident about their mental health, general health and having a successful career.

Table 7.5 Distribution of items related to the grouping *optimism bias* (OB)

	%													
Item	**10% less**	**20% less**	**40% less**	**60% less**	**80% less**	**100% less (no chance)**	**Average**	**10% more**	**20% more**	**40% more**	**60% more**	**80% more**	**100% more**	**3 times average**	**5 times average**
Compare to other employees, what do you think are the chances that your work will be recognised with an award?	2.67	0.89	3.56	2.67	5.78	7.11	31.11	0.89	3.11	4.89	10.67	18.22	6.22	1.78	0.44
Compare to other employees, what do you think are the chances that you expect to live past the age of 80 years old?	1.81	1.36	3.62	3.17	2.26	4.98	28.96	2.71	3.62	3.17	9.50	18.55	15.38	0	0.90
Compare to other employees, what do you think are the chances that you may have contemplated suicide?	7.59	1.79	1.34	2.23	3.13	64.73	6.70	1.79	1.79	3.13	2.23	0.89	0.89	0	1.79
Compare to other employees, what do you think are the chances that you expect to read about your achievements in the newspaper?	7.17	3.59	2.24	2.24	8.52	23.32	21.52	2.69	2.24	4.93	7.17	6.73	5.83	0.90	0.90
Compare to other employees, what do you think are the chances that you don't expect to spend a night in hospital in the next 5 years?	4.91	1.34	6.70	6.70	10.71	12.95	30.80	1.34	2.23	4.02	4.46	6.25	6.25	0.45	0.89
Compare to other employees, what do you think are the chances that you are likely to contract a venereal disease?	6.79	3.17	4.98	6.33	14.03	47.06	13.57	0	0	0	2.26	0.45	1.36	0	0
Compare to other employees, what do you think are the chances that your weight will remain constant for the next 5 years?	4.48	3.59	7.62	4.48	5.83	13.90	25.11	1.35	1.79	4.93	6.73	7.17	12.11	0	0.90
Compare to other employees, what do you think are the chances that you will probably have a heart attack before the age of 60 years old?	9.09	4.55	7.73	5.91	10.45	26.82	21.82	2.73	2.73	1.36	1.82	2.27	2.27	0	0.45
Compare to other employees, what do you think are the chances that you won't fall ill next winter?	5.48	5.94	8.68	7.76	6.39	10.96	35.62	1.83	1.83	4.11	4.11	2.74	4.11	0	0.46
Compare to other employees, what do you think are the chances that you are likely to take an unattractive job?	5.38	4.04	8.97	6.28	8.52	27.35	21.52	2.24	2.69	3.14	4.93	1.35	2.69	0.90	0
Compare to other employees, what do you think are the chances that you are likely to be fired from a job?	5.83	0.90	5.38	8.97	16.59	38.12	17.49	1.35	0.90	1.79	1.35	1.35	0	0	0

7.3.3.5 Intention to behave securely

The results displayed in Table 7.6 show that 9.77% of respondents disagreed that the technical security controls implemented by the IT department would protect them. The majority of the respondents therefore trusted the controls implemented. In addition, 72.77% stated that their attitude towards secure behaviour had improved in the past two years.

Table 7.6 Distribution of items related to the grouping *intention to behave securely*

	%				
Item	**Strongly agree**	**Agree**	**Don't know**	**Disagree**	**Strongly disagree**
I believe my system is secure and will protect me from cyberthreats.	9.33	41.78	39.11	8.44	1.33
My attitude has positively changed towards information security (security behaviour) over the past two years.	17.41	55.36	19.64	7.59	0

7.3.4 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). Given that the study was largely exploratory, the decision was taken not to enforce the usual outer loading cut-off thresholds. For example, some theorists suggest that the outer loadings of items should be greater than 0.7 when conducting a PLS-based analysis (Vinzi et al., 2010). This strict view of outer loadings can, however, stifle exploratory research. It is for this reason that Hair et al. (2017) suggest the following measures:

- Items which exhibit a factor loading below 0.4 should be eliminated without further assessment. In this study, none of the items had factor loadings below 0.4.
- Items with factor loadings that fall between 0.4 and 0.7 may be kept at the researcher's discretion. However, this only applies when the elimination of these

items does not increase the average variance extracted (AVE) value of the associated latent construct. Although some items had factor loadings within this range, their removal did not increase the AVE value of the constructs in question. As such, these items were retained.

All the items with outer loadings in excess of 0.7 were kept and formed part of the resultant multivariate analysis.

7.3.5 Evaluating the measurement model

As part of this evaluation, both convergent and discriminant validity were assessed. To assess convergent validity, all the constructs and their respective items were investigated to establish whether their factor loadings exceeded 0.5. In addition, the significance of the outer loadings of the items using their associated t-statistic values were assessed. The outer loading of each item was subsequently 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, the Fornell-Larcker criterion was used 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). Table 7.7 presents these square root values on the diagonal. The cross loadings were inspected to ensure that the items of each construct loaded highest on itself (see Table 7.8). As a third means of assessing discriminant validity, the mean heterotrait-monotrait (HTMT) ratio values were inspected; these were all found to be below the theoretical threshold of 0.9 (Kline, 2011; Henseler, Ringle and Sarstedt, 2014) (see column 3 in Table 7.9). Together, these tests confirm that the measurement model is valid from both a convergent and a discriminant perspective. Since a PLS-based analysis was performed, the measurement model was assessed 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 Table 7.1 for a complete outline of these VIF values. As a final means of evaluating the measurement model, the reliability of the questionnaire was assessed 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 found to be in excess of the accepted threshold of 0.7 (Tavakol and Dennick, 2011), as presented in Table 7.7.

Table 7.7 Measurement model statistics

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**

Table 7.8. Cross-loading values

	Trust	**Attitude**	**Awareness**	**Intention to behave securely**
Q45	0.537	0.215	0.083	0.265
Q46	0.673	0.248	0.196	0.291
Q47	0.755	0.257	0.069	0.297
Q48	0.777	0.256	0.158	0.29
Q49	0.849	0.418	0.241	0.449
Q50	0.564	0.146	0.126	0.255
Q18	0.307	0.801	0.165	0.642
Q21	0.213	0.688	0.486	0.401
Q25	0.306	0.649	0.349	0.374
Q26	-0.163	0.179	0.762	0.045
Q27	0.28	0.393	0.784	0.357
Q29	-0.155	0.149	0.781	0.063
Q30	0.076	0.154	0.774	0.164
Q23	0.326	0.686	0.33	0.857
Q24	0.432	0.437	0.271	0.795

Table 7.9. Heterotrait-monotrait (HTMT) ratio values

	Original est.	**Bootstrap mean**	**Bootstrap SD**
Trust -> Attitude	0.722	0.721	0.053
Trust -> Awareness	0.677	0.677	0.054
Trust -> Intention to behave securely	0.673	0.676	0.053
Attitude -> Awareness	0.825	0.826	0.030
Attitude -> Intention to behave securely	0.817	0.818	0.038
Awareness -> Intention to behave securely	0.951	0.868	0.030

7.3.6 Evaluating the structural models

To evaluate the models from a structural perspective PLS path modelling was used, 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 7.2. From the results illustrated in Figure 7.2, it is clear that there is support for hypotheses 1, 2, and 3. Additionally, the **global model** (all the responses from both the unrealistically optimistic and 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; Vinzi et al., 2010).

From 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).

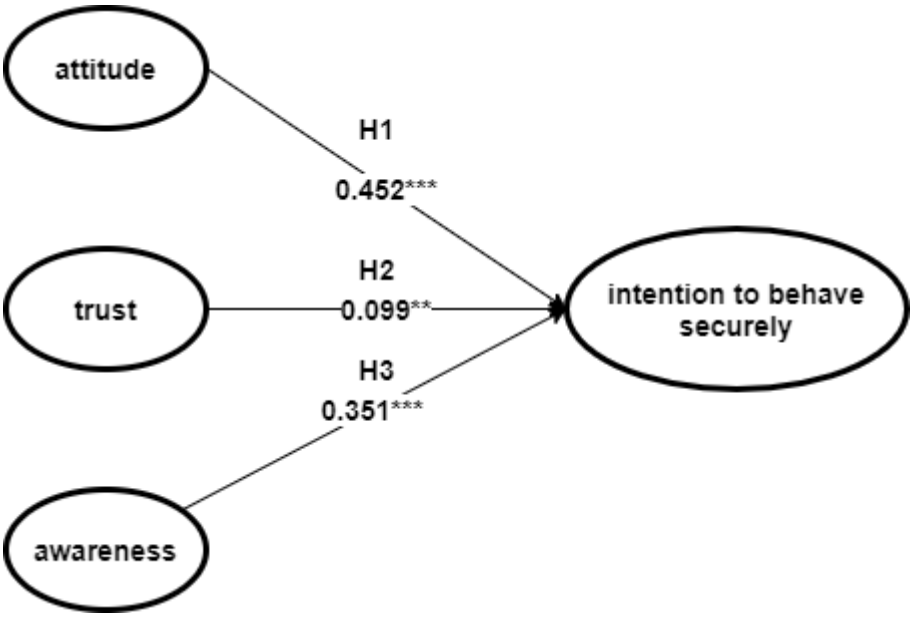


Figure 7.2 Quantitative research model (global), *** at p < 0.01, ** at p < 0.05

In addition to the significance testing that was conducted, the relative impact of each independent variable was also assessed by inspecting their effect sizes 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 *awareness* (0.103 – a small effect), and finally, *trust* (0.023 – the smallest effect).

This indicates that an individual's attitude towards information security is pivotal when explaining their intentions to act securely within the workplace.

Figure 7.2 represents the full sample population, consisting of the unrealistically optimistic and average groups. It is important to note that Figure 7.3 represents the multigroup, distinguishing between the two groups.

7.3.7 PLS multigroup analysis (unrealistically optimistic vs average group)

Because the results of the global model did not allow for it to be inferred that a significant difference exists between those individuals who are optimistically biased as opposed to those who are not, a PLS-based multigroup analysis was conducted. Although a repeated application of unpaired t-tests (or a permutation test, for that matter) could be employed, 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, a bootstrapped significance test was also performed. 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, Henseler and Ringle, 2011). From the results presented in Table 7.10, it is apparent that all the relationships illustrated in Figure 7.3 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 individuals classified as average. Importantly, these multigroup (two groups) results provide support for the fourth hypothesis (H4a, b, and c). Refer to Table 7.11 for a summary of all the models that comprise this study.

Table 7.10 Results of the multigroup analysis, *** at p < 0.01, * at p < 0.10 (unrealistic optimists vs. average)

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

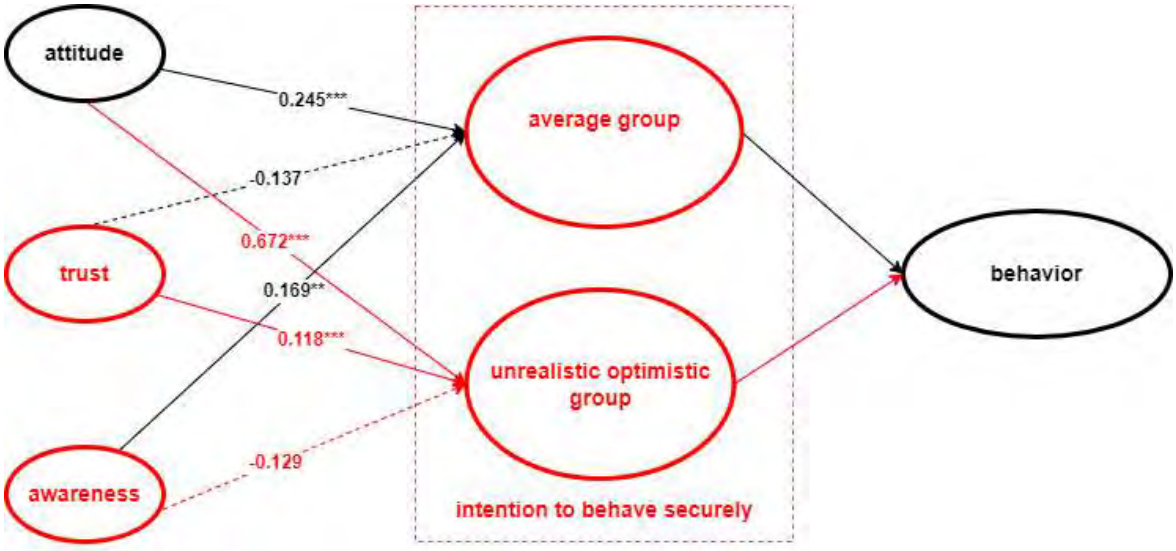


Figure 7.3. Intention to behave securely

The results of Figure 7.3 will be discussed in greater detail in the next section.

Table 7.11 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	0.363	0.672	7.514***	0	0.509	0.245	2.624***	0.01	0.064	0.427	3.841***	0
awareness → intention to behave securely	0.351	5.456***	0	0.103	-0.129	1.092	0.277	0.011	0.169	2.202**	0.03	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	0.13	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						

*** at p < 0.01; ** at p < 0.05; * at p < 0.10

7.4 Discussion

This section discusses the results of the quantitative analysis specifically referring to the three constructs: attitude, trust and awareness. The results are analysed, explained and linked back to the literature where applicable.

7.4.1 The significance of attitude

The quantitative results of this study, based on the survey which used the research instrument (Table 7.1), indicate that respondents were influenced by their *attitude* towards secure behaviour. *Attitude*, for the global group, was shown (Figure 7.2) to exert a significant influence on *intention to behave securely* with a positive relationship observed between the two variables ($\beta = 0.452$, $p < 0.01$, large effect size – 0.363).

This result confirms the literature discussion in Chapter 4, specifically Section 4.2 on the significant influence of attitude on the intention to behave securely. People with a positive attitude towards information security generally want to behave securely and comply with their organisation's information security policies. This is in line with Lowry and Moody's (2015) study which showed that people with a positive attitude want to comply with policies and thus have a willingness to behave securely. Given that two of the questions in the multivariate analysis (Q18, Q21) were related to the secure use of technology, the respondents demonstrated that their intention was to behave securely. The majority of the respondents knew that opening an email from an unknown sender is risky and that they should not use public Wi-Fi when working with sensitive files. It would therefore appear that they were aware of these risks and displayed a positive attitude towards the intention to behave securely. The study by Turkanović and Polančič (2013), mentioned in Chapter 4, confirms that attitude towards privacy and security comprises moving from an unaware state to a point of greater awareness where people try to protect themselves as best as they can. This is understandable, as most employees are loyal to their employers, building a win–win relationship for both parties (Fernandez and Moldogaziev, 2013). Accordingly, there is a chance that only disgruntled employees will deliberately put their employer at risk and it is therefore unlikely that this behaviour would be declared in a survey (Schouteren, 2019).

The third question (Q25) was based on how they experienced their work environment. The majority of the respondents experienced a positive work environment, further enhancing a positive attitude; again, we found literature that makes similar claims (Cuganesan, Steele and Hart, 2018). A positive work environment creates opportunities for learning and development that could lead to greater awareness of information security. By contrast, a negative environment could lead to carelessness and destructive behaviour.

Interestingly, De Kok, Oosting and Spruit (2020) divided attitude into three components:

1. The affective component is made up of an individual's emotions about something or someone.
2. The cognitive component is formed by evaluating character traits.
3. The behavioural component is concerned with attitudes shaped by previous behaviour and experience.

The result of De Kok, Oosting and Spruit's study was that *cognitive attitude* scored higher than affective attitude, but both were significant in the intention to behave securely. They omitted the behavioural component since people acquire their attitude only rarely from their behaviour or experience, for example when an individual cannot explain their behaviour in a credible way (De Kok, Oosting and Spruit, 2020). Interestingly, OB is also defined as a *cognitive* bias.

The results in Figure 7.3 show a significant influence and a positive relationship between the two variables, *attitude* and the *intention to behave securely,* for the average group ($\beta = 0.245$, $p < 0.01$). In general, people are hopeful and have a positive outlook on life (Weinstein, 1980). As expected, a more significant relationship between the two variables was found for the unrealistically optimistic group ($\beta = 0.672$, $p = 0$). Unrealistically optimistic people expect to experience only positive things in life and by default have a positive outlook. In the context of this study, unrealistically optimistic people might have therefore behaved insecurely as they did not believe that anything bad, such as succumbing to a phishing attack, would happen to them.

In Chapter 4 the risks of unrealistic optimism were explained. Unrealistic optimism occurs when someone does not expect bad things to happen to them. Accordingly, unrealistically optimistic people could fall victim to a phishing attack thinking it could never happen to them. In addition, the intention to behave securely might not be closely linked to actual secure behaviour (Jalali et al., 2020). The survey did not test for the

intention to behave securely based on the offering of a reward, but was more inclined to be fear based: “it is risky to …”. Unrealistically optimistic people respond better to reward based cues, thus succumbing to phishing attacks (Sharot, 2011).

In Chapter 5, the theory of planned behaviour (TPB) was discussed. The theory states that there are various motivating factors that influence the intention to behave in a certain way. One of these factors is *attitude*, which is an indication of how hard people are willing to try to perform a certain behaviour (Ajzen, 1991). From the univariate analysis (Section 7.3.3.1) it is clear that people will try their best to behave securely. Therefore, this result supports the fact that attitude has a significant effect on the intention to behave securely.

This study argues that an individual’s attitude towards information security is pivotal in explaining their intentions to act securely within the workplace. Furthermore, the statistical results show that the relationship between the two variables, *attitude* and *intention to behave securely,* is more significant for unrealistically optimistic people than the average group. In Chapter 8, actual behaviour will be evaluated using an experiment and interviews will be conducted to gain a more in-depth understanding.

7.4.2 The significance of trust

The quantitative results (see Figure 7.2) show that *trust,* for the global group, significantly influences *intention to behave securely* with a positive relationship ($\beta = 0.099$, $p < 0.05$). The results of the univariate analysis (items Q45 to Q50) depict that people tend to trust their own judgement more than that of others. Kramer (2009) confirms that people tend to overestimate their own judgement because they only see what they want to see. Logg, Minson and Moore (2019) found that people trusted their own judgement rather than that of an algorithm when they had expertise in forecasting. Thus, people tend to rely on their own knowledge and experiences. People are also more trusting of their peer group, those who look like them and have the same beliefs. They are therefore more likely to trust without validating what is said (Shareef et al., 2020).

The majority of the survey respondents tended to see the best in the people they worked with and therefore could trust the judgement of others when it came to areas of expertise, for example implementing technical IT security controls. Trust was discussed in Chapter 4 (Section 4.3), explaining that in this study the focus was placed on the trust that employees place in the technical security controls implemented by their IT

department. Trust in controls is more than an emotional reaction; it is also a set of assumptions or expectations about these technical controls and their ability to protect data (Butavicius et al., 2020). As previously discussed, this could lead to a false sense of security where the employees blindly trust the implemented security controls to protect them from a cyberattack in the workplace. This is further exacerbated by the current working-from-home paradigm. Employees find it difficult to draw a clear line between work and family life. They spend time on social networking sites during the working day, sharing personal and business information with trusting ignorance (Colwill, 2009; O'Reardon and Rendar, 2020). This results in careless behaviour, more specifically insecure behaviour, as the employee does not take responsibility for their actions.

The quantitative results indicate a positive relationship (β = 0.118, not significant) between *trust* and the *intention to behave securely* for the unrealistically optimistic group, whereas the average group has a negative relationship (β = -0.137, not significant). This result confirms that the unrealistically optimistic group are more trusting than the average group. Furthermore, the result agrees with the *optimistic trust effect* mentioned in Chapter 4, where unrealistically optimistic people have a natural inclination to trust (Wilson and Darke, 2012). As previously mentioned, people who are trusting are more susceptible to becoming victims of social engineering than those who distrust. Furthermore, considering that the unrealistic optimists only expect good things to happen to them, they are more susceptible to phishing attacks.

7.4.3 Information security awareness training (ISAT)

The quantitative results for the global group show that there is a significant and positive relationship between *awareness* and *intention to behave securely* (β = 0.351, $p < 0.01$). This is in agreement with the findings of a study performed by Li et al. (2019), who found that employees who are more aware of their company's information security policy and procedures were better equipped to behave securely. When people can identify a phishing email, their chances of being caught diminishes. Practically speaking, awareness alone is not enough (Aloul, 2012; McCormac et al., 2017) as it should be followed by real-world tests to see if actual behaviour has changed. Topical emails, those that reflect current news or trends, are often seen as legitimate. ISAT must highlight this fact and enable people to know what a phishing email looks like.

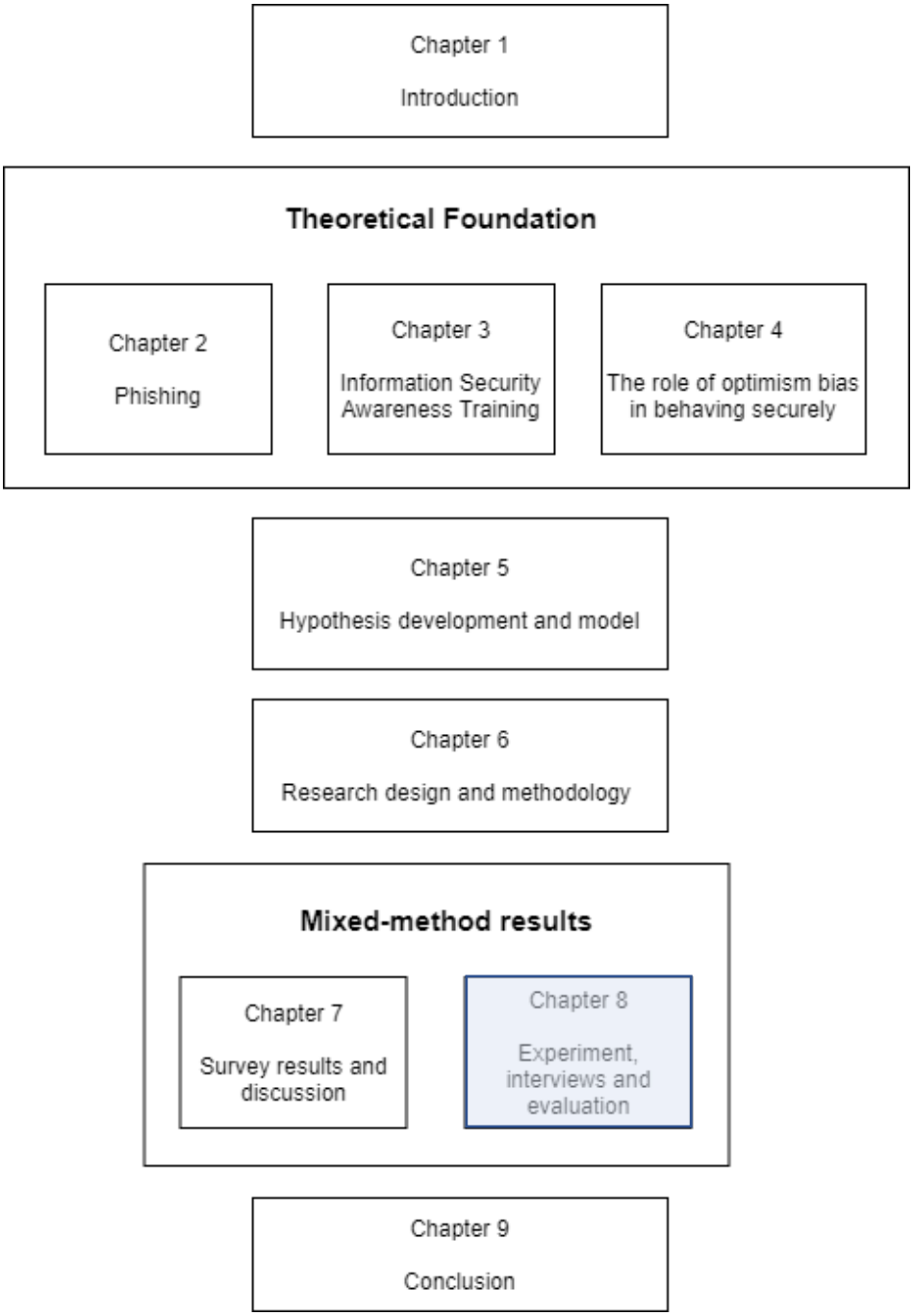
A negative relationship between awareness and the intention to behave securely was found for the unrealistically optimistic group (β = -0.129, p = 0.277). ISAT could be seen as a waste of time, as unrealistically optimistic people do not think it is relevant to them. Because of their bias, they ignore everything that contradicts their view. On the other hand, a positive relationship between *awareness* and *intention to behave securely* (β = 2.202, p = 0.277) was found for the average group, Thus, it seems that the average people realised that anyone can fall victim to a phishing attack and therefore needed to arm themselves with knowledge to protect themselves.

7.5 Summary

The purpose of this chapter was to present the results of the quantitative data analysis in detail. A pilot study was first conducted to determine whether the survey instrument was considered reliable. This was followed by data collection for the main study. A discussion on the sampling strategy was also provided, with the use of systematic random sampling being indicated as a reliable strategy. The results of the reliability and factorial validity test were then presented. PLS-SEM was identified as the appropriate technique for analysing the structural relationships between multiple constructs in this study. In this regard, a detailed discussion of the measurement model and structural model was provided. In Section 7.3.6 the global quantitative model was discussed with the results depicted in Figure 7.2, while Table 7.10 and Figure 7.3 showed the results of the multigroup comparing the two groups of respondents based on their OB responses. In addition, PLS-SEM was used for the statistical analysis of the quantitative multigroup to distinguish between the unrealistically optimistic and average groups. The chapter concluded with an overview of the path estimates of the model and the outcomes of the hypothesis tests. The next chapter provides a detailed discussion on the evaluation methods used.

CHAPTER 8

EXPERIMENT, INTERVIEWS AND EVALUATION



8. EXPERIMENT, INTERVIEWS AND EVALUATION

8.1 Introduction

In this study a model was developed to better understand phishing susceptibility. In Chapter 5, six hypotheses were proposed to investigate why certain individuals are more prone to this phenomenon. The previous chapter presented the theoretical model as a path diagram and reported several statistically significant findings. This chapter delves into the findings of the experiment and discusses how the evaluation was performed. Further, it provides additional insight into how the results and present literature apply to the research problem, namely phishing susceptibility while taking optimism bias (OB) into account. The survey (quantitative analysis) measured the *intention to behave securely*, whereas the experiment measured actual secure *behaviour*. Essentially, the context of this study is theorised throughout, with specific references to how attitude, awareness and trust contribute to the results of the structural model. Semi-structured interviews were conducted after each simulated phishing attack to better understand why people succumbed to the attacks. The chapter concludes with an evaluation of the study model using a concurrent triangulation design.

8.2 Information security awareness and secure behaviour

8.2.1 Phishing experiment

To test actual behaviour, a phishing experiment was conducted that consisted of three simulated phishing attacks and three information security awareness training (ISAT) sessions. Online awareness training was performed before every phishing attack using the company's learner management system (LMS). The experiment took place over a period of seven months, with one of the simulated phishing attacks being fear based and the other two reward based. A number of email addresses were used to send the phishing emails from the various domains used for hosting the phishing sites, none of

which would have been familiar to the employees. The emails and websites should therefore have been treated with caution. This experiment was conducted in such a way that the email appeared as real as possible.

8.2.1.1 Design considerations

The employees would have recognised the content of the phishing email owing to the familiar logos and graphics used, which are publicly available on the internet. It is important to also note that a disgruntled terminated employee could provide these details to a hacker group to perform these attacks. In the experiment, an email with a link to a phishing site was sent to all the survey respondents. When the link was clicked, the phishing website opened and recorded the email address. When the respondent entered their details and clicked on the submit button, their username was stored together with their email address. In the first simulated phishing attack, once the respondent had clicked on the submit button they received a message stating that they had successfully opted out. The other two phishing attacks worked differently. Once they had clicked on the submit button, the page refreshed without displaying an error or a success message, ready to accept their credentials again. This confused the employees into thinking that they had supplied incorrect credentials or that the site had broken down. Consequently, many of them tried again with different credentials hoping to login successfully and progress to a screen where they could carry out their desired action. Notably, to ensure confidentiality passwords were not saved.

Creating a fake phishing site can be done relatively easily and very quickly. The phishing sites for this study were created using the Python programming language; specifically implementing the Flask module (see Appendix D). Saving logos and images from the original websites and using them in a phishing site is a simple task, as there are multiple tools available, from “ripping” content from a website to creating a duplicate of an entire site (see Figures 8.2, 8.4 & 8.6). In addition, various open-source tools, for example King Phisher, Gophish and Zphisher facilitate the entire phishing exercise. Gophish is labelled an open-source phishing framework that assists with setting up phishing templates, creating phishing campaigns that will manage the sending of the emails and track the results. Although this tool was created to be used by organisations to test their employees, nothing stops bad actors from using it maliciously. To make matters worse, phishing is offered as a service on the dark web (Hyslip, 2020).

Setting up the phishing site is the first step. The next step is to craft an email that will contain the required fear appeal or reward motivation to entice someone to click on the link and part with their credentials or install malware. Multiple vendors offer mass email as a service. These services, for example Sendgrid, modify the URL ink in the email into a tracking link making it difficult to determine whether it is malicious or not.

Websites are generally considered to be legitimate if they have a security certificate installed. This certificate is indicated with a lock icon in the address bar. When the icon is clicked it will provide details about the specific certificate. These normally state that communication with the website is secure, for example that it is safe to enter your credit card details. In the past, security certificates were expensive and therefore not purchased by malicious actors. This changed when a non-profit certificate authority called Let's Encrypt (https://letsencrypt.org/) started to provide TLS certificates for free. Today, anyone can register a domain and apply a certificate fairly easily, creating the illusion of a legitimate website.

Therefore, ISAT needs to take the above into consideration in making people aware of how the technology landscape is changing. Technology is forever changing and security best practices and awareness training must be constantly updated.

8.2.1.2 Simulated phishing attack number 1: fear based

The first phishing attack was fear based. Employees were notified by the phishing email (Figure 8.1) that management had decided to change the monthly pay date from the 27th day of the month to the last day of the month, giving the main reason for this change as the fact that it would make the company more profitable. If this email had been carefully considered recipients would have realised that this would not have resulted in a cost saving. The employees were then given a chance to vote against this change by casting their vote on a website (Figure 8.2) specifically created for this purpose.

Hi

Management has reviewed the company's current cost base. In order for the company to be more profitable, certain changes need to be made. A suggestion is to move the current paydate to the last day of the month, allowing for more interest to accrue in the company's bank account. As we respect our people, in line with our values, we are giving you the chance to opt out.

The option to opt-out is only available until 12h00 on Monday, 19 August 2019. To keep the paydate as is, we need at least 50% of our people to opt-out.

Please vote now. It is in your best interest.

Vote now

Regards

Figure 8.1 First simulated phishing attack: email

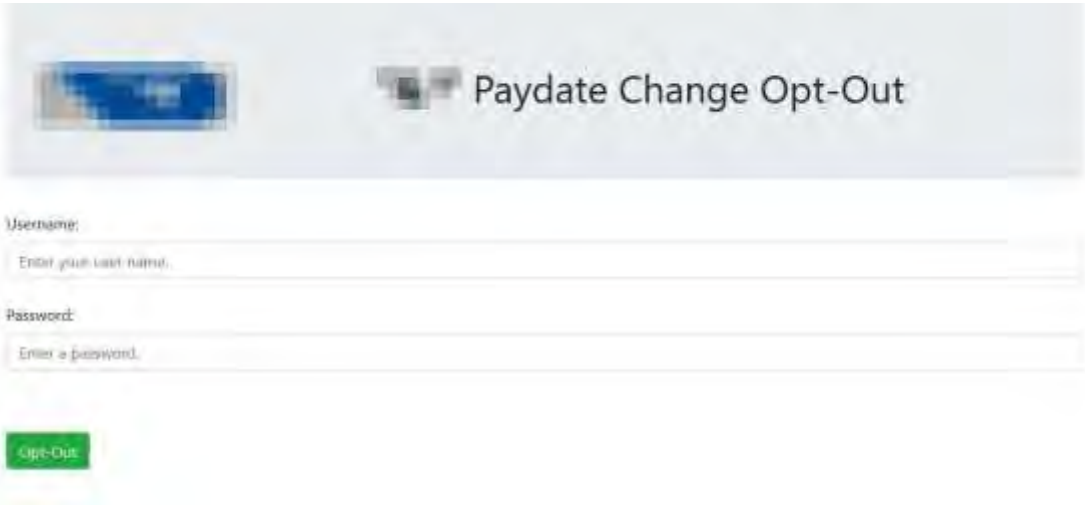


Figure 8.2 First simulated phishing attack: website

8.2.1.3 Simulated phishing attack number 2: reward based

From the literature, it is clear that people are more inclined to respond to reward-based phishing attacks (Bax, McGill and Hobbs, 2021). The second phishing email was sent shortly after Black Friday (Figure 8.3). At the company used in this experiment, Workpoints is an incentive scheme where employees can recognise good performance and award points to one another. These points are redeemed for vouchers that are used at one of the affiliated partners of the programme. The bait was that the employee needed to login to the site (Figure 8.4) to qualify for a lucky draw for 10 000 points. Keeping in mind that the average number of points that can be awarded by one employee to another is between 50 and 100, this was indeed a big reward.

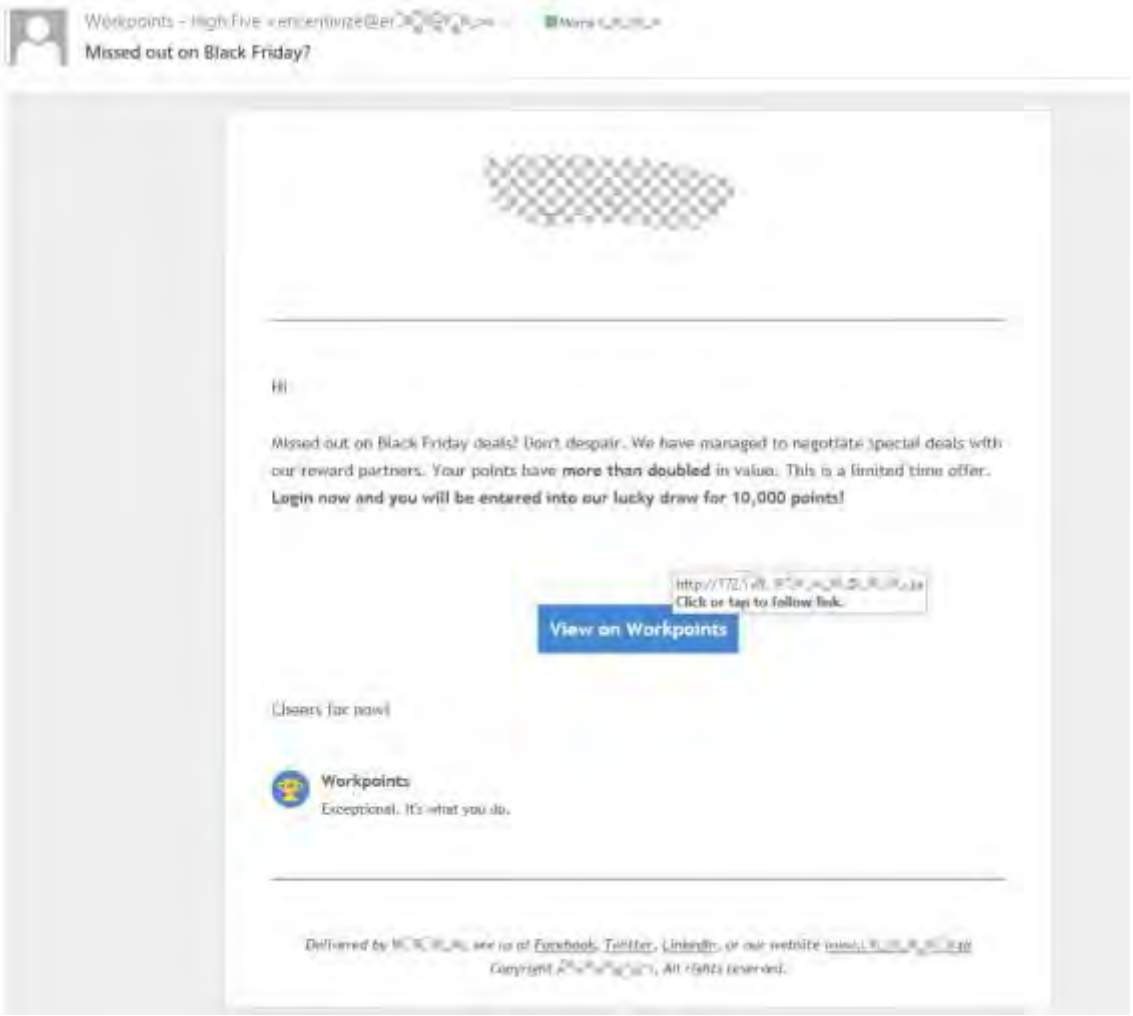


Figure 8.3 Second simulated phishing attack: email

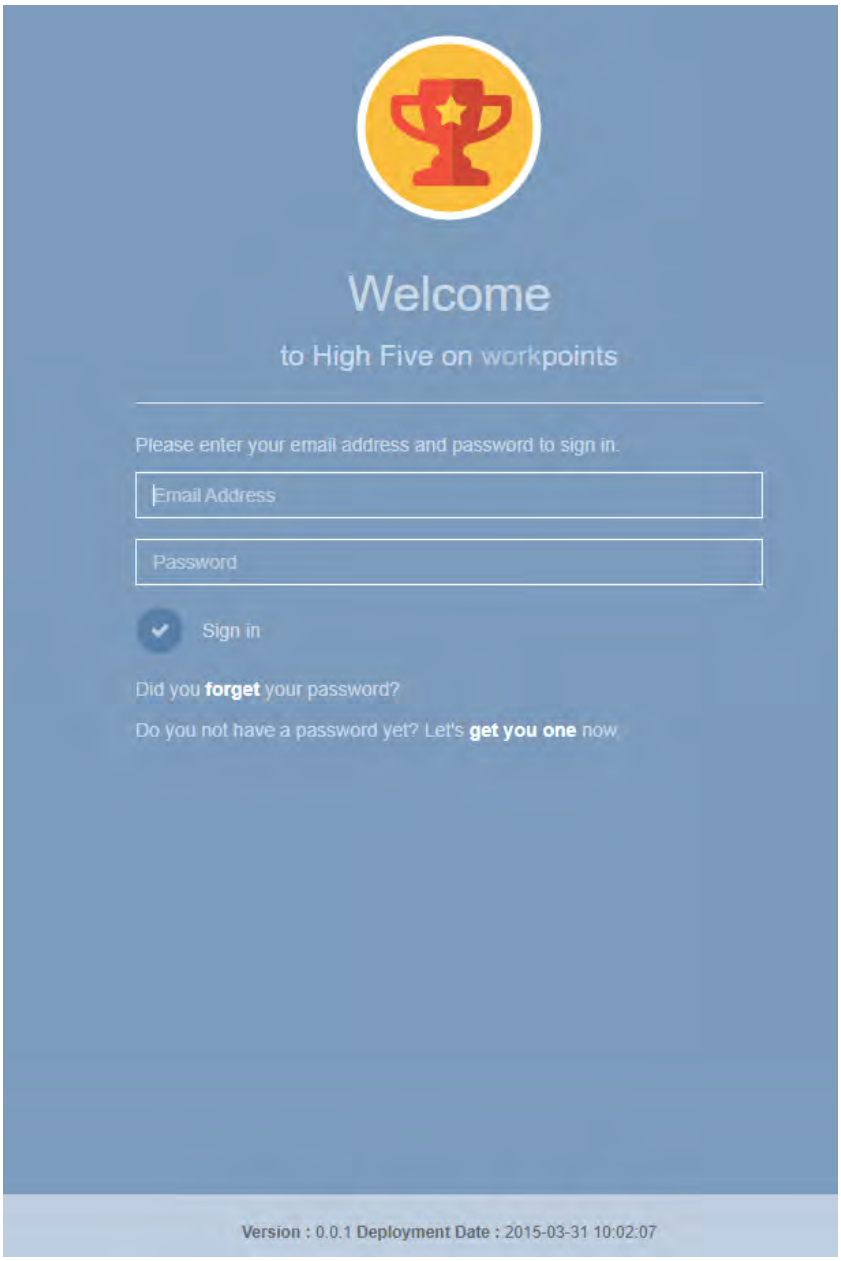


Figure 8.4 Second simulate phishing attack: website

8.2.1.4 Simulated phishing attack number 3: reward based

The third simulated phishing attack was based on changing legislation in South Africa regarding the collection of debit orders. There had been quite a bit of hype in the media about this change as it would affect anyone granting a debit order on their bank account. The DebiCheck website (https://debicheck.co.za/) contained training material for the general public explaining how the new process would work, providing extra security against unauthorised debit orders. As companies had to train their staff to understand the new legislation, this was a good time to launch a phishing attack with anything DebiCheck related. This email (Figure 8.5) differed from the previous phishing emails as there was no URL link in the text. Rather, the link was attached to an image so the employee had to click on the image to go to the site (Figure 8.6).

Figure 8.5 Third simulated phishing attack: email

Figure 8.6 Third simulated phishing attack: website

In the next section, the observed results of the experiment will be discussed.

8.2.2 Observed behaviour following ISAT

In our sample, 49% of respondents were classified as unrealistic optimists. Three phishing attacks in total were conducted and after every attack there was a decrease in the number of users who succumbed. This could be because of the ISAT that was done after each attack. Following each attack, a debriefing email (Figure 8.7) was sent to the participants to explain that the email they had received was a phishing attack. This email was used to create further awareness by explaining what the participants should have noticed to come to the conclusion that it was a phishing attack. Two specific items were highlighted: (1) the sender's email address was not an official company email address, such as debtmanagementconsultants@gmail.com and debicheck@emware.co.za, and (2) the website URL was not a company-owned domain.

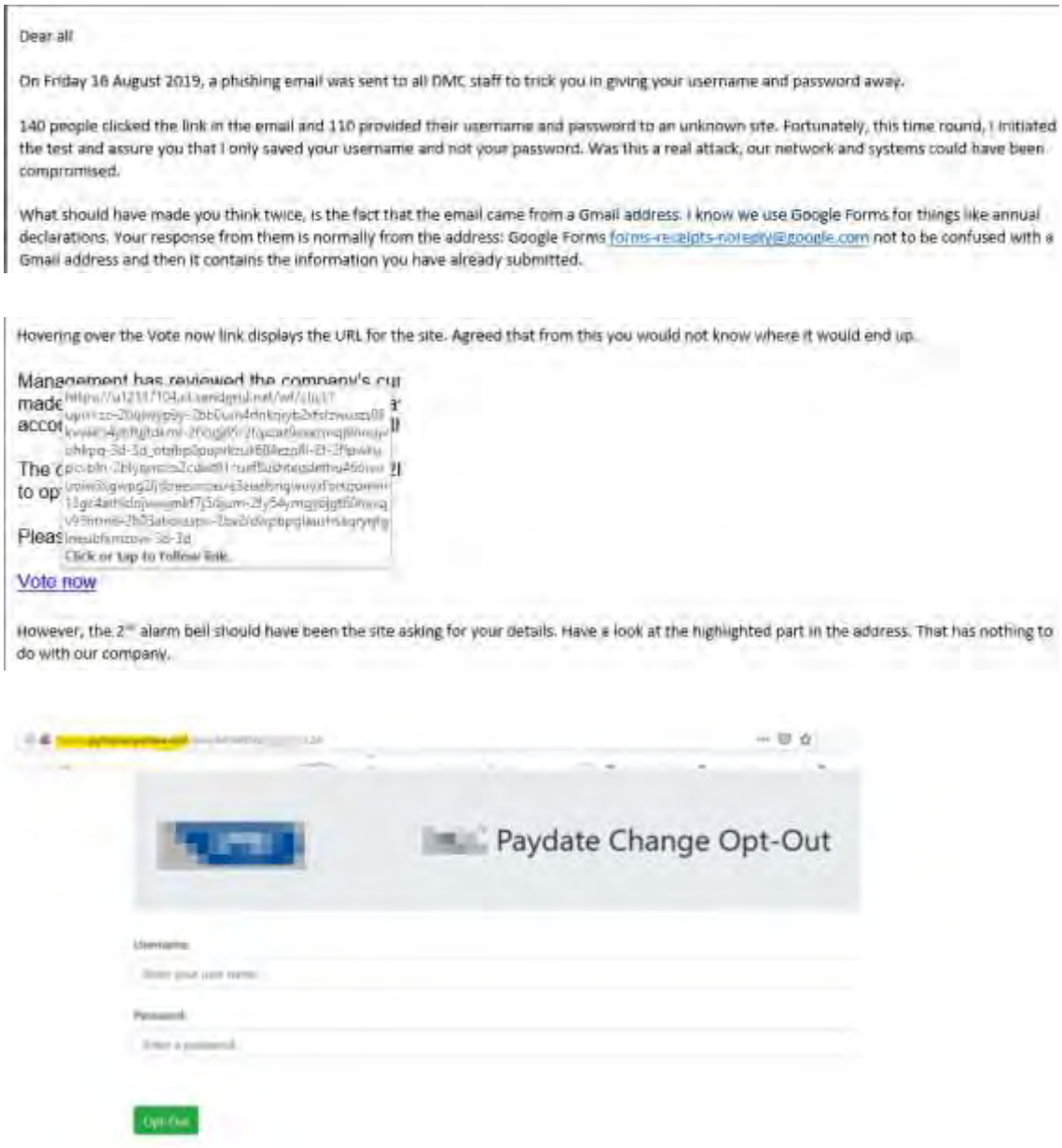


Figure 8.7 Debriefing email sent after first phishing attack

Figure 8.8 shows the percentage of users per group who clicked on the phishing link.

We performed a t-test on the phishing experiment results and found that t = 1.97 and p = 0.04, indicating that there was a significant difference between the average and the unrealistically optimistic groups, thus supporting the quantitative results.

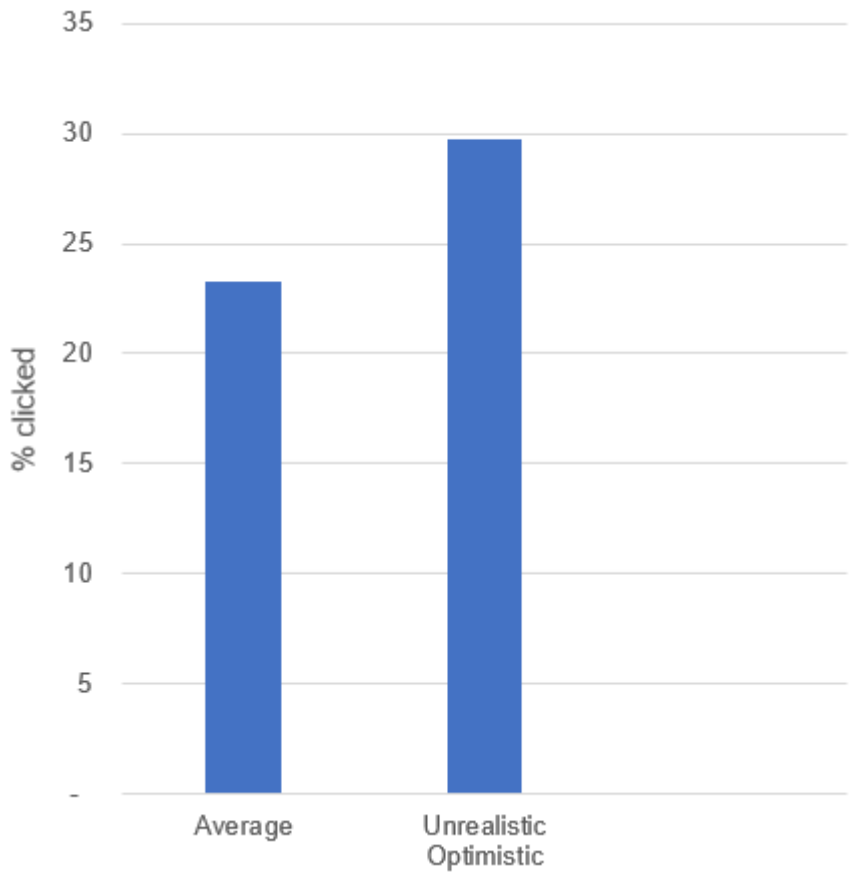


Figure 8.8 Combined phishing experiment result

Intentions on its own was a poor predictor of security behaviour, as more than 93% of the participants agreed that it is risky to open an email from an unknown sender, yet 23% of the participants in the average group and 29% in the unrealistically optimistic group not only opened the email but also clicked on the link. As a result, this study confirms previous findings in non-controlled settings that attitudes and intentions are frequently inconsistent with behaviour (Acquisti and Grossklags, 2004; Gundu, Flowerday and Renaud, 2019; Birch and Memery, 2020). It is therefore desirable to measure behaviour directly in order to understand the true state of information security in an organisation. Even in scenarios where users are quite familiar with the security behaviour in question, such as phishing emails, the need to measure actual security behaviour remains valid.

8.3 Interviews

Semi-structured interviews were conducted after each simulated attack to gain a better understanding as to why employees succumbed to the phishing attacks. See Tables 8.1, 8.2 and 8.3 for the interview plan and responses.

Types of questioning: The interview started with a general discussion, followed by directive questions to clarify the individual's behaviour. We specifically evaluated our three constructs using the following questions:

- Attitude: Did you check for any clues to indicate that it could be a phishing email?
- Trust: Do you trust the security controls implemented by the IT department?
- Awareness: Did you understand the training material?

Sampling method: Individuals who succumbed to the phishing attacks were interviewed until data saturation was reached with no new themes emerging.

Table 8.1 Interview 1 responses

	Participants						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Interview 1 (Fear-based email)							
Did you complete the training?	Yes	Yes	Yes	No	Yes	Yes	Yes
Did you understand the training material?	Yes	Yes	Yes	N/A	Yes	Yes	Yes
Why did you believe the phishing email was real?	Got me emotional; did not think it through	Would expect this from manage-ment	It seemed to be a legiti-mate request	I was upset about it	Looked like a company email	Emo-tional, wanted to stop the change	Looked legitimate and wanted to exercise my vote
Did you check for any clues that it could be a phishing email?	No	Yes	No	No	No	No	No

Do you trust the security controls implemented by the IT department?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Now that we have explained the phishing email, do you know what to look for in the future?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Summary of comments/themes	Emotionally upset that management wanted to change pay date. Inconvenience of debit order dates etc. Felt “short changed”.						

Table 8.2 Interview 2 responses

Interview 2 (Reward-based email)							
Did you complete the training?	Yes	No	Yes	Yes	No	Yes	Yes
Did you understand the training material?	Yes	N/A	Yes	Yes	N/A	Yes	Yes
Why did you believe the phishing email was real?	Looked similar to the incentive scheme used by the company.	It was timely. Black Friday passed and this was a chance to win points if you missed the specials.	I hoped I could win the incentive points.	It looked real.	Familiar with the incentive scheme.	The content of the mail made me believe it.	The logos used and the way it was written seemed legitimate.
Did you check for any clues that it could be a phishing email?	No	No	No	No	No	No	Yes
Do you trust the security controls implemented by the IT department?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Now that we have explained the phishing email, do you know what to look for in the future?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Summary of comments/themes	Did not want to lose the reward. Familiarity with the incentive scheme. Was timeous.						

Table 8.3 Interview 3 responses

Interview 3 (Reward-based email)							
Did you complete the training?	Yes	Yes	Yes	No	Yes	Yes	Yes
Did you understand the training material?	Yes	Yes	Yes	N/A	Yes	Yes	Yes
Why did you believe the phishing email was real?	A DebiCheck competition made sense as we are implementing it in the business.	Currently imple-menting Debi Check.	The compe-tition seemed easy.	Currently working with DebiCheck.	Subject is topical and timely.	We've all received Debi Check training. Seemed real.	Debi Check is a project we are working on.
Did you check for any clues that it could be a phishing email?	No	No	No	No	No	No	No
Do you trust the security controls implemented by the IT department?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Now that we have explained the phishing email, do you know what to look for in the future?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Summary of comments/themes	Familiarity with subject matter. Hoping to get the reward. Seemed easy.						

Sequencing: Since succumbing to a phishing attack is generally regarded as being a potential embarrassment for the individual (Petrič and Roer, 2022), it was important to start by building a foundation of trust between the interviewer and the interviewee. This was accomplished by introducing the topic slowly, beginning with the training and ending the interview with a discussion on why they thought they had succumbed to the attack.

Stance: The interviewer took a friendly approach and sympathising and empathising with the interviewees allowed the dialogue to flow.

Some of the reasons given by the participants as to why they succumbed to the attacks included that

- the email “looked legitimate”
- it was timely in the sense that it was a topic of discussion: “We were busy with DebiCheck training when we received the DebiCheck competition email.”
- they wanted the reward offered and did not want to lose what they deemed to be theirs.

Figure 8.9 describes the process used to derive the themes. Although the respondents declared that they understood the training, many were unable to identify the emails as phishing emails as they had succumbed to the attacks.

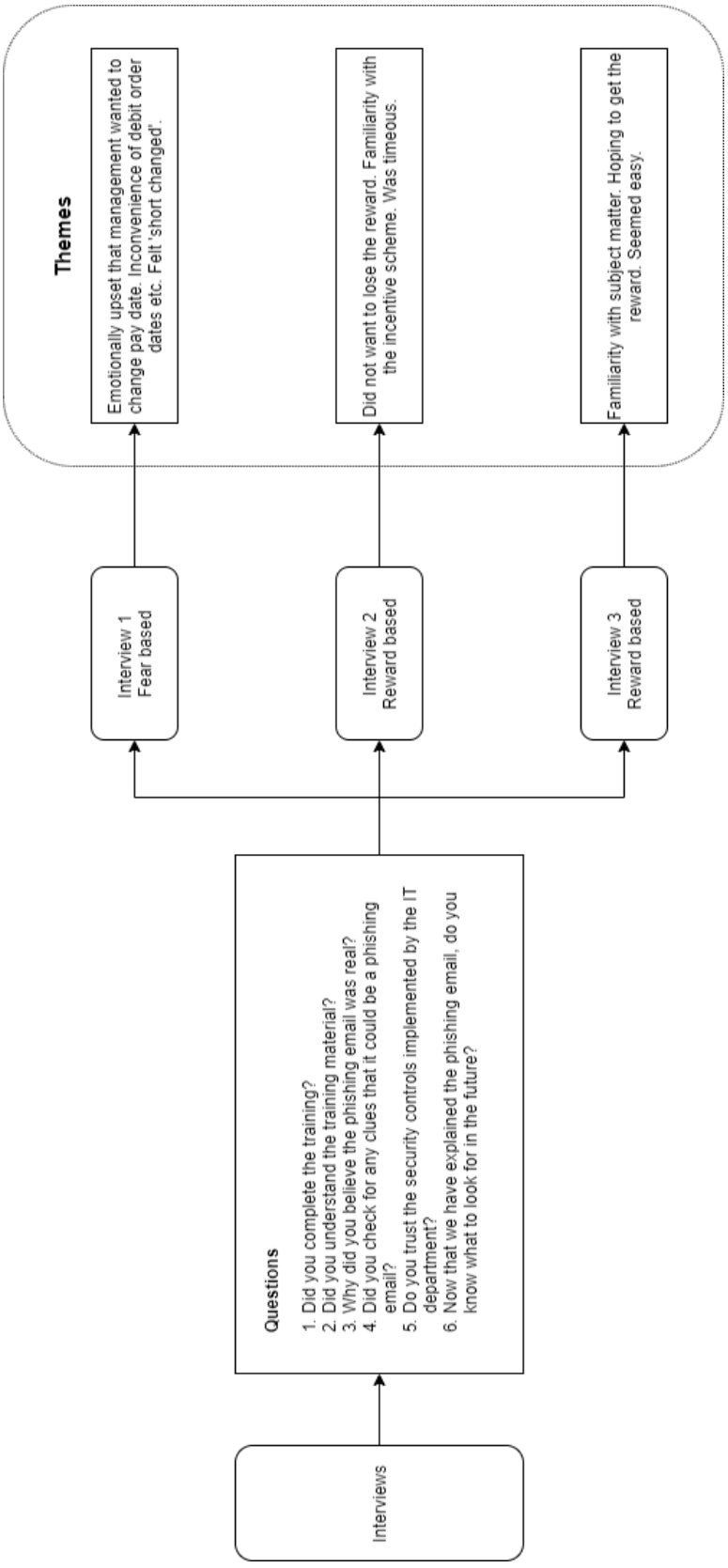


Figure 8.9 Interview mind map

According to the interview results, the fear-based email (simulated phishing attack number one) convinced the participants to take action. Fear is often used to emotionally "hook" someone to perform a specific action and Johnston and Warkentin (2010) found that fear appeals drive certain behaviour. In this instance, the fear was financial loss (being paid later) and inconvenience (debit order dates would have to be changed). Even though there was no real financial loss, emotion trumped cognitive thinking resulting in participants clicking on the phishing email. The respondents stated that the email created an emotional response which they acted on. This is in agreement with the study done by Leventhal (1971) who found that emotion is a strong driver of behaviour.

Similarly, the two reward-based emails (simulated phishing attack number 2 and 3) motivated the participants to click the link. Interestingly, Bax, McGill and Hobbs (2021) found that rewards influenced insecure behaviour more than protective behaviour. In other words, people are more interested in the reward than protecting themselves. This is demonstrated in the interview responses as people wanted the rewards at all costs. For this reason, this study used two reward-based emails and only one fear-based email.

Familiarity further deceived the participants into think that the emails were legitimate. Thus, through the use of the emails, specifically displaying images such as logos and fonts, trust was built. This agrees with the findings of Blythe, Petrie and Clark (2011), which confirm that when personalisation and familiarisation are used in phishing emails the chances of being successful increase. The phishing topics used were current issues and therefore further reinforced their familiarity.

Although the participants had completed the awareness training and confirmed that they understood it, they still succumbed to the attack. As the literature study revealed, awareness training reduces the risk of phishing but does not eradicate it completely (Aloul, 2012). This study therefore argues that to be successful in changing insecure behaviour, the effectiveness of awareness training should be tested and the training modified if necessary.

The participants clearly trusted (placed reliance) the security controls implemented by the IT department. They (the participants) were fully aware of these tools, as the endpoint protection was automatically updated and was visible in the system tray. Should the updates not happen, then they would be contact by an administrator to rectify the issue. This by itself further creates the impression of a father figure watching over them. As discussed, this could lead to a false sense of security and risky behaviour.

The debriefing sessions were done before the interviews making it clear how the respondents should have identified the email as a phishing attack. When they were asked whether they now knew how to identify a phishing email, they all agreed that they would be able to identify a phishing email in future. This indicates that their intention was to behave securely, which was the same behaviour observed in the quantitative results. Unfortunately, the subsequent phishing attacks demonstrated that their intention and actual behaviour were not aligned.

8.4 Unrealistic optimism and secure behaviour

Figure 7.3 depicts the significant differences between the two groups based on the quantitative data pertaining to the *intention to behave securely*. These differences were further confirmed by the experiment, which indicated the difference between the two groups for actual secure behaviour, with a larger proportion of the unrealistically optimistic group succumbing to the phishing attacks than the average group (Figure 8.8). Thus, this study argues that the unrealistically optimistic group behaves more insecurely and is more susceptible to phishing attacks than the average group. Interestingly, the results of the experiment agree with the results of the quantitative data in respect of (1) the *trust* construct, which showed the unrealistically optimistic group to be more trusting, and (2) the *awareness* construct, where the group had a negative relationship to the *intention to behave securely*. On the other hand, the average group was less trusting. Hong et al. (2013) found that less trusting employees deleted not only phishing emails but also some legitimate emails, therefore behaving securely. The average group also had a positive relationship between *awareness* and *the intention to behave securely*, which should result in secure behaviour. This confirms Weinstein's (1980) findings that unrealistically optimistic people see life through rose-tinted spectacles and do not expect "bad things" to happen to them, or more specifically in this study, to succumb to a phishing attack.

8.5 Triangulation

The use of quantitative and qualitative research approaches sequentially or concurrently to refine, evaluate and/or extend theory is known as methodological triangulation (Haase et al., 1999). Accordingly, research using quantitative and qualitative methods may be highly relevant if the theoretical underpinnings of each are considered carefully and the methods used do not contradict those assumptions (Haase et al., 1999). Jahangiri et al. (2008) describe triangulation as a broad collection of data or evidence derived from numerous and diverse sources. They further claim that this composite assessment methodology is thought to be more valuable because it compensates for any shortcomings associated with any single assessment method. For a triangulation method to be most effective, data from different sources should ideally overlap to some extent. For example, a quantitative analysis is complemented by a qualitative analysis, showing an overlap in testing the same relationships and coming to the same conclusion.

There are at least four types of triangulation possible: (1) data source triangulation, (2) analyst triangulation, (3) theory/perspective triangulation, and (4) methods triangulation (Patton, 2002). The data source and method types, in particular, are likely to increase the validity of this study. Data source triangulation entails gathering information from various types of people, such as individuals, groups or communities, in order to gain multiple perspectives and validate data (Carter et al., 2014). Method triangulation involves the use of multiple methods of data collection about the same phenomenon (Polit and Beck, 2008). The resurgence of interest in mixed methods research has emphasised the approaches in which methods triangulation can increase confidence in the findings of a study that combines quantitative and qualitative methods (Yin, 2013).

The evaluation of the model for this study was performed using a concurrent triangulation design (see Figure 8.10) (Saunders, Lewis and Thornhill, 2016). Secondary data was collected via a literature review to obtain an in-depth understanding of the current theories and models that informed this study. Our primary data collection, including both qualitative and quantitative data, was conducted in the same phase of the research in order to compare how these data sets support one another. Our quantitative data consisted of a cross-sectional survey and our qualitative data of an experiment and interviews.

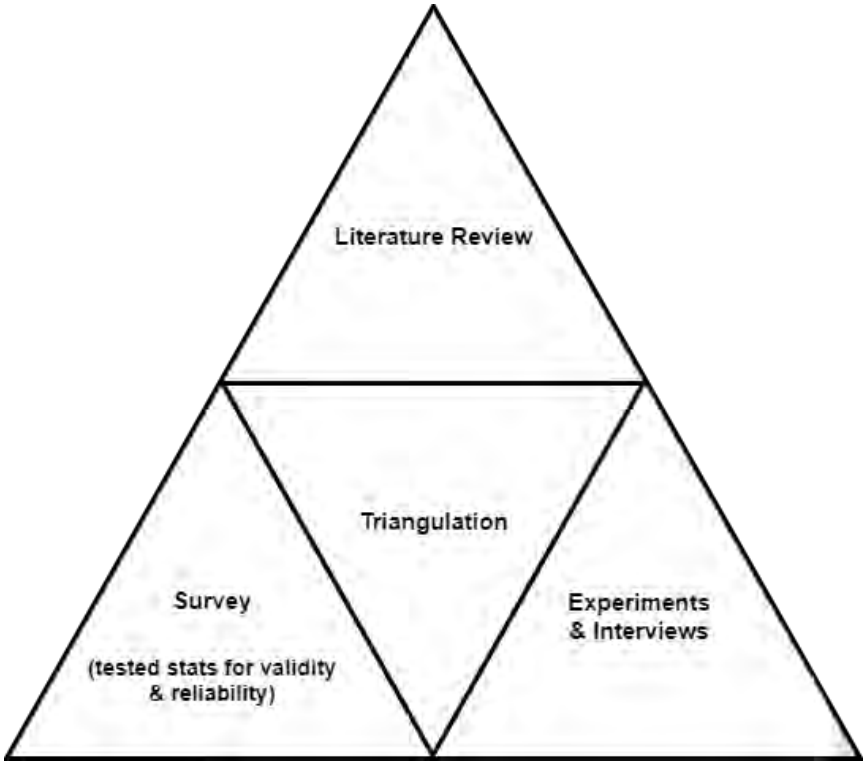


Figure 8.10 Evaluation via triangulation (Saunders, Lewis and Thornhill, 2016).

8.6 Summary

The focus of this study was to gain a better understanding of why certain users are more susceptible to phishing than others. Prior research has shown that ISAT has a positive effect on secure behaviour but is not entirely effective in eradicating insecure behaviour. In an attempt to understand or explain human behaviour, researchers often consider the various personality types (the 'Big 5') (Ifinedo, 2012; Safa et al., 2015). Other human traits that have been considered include attitude and trust (Herath et al., 2014; Guhr, Lebek and Breitner, 2019). In this study we hypothesised that OB plays a significant role in secure behaviour, thus distinguishing our study from previous research.

We found that attitude had a significant influence on the intention to behave securely in the workplace. Interestingly, Chowdhury, Adam and Teubner (2020) found that not only does attitude affect the individual user, but the attitude of supervisors and managers towards secure behaviour also had a direct impact on subordinates. Therefore, ISAT programmes could be adapted to include a section specifically intended to encourage supervisors and managers to set a good example for their subordinates. A bad attitude towards behaving securely could also be related to work stress and therefore ISAT programmes could be adapted to point this out to users. User performance is usually managed by an agreed set of key performance indicators (KPIs). We suggest that KPIs could be modified to include a measure of ISAT programmes completed, including how to avoid being the victim of a simulated or real phishing attack and the need to report suspicious emails to one's manager or the IT department.

The effectiveness of an ISAT programme is also influenced by how it is presented. Using interactive methods to engage participation during training and being able to test the subject matter after the training are critical. ISAT is not a once-off event but an ongoing programme focusing on current threats and scenarios, so that users can relate and correctly respond to these threats (Bauer, Bernroider and Chudzikowski, 2017). We conclude that the number of ISAT interactions that employees are engaged in has a direct impact on their intention to behave securely.

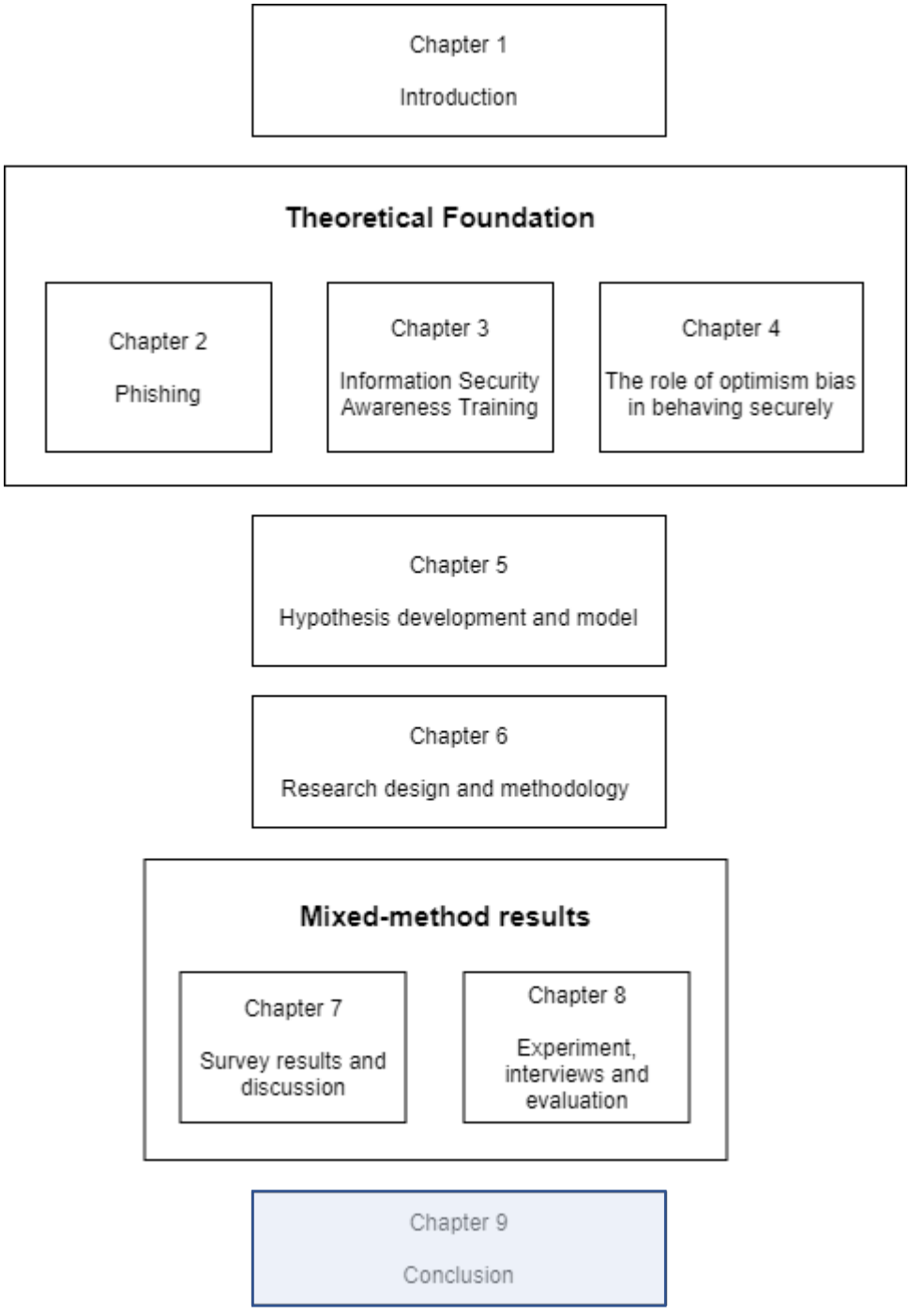
In addition, we found that trust plays a significant role in how users behave in the workplace. The presence of dedicated IT departments that manage the end-user environment by implementing restrictive administration controls and demonstrating to users that a father type figure is watching over them tend to create a false sense of security in organisations. This approach encourages users to blindly trust that these

controls will protect them regardless of their behaviour (Butavicius et al., 2020). Instead, there is a need to educate users through ISAT programmes, so they will understand that the controls which have been implemented could fail, and that the responsibility to behave securely can never be placed solely on systems. Users should be trained to be more sceptical when performing transactions or requests in the online world.

Unfortunately, unrealistic optimists are not sceptical enough. 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 unrealistic optimists has a significant effect on their trust and ultimately their behaviour. Although unrealistic optimists take note of ISAT, they brush it off subconsciously as they do not expect security threats to be a reality in their environment. Nevertheless, these are often diligent and conscientious users with the best intentions. People tend to be optimistic by nature, resulting in a significant portion of the population being unrealistically optimistic (Weinstein, 1980). Since OB has a significant influence on attitude, trust and awareness, ISAT programmes should take this human trait into account in order to be more successful.

CHAPTER 9

CONCLUSION



9. CONCLUSION

9.1 Introduction

This chapter provides an overview of the study with a particular emphasis on how it adds to the information security body of knowledge. The chapter starts with a review of the thesis problem specifically focusing on why this research was undertaken. The next section provides an overview of all the chapters, followed by a review of the research questions and problem statement, showing how they were addressed during the study. The main research objective was to investigate the effect of optimism bias (OB) on phishing susceptibility and how this could be addressed through information security awareness training (ISAT). The contribution of the study is discussed for both theory and practice. The chapter concludes with the limitations of the study and future research directions.

9.2 Overview of the thesis problem

It is estimated that the majority of the world's population is connected to the internet (Neto et al., 2021). Considering the pervasiveness of information systems in our daily lives, controlling basic infrastructure such as electricity, water supply, security, managing traffic, financial systems and communication systems, one basically has to use the internet to be part of society (Pfeiffer, 2021). We are in the information age and some claim that he who controls the information in information systems, ultimately holds the power (Libicki, 2020). It is therefore of the utmost importance to protect the information in such systems to ensure they function as expected.

Social engineering, which exploits human vulnerabilities, is often used to gain unauthorised access to these systems. This study focused on one of the most common social engineering techniques, phishing, which predominantly uses email as its attack platform. Information security breaches are increasing with data being held for ransom and often sold on the dark web, putting people and organisations at risk of possible identity theft, financial loss, intellectual property theft, operational interruption and

reputational damage (Stack, 2018; Sarkar et al., 2019; Steel, 2019; Liu et al., 2020). Thus, researchers have been trying to find ways to eliminate the phishing risk but have up to now been unsuccessful.

Various counter measures are used to reduce the risk of phishing. These include technical controls and ISAT. Unfortunately, these controls merely reduce the phishing risk but do not eradicate it, as is evident from the current phishing statistics (Proofpoint, 2021). Although software security organisations have made major improvements in the last few years, such as incorporating artificial intelligence/machine learning into security products to 'automatically' mitigate both known and unknown security threats, people still succumb to phishing attacks, resulting in security breaches. Therefore, technical controls alone will not solve this problem and, thus, the focus is placed on human behaviour. Humans are considered the weakest link in the security chain (Van Slyke and Belanger, 2020; Abroshan et al., 2021; Hughes-Lartey et al., 2021).

ISAT has been shown to be effective in reducing security breaches caused by phishing (Aloul, 2012). Hence, as human behaviour is influenced by many factors, including personality traits, attitude, trust, knowledge, awareness, and OB to mention a few, the aim of this study was to propose a solution that would increase the effectiveness of ISAT in reducing information security breaches.

To investigate this problem, other studies have focused on personality traits, how people trust, awareness, email cues, employee workload, habits, persuasion and maladaptive behaviour (Blythe, Petrie and Clark, 2011; Vishwanath et al., 2011; Jensen et al., 2017; Ferreira and Teles, 2019; Moul, 2019; Frauenstein and Flowerday, 2020; Steves, Greene and Theofanos, 2020; Frauenstein, 2021; Shahbaznezhad, Kolini and Rashidirad, 2021). In addition, Abroshan et al. (2021) created a predominantly fear-based conceptual model, thus ignoring rewards as a motivator, to determine a susceptibility risk score. Another researcher, Arduin (2021), asked volunteers to participate in an experiment to test their phishing susceptibility. This was performed 'classroom style', thus eliminating the element of surprise that would have been present had the phishing email had to be processed among other legitimate emails. In the past, most phishing susceptibility studies have been quantitative in nature; actual behaviour in normal daily work life has not been measured.

Furthermore, only a few studies have investigated information systems and OB (Campbell et al., 2007; Nandedkar and Midha, 2012; Baek, Kim and Bae, 2014) and phishing and optimism (Wang, Li and Rao, 2016).

This study therefore focused on increasing the effectiveness of ISAT by considering human behaviour and looking specifically at the relationships of attitude, trust and awareness with the intention to behave securely. The effect of OB on these factors was also studied. Since there is a difference between intention and actual behaviour, this study also tested actual behaviour in a normal work setting to better understand what these differences are.

9.3 Chapter summaries

Chapter 1 provided a complete overview of the study. The context of the study was set by highlighting the fact that the phishing problem has not been solved, even though it has been around for decades. Currently, researchers are looking for solutions that can eradicate it completely. Phishing was briefly explained and current statistics quoted on the detrimental effects of a security breach. Current counter measures were discussed, namely technical controls and ISAT. This led to questioning human behaviour. People generally have the intention to behave securely, but their actual behaviour does not reflect this. Accordingly, possible factors that could influence behaviour were discussed.

The literature review was divided into three chapters (Chapters 2–4), which laid the theoretical groundwork for the study and confirmed that the underlying information security issue is related to human behaviour. Owing to the success of phishing attacks and the way such attacks manipulate people, Chapter 2 focused on better understanding how phishing works and how a phishing attack is launched. The many different types of phishing were discussed, illustrating that such attacks have a wide reach, endangering devices and applications including PCs, phone texts and voice messages. A phishing taxonomy was discussed, summarising the various types and covering the communication media, target devices, attack techniques and countermeasures. Although a device with a smaller form factor could make it more difficult to identify a phishing attack, it is not the major reason for phishing success. Attackers prefer to target a platform where they can reach a large number of people. Broadly speaking, people are manipulated either through fear or reward, regardless of the attack platform, with reward-based themes appearing to be more effective (Bax, McGill and Hobbs, 2021). Understanding how phishing works was important in this study as this knowledge was used in the experiment to test behaviour. The literature review was used to guide the setup of the three phishing campaigns (one fear-based and two reward-based).

Chapter 3 introduced ISAT. The aim of the chapter was to provide a general understanding of the various types of malware threat to ensure that ISAT addresses as many risks associated with phishing as possible. The importance of a security culture within an organisation was emphasised as the foundation for implementing good information security governance, thus supporting the goal of ISAT by empowering people to play a more active role in behaving securely. Several training frameworks were discussed to better understand what a successful ISAT programme should look like. Subsequently, certain designs were considered, as well as how people learn to optimise the success of ISAT. This addressed the first research sub-question: *Why is information security awareness training not always effective in changing human behaviour?* Previous studies have concluded that increased ISAT has a positive impact on secure behaviour and enables people to identify security threats (Mittal, 2015; McCormac et al., 2017). However, people still succumb to phishing attacks and therefore the effectiveness of ISAT is questioned (Dodge, Carver and Ferguson, 2007).

Chapter 4 provided a discussion on the behavioural influence of OB, also considering attitude and trust in respect of their influence on the intention to behave securely. OB was discussed as a cognitive bias influencing decision-making and secure behaviour, with people who have this trait believing that they are less at risk of experiencing a negative event than others. Thus, the second research sub-question was addressed: *What effect does optimism bias have on secure behaviour?*

Attitude was described as a way of thinking that represents an emotional condition. Previous studies have found that a positive attitude towards information security could lead to secure behaviour (Bulgurcu, Cavusoglu and Benbasat, 2010; Lowry and Moody, 2015). This allowed for addressing the third research sub-question: *How does attitude affect secure behaviour?*

Lastly, trust was considered. Since this study took place in one organisation, trust was defined as the trust placed in the technical controls implemented by the IT department. However, blindly trusting these controls could lead to insecure behaviour. From the literature (Riegelsberger, Sasse and McCarthy, 2005; Lankton, Mcknight and Tripp, 2015; Beck et al., 2017) trust relationships were explained and the influence they have on secure behaviour, both from a human and a systems perspective, addressed the fourth research sub-question: *How does trust in technology security controls affect secure behaviour?*

Chapter 5 discussed the behavioural influence of attitude, trust, awareness and OB on secure behaviour. The theory of planned behaviour (TPB) was discussed and its suitability for use in this study was argued. The focus of this study was based not only on the intention to behave securely, but also, more importantly, on better understanding the *intention–behaviour gap* (Jenkins, Durcikova and Nunamaker, 2021). The literature study enabled hypotheses to explain the relationships between the constructs to be formally presented, subsequently resulting in the proposed research model for the study.

Chapter 6 provided a detailed discussion of the research design and the methodological approach used in this study. The study adopted a pragmatic paradigm since it fits well with mixed methods research where both quantitative and qualitative research are considered. An abductive approach to theory development was chosen because the study moved back and forth between inductive and deductive reasoning. The surprising fact that people still succumb to phishing attacks even after numerous ISAT interventions and the implementation of technical controls needed further investigation. The secondary data analysis process was discussed together with the various sources used. Next, the research instrument was discussed and the sampling strategy explained. Since the population for the study was from one company, systematic random sampling was used to ensure the population selected was representative of the general population of a financial services organisation. As this study evaluated hypotheses (intention to behave securely) quantitative research was used to test them, with qualitative research using an experiment and interviews being used to measure actual secure behaviour. The model was subsequently evaluated using triangulation. The chapter concluded with an overview of the ethical considerations made in this study.

Chapter 7 provided the survey results (quantitative results), focusing on presenting and interpreting the results of the univariate analysis. On the other hand, the multivariate analysis employed a PLS-SEM-based approach that resulted in the development of both the measurement and structural model. The chapter then reported on the outcomes of the path analysis, specifically the correlation coefficients, effect sizes, t-values and statistical significance. The results subsequently showed support for all three hypotheses for the **global group** (the unrealistically optimistic and average groups combined) as proposed in the study. More importantly, the results of the multigroup analysis further supported the last three hypotheses, clearly showing the **differences between the unrealistically optimistic and average groups**. This was followed by a presentation of the structural model depicting the hypothesised associations between

each of the constructs. The next section discussed the evaluation of both the measurement model and the structural model, as well as emphasising the differences between the **two groups** with regard to the *intention to behave securely.* A discussion followed, highlighting the results for the three defined constructs of this study for the global group, but also discussing the differences between the unrealistically optimistic and average groups with regard to the *intention to behave securely*.

Chapter 8 focused on the results of the experiment and interviews as well as the overall evaluation of the study using triangulation. The phishing experiment was discussed in detail. Taking guidance from previous research, one simulated phishing attack was fear-based and the other two attacks were reward-based. The results of the phishing attacks and observed behaviour after ISAT was done were discussed. In this study the positive effect of ISAT was seen during the experiment as the number of successful phishing attempts decreased with each repetition. However, the findings of this study are in agreement with other studies that ISAT does not eradicate insecure behaviour completely. More importantly, the phishing results showed that the unrealistically optimistic group was more prone to succumb to a phishing attack, which agrees with the literature that they do not expect negative events to happen to them. After each simulated phishing attack, interviews were conducted with participants from both the unrealistically optimistic and average groups to better understand why they had succumbed to the attacks and a mind map of themes was then created. The chapter concluded with an overall evaluation of the study using triangulation.

9.4 Research questions and hypotheses revisited

From the literature review it is clear that phishing remains a serious cybersecurity threat (Alsharnouby, Alaca and Chiasson, 2015; Jensen et al., 2017; Mansfield-Devine, 2018; Torten, Reaiche and Boyle, 2018; Williams, Hinds and Joinson, 2018; Sumner and Yuan, 2019; Bhardwaj et al., 2020; Chen, Gaia and Rao, 2020; Abroshan et al., 2021; Gopavaram et al., 2021; Petrič and Roer, 2022). Phishing has been around for more than two decades and, despite all the awareness training and technical controls implemented, people still succumb to phishing attacks on a daily basis. Thus, the current methods for addressing phishing have been deemed inadequate. Since human behaviour plays a significant role in any phishing attack, there is a need to better understand why some people succumb to the attacks and others not. While there is a

vast body of research on human behaviour in the field of Psychology, human behaviour as it pertains to information systems is scarce. Since awareness is seen as a control for empowering people to behave securely, the objective of this study was to find methods to increase its effectiveness. This led to the main question of the research. To answer the main research question, four research sub-questions had to be answered, all of which focused on either human behaviour or human traits.

> **Main question.** *How should information security awareness training initiatives improve to overcome phishing in susceptible individuals employed by a mid-size financial services company?*

The following section discusses the way in which the sub-questions were answered:

- **Sub-question 1.** *Why is information security awareness training not always effective in changing human behaviour?*

This research question corresponds to the third hypothesis (H3) which states that *An employee's awareness of information security is positively associated with the intention to behave securely.* The results indicate that *awareness* significantly influences *intention to behave securely* ($\beta = 0.351$, $p < 0.01$). This is in agreement with the literature which indicates that when people are aware they know what to look for and therefore behave securely (Li et al., 2019).

The results show that attitude, trust and awareness all have a positive relationship to the intention to behave securely. Yet, people still succumb to phishing attacks. If an employee is under the impression that nothing bad will happen to them, for example falling victim to a phishing attack, then awareness training might not have a positive effect. Hence, could OB cloud one's judgement?

- **Sub-question 2.** *What effect does optimism bias have on secure behaviour?*

This research question corresponds to the fourth, fifth and sixth hypothesis (H4a, H4b & H4c). H4a states: *Employees' attitudes towards information security differ significantly between the OB group and the average group.* The results for H4a (Figure 7.3) indicate that the average group has a significant influence on, and that there is a positive relationship between, the two variables, *attitude* and the *intention to behave securely* ($\beta = 0.245$, $p < 0.01$). On the other hand, the unrealistically optimistic group displayed a more significant relationship between the two variables ($\beta = 0.672$, $p = 0$). H4b states: *Employees' trust is positively associated with information security and differs significantly*

between the OB group and the average group. The results show that the average group has a negative relationship (β = -0.137, not significant) and the unrealistically optimistic group has a positive relationship (β = 0.118, not significant). H4c states: *Employees' awareness of information security is positively associated with the practice of information security and differs significantly between the OB group and the average group.* The results indicate the average group displays a positive relationship between *awareness* and *intention to behave securely* (β = 2.202, p = 0.277) while the unrealistically optimistic group displays a negative relationship between *awareness* and *intention to behave securely* (β = -0.129, p = 0.277).

- **Sub-question 3**. *How does attitude affect secure behaviour?*

This research question corresponds to the first hypothesis (H1) which states: *An employee's attitude towards information security is positively associated with the intention to behave securely.* In line with the structured model (Figure 7.2), *attitude* was shown to have a positive relationship with, and exert a significant influence on, *intention to behave securely* (β = 0.452, p < 0.01). Thus, someone with a positive attitude towards information security should behave securely as they want to comply with, for example, policies and procedures.

- **Sub-question 4.** *How does trust in technology security controls affect secure behaviour?*

This research question corresponds to the second hypothesis (H2) which states: *An employee's trust is positively associated with the intention to behave securely.* The results also indicate that *trust* significantly influences *intention to behave securely* (β = 0.099, p < 0.05). Employees place trust in technical controls to protect them.

9.5 Contributions of the study

9.5.1 Contribution to theory

The TPB attempts to explain what motivates an individual's intention to behave in a certain way which has a significant effect on actual behaviour. The contribution of this study enhances secure behaviour by considering a cognitive bias, OB, when confronted with phishing attacks. Based on the questionnaire, Figure 9.1 depicts only the quantitative analysis with regard to the *intention to behave securely*. The elements colour-coded in red denote the changes that were made to the original TPB. According to Gregor (2006), information systems theory differs from other fields of study as it concerns the use of artifacts in human–machine systems. Lee (2001, p iii) further explains that information systems research consists of more than just the technological system or just the societal system, or a combination of both; it needs to understand the effect that occurs when the two interact. Thus, the information systems discipline has knowledge of both machines and human behaviour. Lewin (1945) is of the opinion "that nothing is as practical as a good theory". This study investigated the interaction between machines and people to provide a practical solution to combat phishing attacks. Studies around secure behaviour have typically focused on personality traits, habits and policy compliance to understand behaviour, yet research understanding the effect of OB in phishing is sparse. The results of this study provide empirical proof that there is a significant difference in secure behaviour between the average and the unrealistically optimistic group. The model created in this study proposes that OB influences both the intention to behave securely and actual behaviour.

Our findings in particular confirm the theoretical importance of OB in the context of phishing, implying that people are not rational decision-makers and that their decisions may be heavily influenced by OB. Thus, the association between perceived phishing risk and attitude toward adopting preventive steps is greatly weakened by OB.

Other studies have used TPB to understand secure behaviour in conjunction with personality traits and protection motivation theory (PMT) to understand why employees behave insecurely, the effect of their rank order in the organisation on secure behaviour, attitude to towards ISAT and policy compliance (Ifinedo, 2012; Safa et al., 2015; Aurigemma and Mattson, 2017). Their conclusions were that attitude towards compliance and ISAT, perceived vulnerability and information security self-efficacy

positively influence secure behaviour. The model for this study contributes to the Information Systems literature, giving a better understanding of why certain employees are more susceptible to insecure behaviour.

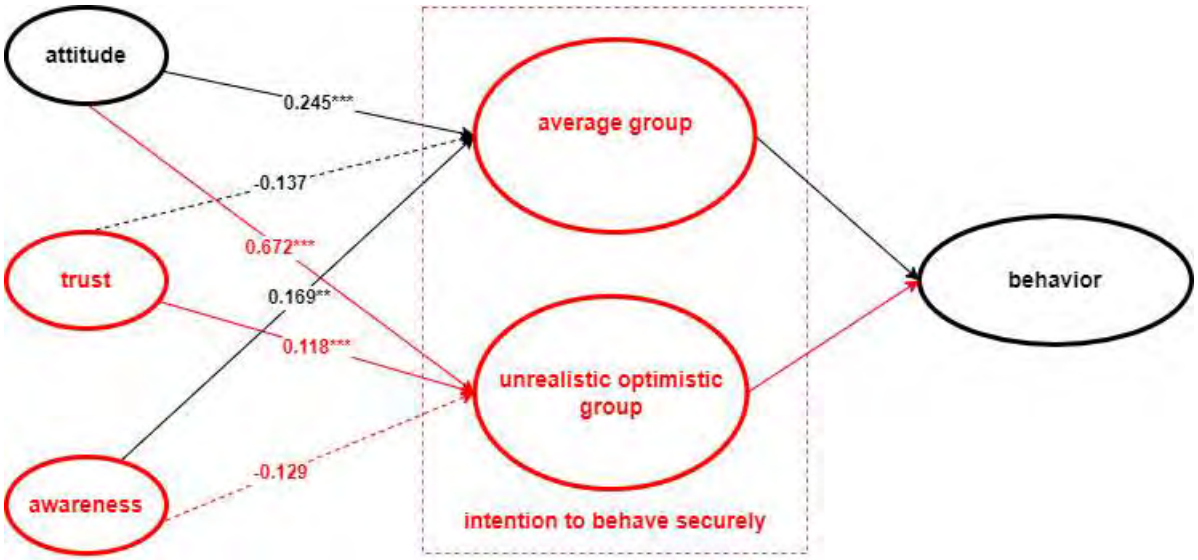


Figure 9.1 Intention to behave securely

9.5.2. Contribution to practice

The contribution of this research to practice is that ISAT programmes need to be adapted to cater for unrealistically optimistic people. ISAT should contain a section to make employees aware of whether or not they are unrealistically optimistic and therefore what the likely outcome of their behaviour could be. Review questions in the training should focus on OB where required to further impart the significance it has on behaviour. Based on the research done in this study, the most effective way to demonstrate this is to perform simulated phishing attacks and to carry out a debriefing with those who succumb so that they can learn through experience. Verkijika (2019) refers to “anticipated regret”, which results in security training changing from a theoretical exercise to practical implementation. For example, employees learn through simulated phishing attacks what the possible negative outcomes resulting from poor security behaviour could be. This

should provide them an opportunity to reflect on the negative consequences of a security incident.

The effectiveness of an ISAT programme is influenced by how it is presented. Using interactive methods to engage participants during training and being able to test the subject matter after the training are critical. ISAT is not a once-off event but an ongoing programme, focusing on current threats and scenarios so that employees can relate and correctly respond to these threats (Bauer, Bernroider and Chudzikowski, 2017). A negative attitude towards behaving securely could also be related to work stress and therefore ISAT programmes could be adapted to point this out to employees. Gamification is often used to create a more relaxed environment to complement ISAT, allowing employees to benchmark themselves against each other (Gjertsen et al., 2017; Scholefield and Shepherd, 2019). Although gamification can improve an employee's attitude towards ISAT, more formal measures should also be introduced. The employee's work performance is usually managed by an agreed set of key performance indicators (KPIs). We suggest that KPIs should be modified to include a measure for ISAT programmes completed, including how to avoid being the victim of a simulated or real phishing attack and the need to report suspicious emails to one's manager or the IT department.

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 demonstrating to users that a father type figure is watching over them. 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 ISAT programmes, so they will understand that the controls which have been implemented could fail, and that the responsibility to behave securely can never be placed solely on systems. Employees should be trained to be more sceptical when performing transactions or requests in the online world. If an employee thinks they are being persuaded to do something which will result in them being deceived, it could result in scepticism about the arguments made for secure behaviour (Schaab, Beckers and Pape, 2016).

Unfortunately, unrealistic optimists are not sufficiently sceptical. A comparison was made between the unrealistically optimistic group and the average group showing 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 influences their trust and

ultimately their behaviour (see Table 7.11). Although unrealistic optimists take note of ISAT, they brush it off subconsciously as they do not expect security threats to be a reality in their environment. Nevertheless, these are often diligent and conscientious employees with the best intentions. People tend to be optimistic by nature, resulting in a significant portion of the population being unrealistically optimistic (Weinstein, 1980).

The results of the experiments conducted confirm that the unrealistic optimists are more prone to insecure behaviour. As discussed, OB is a cognitive bias that could lead to poor judgement calls. An interesting discovery during the interviews with those who succumbed to the phishing attacks was the element of surprise. They could not believe that they had fallen for a scam, especially those in the unrealistically optimistic group. This finding aligns with the belief that 'it won't happen to me'. The interviews revealed that employees were emotionally charged to comply as the email was from management and they feared missing out on rewards. To improve the effectiveness of ISAT, specifically for the unrealistically optimistic, it is vital to perform simulated phishing attacks to demonstrate to them that 'it *can* happen to you'. This should result in more secure behaviour as they experience the reality of a phishing attack.

The result of the experiment has shown that through repeated ISAT interventions there is a steady decline in those who succumb to the phishing attacks. Thus, the number of ISAT interactions that employees engage in has a direct impact on their intention to behave securely. Figure 9.2 depicts both the quantitative data (questionnaire) and the qualitative data (experiment and interviews), including the effect of OB on both the intention to behave securely and actual behaviour.

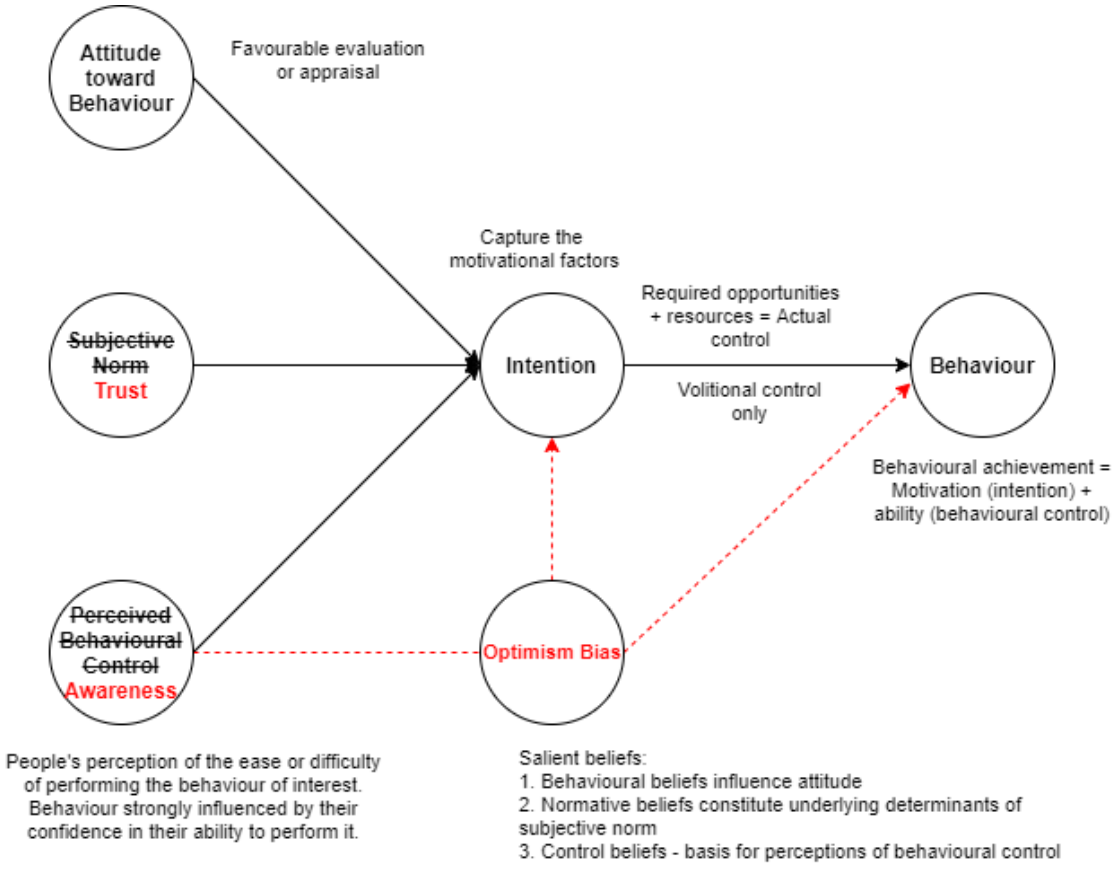


Figure 9.2 Information Security OB Behavioural Model (Adapted from the TPB, Ajzen 1991)

9.6 Limitations and future research directions

While this study makes some key theoretical and practical contributions and provides interesting insights into various areas of behavioural research, it does have several shortcomings that open avenues for further research.

9.6.1 Limitations of the study

Since the questionnaire was not totally anonymous, the results might be influenced by socially desirable behaviour, especially as it was conducted at the workplace. To mitigate this risk, it was made clear that the results would be kept confidential and only used for academic research purposes.

The results of this study have the limitation that they may be valid for short-term conclusions only. Although the experiment was repeated three times, it was concluded within a few months and therefore the long-term effect on behaviour was not measured. It is therefore difficult to determine what the overall success of more iterations of ISAT would be or if at some point it becomes completely obsolete.

Another limitation to consider is the number and quality of previous ISAT programmes completed by the employees, since employees who have greater ISAT experience should be better at identifying security threats. The quality of the ISAT programmes received also has a direct effect on behaviour. Therefore, a deeper understanding of the type of previous training received is required to determine the effectiveness of additional awareness.

The phishing emails were mostly sent during office hours. This could have resulted in employees warning each other not to click on the link as they have identified it as a phishing attack. In a work-from-home scenario where there is no face-to-face interaction, the results might have been different. It also took a while to technically deliver all the emails, so some employees might have received them long before others and had ample time to warn them.

9.6.2 Possible future research directions

Since data was collected from a single South African organisation, the effect of different cultures on OB needs to be studied further. Chang et al (2001) compared OB among American and Japanese people, finding that while both groups had an optimism 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). National culture plays a significant role in human behaviour and future research is needed to address this vital theme.

Furthermore, the same study should be done in a different English-speaking country to determine whether the results are similar. For example, this study could be done in a financial services organisation based in the UK. In this study, phishing scores remained high. South Africa has a high unemployment rate and this could be the reason that any reward is deemed worth the risk. Consequently, the results may differ in a wealthier environment.

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

Our results have shown that OB influences both the intention to behave securely and actual behaviour. Therefore, future research should consider this finding, as a significant portion of people are unrealistically optimistic. Generally speaking, unrealistically optimistic people are quick to trust and less aware of negative events (Wilson and Darke, 2012). Therefore, people should be tested to see if they are unrealistically optimistic and, if they are, they should be made aware of it. The ISAT should be adapted to include a section on OB with the necessary warnings that unrealistically optimistic people can be phished. Once ISAT is done, the behaviour should be tested with a similar experiment as performed in this study.

9.7 Reflection

Eradicating the phishing risk is a complex task, since the solution relates more to human behaviour than to the implementation of technical controls. Fully understanding human behaviour is difficult and therefore actual behaviour often comes as a surprise. From the results of this study, it would appear that even highly qualified survey participants succumbed to the phishing attacks, so this could rule out cognitive processing capabilities. Since this study was conducted in the work environment, there were a number of survey participants who wanted to comply with management instructions and thought they were 'doing the right thing'.

Playing on people's emotions definitely drives them to display certain behaviour. Fear and reward are strong factors in driving behaviour and people cannot think rationally if they are emotionally charged. Furthermore, most people are busy and performance is measured on output. They therefore tend to make hasty decisions to 'tick the box' and get the tasks done. That combination, being emotionally charged and the presence of time constraints, is a recipe for disaster, often resulting in successful phishing attacks. Future research could include the views of psychologists in order to better understand why certain people still succumb to phishing attacks.

In the financial organisation in this study, the fact that phishing was a problem came to light when an international audit firm launched a successful simulated phishing attack as part of a security test. This created the awareness that phishing is a relevant risk and, as flagged by the audit firm, needs to be addressed on an ongoing basis.

9.8 Summary

The objective of this study was to understand how a cognitive bias, referred to as OB, makes certain individuals more susceptible to phishing attacks. Humans remain vulnerable to information security breaches, which is clearly seen in the increasing number of successful phishing attacks. The results of this study indicate that one's attitude, ISAT and trust are critical in reinforcing the intention to behave securely.

Interestingly, a significant difference was found between the average and the unrealistically optimistic employee groups in relation to attitude, awareness and trust in

the intention to behave securely. 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, it was found that unrealistic optimists are more susceptible to security threats. These employees need to be reminded that they cannot trust systems blindly, that not all requests are legitimate, and above all, that they are not immune to security threats.

The quantitative results show that attitude had the largest effect on our model in relation to the intention to behave securely. Specifically, an attitude of 'it won't happen to me' or overconfidence could result in insecure behaviour. In addition, the analysis of the experimental data indicated that phishing emails that evoke an emotional response could result in the recipient succumbing to an attack.

Awareness had the second largest effect in our model. While ISAT plays a pivotal role in reducing the number of successful attacks on information security, more needs to be done. ISAT programmes need to be engaging and interactive to be effective and employees should be given practical examples in phishing tests with immediate feedback to correct behaviour.

Trust had the smallest effect in our model. In the context of this study, all employees are employed by the same organisation. Since many employees trust the internal controls implemented by the IT department, this creates the false impression that their actions are not likely to lead to a security breach.

REFERENCES

Abraham, S. and Chengalur-Smith, I.S., 2010. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), pp.183–196. https://doi.org/10.1016/j.techsoc.2010.07.001.

Abraham, S. and Chengalur-Smith, I.S., 2019. Evaluating the effectiveness of learner controlled information security training. *Computers and Security*, 87, p.101586. https://doi.org/10.1016/j.cose.2019.101586.

Abroshan, H., Devos, J., Poels, G. and Laermans, E., 2021. A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks. *UMAP 2021 – Adjunct Publication of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, pp.345–350. https://doi.org/10.1145/3450614.3464472.

Acharya, B., 2010. *Questionnaire design*. Working paper. Nepal: Nepal Engineering College.

Acquisti, A. and Grossklags, J., 2004. Privacy attitudes and privacy behavior. In: Camp, L.J. and Lewis, S. (eds), *Economics of information security: Advances in information security, Vol 12.* Boston, MA: Springer, pp.165–178.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L., Komanduri, S., Leon, P., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S., 2017. Nudges for privacy and security : Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3).

Ahmed, S., 2021. Who inadvertently shares deepfakes? Analyzing the role of political interest, cognitive ability, and social network size. *Telematics and Informatics*, 57(October 2020), p.101508. https://doi.org/10.1016/j.tele.2020.101508.

AICPA, 2022. *System and organization controls: SOC Suite of Services*. [online] Association of International Certified Professional Accountants. Available at: <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome> [Accessed 6 January 2022].

Ajzen, I., 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, pp.179–211. https://doi.org/10.4135/9781446249215.n22

Ajzen, I. and Fishbein, M., 1977. Attitude-behavior relations : A theoretical analysis and review of empirical research. *Psychological Bulletin*, 84(5), pp.888–918.

Akbari, M., Seydavi, M., Palmieri, S., Mansueto, G., Caselli, G. and Spada, M.M., 2021. Fear of missing out (FoMO) and internet use: A comprehensive systematic review and meta-analysis. *Journal of Behavioral Addictions*, 10(4), pp.879–900.

Albarracin, D. and Shavitt, S., 2018. Attitudes and attitude change. *Annual Review of Psychology* [online], 69, pp.299–327. https://doi.org/10.1146/annurev-psych-122216

Al-Daeef, M.M., Basir, N. and Saudi, M.M., 2017. Security awareness training: A review. In: *Proceedings of the World Congress on Engineering*. London, U.K.

Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet*, https://doi.org/10.3390/fi11030073

Aleroud, A. and Zhou, L., 2017. Phishing environments, techniques, and countermeasures : A survey. *Computers & Security*, [online] 68, pp.160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alghamdi, M.I., 2021. Cybercrime legislation applicable and enforceable. *Materials Today: Proceedings*. [online] https://doi.org/10.1016/j.matpr.2021.04.050

Alhogail, A., Mirza, A. and Bakry, S.H., 2015. A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, 78(2), pp.201–211.

Allan, G.M., Garrison, S. and McCormack, J., 2014. Comparison of cardiovascular disease risk calculators. *Current opinion in lipidology*, 25(4), pp.254–265.

Allcott, H. and Gentzkow, M., 2017. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), pp.211–36. https://doi.org/10.1257/jep.31.2.211.

Allen, N.J. and Meyer, J.P., 1990. The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational Psychology*, 63, pp.1–18.

Al-Moshaigeh, A., Dickins, D. and Higgs, J.L., 2019. Cybersecurity risks and controls. *The CPA Journal*, 89(6), pp.36–41.

Aloul, F.A., 2012. The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), pp.176–183. https://doi.org/10.4304/jait.3.3.176-183

Al-rimy, B.A.S., Maarof, M.A., Zainudeen, S. and Shaid, M., 2018. Ransomware threat success factors, taxonomy , and countermeasures : A survey and research directions. *Computers & Security*, 74, pp.144–166. https://doi.org/10.1016/j.cose.2018.01.001

Alseadoon, I.M.A., 2014. *The impact of users' characteristics on their ability to detect phishing emails*. Queensland University of Technology.

Alshaikh, M., Maynard, S.B. and Ahmad, A., 2021. Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers and Security*, [online] 100, p.102090. https://doi.org/10.1016/j.cose.2020.102090

Alsharnouby, M., Alaca, F. and Chiasson, S., 2015. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human Computer Studies*, [online] 82, pp.69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J., 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, 114. https://doi.org/10.1016/j.chb.2020.106531

Anawar, S., Kunasegaran, D.L., Mas'ud, M.Z. and Zakaria, N.A., 2019. Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *J Eng Sci Technol*, 14(5), pp.2865–2882.

Anderson, B.B., Kirwan, C.B., Jenkins, J.L., Eargle, D., Howard, S. and Vance, A., 2015. How polymorphic warnings reduce habituation in the brain-insights from an FMRI study. In: *Conference on Human Factors in Computing Systems – Proceedings*. Association for Computing Machinery, pp.2883–2892. https://doi.org/10.1145/2702123.2702322.

Andersson, M.A., 2012. Dispositional optimism and the emergence of social network diversity. *The Sociological Quarterly*, 53(1), pp.92–115.

Anon. 2018. *General Data Protection Regulation (GDPR)*. [online] Available at: <https://gdpr-info.eu/> [Accessed 6 January 2022].

APWG, 2020. APWG Trends Report Q2 2020. *Phishing Activities Trends Report*, Q2 2020(August), pp.1–13.

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

Arachchilage, N.A.G., Love, S. and Beznosov, K., 2016. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60, pp.185–197. https://doi.org/10.1016/j.chb.2016.02.065

Arduin, P., 2021. A cognitive approach to the decision to trust or distrust phishing emails. *International Transactions in Operational Research*, [online] 0, p.itor.12963. https://doi.org/10.1111/itor.12963

Armor, D.A. and Taylor, S.E., 2002. When predictions fail: The dilemma of unrealistic optimism. In: *Heuristics and Biases*. Cambridge University Press, pp.334–347. https://doi.org/10.1017/CBO9780511808098.021

Arnett, J.J., 2000. Optimistic bias in adolescent and adult smokers and nonsmokers. *Addictive Behaviors*, 25(4), pp.625–632.

Asch, S.E., 1946. Forming impressions of personality. *Journal of Abnormal and Social Psychology*, 41, pp.258–290.

Aslaksen, K. and Lorås, H., 2018. The Modality-Specific Learning Style Hypothesis: A mini-review. *Frontiers in Psychology*, [online] 9. https://doi.org/10.3389/fpsyg.2018.01538.

Aslaner, M., 2018. *How to disrupt attacks caused by social engineering*. Microsoft Security Blog. [online] Available at: <https://www.microsoft.com/security/blog/2018/01/10/how-to-disrupt-attacks-caused-by-social-engineering/> [Accessed 3 September 2021].

Aue, T., Dricu, M., Moser, D.A., Mayer, B. and Bührer, S., 2021. Comparing personal and social optimism biases: Magnitude, overlap, modifiability, and links with social

identification and expertise. *Humanities and Social Sciences Communications*, 8(1), pp.1–12.

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*, 66, pp.218–234. https://doi.org/10.1016/j.cose.2017.02.006

Baadel, S. and Lu, J., 2019. Data analytics: Intelligent anti-phishing techniques based on machine learning. *Journal of Information & Knowledge Management*, 18(01), p.1950005.

Bada, M. and Sasse, A., 2014. Security awareness campaigns: Why do they fail to change behaviour? [Draft Working Paper]. *Global Cyber Security Capacity Centre*, [online] (July), pp.1–38. Available at: <http://discovery.ucl.ac.uk/1468954/1/AwarenessCampaignsDraftWorkingPaper.pdf>

Baek, Y.M., Kim, E.M. and Bae, Y., 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, 31(1), pp.48–56. https://doi.org/10.1016/j.chb.2013.10.010

Bahtiyar, Ş., 2016. Anatomy of targeted attacks with smart malware. *Security and Communication Networks*, 9(18), pp.6215–6226. https://doi.org/10.1002/sec.1767

Baker, M., Ruback, R. and Wurgler, J., 2006. Behavioral corporate finance: A survey. In: B. Espen, ed. *The handbook of corporate finance: Empirical corporate finance*. New York: Elsevier/North Holland.

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*, 8(8), p.e71303.

Baron, J., Hershey, J.C. and Kunreuther, H., 2000. Determinants of priority for risk reduction: the role of worry. *Risk Analysis*, 20(4), pp.413–428.

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. [online] https://doi.org/10.1016/j.cose.2017.04.009

Bax, S., McGill, T. and Hobbs, V., 2021. Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers and Security*, [online] 106, p.102278. https://doi.org/10.1016/j.cose.2021.102278

Beck, R., Avital, M., Rossi, M. and Thatcher, J.B., 2017. Blockchain technology in business and information systems research. *Business and Information Systems Engineering*, 59, pp.381–384. https://doi.org/10.1007/s12599-017-0505-1

Bélanger, F., Collignon, S., Enget, K. and Negangard, E., 2017. Information & management determinants of early conformance with information security policies. *Information & Management*, [online] 54(7), pp.887–901. https://doi.org/10.1016/j.im.2017.01.003.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M.A. and Passingham, N., 2015. *Awareness is only the first step: A framework for progressive engagement of staff in cyber security*. [online] Hewlett Packard Enterprise. Available at: <https://riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf> [Accessed 12 September 2020].

Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N. and Arthi, S., 2020. Why is phishing still successful? *Computer Fraud and Security*, [online] (9), pp.15–19. https://doi.org/10.1016/S1361-3723(20)30098-1

Bilge, L., Han, Y. and Dell'Amico, M., 2017. RiskTeller: Predicting the risk of cyber incidents. In: *Proceedings of the ACM Conference on Computer and Communications Security*. pp.1299–1311. https://doi.org/10.1145/3133956.3134022

Birch, D. and Memery, J., 2020. Tourists, local food and the intention-behaviour gap. *Journal of Hospitality and Tourism Management*, [online] 43(July 2019), pp.53–61. https://doi.org/10.1016/j.jhtm.2020.02.006

Blanco, F., 2017. Cognitive Bias. In: *Encyclopedia of animal cognition and behavior*. [online] Cham: Springer, pp.1–7. https://doi.org/10.1007/978-3-319-47829-6_1244-1

Blythe, J.M. and Coventry, L., 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87(August 2017), pp.87–97. https://doi.org/10.1016/j.chb.2018.05.023

Blythe, M., Petrie, H. and Clark, J.A., 2011. F for fake: Four studies on how we fall for phish. *Conference on Human Factors in Computing Systems: Proceedings*, pp.3469–3478. https://doi.org/10.1145/1978942.1979459

Boddy, M., 2018. Phishing 2.0: The new evolution in cybercrime. *Computer Fraud & Security Bulletin*, [online] (11), pp.8–10. https://doi.org/10.1016/S1361-3723(18)30108-8

Bonner, C., Jansen, J., Newell, B.R., Irwig, L., Glasziou, P., Doust, J., Dhillon, H., McCaffery, K. and others, 2014. I don't believe it, but I'd better do something about it: patient experiences of online heart age risk calculators. *Journal of Medical Internet Research*, 16(5), p.e3190.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems*, 39(4), pp.837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Botacin, M., Ceschin, F., de Geus, P. and Grégio, A., 2020. We need to talk about antiviruses: Challenges & pitfalls of AV evaluations. *Computers and Security*, 95. https://doi.org/10.1016/j.cose.2020.101859

Bracha, A. and Brown, D.J., 2012. Affective decision making: A theory of optimism bias. *Games and Economic Behavior*, 75(1), pp.67–80. https://doi.org/10.1016/j.geb.2011.11.004.

Bradburn, N., Sudman, S. and Wansink, B., 2004. *Asking questions: the definitive guide to questionnaire design - for market research, political polls, and social and health questionnaires*. Revised edition. [online] Available at: <https://books.google.com/books?hl=en&lr=&id=YXKbTx2j9i4C&oi=fnd&pg=PR7&dq=Bradburn,+N.+M.,+Sudman,+S.,+%26+Wansink,+B.+(2004).+Asking+questions:+the+definitive+guide+to+questionnaire+design--for+market+research,+political+polls,+and+social+and+health+questionnaires.+&ots=w9Da9EF06a&sig=kYrg-tlReNivF-2s61Iq0WB55gA> [Accessed 10 May 2022].

Brannon, A.L., Brannon, S.M., Dejong, A. and Gawronski, B., 2019. Determinants of lateral attitude change: the roles of object relatedness, attitude certainty, and moral conviction. *Social Cognition,* 37(6), pp.624–658.

Brehm, J.W., 1966. *A theory of psychological reactance*. New York: Academic Press.

Brown, J.D., 2012. Understanding the better than average effect: Motives (still) matter. *Personality and Social Psychology Bulletin*, 38(2), pp.209–219.

Brown, S.L. and Imber, A., 2003. The effect of reducing opportunities for downward comparison on comparative optimism. *Journal of Applied Social Psychology*, 33(5), pp.1058–1068.

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*, 67(3), pp.366–381. https://doi.org/10.1037/0022-3514.67.3.366

Bueno, N., 2005. *Learning styles in an online environment: Students’ dominant learning styles and learning outcomes in an online health education class*. Doctoral dissertation.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, [online] 34(3), pp.523–548. Available at: <https://www.jstor.org/stable/25750690>

Burgess-Allen, J. and Owen-Smith, V., 2010. Using mind mapping techniques for rapid qualitative data analysis in public participation processes. *Health Expectations*, 13(4), pp.406–415. https://doi.org/10.1111/j.1369-7625.2010.00594.x

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*, [online] 98, p.102020. https://doi.org/10.1016/j.cose.2020.102020

Butler, J.K., 1991. Toward understanding and measuring conditions of trust: evolution of a conditions of trust inventory. *Journal of Management*, 17(3), pp.643–663.

Button, M. and Cross, C., 2017. *Technology and fraud: The ‘fraudogenic’ consequences of the internet revolution.* [online] Available at: <https://www.researchgate.net/publication/318041431_Technology_and_Fraud_The_’Fraudogenic’_Consequences_of_the_Internet_Revolution> [Accessed 22 March 2021].

Cacioppo, J.T., Cacioppo, S., Petty, R.E., Cacioppo, J.T., Cacioppo, S. and The, R.E.P., 2018. The neuroscience of persuasion : A review with an emphasis on issues and opportunities. *Social Neuroscience*, 13(2), pp.129–172. https://doi.org/10.1080/17470919.2016.1273851

Campbell, J., Greenauer, N., Macaluso, K. and End, C., 2007. Unrealistic optimism in internet events. *Computers in Human Behavior*, 23(3), pp.1273–1284. https://doi.org/10.1016/j.chb.2004.12.005

Carpenter, P., 2020. *2020 Elections: Be wary of these five disinformation tactics*. Forbes.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J. and Neville, A.J., 2014. The use of triangulation in qualitative research. *Oncology Nursing Forum*, [online] 41(5), pp.545–547. https://doi.org/10.1188/14.ONF.545-547

Carver, C.S., Scheier, M.F. and Segerstrom, S.C., 2010. Optimism. *Clinical Psychology Review*, 30(7), pp.879–889. https://doi.org/10.1016/J.CPR.2010.01.006

Certnz, 2018. *Invoice scams affecting New Zealand businesses | CERT NZ*. [online] Available at: <https://www.cert.govt.nz/individuals/alerts/invoice-scams-affecting-new-zealand-businesses/> [Accessed 3 September 2021].

Cha, M.K. and Lee, H.J., 2021. The relationship between anti-consumption lifestyle and the trust triangle in a ride-sharing platform: A cross-cultural study of U.S. and Indian consumers. *International Journal of Consumer Studies*. https://doi.org/10.1111/ijcs.12676

Chadee, D., Ren, S. and Tang, G., 2021. Is digital technology the magic bullet for performing work at home? Lessons learned for post COVID-19 recovery in hospitality management. *International Journal of Hospitality Management*, 92, p.102718.

Chaiken, S. and Trope, Y., 1999. *Dual-process theories in social psychology*. New York: The Guilford Press.

Chakraborty, M., Pal, S., Pramanik, R. and Ravindranath Chowdary, C., 2016. Recent developments in social spam detection and combating techniques: A survey. *Information Processing and Management*, 52(6), pp.1053–1073. https://doi.org/10.1016/j.ipm.2016.04.009

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*, 81(3), pp.476–491. https://doi.org/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*, [online] 133(September 2019), p.113287. https://doi.org/10.1016/j.dss.2020.113287

Cherry, K., 2020. *Understanding the optimism bias*. [online] Available at: <https://www.verywellmind.com/what-is-the-optimism-bias-2795031> [Accessed 24 August 2021].

Chiew, K.L., Yong, K.S.C. and Tan, C.L., 2018. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106, pp.1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Chivers, K., 2020. *What is a man-in-the-middle attack?* [online] Available at: <https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html> [Accessed 3 September 2021].

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*, [online] 26(5), pp.987–995. https://doi.org/10.1016/j.chb.2010.02.012

Cho, Y.J. and Perry, J.L., 2012. Intrinsic motivation and employee attitudes: Role of managerial trustworthiness, goal directedness, and extrinsic reward expectancy. *Review of Public Personnel Administration*, 32(4), pp.382–406. https://doi.org/10.1177/0734371X11421495

Chou, K.L., Lee, T.M.C. and Ho, A.H.Y., 2007. Does mood state change risk taking tendency in older adults? *Psychology and Aging*, 22(2), pp.310–318. https://doi.org/10.1037/0882-7974.22.2.310

Chowdhury, N., Katsikas, S. and Gkioulos, V., 2022. Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security*, [online] 113, p.102551. https://doi.org/10.1016/j.cose.2021.102551

Chowdhury, N.H., Adam, M.T.P. and Teubner, T., 2020. Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, 97, p.101963. https://doi.org/10.1016/j.cose.2020.101963

Christenson, S.L., Reschly, A.L. and Wylie, C. eds., 2012. *Handbook of research on student engagement*. [online] Boston, MA: Springer US. https://doi.org/10.1007/978-1-4614-2018-7

Christensson, P., 2006. *Trojan Horse definition*. [online] Available at: <https://techterms.com> [Accessed 8 October 2020].

Cialdini, R.B., 2006. *Influence: The psychology of persuasion*. Revised edition. New York: Quil William Morrow.

CIS, 2022. *Center for Internet Security*. [online] Available at: <https://www.cisecurity.org/> [Accessed 6 January 2022].

Clarke, T., 2013. The advance of the MOOCs (massive open online courses): The impending globalisation of business education? *Education and Training*, 55(4), pp.403–413. https://doi.org/10.1108/00400911311326036

Cohen, J., 1988. *Statistical power analysis for the behavioral sciences*. New York: Lawrence Erlbaum Associates.

Collin, K., 2006. Connecting work and learning: design engineers' learning at work. *Journal of Workplace Learning*, [online] 18(7/8), pp.403–413. https://doi.org/10.1108/13665620610692971

Collis, J. and Hussey, R., 2003. *Business research: A practical guide for undergraduate and postgraduate students*. 2nd edition. New York: Palgrave Macmillan.

Collis, J. and Hussey, R., 2014. *Business research: A practical guide for undergraduate and postgraduate students*. 4th edition. Palgrave Macmillan Higher Education.

Colwill, C., 2009. Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, 14(4), pp.186–196. https://doi.org/10.1016/j.istr.2010.04.004

Coutlee, C.G., Politzer, C.S., Hoyle, R.H. and Huettel, S.A., 2014. An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt impulsiveness scale version 11. *Archives of Scientific Psychology*, 2(1), p.1.

de Craen, S., Twisk, D.A.M., Hagenzieker, M.P., Elffers, H. and Brookhuis, K.A., 2011. Do young novice drivers overestimate their driving skills more than experienced drivers? Different methods lead to different conclusions. *Accident Analysis & Prevention*, 43(5), pp.1660–1665.

Craney, T.A. and Surles, J.G., 2002. Model-dependent variance inflation factor cutoff values. *Quality Engineering*, 14(3), pp.391–403.

Creswell, J.W., 2014. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Creswell, J.W. and Poth, C.N., 2016. *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications.

Cronbach, L.J., 1951. Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), pp.297–334.

Crowe, M. and Sheppard, L., 2012. Mind mapping research methods. *Quality & Quantity*, [online] 46(5), pp.1493–1504. https://doi.org/10.1007/s11135-011-9463-8

Cuganesan, S., Steele, C. and Hart, A., 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour and Information Technology*, 37(1), pp.50–65. https://doi.org/10.1080/0144929X.2017.1397193

D'Arcy, J. and Lowry, P.B., 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), pp.43–69. https://doi.org/10.1111/isj.12173

Da Silva, C.M.R. Feitosa, E.L. and Garcia, V.C., 2020. Heuristic-based strategy for Phishing prediction: A survey of URL-based approach. *Computers and Security*, [online] 88, p.101613. https://doi.org/10.1016/j.cose.2019.101613

Da Veiga, A., Astakhova, L. v., Botha, A. and Herselman, M., 2020. Defining organisational information security culture: Perspectives from academia and industry. *Computers and Security*, 92. https://doi.org/10.1016/j.cose.2020.101713

Deci, E.L. and Ryan, R.M., 1985. Cognitive evaluation theory. In: *Intrinsic motivation and self-determination in human behavior*. [online] Boston, MA: Springer US, pp.43–85. https://doi.org/10.1007/978-1-4899-2271-7_3

Dekker, S., Lee, N.C., Howard-Jones, P. and Jolles, J., 2012. Neuromyths in education: Prevalence and predictors of misconceptions among teachers. *Frontiers in Psychology*, 3. https://doi.org/10.3389/fpsyg.2012.00429

Denney, A.S. and Tewksbury, R., 2013. How to write a literature review. *Journal of Criminal Justice Education*, 24(2), pp.218–234. https://doi.org/10.1080/10511253.2012.730617

Dhamija, R., Tygar, J.D. and Hearst, M., 2006. Why phishing works. *Conference on Human Factors in Computing Systems – Proceedings*, 1(November 2005), pp.581–590. https://doi.org/10.1145/1124772.1124861

Dictionary.com. 2021. *Definition of perception*. [online] Available at: <https://www.lexico.com/definition/perception> [Accessed 9 August 2021].

Dodge, R.C., Carver, C. and Ferguson, A.J., 2007. Phishing for user security awareness. *Computers and Security*, 26(1), pp.73–80. https://doi.org/10.1016/j.cose.2006.10.009

Dolinski, D., Kulesza, W., Muniak, P., Dolinska, B., Wegrzyn, R. and Izydorczak, K., 2022. Media intervention program for reducing unrealistic optimism bias: The link between unrealistic optimism, well-being, and health. *Applied Psychology: Health and Well-Being*, 14(2), pp.499–518.

Downs, J.S., Holbrook, M. and Cranor, L.F., 2007. Behavioral response to phishing risk. *ACM International Conference Proceeding Series*, 269, pp.37–44. https://doi.org/10.1145/1299015.1299019

Drolet, M., 2018. *The rise of mobile phishing attacks and how to combat them | CSO Online*. [online] Available at: <https://www.csoonline.com/article/3268109/the-rise-of-mobile-phishing-attacks-and-how-to-combat-them.html> [Accessed 3 September 2021].

Dupont, Q. and Karpoff, J.M., 2020. The trust triangle: Laws, reputation, and culture in empirical finance research. *Journal of Business Ethics*, 163(2), pp.217–238. https://doi.org/10.1007/s10551-019-04229-1

Egelman, S. and Peer, E., 2015. Scaling the security wall : Developing a security behavior intentions scale (SeBIS). In: *Conference on Human Factors in Computing Systems - Proceedings*. pp.2873–2882. https://doi.org/10.1145/2702123.2702249.

Fagade, T. and Tryfonas, T., 2017. Hacking a bridge: An exploratory study of compliance-based information security management in banking organization. In: *21st World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings*, pp.94–99.

Farquhar, M., 2005. *A treasury of deception: Liars, misleaders, hoodwinkers, and the extraordinary true stories of history's greatest hoaxes, fakes, and frauds*. New York: Penguin Books.

FBI Internet Crime Complaint Center, 2019. 2019 Internet Crime Report. [online] pp.1–28. Available at: <https://pdf.ic3.gov/2019_IC3Report.pdf>

Fearnley, C.J., 2022. Mind mapping in qualitative data analysis: Managing interview data in interdisciplinary and multi-sited research projects. *Geo: Geography and Environment*, [online] 9(1). https://doi.org/10.1002/geo2.109

Feilzer, M.Y., 2010. Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research*, 4(1), pp.6–16. https://doi.org/10.1177/1558689809349691

Feng, S., Wong, Y.K., Wong, L.Y. and Hossain, L., 2019. The internet and Facebook usage on academic distraction of college students. *Computers and Education*, [online] 134(October 2018), pp.41–49. https://doi.org/10.1016/j.compedu.2019.02.005

Fernandez, S. and Moldogaziev, T., 2013. Employee empowerment, employee attitudes, and performance: Testing a causal model. *Public Administration Review*, [online] 73(3), pp.490–506. https://doi.org/10.1111/puar.12049

Ferreira, A. and Teles, S., 2019. Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human Computer Studies*, 125(December 2018), pp.19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

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*, [online] 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>

Fertig, T. and Schütz, A., 2020. About the measuring of information security awareness: A systematic literature review. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. [online] https://doi.org/10.24251/HICSS.2020.798

Filstead, W.J., 1979. Qualitative methods: A needed perspective in evaluation research. In: *Qualitative and quantitative methods in evaluation research*, 1. Sage Publications.

Fischer, P., Lea, S.E.G. and Evans, K.M., 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of

scam compliance. *Journal of Applied Social Psychology*, 43(10), pp.2060–2072. https://doi.org/10.1111/jasp.12158

Fleetwood, S., 2005. Ontology in organization and management studies: A critical realist perspective. *Organization*, 12(2), pp.197–222. https://doi.org/10.1177/1350508405051188

Fleischmann, M., Amirpur, M., Benlian, A. and Hess, T., 2014. Cognitive biases in information systems research: A scientometric analysis. In: *Proceedings of the European Conference on Information Systems (ECIS)*. Tel Aviv, Israel.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), pp.407–429.

Fornell, C. and Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), pp.39–50.

Fox, A.B., Rosen, J. and Crawford, M., 2009. Distractions, distractions: Does instant messaging affect college students' performance on a concurrent reading comprehension task? *Cyberpsychology and Behavior*, 12(1), pp.51–53. https://doi.org/10.1089/cpb.2008.0107

Fox, N.J., 2008. Post-positivism. In: *The SAGE encyclopedia of qualitative research methods*, 2, pp.659–664.

Franchina, V., Abeele, M. Vanden, Van Rooij, A.J., Lo Coco, G. and De Marez, L., 2018. Fear of missing out as a predictor of problematic social media use and phubbing behavior among flemish adolescents. *International Journal of Environmental Research and Public Health*, 15(10). https://doi.org/10.3390/ijerph15102319

Frauenstein, E.D., 2021. *A personality-based behavoural model: susceptibility to phishing on social networking sites*. Rhodes University.

Frauenstein, E.D. and Flowerday, S., 2020. Susceptibility to phishing on social network sites: A personality information processing model. *Computers and Security*, [online] 94, p.101862. https://doi.org/10.1016/j.cose.2020.101862

Fromm, J., 2005. *Risk denial and neglect: Studies in risk perception*. Doctoral dissertation. Stockholm School of Economics.

Furnell, S. and Vasileiou, I., 2017. Security education and awareness: Just let them burn? *Network Security*, 2017(12), pp.5–9. https://doi.org/10.1016/S1353-4858(17)30122-8

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*, 42(3), pp.648–661.

Garrote Sanchez, D., Gomez Parra, N., Ozden, C., Rijkers, B., Viollaz, M. and Winkler, H., 2021. Who on earth can work from home? *The World Bank Research Observer*, 36(1), pp.67–100.

Gartner, 2020. *Managing remote teams during the coronavirus (COVID-19) outbreak*. [online] Available at: <https://www.gartner.com/en/documents/3982118/managing-remote-teams-during-the-coronavirus-covid-19-ou> [Accessed 3 September 2021].

Gavett, B.E., Zhao, R., John, S.E., Bussell, C.A., Roberts, J.R. and Yue, C., 2017. Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS One*, 12(2), p.e0171620.

Ge, Y., Lu, L., Cui, X., Chen, Z. and Qu, W., 2021. How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, 97, p.103526.

Geisser, S. and Eddy, W.F., 1979. A predictive approach to model selection. *Journal of the American Statistical Association*, 74(365), pp.153–160. https://doi.org/10.1080/01621459.1979.10481632

Giandomenico, N., 2017. *What is a whaling attack? Defining and identifying whaling attacks*. [online] Available at: <https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks> [Accessed 23 July 2020].

Gil, P., 2020. *What is Whaling?* [online] Available at: <https://www.lifewire.com/what-is-whaling-2483605> [Accessed 23 July 2020].

Giles, H. and Wiemann, J.M., 1987. Language, social comparison and power. In: C.R. Berger and S.H. Chaffee, eds. *The handbook of communication science*. Newbury Park, CA: Sage, pp.350–384.

Gjertsen, E.G.B., Gjære, E.A., Bartnes, M. and Flores, W.R., 2017. Gamification of information security awareness and training. In: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*. SciTePress, pp.59–70. https://doi.org/10.5220/0006128500590070

González-Manzano, L. and de Fuentes, J.M., 2019. Design recommendations for online cybersecurity courses. *Computers and Security*, 80(March 2018), pp.238–256. https://doi.org/10.1016/j.cose.2018.09.009

Goodin, D., 2008. *Fake subpoenas harpoon 2,100 corporate fat cats*. [online] Available at: <https://www.theregister.com/2008/04/16/whaling_expedition_continues/> [Accessed 23 July 2020].

Gopavaram, S.R., Dev, J., Grobler, M., Kim, D., Das, S. and Camp, L.J., 2021. Cross-national study on phishing resilience. In: *Workshop on Usable Security and Privacy (USEC)*. [online] Available at: <https://ssrn.com/abstract=3859057> [Accessed 9 March 2022].

Grassegger, T. and Nedbal, D., 2021. The role of employees' information security awareness on the intention to resist social engineering. In: *Procedia Computer Science*. Elsevier B.V.pp.59–66. https://doi.org/10.1016/j.procs.2021.01.103

Gray, J.R., Braver, T.S. and Raichle, M.E., 2002. Integration of emotion and cognition in the lateral prefrontal cortex. *Proceedings of the National Academy of Sciences of the United States of America*, 99(6), pp.4115–4120. https://doi.org/10.1073/pnas.062381899

Gregor, S., 2006. The nature of theory in information systems. *MIS Quarterly*, 30(3), pp.611–642.

Guhr, N., Lebek, B. and Breitner, M.H., 2019. The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, 29(2), pp.340–362. https://doi.org/10.1111/isj.12202

Gundu, T., Flowerday, S. and Renaud, K., 2019. Deliver security awareness training, then repeat:{Deliver; Measure Efficacy}. In: *2019 conference on information communications technology and society (ICTAS)*. pp.1–6.

Gundy, M. Van and Chen, H., 2012. Noncespaces : Using randomization to defeat cross-site scripting attacks. *Computers & Security*, 31(4), pp.612–628. https://doi.org/10.1016/j.cose.2011.12.004

Gyongyi, A. and Garcia, M.H., 2005. Web Spam Texonomy. *First international workshop on adversarial information retrieval on the web (AIRWeb 2005)*, pp.39–47.

Haase, J.E., Heiney, S.P., Ruccione, K.S. and Stutzer, C., 1999. Research triangulation to derive meaning-based quality-of-life theory: Adolescent resilience model and instrument development. *Int. J. Cancer*, 12, pp.125–131.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, [online] 3(7), p.e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L., 2018. Employees' attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), pp.262–274.

Hadnagy, C., 2014. *Unmasking the social engineer: The human element of security*. Wiley.

Hadnagy, C., 2018. *Social engineering: The science of human hacking*. Indianapolis: Wiley.

Hair, J., Hult, T., Ringle, C. and Sarstedt, M., 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*. 2nd edition. Los Angeles: Sage.

Hair, J.F., Black, W., Babin, B.Y.A., Anderson, R. and Tatham, R., 2010. *Multivariate data analysis: A global perspective*. New York: Pearson Higher Education.

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*, 31(1), pp.2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hale, M.L. and Gamble, R.F., 2019. Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requirements Engineering*, 24(3), pp.365–402. https://doi.org/10.1007/s00766-017-0287-5

Halevi, T., Memon, N. and Nov, O., 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2544742

Hall, R., 2013. Mixed methods: In search of a paradigm. *Conducting research in a changing and challenging world*, pp.71–78.

Han, J., Kim, Y.J. and Kim, H., 2017. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. [online] https://doi.org/10.1016/j.cose.2016.12.016

Han, W., Xue, J., Wang, Y., Liu, Z. and Kong, Z., 2019. MalInsight: A systematic profiling based malware detection framework. *Journal of Network and Computer Applications*, 125(October 2018), pp.236–250. https://doi.org/10.1016/j.jnca.2018.10.022

Hasle, H., Kristiansen, Y., Kintel, K. and Snekkenes, E., 2005. Measuring resistance to social engineering. *Lecture Notes in Computer Science*, 3439, pp.132–143. https://doi.org/10.1007/978-3-540-31979-5_12

Hatfield, J. and Job, R.F., 2001. Optimism bias about environmental degradation: the role of the range of impact of precautions. *Journal of Environmental Psychology*, 21(1), pp.17–30. https://doi.org/10.1006/jevp.2000.0190

Helweg-Larsen, M., Sadeghian, P. and Webb, M.S., 2002. The stigma of being pessimistically biased. *Journal of Social and Clinical Psychology*, 21(1), pp.92–107.

Helweg-Larsen, M. and Shepperd, J.A., 2001. Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Review*, 5(1), pp.74–95.

Henseler, J., Hubona, G. and Ray, P.A., 2016. Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management and Data Systems*, 116(1), pp.2–20. https://doi.org/10.1108/IMDS-09-2015-0382

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*, 43(1), pp.115–135. https://doi.org/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*, 24(1), pp.61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x

Hernon, P., 1995. Disinformation and misinformation through the internet: Findings of an exploratory study. *Government Information Quarterly*, 12(2), pp.133–139. https://doi.org/10.1016/0740-624X(95)90052-7

Hina, S., Panneer Selvam, D.D.D. and Lowry, P.B., 2019. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, 87. https://doi.org/10.1016/j.cose.2019.101594

Hong, K.W., Kelley, C.M., Tembe, R., Murphy-Hill, E. and Mayhorn, C.B., 2013. Keeping up with the joneses: Assessing phishing susceptibility in an email task. *Proceedings of the Human Factors and Ergonomics Society*, pp.1012–1016. https://doi.org/10.1177/1541931213571226

Hoorens, V., 1994. Unrealistic optimism in health and safety risks. In: *Social psychology and health: European perspectives.* Brookfield, VT: Avebury/Ashgate Publishing, pp.153–174.

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*, 89(2), pp.172–178. https://doi.org/10.1016/j.beproc.2011.10.015

Howard-Jones, P.A., 2014. Neuroscience and education: myths and messages. *Nature Reviews Neuroscience*, 15(12), pp.817–824. https://doi.org/10.1038/nrn3817

Howe, C.Q. and Purves, D., 2005. The Muller-Lyer illusion explained by the statistics of image-source relationships. *Proceedings of the National Academy of Sciences*, [online] 102(4), pp.1234–1239. https://doi.org/10.1073/pnas.0409314102

Hoyle, R.H., Stephenson, M.T., Palmgreen, P., Lorch, E.P. and Donohew, R.L., 2002. Reliability and validity of a brief measure of sensation seeking. *Personality and Individual Differences*, 32(3), pp.401–414.

Hristov, I. and Chirico, A., 2019. The role of sustainability key performance indicators (KPIs) in implementing sustainable strategies. *Sustainability (Switzerland)*, 11(20). https://doi.org/10.3390/su11205742.

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*, 43(4), pp.615–659.

Huculak, M., 2016. *How to turn your Windows 10 PC into a wireless hotspot | Windows Central*. [online] Available at: <https://www.windowscentral.com/how-turn-your-windows-10-pc-wireless-hotspot> [Accessed 3 September 2021].

Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z., 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, [online] 7(3), p.e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Hwang, I., Wakefield, R., Kim, S. and Kim, T., 2021. Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 61(4), pp.345–356. https://doi.org/10.1080/08874417.2019.1650676

Hyslip, T.S., 2020. Cybercrime-as-a-service operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp.815–846.

IASME Consortium Limited, 2018. *The IASME Governance Standard for Information and Cyber Security*.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. In: *Computers and Security*. [online] Elsevier, pp.83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P., 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, [online] 51(1), pp.69–79. https://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P., 2018. Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal*, 31(1), pp.53–82. https://doi.org/10.4018/IRMJ.2018010103

ISACA, 2018. *COBIT: Control objectives for information technologies*. [online] Available at: <https://www.isaca.org/resources/cobit> [Accessed 6 January 2022].

ISO/IEC, 2013. *ISO/IEC 27001:2013 Information technology -- Security techniques -- Specification for an Information Security Management System*.

J2 Global, I., 2020. *How to send & receive faxes online by email or computer*. [online] Available at: <https://www.efax.com/how-it-works> [Accessed 3 September 2021].

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F., 2007. Social phishing. *Communications of the ACM*, 50(10), pp.94–100. https://doi.org/10.1145/1290958.1290968

Jahangiri, L., Mucciolo, T.W., Choi, M. and Spielman, A.I., 2008. Assessment of teaching effectiveness in U.S. dental schools and the value of triangulation. *Journal of Dental Education*, 72(6), pp.707–718. https://doi.org/10.1002/j.0022-0337.2008.72.6.tb04536.x

Jakobsson, M. and Myers, S., 2007. *Phishing and countermeasures : understanding the increasing problem of electronic identity theft*. Hoboken, NJ: John Wiley & Sons.

Jalali, M.S., Bruckes, M., Westmattelmann, D. and Schewe, G., 2020. Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, 22(1). https://doi.org/10.2196/16775

James, W., 1890. *Habit*. New York: Henry Holt & Co.

Jansen, J. and Van Schaik, P., 2018. Persuading end users to act cautiously online: a fear appeals study on phishing. *Information and Computer Security*, 26(3), pp.264–276. https://doi.org/10.1108/ICS-03-2018-0038

Janz, N.K. and Becker, M.H., 1984. The health belief model: A decade later. *Health Education Quarterly*, 11(1), pp.1–47.

Jefferson, A., Bortolotti, L. and Kuzmanovic, B., 2017. What is unrealistic optimism? *Consciousness and Cognition*, 50, pp.3–11. https://doi.org/10.1016/j.concog.2016.10.005

Jenkins, J.L., Durcikova, A. and Nunamaker, J.F., 2021. Mitigating the security intention-behavior gap: The moderating role of required effort on the intention-behavior relationship. *Journal of the Association for Information Systems*, 22(1), pp.246–272. https://doi.org/10.17705/1jais.00660

Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B., 2017. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2), pp.597–626. https://doi.org/10.1080/07421222.2017.1334499

Jeong, S., Lee, J., Park, J. and Kim, C. kwon, 2017. The social relation key: A new paradigm for security. *Information Systems*, 71, pp.68–77. https://doi.org/10.1016/j.is.2017.07.003

Jiang, L. and Probst, T.M., 2015. Do your employees (collectively) trust you? The importance of trust climate beyond individual trust. *Scandinavian Journal of Management*, 31(4), pp.526–535. https://doi.org/10.1016/j.scaman.2015.09.003

Johnson, D.B., 2020. *Vishing attacks on the rise, FBI, CISA warn -- GCN*. [online] Available at: <https://gcn.com/articles/2020/08/24/fbi-cisa-vishing-warning.aspx> [Accessed 3 September 2021].

Johnston, A.C. and Warkentin, M., 2010. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), pp.549–566.

Johnston, M.P., 2014. Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries (QQML)*, 3, pp.619–626.

Jones, H.S., Towse, J.N., Race, N. and Harrison, T., 2019. Email fraud: The search for psychological predictors of susceptibility. *PloS One*, 14(1), p.e0209684.

Jouriles, E. and Sargent, K., 2017. Cyberbullying and its relationship to other forms of violence: The risks and dangers of polyvictimization. Assessment instruments for special populations view project Textbook of Disaster Psychiatry View project□. *Joining Forces Joining Families*, 17(1), pp.1–3.

Junco, R. and Cotten, S.R., 2012. No A 4 U: The relationship between multitasking and academic performance. *Computers and Education*, 59(2), pp.505–514. https://doi.org/10.1016/j.compedu.2011.12.023

Kahneman, D., 2003. Maps of bounded rationality: Psychology for behavioral economics. *The American Economic Review*, 93(5), pp.1449–1475.

Kara, I. and Aydos, M., 2022. The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems With Applications*, [online] 190, p.116198. https://doi.org/10.1016/j.eswa.2021.116198

Kearney, W.D. and Kruger, H.A., 2016. Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers and Security*, 61, pp.46–58. https://doi.org/10.1016/j.cose.2016.05.006

Keet, C.M., 2021. An exploration into cognitive bias in ontologies. In: *CAOS 2021: 5th Workshop on Cognition And OntologieS*. [online] Bolzano, Italy. Available at: <http://ceur-ws.org>

Keller, J., 2001. *Attitude is everything*. [online] Available at: <http://www.AsAManThinketh.net.>

Kelloway, E.K., 1995. Structural equation modelling in perspective. *Journal of Organizational Behavior*, [online] 16(3), pp.215–224. Available at: <https://www.jstor.org/stable/2488509>

Keyworth, M., 2016. Vishing and smishing: The rise of social engineering fraud. *BBC News.* [online] Available at: <https://www.bbc.com/news/business-35201188> [Accessed 3 September 2021].

Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, [online] 106, p.102267. https://doi.org/10.1016/j.cose.2021.102267

Ki-Aries, D. and Faily, S., 2017. Persona-centred information security awareness. *Computers and Security*, 70, pp.663–674. https://doi.org/10.1016/j.cose.2017.08.001

Kießling, S., Hanka, T. and Merli, D., 2021. Salt & pepper: Spice up security behavior with cognitive triggers. In: *European Interdisciplinary Cybersecurity Conference*. New York, NY: ACM, pp.26–31. https://doi.org/10.1145/3487405.3487656

Kinari, Y., 2016. Properties of expectation biases: Optimism and overconfidence. *Journal of Behavioral and Experimental Finance*, 10, pp.32–49. https://doi.org/10.1016/j.jbef.2016.02.003

Kirda, E. and Kruegel, C., 2005. Protecting users against phishing attacks with antiphish. In: *29th Annual International Computer Software and Applications Conference (COMPSAC'05)*. pp.517–524.

Kisak, P.F., 2015. *Cognitive science & bias: The dynamics of subjective truth & human nature*. CreateSpace Independent Publishing Platform.

Klein, W.M. and Weinstein, N.D., 1997. Social comparison and unrealistic optimism about personal risk. In: Buunk, B.P. & Gibbons, F.X. eds. *Health, coping, and well-being: Perspectives from social comparison theory.* Mahwah, NJ: Lawrence Erlbaum Associates, pp.25–61.

Klesel, M., Schuberth, F., Henseler, J. and Niehaves, B., 2019. A test for multigroup comparison using partial least squares path modeling. *Internet Research*, 29(3), pp.464–477. https://doi.org/10.1108/IntR-11-2017-0418

Kline, R.B., 2011. *Principles and practice of structural equation modeling*. 3rd edition. New York: Guilford Press.

KnowBe4, 2017. *Phishing | Common Phishing Scams*. [online] Available at: <https://www.phishing.org/common-phishing-scams> [Accessed 1 September 2018].

de Kok, L.C., Oosting, D. and Spruit, M., 2020. The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security: An International Journal*, [online] 46(3), pp.251–266. https://doi.org/10.11610/isij.4618

Komiak, S.Y.X. and Benbasat, I., 2006. The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly: Management Information Systems*, 30(4), pp.941–960. https://doi.org/10.2307/25148760

Kooken, J., Ley, T. and de Hoog, R., 2007. How do people learn at the workplace? Investigating four workplace learning assumptions. In: Duval, E., Klamma R. and Wolpers, M. eds. *Creating New Learning Experiences on a Global Scale*. [online] Berlin: Springer, pp.158–171. https://doi.org/10.1007/978-3-540-75195-3_12

Kramer, R.M., 2009. Rethinking trust. *Harvard Business Review*, 87(6), pp.68–77.

Krizan, Z. and Windschitl, P.D., 2009. Wishful thinking about the future: Does desire impact optimism? *Social and Personality Psychology Compass*, 3(3), pp.227–243.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J., 2008. Lessons from a real world evaluation of anti-phishing training. In: *2008 eCrime Researchers Summit*. pp.1–12.

Kunda, Z., 1990. The case for motivated reasoning. *Psychological Bulletin*, 108(3), pp.480–498. https://doi.org/10.1037/0033-2909.108.3.480

Langer, E.J. and Roth, J., 1975. Heads I win, tails it's chance: The illusion of control as a function of the sequence of outcomes in a purely chance task. *Journal of Personality and Social Psychology*, 32(6), p.951.

Lankton, N.K., Mcknight, D.H. and Tripp, J., 2015. Technology, humanness, and trust: rethinking trust in technology. *Journal of the Association for Information Systems*, 16(10), pp.880–918.

Lawson, P., Pearson, C.J., Crowson, A. and Mayhorn, C.B., 2020. Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, 86, p.103084.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H., 2014. Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), pp.1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, A.S., 2001. Editorial. *MIS Quarterly*, [online] 25(1), pp.iii–vii. Available at: <http://www.jstor.org/stable/3250954>

Lee, C., Lee, C.C. and Kim, S., 2016. Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*, [online] 59, pp.60–70. https://doi.org/10.1016/j.cose.2016.02.004

Leedy, P.D. and Ormrod, J.E., 2001. *Practical research: Planning and design*. 7th edition. Thousand Oaks, CA: SAGE Publications.

Lemmetty, S. and Collin, K., 2020. Self-directed learning as a practice of workplace learning: Interpretative repertoires of self-directed learning in ICT work. *Vocations and Learning*, [online] 13(1), pp.47–70. https://doi.org/10.1007/s12186-019-09228-x.

Leukfeldt, R. and Holt, T.J., 2019. *The human factor of cybercrime*. Routledge.

Leventhal, H., 1970. Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, 5(C), pp.119–186. https://doi.org/10.1016/S0065-2601(08)60091-X

Leventhal, H., 1971. Fear appeals and persuasion: the differentiation of a motivational construct. *American Journal of Public Health*, 61(6), pp.1208–1224.

Levine, L.E., Waite, B.M. and Bowman, L.L., 2007. Electronic media use, reading, and academic distractibility in college youth. *Cyberpsychology and Behavior*, 10(4), pp.560–566. https://doi.org/10.1089/cpb.2007.9990

Levy, Y. and Ellis, T.J., 2006. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, [online] 9, pp.181–212. https://doi.org/10.28945/479

Lewin, K., 1945. The Research Center for Group Dynamics at Massachusetts Institute of Technology. *Sociometry*, 8(2), pp.126–136.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45(October 2018), pp.13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liberman, B., Seidman, G., McKenna, K.Y.A. and Buffardi, L.E., 2011. Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior*, 27(6), pp.2192–2199. https://doi.org/10.1016/j.chb.2011.06.015

Libicki, M., 2020. Cyberwar is what states make of it. *The Cyber Defense Review*, 5(2), pp.77–88.

Lin, T., Capecci, D.E., Ellis, D.M., Rocha, H.A., Dommaraju, S., Oliveira, D.S. and Ebner, N.C., 2019. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(5), pp.1–28.

Lin, Y., Liu, R., Divakaran, D.M., Ng, J.Y., Chan, Q.Z., Lu, Y., Si, Y., Zhang, F. and Dong, J.S., 2021. Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. In: *30th USENIX Security Symposium (USENIX Security 21)*. pp.3793–3810.

Liu, Y., Lin, F.Y., Ahmad-Post, Z., Ebrahimi, M., Zhang, N., Hu, J.L., Xin, J., Li, W. and Chen, H., 2020. Identifying, collecting, and monitoring personally identifiable information: From the dark web to the surface web. In: *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. pp.1–6.

Livingstone, D.W., 2001. *Adults' informal learning: definitions, findings, gaps and future research*. *WALL Working Paper*.

Locke, E.A., 2007. The case for inductive theory building. *Journal of Management*, 33(6), pp.867–890. https://doi.org/10.1177/0149206307307636

Loeb, L., 2018. *Autofill brings automatic vulnerability*. [online] Available at: <https://www.darkreading.com/application-security/autofill-brings-automatic-vulnerability/a/d-id/739323> [Accessed 3 September 2021].

Logg, J.M., Minson, J.A. and Moore, D.A., 2019. Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes*, 151, pp.90–103. https://doi.org/10.1016/j.obhdp.2018.12.005

Lowry, P.B. and Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, 57(2), pp.123–146. https://doi.org/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*, 25(5), pp.433–463. https://doi.org/10.1111/isj.12043

Lowry, P.B., Zhang, D., Zhou, L. and Fu, X., 2010. Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal*, 20(3), pp.297–315. https://doi.org/10.1111/j.1365-2575.2009.00334.x

Mackenzie, N. and Knipe, S., 2006. Research dilemmas: Paradigms, methods and methodology. *Issues In Educational Research*, 16.

Mäkitalo, H., 2017. *Measuring users' level of information security awareness: Research and development of sample questions*. Master's thesis in Information Systems. University of Jyväskylä.

Malwarebytes, 2018. *Bad romance: catphishing explained | Malwarebytes Labs*. [online] Available at: <https://blog.malwarebytes.com/cybercrime/2017/11/bad-romance-catphishing-explained/> [Accessed 3 September 2021].

Mamonov, S. and Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, pp.32–44. https://doi.org/10.1016/j.chb.2018.01.028

Manke, S. and Winkler, I., 2012. *The habits of highly successful security awareness programs: A cross-company comparison*. [online] Available at: <http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf> [Accessed 1 November 2021].

Mansfield-Devine, S., 2013. Interview: Joe Ferrara – Fighting phishing. *Computer Fraud and Security*, [online] (7), pp.17–20. https://doi.org/10.1016/S1361-3723(13)70064-2

Mansfield-Devine, S., 2018. The ever-changing face of phishing. *Computer Fraud and Security*, [online] 2018(11), pp.17–19. https://doi.org/10.1016/S1361-3723(18)30111-8

Marsh, S., 1994. Optimism and pessimism in trust. In: *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*, 28(8), pp.469–473. https://doi.org/10.1016/j.tree.2013.05.013

McAfee, 2013. *What is a "drive-by" download? | McAfee Blogs*. [online] Available at: <https://www.mcafee.com/blogs/family-safety/drive-by-download/> [Accessed 3 September 2021].

Mcanyana, W., Brindley, C. and Seedat, Y., 2020. Insight into the cyberthreat landscape in South Africa. *Accenture*, p.12.

McCaul, H.S., Hinsz, V.B. and McCaul, K.D., 1995. Assessing organizational commitment: An employee's global attitude toward the organization. *Journal of Applied Behavioral Science*, 31, pp.80–90.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M., 2017. Individual differences and Information Security Awareness. *Computers in Human Behavior*, [online] 69, pp.151–156. https://doi.org/10.1016/j.chb.2016.11.065

McKinsey & Company, 2020. *COVID-19 digital transformation & technology | McKinsey*. [online] Available at: <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-

technology-tipping-point-and-transformed-business-forever> [Accessed 3 September 2021].

McLeod, S.A., 2018. Attitudes and behavior. [online] *Simply Psychology*. Available at: <https://www.simplypsychology.org/attitudes.html> [Accessed 2 August 2021].

McVay Lynch, M., 2012. *Learning online*. Routledge. https://doi.org/10.4324/9780203353455

Mendelsohn, A.I., 2019. Creatures of habit: The neuroscience of habit and purposeful behavior. *Biological Psychiatry*, 85(11), pp.e49–e51. https://doi.org/10.1016/j.biopsych.2019.03.978

Metzger, M.J. and Suh, J.J., 2017. Comparative optimism about privacy risks on Facebook. *Journal of Communication*, 67(2), pp.203–232.

Milgram, S., 1983. *Obedience to authority: An experimental view*. New York: Harper Collins.

Miller, F.G., Gluck Jr, J.P. and Wendler, D., 2008. Debriefing and accountability in deceptive research. *Kennedy Institute of Ethics Journal*, 18(3), pp.235–251.

Mishra, S. and Soni, D., 2019. SMS phishing and mitigation approaches. In: *2019 12th International Conference on Contemporary Computing, IC3 2019*. https://doi.org/10.1109/IC3.2019.8844920

Mishra, S. and Soni, D., 2020. Smishing detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, 108, pp.803–815. https://doi.org/10.1016/J.FUTURE.2020.03.021

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

Modic, D. and Lea, S.E.G., 2014. Scam compliance and the psychology of persuasion. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2364464

Moody, G.D., Galletta, D.F. and Dunn, B.K., 2017. Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, 26(6), pp.564–584.

Moody, G.D., Siponen, M. and Pahnila, S., 2018. Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems*, 42(1), pp.285–311. https://doi.org/10.25300/MISQ/2018/13853

Moore, D.A. and Healy, P.J., 2008. The Trouble With Overconfidence. *Psychological Review*, 115(2), pp.502–517. https://doi.org/10.1037/0033-295X.115.2.502

Moreno-Fernández, M.M., Blanco, F., Garaizar, P. and Matute, H., 2017. Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior*, 69, pp.421–436. https://doi.org/10.1016/j.chb.2016.12.044

Morgan, D.L., 2014. Pragmatism as a paradigm for social research. *Qualitative Inquiry*, 20(8), pp.1045–1053. https://doi.org/10.1177/1077800413513733

Morgan, D.L., 2015. From themes to hypotheses: Following up with quantitative methods. *Qualitative Health Research*, 25(6), pp.789–793. https://doi.org/10.1177/1049732315580110

Moul, K.A., 2019. Avoid phishing traps. *Proceedings ACM SIGUCCS User Services Conference*, (August 2017), pp.199–208. https://doi.org/10.1145/3347709.3347774

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*, 94(December 2018), pp.154–175. https://doi.org/10.1016/j.chb.2018.12.036

Nakhila, O., Amjad, M.F., Dondyk, E. and Zou, C., 2018. Gateway independent user-side wi-fi Evil Twin Attack detection using virtual wireless clients. *Computers and Security*, 74, pp.41–54. https://doi.org/10.1016/j.cose.2017.12.009

Nandedkar, A. and Midha, V., 2012. Computers in human behavior It won't happen to me : An assessment of optimism bias in music piracy. *Computers in Human Behavior*, [online] 28(1), pp.41–48. https://doi.org/10.1016/j.chb.2011.08.009

Neto, N.N., Madnick, S., Paula, A.M.G.D. and Borges, N.M., 2021. Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality*, [online] 13(1), pp.1–33. https://doi.org/10.1145/3439873

Newman, E.J., Garry, M., Unkelbach, C., Bernstein, D.M., Lindsay, D. and Nash, R.A., 2015. Truthiness and falsiness of trivia claims depend on judgmental contexts. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 41(5), pp.1337–1348.

NIST, 2020. *National Institute of Standards and Technology Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. [online] Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-53r5

Norris, G. and Brookes, A., 2021. Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, [online] 169, p.109847. https://doi.org/10.1016/j.paid.2020.109847

Norris, G., Brookes, A. and Dowell, D., 2019. The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34(3), pp.231–245. https://doi.org/10.1007/s11896-019-09334-5

Norton, 2018. *What is smishing?* [online] Available at: <https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html> [Accessed 3 September 2021].

Noura, M., Atiquzzaman, M. and Gaedke, M., 2019. Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications*, 24(3), pp.796–809.

Nunes, P., Antunes, M. and Silva, C., 2021. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. In: *Procedia Computer Science*. Elsevier B.V., pp.173–181. https://doi.org/10.1016/j.procs.2021.01.118

NZ Herald, 2018. House invoice scam leaves couple $53k out of pocket. *NZ Herald*. [online] Available at: <https://www.nzherald.co.nz/business/house-invoice-scam-leaves-couple-53k-out-of-pocket/VNE22E6I3N4JV57C64WWOKATOI/> [Accessed 3 September 2021].

Oates, B.J., Griffiths, M. and McLean, R., 2022. *Researching information systems and computing*. Sage.

Oczak, M. and Niedźwieńska, A., 2007. Debriefing in deceptive research: A proposed new procedure. *Journal of Empirical Research on Human Research Ethics*, 2(3), pp.49–59.

Ögütçü, G., Testik, Ö.M. and Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. *Computers and Security*, 56, pp.83–93. https://doi.org/10.1016/j.cose.2015.10.002

Ollmann, G., 2004. *The phishing guide: Understanding and prevent phishing attacks*. NGS Software Insight Security Research.

O'Reardon, M.E. and Rendar, M., 2020. Managing security risk: How COVID-19 pandemic and work-from-home arrangements pose new security considerations. *Employee Relations Law Journal*, 46(2).

OWASP, 2017. *OWASP top ten 2017*. [online] Available at: <https://owasp.org/www-project-top-ten/2017/A1_2017-Injection#> [Accessed 3 September 2021].

Pandya, P., 2013. The enemy (the intruder's genesis). *Computer and Information Security Handbook*, pp.e45–e56. https://doi.org/10.1016/B978-0-12-803843-7.00028-4

Panhwar, A.H., Ansari, S. and Shah, A.A., 2017. Post-positivism: An effective paradigm for social and educational research. *International Research Journal of Arts & Humanities (IRJAH)*, 45(45).

Park, J. and Oh, C.-G., 2016. Cognitive bias and information security research: Research trends and opportunities. *Asia Pacific Journal of Information Systems*, [online] 26(2), pp.270–298. https://doi.org/10.14329/apjis.2016.26.2.290

Park, Y.S., Konge, L. and Artino, A.R., 2020. The positivism paradigm of research. *Academic Medicine*, pp.690–694. https://doi.org/10.1097/ACM.0000000000003093

Parker, H.J. and Flowerday, S., 2021. Understanding the disclosure of personal data online. *Information & Computer Security*, [online] 29(3), pp.413–434. https://doi.org/10.1108/ICS-10-2020-0168

Parmar, B., 2012. Protecting against spear-phishing. *Computer Fraud and Security*, 2012(1), pp.8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M., 2019. Predicting susceptibility to social influence in phishing emails. *International Journal of Human Computer Studies*, [online] 128, pp.17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

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*, 66, pp.40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, pp.165–176. https://doi.org/10.1016/j.cose.2013.12.003

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C., 2013. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In: *IFIP international information security conference*, pp.366–378.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C., 2015. The design of phishing studies: Challenges for researchers. *Computers and Security*, [online] 52, pp.194–206. https://doi.org/10.1016/j.cose.2015.02.008

Pashler, H., Mcdaniel, M., Rohrer, D. and Bjork, R., 2008. Learning styles: Concepts and evidence learning styles concepts and evidence. *Psychological Science in the Public Interest*, 9(3), pp.105–119.

Patomaki, H. and Wight, C., 2000. After postpositivism? The promises of critical realism. *International Studies Quarterly*, [online] 44(2), pp.213–237. https://doi.org/10.1111/0020-8833.00156

Pattinson, M., Butavicius, M., Parsons, K., Mccormac, A., Calic, D. and Jerram, C., 2016. The information security awareness of bank employees. (Haisa), pp.189–198.

Patton, M.Q., 2002. *Qualitative research & evaluation methods*. Sage.

Pessoa, L., 2008. On the relationship between emotion and cognition. *Nature Reviews Neuroscience*, 9(2), pp.148–158. https://doi.org/10.1038/nrn2317

Petersen, R., Santos, D., Smith, M.C., Wetzel, K.A. and Witte, G., 2020. *Workforce Framework for Cybersecurity (NICE Framework)*. [online] Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-181r1

Peterson, R.C. and Thurstone, L.L., 1932. *The effect of motion pictures on the social attitudes of high school children*. Edwards Brothers.

Petrič, G. and Roer, K., 2022. The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, 67. https://doi.org/10.1016/j.tele.2021.101766

Petty, R.E. and Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. *Communication and Persuasion*, pp.1–24. https://doi.org/10.1007/978-1-4612-4964-1_1

Pfeiffer, S., 2021. The greater transformation: Digitalization and the transformative power of distributive forces in digital capitalism. *International Critical Thought*, 11(4), pp.535–552. https://doi.org/10.1080/21598282.2021.2005656

Pfleeger, S.L. and Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, 31(4), pp.597–611. https://doi.org/10.1016/j.cose.2011.12.010

Philips, M., Sander, P. and Govers, C., 1994. Policy formulation by use of QFD techniques: A case study. *International Journal of Quality & Reliability Management*, 11(5), pp.46–58. https://doi.org/10.1108/02656719410062876/FULL/PDF

Plous, S., 1993. *The psychology of judgment and decision making.* McGraw-Hill series in social psychology. New York, NY/UK: McGraw-Hill.

Polit, D.F. and Beck, C.T., 2008. *Nursing research: Generating and assessing evidence for nursing practice*. Lippincott Williams & Wilkins.

Pronin, E., Lin, D. and Ross, L., 2002. The bias blind spot: Perceptions of bias in self versus others. *PSPB*, 28(3), pp.369–381.

Proofpoint, 2021. *2021 State of the phish*. [online] Available at: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish> [Accessed 16 May 2021].

Protection of Personal Information Act, 2013. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Punch, K., 2003. *Survey research: The basics*. New Delhi: Sage.

Purwanto, E. and Tannady, H., 2020. The factors affecting intention to use Google Meet amid online meeting platforms competition in Indonesia. *Technology Reports of Kansai University*, 62(06), pp.2829–2838.

Qabajeh, I., Thabtah, F. and Chiclana, F., 2018. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review*, 29, pp.44–55.

Rader, M.A. and Rahman, S. (Shawon) M. 2013. Phishing techniques and mitigating the associated security risks. *International Journal of Network Security & Its Applications*, 5(4), pp.23–41. https://doi.org/10.5121/ijnsa.2013.5402

Ramzan, Z., 2010. Phishing attacks and countermeasures. In: *Handbook of information and communication security*., Berlin, Heidelberg: Springer, pp.433–448. https://doi.org/10.1007/978-3-642-04117-4_23

Reddy, S., Labutov, I., Banerjee, S. and Joachims, T., 2016. Unbounded Human Learning. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. [online] New York, NY, pp.1815–1824. https://doi.org/10.1145/2939672.2939850

Reisberg, D., 2001. *Cognition: Exploring the science of the mind*. New York: Norton.

Rempel, J.K., Holmes, J.G. and Zanna, M.P., 1985. Trust in close relationships. *Journal of Personality and Social Psychology*, 49(1), pp.95–112. https://doi.org/10.1037/0022-3514.49.1.95

Resnik, D.B. and Finn, P.R., 2018. Ethics and phishing experiments. *Science and Engineering Ethics*, 24(4), pp.1241–1252.

Reuters, 2005. *Identity thieves take advantage of VoIP – silicon.com*. [online] Available at: <https://web.archive.org/web/20050324073507/http://www.silicon.com/research/specialreports/voip/0%2C3800004463%2C39128854%2C00.htm> [Accessed 3 September 2021].

Rhee, H., Kim, C. and Kim, C., 2005. I am fine but you are not : Optimistic bias and illusion of control on information security. IN: *Proceedings of the International Conference on Information Systems,* December.

Rhee, H., Ryu, Y.U. and Kim, C., 2011. Unrealistic optimism on information security management. *Computers & Security*, [online] 31(2), pp.221–232. https://doi.org/10.1016/j.cose.2011.12.001

Riegelsberger, J., Sasse, M.A. and McCarthy, J.D., 2005. The mechanics of trust: A framework for research and design. *International Journal of Human Computer Studies*, 62(3), pp.381–422. https://doi.org/10.1016/j.ijhcs.2005.01.001

Roberts, A., Sharman, S. and Bowden-Jones, H., 2022. Clinical services for problematic internet usage. *Current Opinion in Behavioral Sciences*, 46, p.101180

Robertson, C.T. and Kesselheim, A.S. eds., 2016. *Blinding as a solution to bias:strengthening biomedical science, forensic science, and law.* [online] Boston, MA: Elsevier. Available at: <https://books.google.co.za/books?hl=en&lr=&id=fnjICgAAQBAJ&oi=fnd&pg=PA13&dq=cognitive+bias&ots=5mDjnhSF_v&sig=eFBjSTdolsE_ND9o9rmwKko5nTg#v=onepage&q=cognitive%20bias&f=false> [Accessed 7 February 2022].

Rodríguez, G.E., Torres, J.G., Flores, P. and Benavides, D.E., 2020. Cross-site scripting (XSS) attacks and mitigation: A survey. *Computer Networks*, 166. https://doi.org/10.1016/j.comnet.2019.106960

Rogers, R.W., 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In: Cacioppo, J. and Petty, R., eds. *Social psychophysiology.* New York: Guilford Press, pp.153–177.

Rotter, J.B., 1967. A new scale for the measurement of interpersonal trust1. *Journal of Personality*, 35(4), pp.651–665. https://doi.org/10.1111/j.1467-6494.1967.tb01454.x

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C., 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), pp.393–404. https://doi.org/10.5465/amr.1998.926617

Rowley, J., 2014. Designing and using research questionnaires. *Management Research Review*, [online] 37(3), pp.308–330. https://doi.org/10.1108/MRR-02-2013-0027

RSA, 2016. *What is a drive-by download?* [online] Available at: <https://www.rsa.com/content/dam/en/case-study/asoc-drive-by-download.pdf> [Accessed 3 September 2021].

Ruhwanya, Z. and Ophoff, J., 2019. Information security culture assessment of small and medium-sized enterprises in Tanzania. *IFIP Advances in Information and Communication Technology*, [online] 551, pp.776–788. https://doi.org/10.1007/978-3-030-18400-1_63

Runes, D.D., 1984. *Dictionary of philosophy: Revised and enlarged*. Rowman & Littlefield.

Sachs, J., 2017. *"It's 4,000 times easier to do it today than when I did it:" Famous con man offers advice to avoid online scams*. [online] FOX 6 Now Milwaukee. Available at: <https://www.fox6now.com/news/its-4000-times-easier-to-do-it-today-than-when-i-did-it-famous-con-man-offers-advice-to-avoid-online-scams> [Accessed 22 March 2021].

Sadowsky, G., Dempsey, J.X., Greenberg, A., Mack, B.J. and Schwartz, A., 2003. *Information technology security handbook*. The International Bank for Reconstruction and Development (The World Bank).

Safa, N.S., Maple, C., Watson, T. and Von Solms, R., 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, 40, pp.247–257. https://doi.org/10.1016/j.jisa.2017.11.001

Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organizations. *Computers and Security*, [online] 56, pp.1–13. https://doi.org/10.1016/j.cose.2015.10.006

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*, [online] 53, pp.65–78. https://doi.org/10.1016/j.cose.2015.05.012

Sanders, J., 2018. *Ransomware: What IT pros need to know (free PDF) - TechRepublic*. [online] Available at: <https://www.techrepublic.com/resource-library/whitepapers/ransomware-what-it-pros-need-to-know-free-pdf/> [Accessed 3 September 2021].

Sarkar, S., Almukaynizi, M., Shakarian, J. and Shakarian, P., 2019. Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. *The Cyber Defense Review*, pp.87–102.

Sarstedt, M., Henseler, J. and Ringle, C.M., 2011. Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. In: M. Sarstedt, M. Schwaiger and C. Taylor, eds. *Measurement and research methods in international marketing (Advances in international marketing)*. London, UK: Emerald Group.

Sas, M., Reniers, G., Ponnet, K. and Hardyns, W., 2021. The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, [online] 144(February), p.105447. https://doi.org/10.1016/j.ssci.2021.105447

Saunders, M., Lewis, P. and Thornhill, A., 2016. *Research methods for business students*. 7th edition. Pearson Education.

Schaab, P., Beckers, K. and Pape, S., 2016. A systematic gap analysis of social engineering defence mechanisms considering social psychology. In: *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, pp.241–251.

Scheier, M.F., Carver, C.S. and Bridges, M.W., 1994. Distinguishing optimism from neuroticism (and trait anxiety, self-mastery, and self-esteem): A reevaluation of the Life Orientation Test. *Journal of Personality and Social Psychology*, 67(6), p.1063.

Schneider, D., Slaughter, V.P. and Dux, P.E., 2017. Current evidence for automatic Theory of Mind processing in adults. *Cognition*, 162, pp.27–31. https://doi.org/10.1016/j.cognition.2017.01.018

Scholefield, S. and Shepherd, L.A., 2019. Gamification techniques for raising cyber security awareness. In: *International Conference on Human-Computer Interaction*. [online] pp.191–203. https://doi.org/10.1007/978-3-030-22351-9_13

Schouteren, S., 2019. From wooden shoe to click of a button: The risk of disgruntled employees. *Computer Fraud & Security*, 2019(3), pp.10–13. https://doi.org/10.1016/S1361-3723(19)30029-6

Schwind, C. and Buder, J., 2012. Reducing confirmation bias and evaluation bias: When are preference-inconsistent recommendations effective – And when not? *Computers in Human Behavior*, 28(6), pp.2280–2290. https://doi.org/10.1016/j.chb.2012.06.035

Sechrest, L. and Sidani, S., 1995. Quantitative and qualitative methods:: Is There an Alternative? *Evaluation and Program Planning*, 18(1), pp.77–87.

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*, 12(1), pp.237–265.

Seemann, P., Stofkova, Z. and Binasova, V., 2019. Analysis of possibilities and key competences of lifelong learning in selected organization. In: *EDULEARN19 Proceedings*. [online] IATED, pp.6998–7006. https://doi.org/10.21125/edulearn.2019.1680

Shafiee Hasanabadi, S., Habibi Lashkari, A. and Ghorbani, A.A., 2020. A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour. *Forensic Science International: Digital Investigation*, 35. https://doi.org/10.1016/j.fsidi.2020.301024

Shahbaznezhad, H., Kolini, F. and Rashidirad, M., 2021. Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, [online] 61(6), pp.539–550. https://doi.org/10.1080/08874417.2020.1812134

Shareef, M.A., Kapoor, K.K., Mukerji, B., Dwivedi, R. and Dwivedi, Y.K., 2020. Group behavior in social media: Antecedents of initial trust formation. *Computers in Human Behavior*, 105. https://doi.org/10.1016/j.chb.2019.106225

Sharot, T., 2011. The optimism bias. *Current Biology*, 21(23), pp.941–945. https://doi.org/10.1016/j.cub.2011.10.030

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.J., 2009. The impact of information richness on information security awareness training effectiveness. *Computers and Education*, 52(1), pp.92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. pp.373–382.

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*, 70(4), pp.844–855. https://doi.org/10.1037/0022-3514.70.4.844

Shepperd, J.A., Pogge, G. and Howell, J.L., 2017. Assessing the consequences of unrealistic optimism: Challenges and recommendations. *Consciousness and Cognition*, [online] 50, pp.69–78. https://doi.org/10.1016/j.concog.2016.07.004

Shropshire, J., Warkentin, M. and Sharma, S., 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, [online] 49, pp.177–191. https://doi.org/10.1016/j.cose.2015.01.002

Sikolia, D., Twitchell, D. and Sagers, G., 2016. Employees' Adherence to Information Security Policies Employees' Adherence to Information Security Policies: A Partial Replication. In: *Twenty-second Americas Conference on Information Systems*. San Diego.

Simons, D.J. and Chabris, C.F., 1999. Gorillas in our midst: Sustained inattentional blindness for dynamic events. *Perception*, 28, pp.1059–1074.

Singh, J. and Singh, J., 2021. A survey on machine learning-based malware detection in executable files. *Journal of Systems Architecture*, [online] 112, p.101861. https://doi.org/10.1016/j.sysarc.2020.101861

Siponen, M., Adam Mahmood, M. and Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), pp.217–224. https://doi.org/10.1016/j.im.2013.08.006

Sitkin, S.B. and Roth, N.L., 1993. Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, [online] 4(3), pp.367–392. Available at: <https://www.jstor.org/stable/2634950> [Accessed 30 January 2022].

Social-Engineer, L., 2020. *Vishing: Security through education*. [online] Available at: <https://www.social-engineer.org/framework/attack-vectors/vishing/> [Accessed 3 September 2021].

Sood, A.K. and Enbody, R.J., 2011a. Frametrapping the framebusting. *Network Security*, 2011(10), pp.8–12. https://doi.org/10.1016/S1353-4858(11)70105-2

Sood, A.K. and Enbody, R.J., 2011b. Malvertising: Exploiting web advertising. *Computer Fraud and Security*, 2011(4), pp.11–16. https://doi.org/10.1016/S1361-3723(11)70041-0

Spencer, H., 1867. *First principles*. 2nd edition. London: Williams and Norgate.

Stack, B., 2018. Here's how much your personal information is selling for on the dark web. *Experian. Haettu*, 4, p.2021.

Steel, C.M.S., 2019. Stolen identity valuation and market evolution on the dark web. *International Journal of Cyber Criminology*, 13(1), pp.70–83.

Stefaniuk, T., 2020. Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, 7(3), pp.1832–1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Stenberg, G., 2006. Conceptual and perceptual factors in the picture superiority effect. *European Journal of Cognitive Psychology*, 18(6), pp.813–847.

Stern, P.C., Dietz, T., Abel, T.D., Guagnano, G. and Kalof, L., 1999. *A value-belief-norm theory of support for social movements: The case of environmentalism recommended citation*. [online] Available at: <https://cedar.wwu.edu/hcop_facpubs>.

Steves, M., Greene, K. and Theofanos, M., 2020. Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*, 6(1). https://doi.org/10.1093/CYBSEC/TYAA009.

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

Suddaby, R., 2006. From the editors: What grounded theory is not. *Academy of Management Journal*, 49(4), pp.633–642. https://doi.org/10.5465/amj.2006.22083020

Sultan, P., Tarafder, T., Pearson, D. and Henryks, J., 2020. Intention-behaviour gap and perceived behavioural control-behaviour gap in theory of planned behaviour: moderating roles of communication, satisfaction and trust in organic food consumption. *Food Quality and Preference*, [online] 81(January 2019), p.103838. https://doi.org/10.1016/j.foodqual.2019.103838

Sumner, A. and Yuan, X., 2019. Mitigating phishing attacks: An overview. In: *ACMSE 2019 – Proceedings of the 2019 ACM Southeast Conference*. pp.72–77. https://doi.org/10.1145/3299815.3314437

Svenson, O., 1981. Are we all less risky and more skillful than our fellow drivers? *Acta Psychologica*, 47(2), pp.143–148.

Svenson, O., Fischhoff, B. and MacGregor, D., 1985. Perceived driving safety and seatbelt usage. *Accident Analysis & Prevention*, 17(2), pp.119–133.

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*, 124(2), pp.229–244. https://doi.org/10.1016/j.obhdp.2014.03.007.

Sweller, J., 1994. Cognitive load theory, learning difficulty, and instructional design. *Learning and Instruction*, 4(4), pp.295–312. https://doi.org/10.1016/0959-4752(94)90003-5

Symantec, 2019. *Internet Security Threat Report VOLUME 24, February 2019*. *Internet Security Threat Report*.

Syofyan, R. and Siwi, M.K., 2018. The impact of visual, auditory, and kinesthetic learning styles on economics education teaching. In: *1st International Conference on Economics Education, Economics, Business and Management, Accounting and Entrepreneurship*. Atlantis Press.pp.642–649.

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

Thomas, J. and Mantri, P., 2015. Axiomatic design/design patterns mashup: Part 2 (cyber security). In: *Procedia CIRP*. Elsevier B.V.pp.276–283. https://doi.org/10.1016/j.procir.2015.08.011

Tornblad, M.K., Jones, K.S., Namin, A.S. and Choi, J., 2021. Characteristics that predict phishing susceptibility: A review. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. pp.938–942.

Torten, R., Reaiche, C. and Boyle, S., 2018. The impact of security awareness on information technology professionals' behavior. *Computers and Security*, 79, pp.68–79. https://doi.org/10.1016/j.cose.2018.08.007

Trend Micro, 2019. *Whale phishing*. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/definition/whale-phishing> [Accessed 14 July 2020].

Tschakert, K.F. and Ngamsuriyaroj, S., 2019. Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6), p.e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

Tsohou, A., Karyda, M. and Kokolakis, S., 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers and Security*, [online] 52, pp.128–141. https://doi.org/10.1016/j.cose.2015.04.006

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*, 24(1), pp.38–58. https://doi.org/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*, 18(4), pp.193–205. https://doi.org/10.1016/j.jisa.2013.07.003

Tversky, A. and Kahneman, D., 1986. *Judgment under uncertainty: Heuristics and biases. Judgment and decision making: An interdisciplinary reader.* New York, NY, US: Cambridge University Press.

Twidale, M.B., 2005. Over the shoulder learning: Supporting brief informal learning. *Computer Supported Cooperative Work (CSCW)*, 14(6), pp.505–547. https://doi.org/10.1007/s10606-005-9007-7

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. *Computers and Security*, 109. https://doi.org/10.1016/j.cose.2021.102387

Umawing, J., 2019. *Something else is phishy: How to detect phishing attempts on mobile phones – Malwarebytes Labs | Malwarebytes Labs*. [online] Available at: <https://blog.malwarebytes.com/101/2018/12/something-else-phishy-detect-phishing-attempts-mobile/> [Accessed 3 September 2021].

Vasanthi, S. and Basariya, S.R., 2019. On the job training implementation and its benefits. *International Journal of Research and Analytical Reviews*, [online] 6(1), pp.210–215. Available at: <https://www.researchgate.net/publication/331486221>

Van der Schyff, K., 2019. *A personality-based surveillance model for Facebook apps*. Rhodes University.

Van Maanen, J., Sørensen, J.B. and Mitchell, T.R., 2007. The interplay between theory and method. *Academy of Management Review*, 32(4), pp.1145–1154. https://doi.org/10.5465/amr.2007.26586080

Van Slyke, C. and Belanger, F., 2020. Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. *Computers and Security*, 99. https://doi.org/10.1016/j.cose.2020.102064

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C.H., Klievink, B., Christin, N. and Van Eeten, M., 2018. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In: *27th USENIX security symposium (USENIX security 18)*. pp.1009–1026.

Verizon, 2022. *Data breach investigations report*. [online] Available at: <https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/> [Accessed 21 July 2022].

Verkijika, S.F., 2019. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, [online] 101(July), pp.286–296. https://doi.org/10.1016/j.chb.2019.07.034

Vincent, A. and Ross, D., 2001. Personalize training: Determine learning styles, personality types and multiple intelligences online. *The Learning Organization*, 8(1), pp.36–43. https://doi.org/10.1108/09696470110366525/FULL/PDF

Vinzi, V., Chin, W., Henseler, J. and Wang, H., 2010. *Handbook of partial least squares*. Berlin: Springer.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), pp.576–586. https://doi.org/10.1016/j.dss.2011.03.002

Walker, P.M.B. (ed.), 1988. *Chambers science and technology dictionary*.

Walsham, G., 1995. The emergence of interpretivism in IS research. *Information Systems Research*, [online] 6(4), pp.376–394. Available at: <https://www.jstor.org/stable/23010981?seq=1&cid=pdf->

Wang, J., Li, Y. and Rao, H.R., 2016. Overconfidence in phishing email detection. *Journal of Association for Information Systems*, 17(11), pp.759–783.

Wash, R. and Cooper, M.M., n.d. Who provides phishing training? Facts, stories, and people like me. In: *Conference on Human Factors in Computing Systems - Proceedings*. pp.1–12. https://doi.org/10.1145/3173574.3174066

Waziri, I., 2016. Website forgery: Understanding phishing attacks and nontechnical countermeasures. In: *Proceedings of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*. pp.445–450. https://doi.org/10.1109/CSCloud.2015.77

Weber, M., 1978. *Economy and society: An outline of interpretive sociology*. University of California Press.

Wei, D., Ning, H., Shi, F., Wan, Y., Xu, J., Yang, S. and Zhu, L., 2021. Dataflow management in the internet of things: Sensing, control, and security. *Tsinghua Science and Technology*, 26(6), pp.918–930.

Weinstein, N.D., 1980. Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), pp.806–820. https://doi.org/10.1037//0022-3514.39.5.806

Weinstein, N.D., Marcus, S.E. and Moser, R.P., 2005. Smokers' unrealistic optimism about their risk. *Tobacco control*, 14(1), pp.55–59.

Weiss, A., Michels, C., Burgmer, P., Mussweiler, T., Ockenfels, A. and Hofmann, W., 2021. Trust in everyday life. *Journal of Personality and Social Psychology*, [online] 121(1), pp.95–114. https://doi.org/10.1037/pspi0000334

Wetzel, R., 2005. Tackling phishing. [online] *Business Communications Review*. Available at: <https://web.archive.org/web/20061115041655/http://www.netforecast.com/Articles/RW-Phishing-BCR05,02.pdf> [Accessed 3 September 2021].

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*, 43(4), pp.1309–1315. https://doi.org/10.1016/j.aap.2011.01.013

Williams, C., 2007. Research methods. *Journal of Business & Economic Research,* March, 5, p.65.

Williams, E.J., Beardmore, A. and Joinson, A.N., 2017. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, pp.412–421. https://doi.org/10.1016/j.chb.2017.03.002

Williams, E.J., Hinds, J. and Joinson, A.N., 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, [online] 120, pp.1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, E.J. and Joinson, A.N., 2020. Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 6(1), pp.1–16. https://doi.org/10.1093/cybsec/tyaa001

Wilson, A.E. and Darke, P.R., 2012. The optimistic trust effect: Use of belief in a just world to cope with decision- generated threat. *Journal of Consumer Research*, 39(3), pp.615–628. https://doi.org/10.1086/664499

Woiceshyn, J. and Daellenbach, U., 2018. Evaluating inductive vs deductive research in management studies. *Qualitative Research in Organizations and Management: An International Journal*, 13(2), pp.183–195. https://doi.org/10.1108/qrom-06-2017-1538

Workman, M., 2008. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), pp.662–674. https://doi.org/10.1002/asi

Wright, R.T. and Marett, K., 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1), pp.273–303. https://doi.org/10.2753/MIS0742-1222270111

Xu, W., 2011. Learning styles and their implications in learning and teaching. *Theory and Practice in Language Studies*, 1(4). https://doi.org/10.4304/tpls.1.4.413-416

Yamagishi, T., Akutsu, S., Cho, K., Inoue, Y., Li, Y. and Matsumoto, Y., 2015. Two-component model of general trust: Predicting behavioral trust from attitudinal trust. *Social Cognition*, 33(5), pp.436–458. https://doi.org/10.1521/soco.2015.33.5.436

Yin, R.K., 2013. Validity and generalization in future case study evaluations. *Evaluation*, [online] 19(3), pp.321–332. https://doi.org/10.1177/1356389013497081

Yuen, K.S.L. and Lee, T.M.C., 2003. Could mood state affect risk-taking decisions? *Journal of Affective Disorders*, 75(1), pp.11–18. https://doi.org/10.1016/S0165-0327(02)00022-8

ZD Net, 2020. *This latest phishing scam is spreading fake invoices loaded with malware | ZDNet*. [online] Available at: <https://www.zdnet.com/article/this-latest-phishing-scam-is-spreading-fake-invoices-loaded-with-malware/> [Accessed 3 September 2021].

Zhang, H., Huang, T., Liu, S., Yin, H., Li, J., Yang, H. and Xia, Y., 2020. A learning style classification approach based on deep belief network for large-scale online education. [online] https://doi.org/10.1186/s13677-020-00165-y

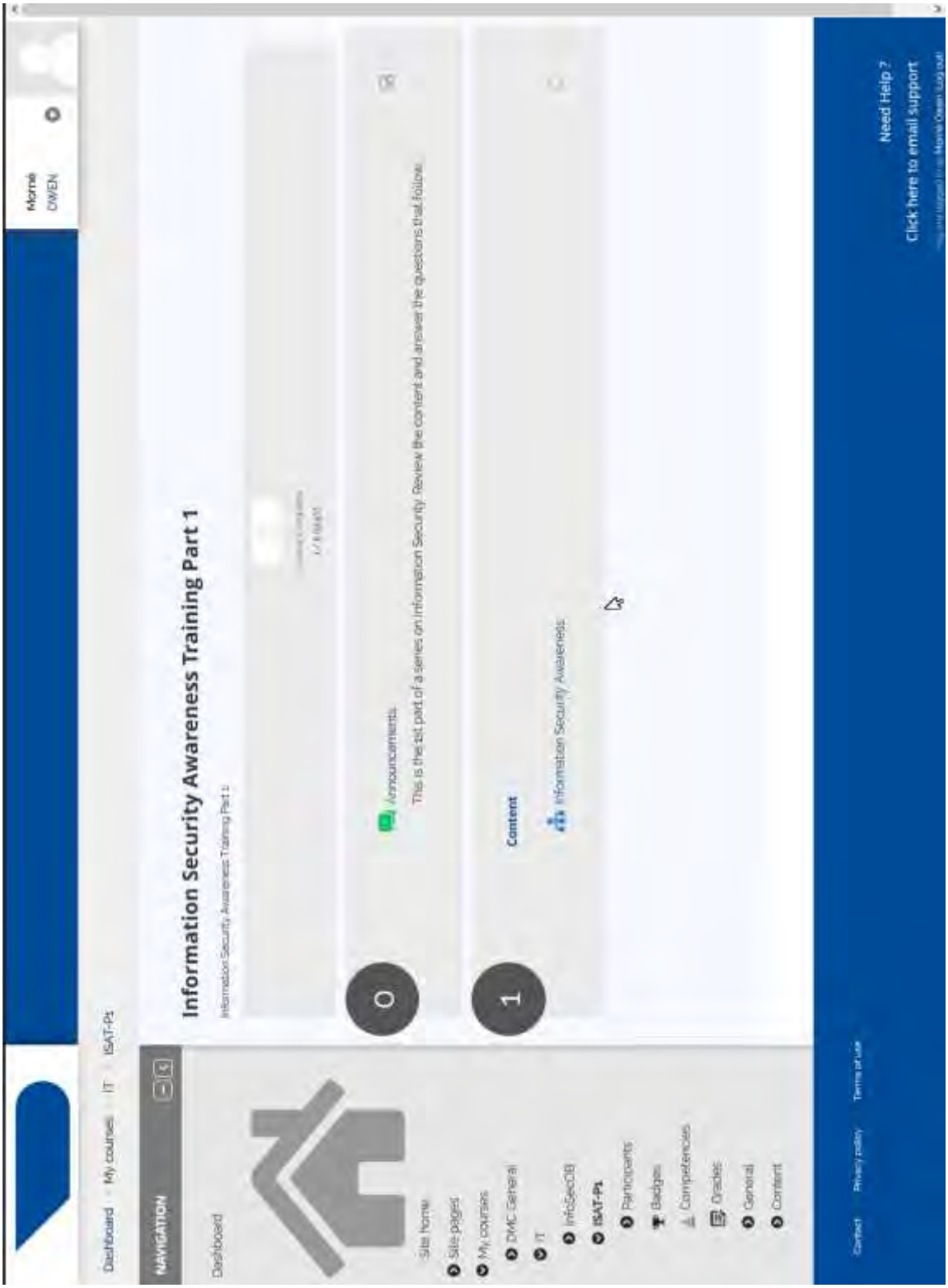
Zhao, R., John, S., Karas, S., Bussell, C., Roberts, J., Six, D., Gavett, B. and Yue, C., 2017. Design and evaluation of the highly insidious extreme phishing attacks. *Computers and Security*, 70, pp.634–647. https://doi.org/10.1016/j.cose.2017.08.008

Zhghenti, T. and Gedenidze, G., 2022. Sharing economy platforms in Georgia: Digital trust, loyalty and satisfaction.

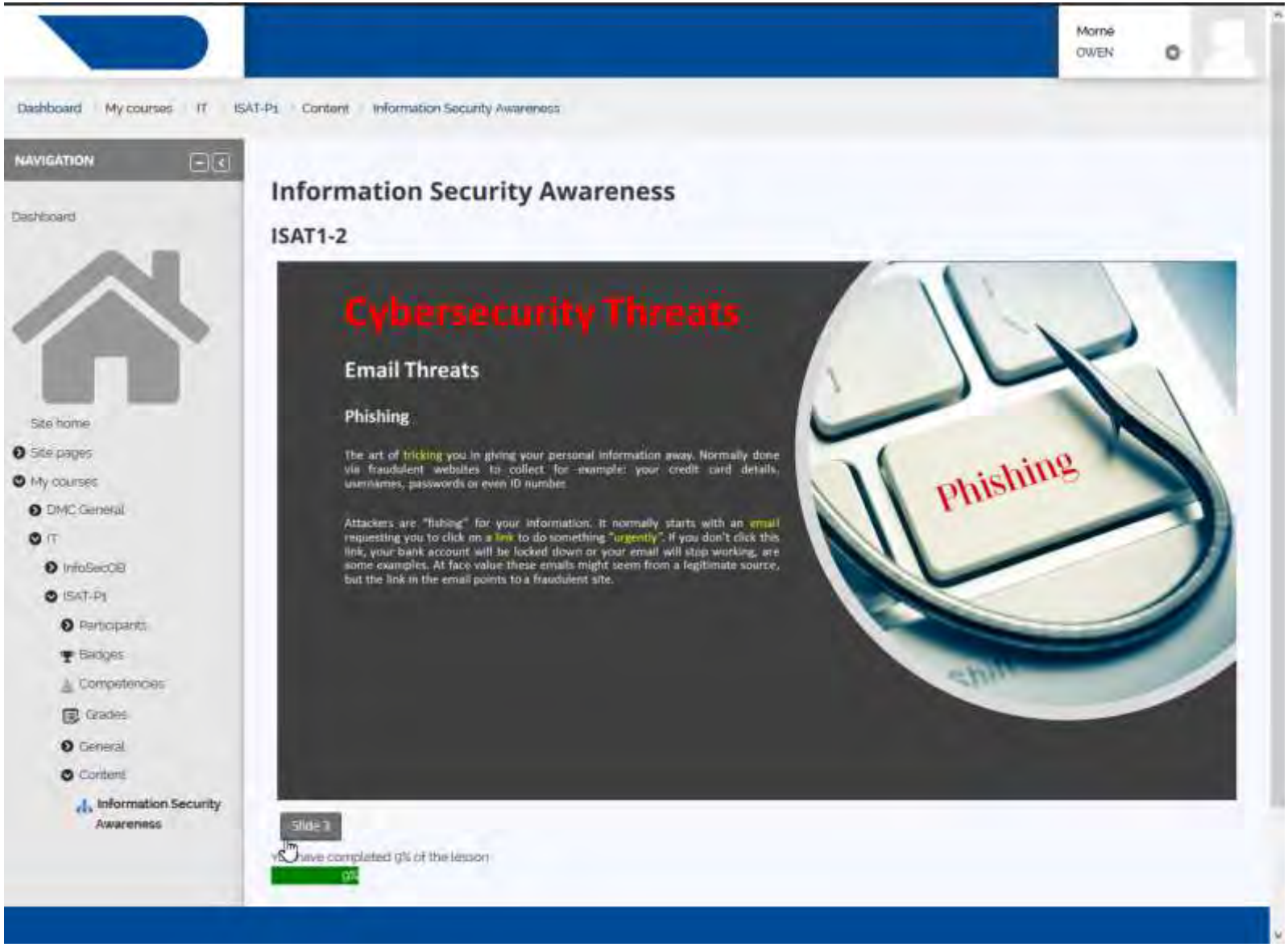
Zielinska, O.A., Tembe, R., Hong, K.W., Ge, X., Murphy-Hill, E. and Mayhorn, C.B., 2014. One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. pp.1466–1470.

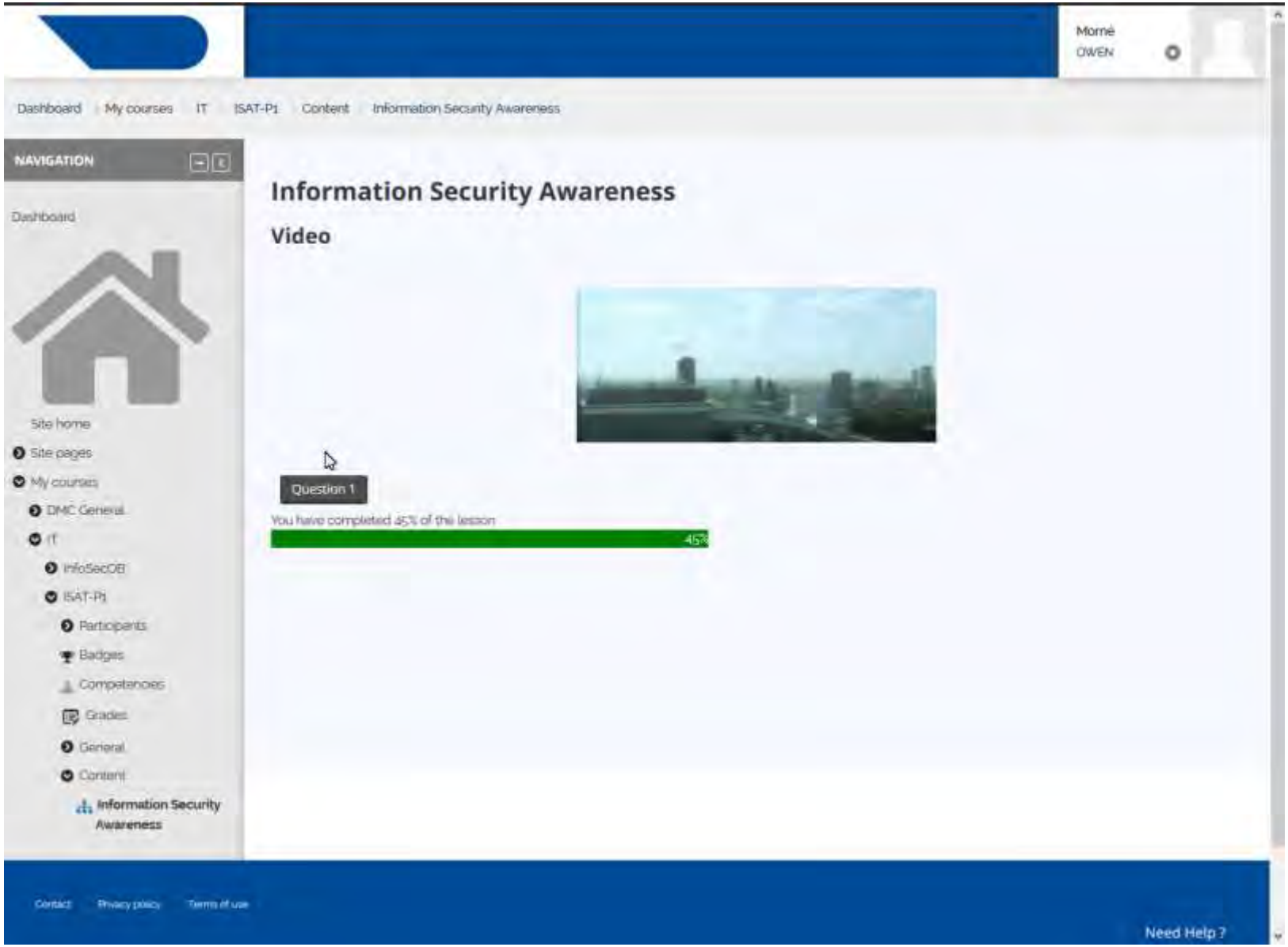
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N., 2022. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), pp.82–97. https://doi.org/10.1080/08874417.2020.1712269

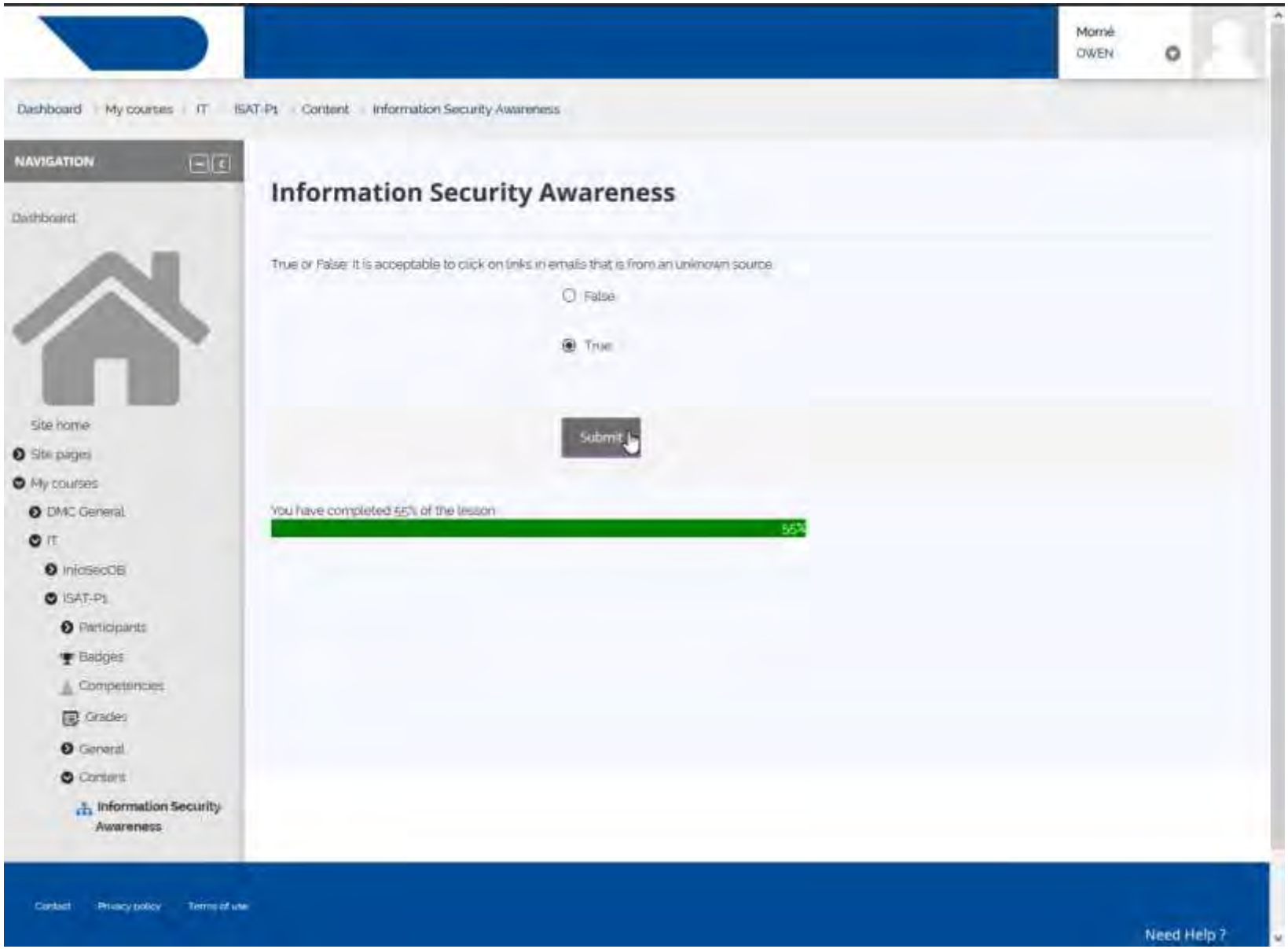
APPENDIX A: ADDITIONAL QUALITATIVE DATA

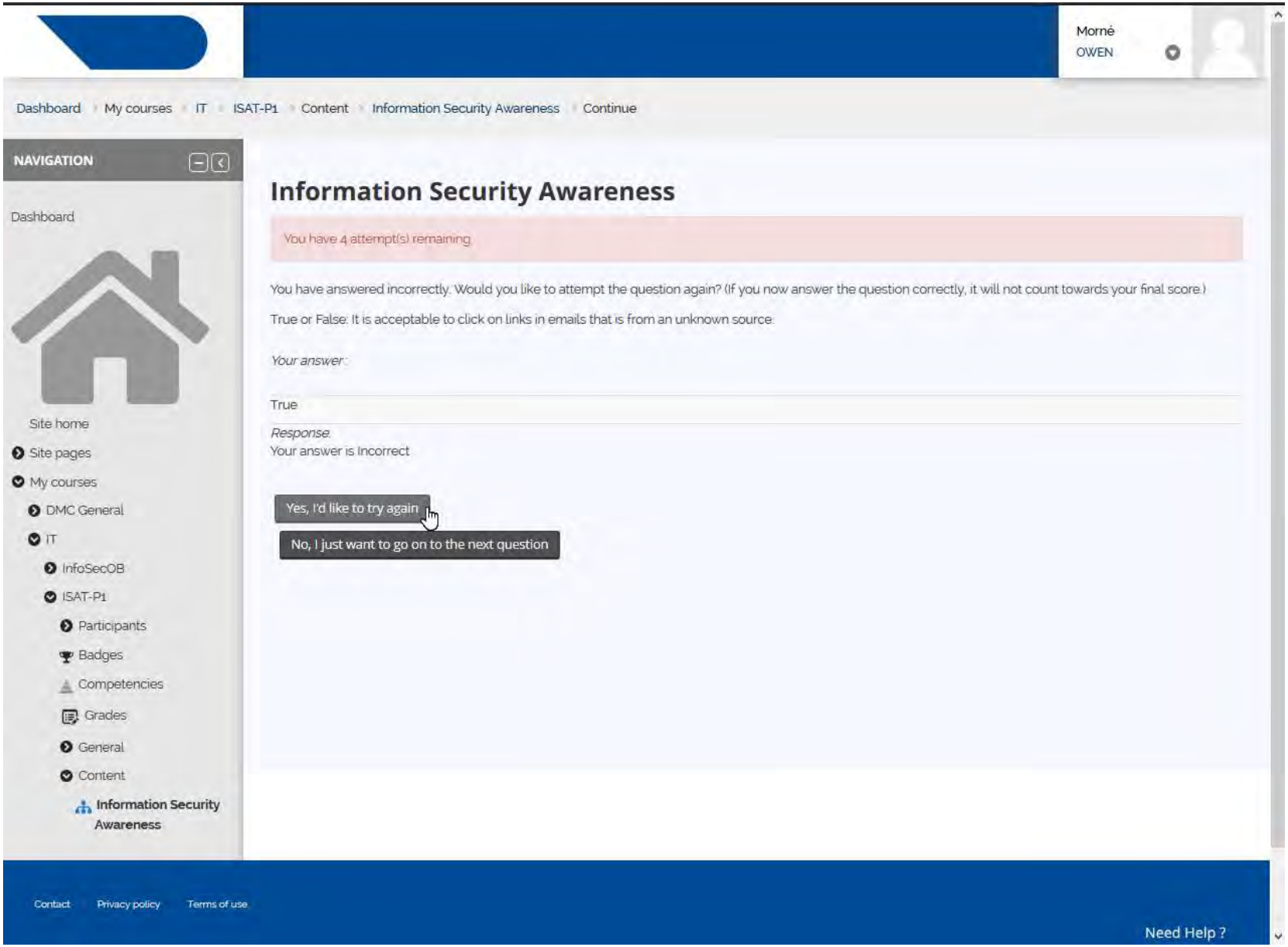


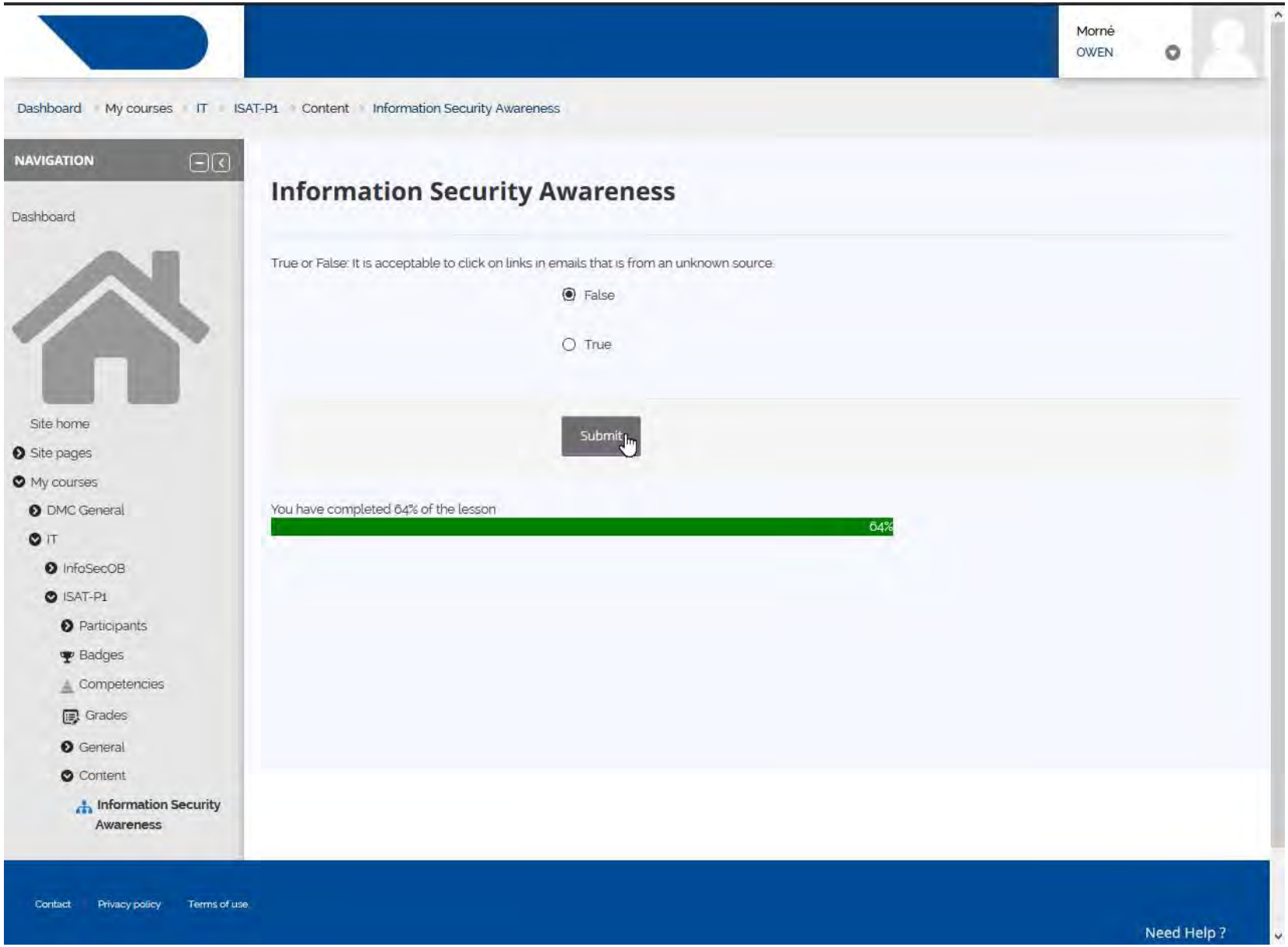

Marné
OWEN
Dashboard | My courses | IT | ISAT-P1 | Content | Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecQB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
Attempt: 1
ISAT1-1
Cybersecurity is everyone's responsibility
In a connected world, our private information and our organization's information, is vulnerable to exposure and misuse. Hackers or malicious threat actors don't care about age, gender, race, culture or beliefs. They are interested in opportunities to steal or compromise your information for their gain.
People, you and I, are defined as the weakest link in the information security chain. Our trusting nature wanting to help or contribute to the greater good in getting our jobs done, is often the stumbling block resulting in cybersecurity failures. Hackers capitalize on your willingness or curiosity to cooperate by clicking on that link in an email. One simple click can result in the download and execution of malware that can lock up your computer demanding a ransom amount to unlock it (ransomware). Certain malware silently collects data aiming to get your credentials and passwords for exploit later.
Often our actions are accidental with no intention to be harmful, but could result in serious damage to ourselves, our family, co-workers, the organization or the community.
Cyber criminals have a vested interest in both your money and your personal information.
Slide 2
You have completed 0% of the lesson

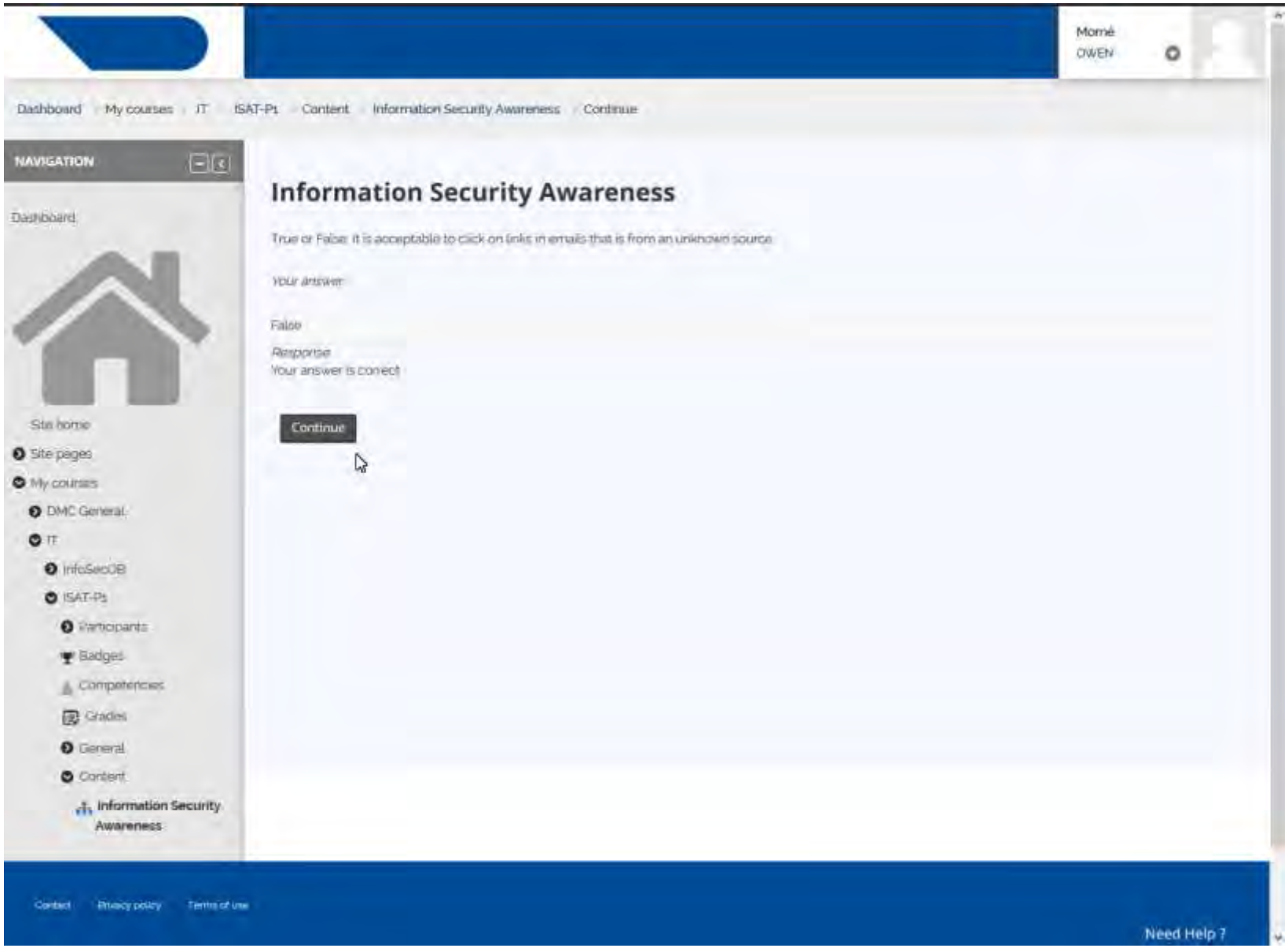

Monné
OWEN
Dashboard
My courses
IT
ISAT-P1
Content
Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
ISAT1-2
Cybersecurity Threats
Email Threats
Phishing
The art of tricking you in giving your personal information away. Normally done via fraudulent websites to collect for example: your credit card details, usernames, passwords or even ID number.
Attackers are "fishing" for your information. It normally starts with an email requesting you to click on a link to do something "urgently". If you don't click this link, your bank account will be locked down or your email will stop working, are some examples. At face value these emails might seem from a legitimate source, but the link in the email points to a fraudulent site.
Phishing
Slide 3
have completed 0% of the lesson
0%


Morné
OWEN
Dashboard
My courses
IT
ISAT-P1
Content
Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
Video
Question 1
You have completed 45% of the lesson
45%
Contact
Privacy policy
Terms of use
Need Help ?


Momé
OWEN
Dashboard
My courses
IT
ISAT-P1
Content
Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOBI
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
True or False: It is acceptable to click on links in emails that is from an unknown source
False
True
Submit
You have completed 55% of the lesson
55%
Contact
Privacy policy
Terms of use
Need Help ?


Morné
OWEN
Dashboard › My courses › IT › ISAT-P1 › Content › Information Security Awareness › Continue
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
You have 4 attempt(s) remaining.
You have answered incorrectly. Would you like to attempt the question again? (If you now answer the question correctly, it will not count towards your final score.)
True or False: It is acceptable to click on links in emails that is from an unknown source.
Your answer:
True
Response:
Your answer is Incorrect
Yes, I'd like to try again
No, I just want to go on to the next question
Contact
Privacy policy
Terms of use
Need Help ?


Morné
OWEN
Dashboard
My courses
IT
ISAT-P1
Content
Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
True or False: It is acceptable to click on links in emails that is from an unknown source.
False
True
Submit
You have completed 64% of the lesson
64%
Contact
Privacy policy
Terms of use
Need Help ?


Morné
OWEN
Dashboard My courses IT ISAT-P1 Content Information Security Awareness Continue
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
True or False: It is acceptable to click on links in emails that is from an unknown source
Your answer
False
Response
Your answer is correct
Continue
Contact
Privacy policy
Terms of use
Need Help ?

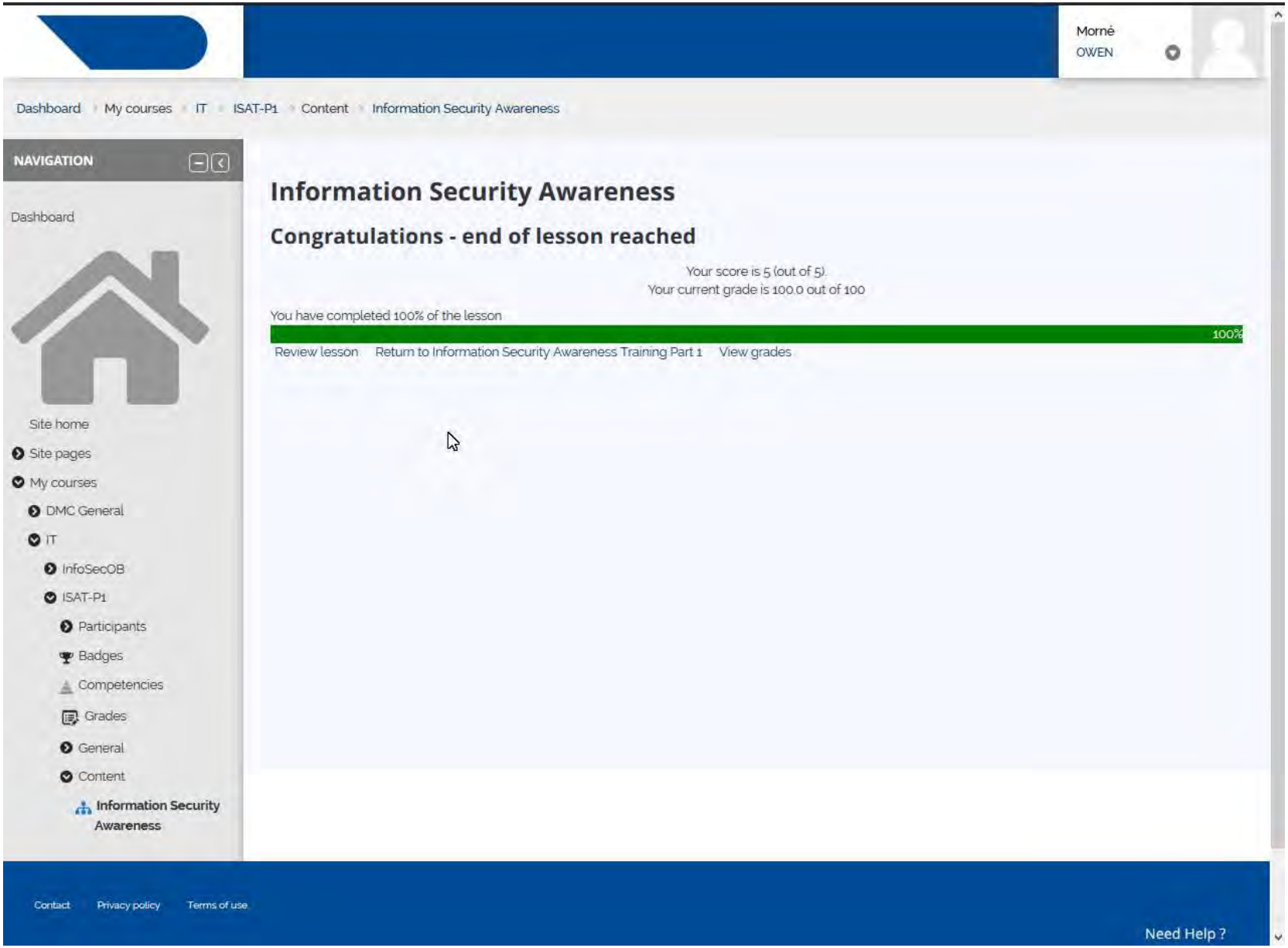

Morné
OWEN
Dashboard
My courses
IT
ISAT-P1
Content
Information Security Awareness
NAVIGATION
Dashboard
Site home
Site pages
My courses
DMC General
IT
InfoSecOB
ISAT-P1
Participants
Badges
Competencies
Grades
General
Content
Information Security Awareness
Information Security Awareness
Congratulations - end of lesson reached
Your score is 5 (out of 5).
Your current grade is 100.0 out of 100
You have completed 100% of the lesson
100%
Review lesson
Return to Information Security Awareness Training Part 1
View grades
Contact
Privacy policy
Terms of use
Need Help ?

Table A1. ISAT questions

Question	Possible answer
Training Session 1	
It is acceptable to click on links in emails that is from an unknown source.	True or **False**
Since anti-virus cannot detect all threats, there is no need to keep it updated.	True or **False**
Information security is the IT department's responsibility.	True or **False**
Training Session 2	
!@#$%^& is a secure password as it is not an easily guessable word and is a minimum of eight characters	True or **False**
What is required for a strong password?	Use the same password for different sites so that you don't forget it; **Use a combination of alphabet, numbers and special characters to create a unique password;** Use a password from the top 100 list as they are the most secure; Write your password down so that you don't forget it.
Training Session 3	
I can download any apps from any app store as long as they work on my device.	True or **False**
Using automatic locks on my cell phone makes it more secure	**True** or False
The sooner a security incident is reported the better as it could minimize the possible damage/loss	**True** or False
Printed documents containing sensitive data can be left unattended at the printer	True or **False**

APPENDIX B: INFORMED CONSENT FORM

Information Security Awareness Survey

Overview Edit questions Templates Analysis Show responses Show non-respondents

You are invited to participate in a web-based online survey. This research is being conducted by Moniek Owens a PhD student at Rhodes University. It should take approximately 10 minutes to complete.

PARTICIPATION

Your participation in this survey is voluntary. You may refuse to take part in the research or exit the survey at any time without penalty. You are free to decline to answer any question you do not wish to answer for any reason.

BENEFITS

This research will benefit the organisation and you as an individual by providing more effective ISAT (Information Security Awareness Training) protecting you from possible cyber threats which could result in compromised information security assets, loss of personal information or even loss of income.

RISKS

There are no foreseeable risks involved in participating in the study other than those encountered in daily-to-day life.

CONFIDENTIALITY

The information collected will be used purely to enhance the effectiveness of ISAT. Individual results will not be published.

CONTACT

If you have questions at any time about the study or the procedures, you may contact me via email at moniekowens@gmail.com.

APPENDIX C: ETHICAL CLEARANCE

RHODES UNIVERSITY
Where leaders learn

Department of Information Systems
Hamilton building, Prince Alfred Street, Grahamstown, 6139, South Africa
PO Box 94, Grahamstown, 6140, South Africa
t: +27 (0) 46 603 8244
f: +27 (0) 46 603 7608
e: informationsystems@ru.ac.za
www.ru.ac.za

NUMBER: CIS18-11
(for office use)

16/11/2018

Dear Morné

Re: Research Ethics Approval Feedback

Research Title: An optimism bias information security and awareness training behavioural model for a South African financial organisation.
Principal Investigator: Morné Owen

This letter confirms that the ethical application was:

Recommended for approval for ethical clearance	x
Provisionally Recommended for approval for ethical clearance	
Deemed to need modifications and to be resubmitted for ethical clearance	
Not recommended for approval for ethical clearance	
Deemed to not require ethical approval	
Recommended for approval for ethical clearance of high risk research AND applicant required to submit application to RUESC via "Submittable"	

IN THE EVENT THAT THE APPLICATION WAS PROVISIONALLY APPROVED FOR ETHICAL CLEARANCE:

The student addressed two issues. One was the storage of data from 1 year to 5 years. The second issue was exploring the concerns around potential embarrassment and the consequences / no consequences of that concern. It was felt that while a person falling for a particular Phishing attack may feel a little embarrassed for being "caught out", there would be no personal consequences as all data collected is kept confidential and will not be shared with anyone from within or outside of the organisation. Data for research publication purposes will be anonymised.

Yours sincerely

Chris Upfold, 16 November 2018

Chairperson: Department of Information Systems Ethical Standards Sub-Committee

Page 1 of 1

APPENDIX D: PYTHON CODE

Phishing Test 1

*Certain items obfuscated using an **

```
from flask import Flask
from flask import request
from flask_mail import Mail,  Message
import mysql.connector
from mysql.connector import errorcode
import datetime
from flask import render_template, flash
from wtforms import Form, TextField, TextAreaField, validators, StringField, SubmitField


app = Flask(__name__)
app.config['MAIL_SERVER']='smtp.gmail.com'
app.config['MAIL_PORT'] = 465
app.config['MAIL_USERNAME'] = 'humancapital.*****@gmail.com'
app.config['MAIL_PASSWORD'] = '*******'
app.config['MAIL_USE_TLS'] = False
app.config['MAIL_USE_SSL'] = True
mail = Mail(app)

app.config['SECRET_KEY'] = '********7d441f27d441f27567d441f2b6176a'

class ReusableForm(Form):
    username = TextField('Username:', validators=[validators.required()])
    password = TextField('Password:', validators=[validators.required(), validators.Length(min=3,
max=35)])

    @app.route('/***/<guest>', methods=['GET', 'POST'])
    def hello(guest):
        try:
            con = mysql.connector.connect(user='*******',
                                          password='********',
                                          host = '******.mysql.pythonanywhere-services.com',
                                          database = '*****$test')
        except mysql.connector.Error as err:
            if err.errno == errorcode.ER_ACCESS_DENIED_ERROR:
                print('Something is wrong with your username or password')
            elif err.errno == errorcode.ER_BAD_DB_ERROR:
                print('Database does not exist')
            else:
```

```
                print(err)

        cur = con.cursor()

        dtnow = datetime.datetime.today()
           cur.execute(f"INSERT INTO Test1 (UserEmailAddress, ClickedDT) VALUES ('{guest}',
'{dtnow}')")
        con.commit()

        form = ReusableForm(request.form)

        print(form.errors)
        if request.method == 'POST':
            username=request.form['username']
            password=request.form['password']

        if form.validate():
        # Save the comment here.
            dtnow = datetime.datetime.today()
              cur.execute(f"INSERT INTO UserLogins (UserName, ClickedDT) VALUES ('{username}',
'{dtnow}')")
            con.commit()
            flash('Thanks. You have successfully opt-out of the paydate change.')
        else:
            flash('Error: All the form fields are required. ')

        return render_template('***.html', form=form)


if __name__ == '__main__':
   app.run()
```

HTML Template

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>*** Paydate Change Opt-Out</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
  <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></scri
pt>
  <script
src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.j
s"></script>
  <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js"></s
cript>
</head>

<body>
<div class="container">
<div class="jumbotron text-center">
  <img src="http://**.pythonanywhere.com/static/xyz.jpg" class="float-left">
  <h1>*** Paydate Change Opt-Out</h1>
</div>

<form action="" method="post" role="form">

<div class="form-group">
      <label for="username">Username:</label>
<input type="text" class="form-control" id="username" name="username"
placeholder="Enter your user name.">
<br>
<label for="password">Password:</label>
<input type="password" class="form-control" id="password" name="password"
placeholder="Enter a password.">
<br>
<br>
</div>
<button type="submit" class="btn btn-success">Opt-Out</button>
<br><br>
</form>{% with messages = get_flashed_messages(with_categories=true) %}
{% if messages %}
    {% for message in messages %}
        {% if "Error" not in message[1]: %}
            <div class="alert alert-info">
```

```
            {{ message[1] }}
            </div>
        {% endif %}
    {% endfor %}
{% endif %}
{% endwith %}

</div>

</body>
</html>
```

Using Sendgrid to email

```
# using SendGrid's Python Library
# https://github.com/sendgrid/sendgrid-python
import os
from sendgrid import SendGridAPIClient
from sendgrid.helpers.mail import Mail
import openpyxl
import time
import subprocess as sp
from termcolor import colored, cprint

tmp = sp.call('cls',shell=True)
ucfix = sp.call('chcp 65001', shell=True)
ucfix = sp.call('set PYTHONIOENCODING=utf-8', shell=True)

htmlmessage="""
<html>
<head>
<title></title>
</head>
<body>
<p style="font-family:arial">Hi<br>
<br>
At the last board meeting, management was asked to do a quick survey with
all staff members regarding the December 2019 pay date. As you know,
December is normally a high volume month placing the company's capital
adequacy under pressure. The board therefore requests that the December
pay date, and any bonus payout, is delayed until 31 December 2019.
<br>
<br>
We realise that this might not be suitable to all our staff. As we
respect our staff, we want to grant you the opportunity to vote for or
against this proposal. Voting will only be available until 12h00 on
Monday, 2 September 2019. To keep the paydate as is, we need at least 50%
of our people to opt-out.
<br>
<br>
Please act ASAP as we need to provide an answer to the board.
<br>
<br>
<a href="http://*****.pythonanywhere.com/***/[]">Vote here</a>
<br>
<br>
Regards<br>
<br>
Management
<br>
```

```
 <br>
<br>
<table>
<tr>
<td>
<img title="" alt="" src="***reduced not to show
image here in this text**** ==" />
</td>
<td>
</td>
</tr>
</table>
</p>
<table class="MsoNormalTable"
style="border-collapse: collapse; width: 15cm;" border="0"
cellpadding="0" cellspacing="0" width="567">
<tbody>
    <tr style="height: 5.05pt;">
    <td colspan="4"
style="padding: 0cm; width: 100%; height: 5.05pt;" width="100%">
    <p class="MsoNormal"
style="text-align: justify; line-height: 105%;"><span
style="font-size: 7pt; line-height: 105%; font-family: &quot;Century
Gothic&quot;,sans-serif;"><o:p> </o:p></span></p>
    <p class="MsoNormal"
style="text-align: justify; line-height: 105%;"><span
style="font-size: 6pt; line-height: 105%; font-family: &quot;Century
Gothic&quot;,sans-serif; color: gray;">Information
contained in this email is confidential and is intended solely for the
use of the individual or entity to whom it is addressed or such
person's authorised representative. This e-mail legal notice is
enforceable and binding on the recipient / addressee in terms of
sections 11(1) to 11(3) of the Electronic Communications and
Transactions ("ECT") Act 25 of 2002. The following link will take you
to the </span><span style=""><a
href="http://www.*******.co.za/index.php?nav=disclaimer"><span
style="font-size: 6pt; line-height: 105%; font-family: &quot;Century
Gothic&quot;,sans-serif; color: gray;">Group's
Disclaimer and Board of Directors</span></a></span><span
style="font-size: 6pt; line-height: 105%; font-family: &quot;Century
Gothic&quot;,sans-serif; color: gray;">.
Please consider your environmental impact before printing this
email.</span><span
style="font-size: 8pt; line-height: 105%; font-family: &quot;Century
Gothic&quot;,sans-serif;"><o:p></o:p></span></p>
    </td>
    </tr>
</tbody>
```

```
</table>
<p class="MsoNormal"><span style=""><o:p> </o:p></span></p>
</body>
</html>
"""

xls = "test1-target2.xlsx"

wb = openpyxl.load_workbook(xls, data_only=True) #ignores formulae
sheet = wb.worksheets[0]
cprint(xls,"cyan")
for r in range(2, sheet.max_row+1):
    emailaddress = sheet.cell(row=r, column=1).value
    if emailaddress == None:
        #take a break
        cprint("Break time!","yellow")
        time.sleep(30)
        continue

    cprint(f"{emailaddress} - {r}","cyan")

    htmlmessage2 = htmlmessage  #reset it so that we can replace with the
next email address
    htmlmessage2 = htmlmessage2.replace('[]',emailaddress)

    message = Mail(
        from_email='Human Capital <***************@gmail.com>',
        to_emails=emailaddress,
        subject='Proposal to change monthly employee paydate',
        html_content=htmlmessage2)
    time.sleep(5)
    try:
        sg_humancapital =
SendGridAPIClient('SG.oBi9NXvNRIyXSvfBITwCoA.*********')
        response = sg_humancapital.send(message)
    except Exception as e:
        cprint(str(e),"red")
```

APPENDIX E: FINAL QUESTIONNAIRE

Question		Source	Question Type	Response Anchors
1	What is your age?	N/A	Multiple Choice	20 – 30, 31 – 49, 50+
2	What is your gender?	N/A	Multiple Choice	Male, Female, Rather not declare
3	What is your job role?	N/A	Multiple Choice	Executive, Senior Manager, Manager, Admin, Call Centre Consultant
4	How many formal computer courses have you done?	N/A	Multiple Choice	0, 1-3, >= 4
5	How many years work experience do you have with computers?	Adapted from Mittal (2015)	Multiple Choice	0-3, 4-6, 7-9, >= 10
6	Compared to other employees, what do you think are the chances that the following events will happen to you? Your work will be recognized with an award.	Adapted from 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.
7	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.	Adapted from 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.

8	Compared to other employees, what do you think are the chances that the following events will happen to you? You may have contemplated suicide.	Adapted from 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.
9	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.	Adapted from 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.
10	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.	Adapted from 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.
11	Compared to other employees, what do you think are the chances that the following events will happen to you?	Adapted from 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,

	You are likely to contract a venereal disease.			100% more, 3 times average, 5 times average.
12	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 5 years.	Adapted from 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.
13	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.	Adapted from 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.
14	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.	Adapted from 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.

15	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.	Adapted from 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.
16	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.	Adapted from 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.
17	It's risky to open an email attachment from an unknown sender.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
18	If it helps me to do my job, it doesn't matter what information I put on a website.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
19	It doesn't matter if I post things on social media that I would not normally say in public.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
20	It's risky to send sensitive work files using a public wifi network.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
21	Nothing bad can happen if I ignore poor security behaviour.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree

22	I believe my system is secure and will protect me from cyber threats.	New item	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
23	My attitude positively changed towards information security (security behaviour) over the past 2 years.	New item	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
24	My work environment is positive and provides for satisfactory work conditions.	Adapted from Mittal (2015)	Adapted from Mittal (2015)	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
25	It's acceptable to use my social media passwords on my work accounts.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
26	I am not permitted to click on a link in an email from an unknown sender.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
27	I am allowed to download any files onto my work computer if they help me do my job.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
28	I can't be fired for something I post on social media.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
29	Sensitive printouts can be disposed of in the same way as non-sensitive ones.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
30	If I see someone acting suspiciously in my workplace, it is my duty to report it.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
31	If I noticed my colleague ignoring security rules, I wouldn't take any action.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
32	If I noticed a security incident, I would report it.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree

33	I share my work passwords with my colleagues.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
34	I leave printouts that contain sensitive information on my desk when I'm not there.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
35	I don't see anything wrong with sharing content from pirated sites as everyone does so.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
36	I accept new friend requests on social media even if I have not physically met the person.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
37	I trust my computer knowledge and abilities not to fall victim to a cyber attack.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
38	I'm comfortable working with computers in a secure fashion.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
39	I trust my IT department to protect me from cyber threats.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
40	I have never been a victim of a cyber security incident.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
41	I use two-factor authentication wherever I can.	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
42	How many times in a month do you make use of internet banking using the company computers?	HAIS-Q. Adapted from Parsons et al. (2017)	Multiple Choice	0, 1 – 10 , 11 – 19, >= 20
43	What kind of security measures do you implement on your personal devices? Select all appropriate options.	Adapted from Pattinson and Anderson (2007)	Multiple Choice	a. Installed anti-virus or use a service provider b. Installed firewall or use firewall service

				c. Back up files regularly d. Change passwords regularly e. Don't use the same password for multiple accounts f. None of the above
44	Most people at my workplace are basically honest.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
45	I tend to trust the people I work with.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
46	Most of the people I work with are basically good and kind.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
47	Most of the people I work with trust others.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
48	Most of the people I work with can be trusted.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
49	I tend to see the best in the people I work with.	Adapted from Ferres and Travaglione (2003)	Multiple Choice	Strongly agree, Agree, Don't know, Disagree, Strongly disagree
50	Please provide any feedback on how you perceive or experience information security.	N/A	Input text	N/A