Understanding the factors that motivate South African home fibre users to protect their home networking devices: a protection motivation theory

Received 16 April 2024
Revised 9 July 2024
Accepted 11 July 2024

Luzuko Tekeni
Department of Information Technology, Nelson Mandela University, Gqeberha, South Africa and Information Systems Department, University of Cape Town, Cape Town, South Africa, and

Reinhardt A. Botha
Department of Information Technology, Nelson Mandela University, Gqeberha, South Africa and Noroff University of College, Oslo, Norway,

Abstract

Purpose – As home users are increasingly responsible for securing their computing devices and home networks, there is a growing need to develop interventions to assist them in protecting their home networking devices, which are vulnerable to attack. To this end, this paper aims to examine the motivating factors that drive South African fibre users to protect their home networking devices.

Design/methodology/approach – Using the protection motivation theory as the primary framework, a measurement instrument comprising 53 questionnaire items was developed to measure 13 constructs. The study collected empirical data from a sample of 392 South African home fibre users and evaluated the research model using structural equation modelling.

Findings – The evaluation showed a good fit, with 12 out of 15 predicted hypotheses being accepted for the final research model, contributing to the understanding of the factors that motivate home users to protect their home networking devices.

Originality/value – To the best of the authors' knowledge, this study is the first to model the factors that drive South African home fibre users to protect their home networking devices. Knowing these factors could help home internet service providers and security software vendors of home products to develop security interventions that could assist home fibre users to secure their home networking devices.

Keywords Home fibre users, Home networking devices, Structural equation modelling, Protection motivation theory

Paper type Research paper

Funding: This study was supported by Black Academics Advancement Programme (BAAP) (129444).

1. Introduction

The rapid growth of internet usage and security threats has made organisations and individuals more susceptible to cybercrime. Despite efforts to protect data, cybercriminals are evolving faster than security measures, rendering traditional methods ineffective (ActionFraud, 2020). As a result, organisations and individuals are increasing their spending on cybersecurity. The global cost of cybersecurity threats was projected to reach US$6tn in 2021, doubling from US$3tn in 2015 (Herjavec Group, 2020).

With 5 billion people using the internet (Statista, 2022a), it is crucial to take the security practices of home users seriously. Their actions can impact not only their own environment but also the entire cyberspace. New internet risks and attacks are emerging from trends like the Internet of Things (IoT) (Kopetz and Steiner, 2022) and Smart Home Services (Andrade *et al.*, 2020). Therefore, studying and addressing the security challenges faced by home users is essential to mitigate the growing threat of cybercrime.

By 2025, the number of users connected to IoT devices is expected to reach 75.44 billion globally, a significant increase from 42.62 billion in 2022 (Statista, 2022b). In addition, approximately 290 million individuals were expected to be using smart home devices by the end of 2022 (Statista, 2022c). This amplifies the number of home users vulnerable to online threats.

In March 2020, the declaration of COVID-19 as a global pandemic by the World Health Organisation resulted in a significant shift towards remote work. This situation heightened the existing risks and internet threats faced by home users. According to Panda Security (2020), there was a 400% increase in internet scams during this period, making COVID-19 a playground for the most significant cybersecurity threats. Email phishing attacks were the most prevalent security vulnerabilities encountered while working from home, with the financial and healthcare sectors being impacted particularly by security breaches. The healthcare industry, in particular, suffered severe consequences from cybersecurity breaches, amounting to US$10.10m (Panda Security, 2020). In 2020, worldwide government IT spending was projected to surpass US$438bn (Gartner, 2020).

A global survey of IT and IT security personnel from various countries indicated that 71% of organisations are very concerned about the risk of data breaches caused by remote workers (Ponemon Institute, 2020). The effectiveness of organisational IT security dropped from 71% to 44% owing to the COVID-19 pandemic. In addition, 73% of respondents expressed concern about the lack of adequate training on secure access to company resources while working remotely (Ponemon Institute, 2020).

The adoption of fibre-to-the-home among home users has increased significantly, with subscriptions in South Africa experiencing a surge of 5,000% between 2015 and 2019, as reported in the State of the ICT Sector report (ICASA, 2020). The number of fibre customers in the country rose from 31,843 in 2015 to 1.6 million in 2019 (ICASA, 2020).

The prevalence of multiple electronic devices such as smartphones, tablets, IoT devices, desktops and laptops among home users has expanded the potential targets for hackers and virus distributors (Li *et al.*, 2022a, 2022b). These devices are vulnerable to various threats when connected to the internet, including ransomware, information theft, fraudulent advertisements and phishing attacks (Li *et al.*, 2022a, 2022b).

Applying organisational security practices directly to home-user environments may have limitations owing to the differences in user experience and control. Home users are responsible for their own network security and often lack knowledge of the technology and its implications (Howe *et al.*, 2012; Thompson *et al.*, 2017). They do not have access to technical staff for support or attend mandated security training (White *et al.*, 2017).

Security is not solely a technological issue, since user complacency contributes to numerous breaches (Furnell *et al.*, 2008). With the increasing number of individuals using the internet at

home, it is crucial to understand the factors that motivate home users to implement security measures on their networking devices (Furnell *et al.*, 2008). Therefore, this paper investigates and identifies the factors that motivate home users to protect their home fibre networks against security threats.

2. The protection motivation theory

The present study aims to explore the constructs of the protection motivation theory (PMT) in greater detail with additional constructs from other theories. The PMT is a widely recognised theoretical framework for explaining how individuals respond to threats and engage in protective behaviours. The PMT comprises two primary appraisals: threat appraisal and coping appraisal (Rogers, 1975; 1985).

Threat appraisal refers to an individual's evaluation of the danger posed by a threat (Sommestad *et al.*, 2015). Researchers have defined threat appraisal in different ways, but two primary constructs are consistently identified: perceived vulnerability and perceived severity (Sommestad *et al.*, 2015; Thompson *et al.*, 2017). Perceived vulnerability is an individual's perception of the probability that the threat will occur, while perceived severity is the perceived consequences of the threat if it occurs.

Coping appraisal, on the other hand, focuses on an individual's ability to respond to the threat and the factors that may influence their likelihood of performing a defensive or adaptive response (Verkoeyen and Nepal, 2019). Response efficacy, self-efficacy and response cost are the three primary constructs of coping appraisal (Rogers, 1983; Sommestad *et al.*, 2015). Response efficacy refers to the belief that a defensive or adaptive response will help to avoid or minimise the threat. Self-efficacy refers to an individual's belief in their capability to perform the defensive or adaptive response. Response cost refers to the perceived costs associated with performing the defensive or adaptive response, which may act as a barrier to engaging in protective behaviours.

In summary, the PMT provides a theoretical framework for understanding how individuals respond to threats and engage in protective behaviours. The two primary appraisals, threat appraisal and coping appraisal, have several constructs that influence an individual's likelihood of engaging in protective behaviours. By understanding these constructs, researchers can develop effective interventions to promote protective behaviours and reduce risky behaviours.

3. Research model and hypotheses

This study applies the PMT to South African home fibre users and, more particularly, to the intention to protect their home networking devices. In the context of our study, we perceive a home user to be anyone who accesses the internet from their home networking devices using fibre connection. Furnell *et al.* (2008) note that security is no longer just a technological problem. Home users now play a critical part in protecting important assets, with many breaches taking advantage of user complacency. Given the exponential growth in the number of people using the internet at home, it makes sense to study the home-user environment. We will discuss our research model, as shown in Figure 1, by first elaborating on threat appraisal and coping appraisal and consequently clarifying the hypothesised relationships of our research model.

3.1 Threat appraisal

The PMT's threat appraisal dimension comprises three constructs, namely, perceived vulnerability, perceived severity and rewards (Rogers, 1975; 1985). However, this study will only consider perceived vulnerability and perceived severity, as rewards will not be included. The exclusion of rewards is not uncommon, as previous studies (Ifinedo, 2012; Tsai *et al.*, 2016; Verkijika, 2018) have also omitted this construct. It is argued that response cost and rewards can

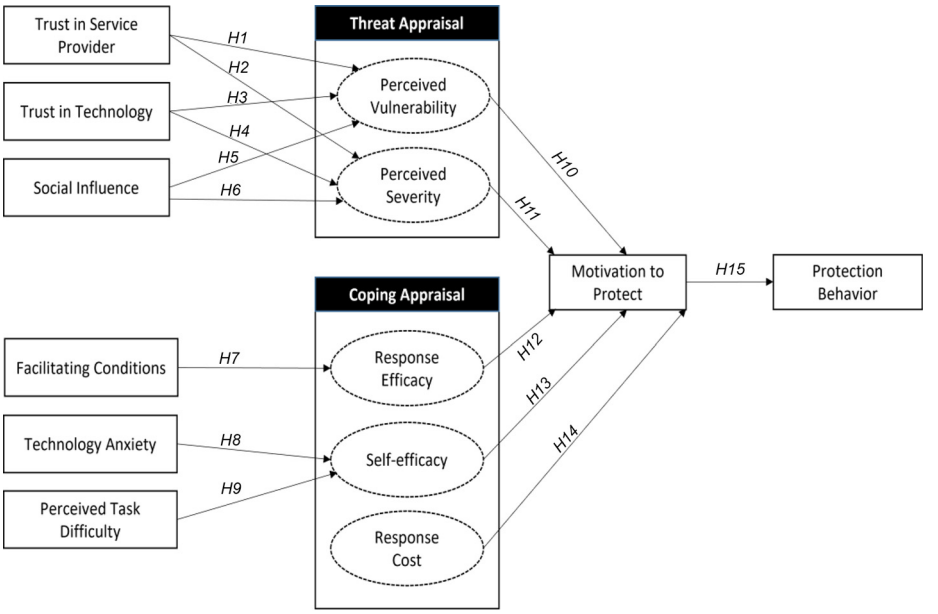

Figure 1.
Conceptual model

Source: Own work, based on PMT by Rogers (1975)

be combined into a single construct, as demonstrated in the Hanus and Vu (2016) study. Therefore, response cost was chosen over rewards to be included in the proposed model.

3.1.1 Perceived vulnerability. Perceived vulnerability, according to Ifinedo (2012), refers to an individual's self-assessment of the likelihood of a security threat occurring. It reflects an individual's perception of their susceptibility to the threat. Perceived vulnerability has been shown to have a significant impact on security behaviour in organisational settings (Ifinedo, 2012; Vance *et al.*, 2012). However, its effect in other contexts is somewhat inconsistent. For instance, Thompson *et al.* (2017) found that perceived vulnerability has a significant positive effect on security behaviours in the context of personal computing. In contrast, Woon *et al.* (2005) did not find a significant association between perceived vulnerability and the motivation to secure wireless networks. Despite the mixed findings, we postulate that perceived vulnerability will have a positive influence on home users' intention to protect their home networking devices. Hence, we propose the following hypothesis:

H10. Perceived vulnerability will influence the motivation to protect home networking devices positively.

3.1.2 Perceived severity. Perceived severity and perceived vulnerability have been widely recognised in literature to influence security practices positively. Specifically, individuals who perceive high levels of vulnerability and severity are more likely to take protective measures to secure their personal devices (Tsai *et al.*, 2016; Verkijika, 2018). For instance, Thompson *et al.* (2017) found that perceived vulnerability has a significant positive effect on security intention for mobile devices. However, Crossler (2010) discovered a negative relationship between perceived severity and determinants for backing up personal data, which contrasts with the general

postulation. These mixed results from prior studies highlight the need for further investigation into the influence of threat appraisal dimensions on security practices in other contexts, such as the security of home networking devices.

Building on the findings of Verkijika (2018) and Thompson *et al.* (2017), this study postulates a positive relationship between perceived severity and motivation to protect home networking devices. Specifically, it is predicted that individuals who perceive a high level of security breach on their home networking devices will be more inclined to protect them. Thus, the following hypothesis is proposed:

H11. Perceived severity will influence the motivation to protect home networking devices positively.

3.2 Coping appraisal

In the PMT, the coping appraisal dimension encompasses response efficacy, self-efficacy and response cost. Despite individuals perceiving a high likelihood and severity of a threatening event, they may or may not take protective measures. Therefore, the coping appraisal dimension is crucial in determining whether individuals adopt a given coping response. Previous research by Crossler and Belanger (2014) highlights the importance of the coping dimension in determining individuals' adoption of coping responses. Furthermore, Verkijika (2018) notes that the coping appraisal dimensions have been shown to have a more significant and positive relationship with information security intentions in various contexts compared to the threat appraisal dimensions.

3.2.1 Response and self-efficacy. Several studies have emphasised the crucial role played by the two efficacy dimensions (self-efficacy and response efficacy) in driving the coping dimension of the PMT (Crossler and Belanger, 2014; Ifinedo, 2012; Rogers, 1983; Thompson *et al.*, 2017; Verkijika, 2018). The literature suggests that an individual's perceived control over performing a behaviour is primarily influenced by their belief in possessing the necessary knowledge and skills, instilling confidence in their ability to execute the behaviour. In addition, response efficacy pertains to the individual's belief in the perceived benefits arising from their actions (Ifinedo, 2012; Rogers, 1983; Verkijika, 2018). Based on this understanding, this study posits the following hypotheses concerning self-efficacy and response cost:

H12. Response efficacy will influence the motivation to protect home networking devices positively.

H13. Self-efficacy will influence the motivation to protect home networking devices positively.

3.2.2 Response cost. The coping appraisal dimension of the PMT concludes with response cost, which refers to the costs associated with engaging in a protective behaviour. These costs can take various forms, such as time, money, effort and convenience. As stated by Rogers (1983), and supported by Verkijika (2018), when the cost of engaging in a protective behaviour is high, individuals are less likely to adopt said behaviour. This assertion is well established in the literature, with studies such as those by Tsai *et al.* (2016), Vance *et al.* (2012) and Verkijika (2018) showing a significant negative relationship between response cost and motivation to protect. Therefore, this study postulates the following hypothesis for response cost:

H14. Response cost will influence the motivation to protect home networking devices negatively.

3.3 Motivation to protect

The concept of motivation to protect has been suggested to be a robust predictor of human behaviour. Several studies have investigated the relationship between motivation to protect and self-reported protection behaviour, including those conducted by Li *et al.* (2019), Liang and Xue (2010) and Verkijika (2018). It is worth noting that a significant number of studies tend to focus on measuring future behavioural intentions, rather than assessing current behavioural activities. However, recent studies by Li *et al.* (2019) and Boss *et al.* (2015) have adopted a self-reporting approach, by which participants are asked questions about their current behaviour.

In line with this approach, the current study seeks to investigate the security behaviours of home users with respect to their networking devices. Participants were asked to report on their current security practices, including whether they changed the login credentials on their devices when they received them, whether they updated the firmware and whether they reviewed security features before installing them.

Previous research has demonstrated a positive relationship between avoidance motivation and self-reported avoidance behaviour in the context of personal computer usage (Liang and Xue, 2010). Based on these findings and the results of other studies, this study hypothesises that motivation to protect will have a positive relationship with protection behaviour. Specifically, when home users are motivated to protect their networking devices, and possess the necessary resources and skills, they are more likely to engage in protective behaviour. Therefore, this study hypothesises the following:

H15. Motivation to protect will influence the protection behaviour of home networking devices positively.

3.4 Trust in service provider

The impact of trust in service providers was examined in terms of perceived vulnerability and perceived severity of home networking devices. Specifically, the study hypothesised that trust in service providers would have a negative effect on both perceived vulnerability and perceived severity of home networking devices, as increased trust may lead to reduced vigilance and a false sense of security.

While prior research has shown a positive relationship between trust and various outcomes in different contexts (Al-Somali *et al.*, 2009; Astrachan *et al.*, 2014; Cheung and To, 2017; Gefen *et al.*, 2003; Thatcher *et al.*, 2010), the current study challenges this notion and argues that excessive trust in service providers may leave home networking devices vulnerable to security threats. Therefore, the study predicted a negative relationship between trust in service providers and both perceived vulnerability and perceived severity of home networking devices:

H1. Trust in service providers will have a negative relationship with perceived vulnerability towards the motivation to protect home networking devices.

H2. Trust in service providers will have a negative relationship with perceived severity towards the motivation to protect home networking devices.

We investigated the relationship between trust in technology and perceived vulnerability, and perceived severity of home networking devices, with the expectation that trust will have a negative impact on both variables. Previous research has highlighted the significance of trust in predicting the adoption of new technology (Dinev *et al.*, 2006; Gefen *et al.*, 2003).

According to the definition provided by Mayer *et al.* (1995), trust refers to the willingness of an individual to be vulnerable to the actions of another party based on the belief that the other party will act in their best interest, regardless of their ability to monitor or control that party. In the context of this study, this means that the home user trusts that their home networking devices will protect them against security threats, which may result in a decreased likelihood of the user taking steps to safeguard their devices.

Therefore, this study hypothesised that trust in technology would impact both perceived vulnerability and perceived severity of home networking devices negatively:

H3. Trust in technology will have a negative relationship with perceived vulnerability towards the motivation to protect home networking devices.

H4. Trust in technology will have a negative relationship with perceived severity towards the motivation to protect home networking devices.

3.5 Social influence

To enhance the threat appraisal of the PMT, this study introduces social influence as an independent construct, which is expected to have a direct impact on the perceived vulnerability and severity towards motivating individuals to protect their home networking devices. Ajzen (1991) defines social influence as the perceived pressure to engage or refrain from a particular behaviour based on the opinions of people who are significant to an individual, including colleagues, friends, family members and the wider community (Cheung and To, 2017). Such people can influence an individual's decision-making, positively or negatively (Kim *et al.*, 2013).

Research on Facebook privacy settings by Taneja *et al.* (2014) has found that social influence has a positive effect on individual behaviour. In the context of this study, it is predicted that social influence will have a positive impact on both perceived vulnerability and severity, motivating home users to protect their home networks. Hence, the following hypotheses are tested:

H5. Social norms will influence perceived vulnerability towards the motivation to protect home networking devices positively.

H6. Social norms will influence perceived severity towards the motivation to protect home networking devices positively.

3.6 Facilitating conditions

The construct of facilitating conditions is concerned with the belief that necessary resources are available to carry out a behaviour (Taylor and Todd, 1995). In this study, it is expected that facilitating conditions will have a direct association with response efficacy. This aligns with the findings of Taylor and Todd (1995), who discovered a positive correlation between facilitating conditions and perceived behavioural control. In addition, Ng and Rahim (2005) assert that response efficacy and self-efficacy pertain to internal factors, whereas facilitating conditions pertain to external factors such as financial resources and time. Following from this, the current study predicts a positive relationship between facilitating conditions and response efficacy. As such, the following hypothesis is examined:

H7. Facilitating conditions will influence response efficacy positively towards the motivation to protect home networking devices.

We hypothesised that a direct relationship exists between technology anxiety and self-efficacy. Previous research conducted by Thatcher and Perrewe (2002) and Compeau and Higgins (1995) indicates a negative association between technology anxiety and self-efficacy, implying that increased levels of anxiety can lead to lower levels of self-efficacy. Conversely, higher levels of self-efficacy can lead to lower levels of technology anxiety. In line with these findings, the structural model of this study predicts a negative relationship between technology anxiety and self-efficacy. Specifically, if individuals perceive that they are more capable of protecting their home networking devices, their technology anxiety levels are expected to decrease and vice versa. Therefore, the hypothesis tested is:

H8. Technology anxiety will have a significant negative influence on self-efficacy towards the motivation to protect home networking devices.

3.7 Perceived task difficulty

This study posits a negative relationship between task difficulty and self-efficacy. The idea that task difficulty in IT use may impact self-efficacy negatively is not a novel concept. Elie-Dit-Cosaque *et al.* (2011) discovered a negative correlation between perceived task difficulty and perceived behavioural control (which is similar to self-efficacy) when examining the influence of individual, contextual and social factors on perceived behavioural control of IT. This implies that if an individual believes that using or adopting a system requires skills that they do not currently possess, they will be less likely to have control over the system until they gain the necessary skills to complete the task at hand (Ahuja and Thatcher, 2005). In the context of this study, if an individual believes that they lack the skills needed to protect their home networking devices, they are less likely to have confidence in their ability to do so. Therefore, the following hypothesis is tested:

H9. Perceived task difficulty will have a significant negative influence on self-efficacy towards the motivation to protect home networking devices.

4. Methodology

This study used a quantitative research design (Ishtiaq, 2019) and a deductive approach (Gelo *et al.*, 2008) to investigate the factors influencing the protection of home networking devices among South African home fibre users. The data were collected using self-administered questionnaires from a sample of 392 participants. The questionnaire consisted of three sections. Section A provided clarity and consistent understanding of home networking devices, while Section B collected demographic-related information. Section C comprised 53 five-point Likert scale questions that evaluated the 13 constructs of the proposed research model in Figure 1. The self-administered questionnaire was designed based on the PMT with additional constructs from the theory of reasoned action (TRA) and the theory of planned behaviour in line with the proposed research model. The questionnaire underwent a pilot test with the help of six friends who were home fibre users, and feedback from the pilot test was integrated into the final research instrument.

The questionnaire was distributed via social networking sites, namely, Facebook, WhatsApp, Instagram and LinkedIn. The survey link was made available for four months and seven days, from 11 August 2021 to 17 December 2021. The data obtained from the questionnaires were analysed using structural equation modelling (SEM) in SPSS AMOS. The SEM was used to test the hypotheses comprehensively and to establish the significance

of the relationships among the observed variables and latent variables of the proposed model using confirmatory factor analysis.

5. Results

5.1 Descriptive analysis

The measurement instrument was divided into three sections: Section A, which was an invitation letter requesting consent from participants to participate in the research survey; Section B, which was designed to collect demographic information; and Section C, which contained questions about the construct measurement items. The descriptive statistics were based on Section B of the questionnaire. Table 1 provides a summary of the descriptive statistics of our study.

5.1.1 Gender. We analysed the gender distribution of the participants. Out of a total of 389 responses, 384 participants specified their gender. The results revealed that 182 individuals (46.91%) identified as male, whereas 202 individuals (52.06%) identified as

Characteristics	Item	Frequency	%
Gender	Male	182	46.8
	Female	199	51.2
	Prefer not to say	4	1
	Missing data	4	1
Age	18–25	129	35.14
	26–35	132	35.96
	36–45	50	13.62
	46–49	21	5.72
	>50	35	9.53
	Prefer not to say	22	5.99
Education	No schooling	1	0.3
	Primary school	0	0.0
	Grade 11 or lower	2	0.5
	Matric	48	12.3
	Undergraduate	192	49.5
	Postgraduate	144	37.0
	Prefer not to say	2	0.5
Fibre responsibility at home	I am responsible for my own fibre connection at home	209	53.6
	A family/household member looks after our fibre connection	46	11.8
	I get my internet connection though my landlord, therefore he/she is responsible for my fibre connection	54	13.9
	I leave it up to my internet service provider to set up and configure my fibre connection	76	19.5
	I am on an employer-sponsored connection and they require full control of my home networking device	5	1.3
General computer skills	I really struggle working with a computer	13	3
	I have basic knowledge in word processing, spreadsheet, presentation, etc.	73	16.8
	I feel comfortable working with a computer	203	46.8
	I am an expert user in working with a computer	145	33.4
Technical training exposure	have never had a technical IT training	130	31.2
	I did some short courses on technical topics	101	24.2
	I did a formal qualification at a university/registered training provider regarding the administration/configuration of computer networks	161	38.6
	I am an expert in administration/configuration of computer networks	25	6

Source: Own work

Table 1. Respondents' demographic data

female, as presented in Table 6A small proportion of the participants, comprising four individuals (1.03%), declined to state their gender, and an equal number of participants did not respond to the gender-based question. Overall, the study demonstrated a balanced representation of genders among participants.

5.1.2 Age. Of the total 389 responses, 367 participants provided their age, as presented in Table 1. The age range of participants varied from 18 to over 50 years, with no upper age limit for inclusion in the study.

The analysis revealed that the age group between 26 and 35 had the highest number of participants, accounting for 132 (35.96%) of the sample population. The second-highest age group was between 18 and 25, with 129 participants (35.14%). Participants between the ages of 36 and 45 came in third, with 50 individuals (13.62%), followed by 21 individuals (5.72%) in the age group of 46 to 50. A total of 35 participants (9.53%) were over the age of 50, while 22 responses (5.99%) did not provide age data.

Remarkably, the study findings indicated that the majority of participants interested in home network security were aged between 18 and 45 and beyond 50, with a lower participation rate observed among those between 46 and 50. This trend may reflect the increased usage and familiarity of social networks among the younger generation (ages 18 to 45) and the greater sense of responsibility for network security among older participants (over 50). Notably, the age group between 26 and 35 represented the largest number of participants, with 35.96% of the sample, followed closely by the age group between 18 and 25, comprising 35.14% of the participants.

5.1.3 Highest level of education. Of the responses received, 390 participants (99.48%) provided information about their level of education, as presented in Table 1. The educational backgrounds of the participants ranged from elementary school to postgraduate degrees, including master's and doctoral degrees. The analysis revealed that the majority of participants had received some form of education, with only one participant (0.26%) reporting no formal education. Notably, no one had stopped at primary school, while two (0.51%) participants had a Grade 11 or lower education level, and 48 (12.31%) had matriculated. Furthermore, 193 (49.49%) participants had obtained undergraduate degrees, such as higher certificates, diplomas and degrees, while 144 (36.92%) had completed an honours, master's or doctoral degree.

The findings indicated that the participants were generally well educated, with most reporting having completed some form of higher education. However, caution should be exercised when interpreting these results, as the sample size was relatively small ($n = 392$) and may not be representative of the broader population of South African home fibre users.

In light of these findings, education could be a key factor in promoting home network security awareness and encouraging users to take preventive measures to secure their networking devices. Therefore, understanding the education levels of home fibre users could inform the development and implementation of effective interventions aimed at promoting home network security.

5.1.4 Fibre responsibility at home. The current study focuses on home fibre users, specifically those who are responsible for the configuration and management of their home fibre network. The study also invited anyone else who uses fibre at home to participate. Participants were asked to identify who is responsible for their home fibre network by selecting the statement that best reflected their scenario. The responses of the participants are presented in Table 1.

The findings of the study indicate that the majority of the participants, 209 (53.59%), were responsible for their own fibre connection at home. On the other hand, 46 (11.79%) indicated that a family or household member was responsible for their fibre connection.

Furthermore, 54 (13.85%) of the participants indicated that their internet connection was provided by their landlord, making the landlord responsible for their fibre connection. In addition, 76 (19.49%) participants indicated that they relied on their internet service provider to set up and configure their fibre connection. Finally, five (1.28%) participants indicated that they were on an employer-sponsored connection, and therefore their employer required full control of their home networking devices.

These findings confirm that the study's ideal participants were well represented during data collection, as the majority of participants, 53.59%, were responsible for their own fibre connection at home. These findings provide important insights for network security developers to understand who is responsible for securing home networks and to develop appropriate interventions accordingly.

5.1.5 Technical training exposure. The assessment of participants' general computer skills is a crucial aspect of this study, as it provides insight into potential barriers to securing home networking devices. Participants were asked to self-report their level of comfort when working with computers, which is considered a vital factor in determining their ability to safeguard their home networks. Table 1 presents the findings of the participants' responses regarding their level of comfort when working with computers.

Of the valid responses collected, 13 (3.00%) participants reported struggling with computer usage, while 73 (16.82%) indicated that they had basic knowledge. In contrast, the majority of participants were found to be comfortable with computer usage, with 204 (46.77%) responses recorded. Interestingly, 145 (33.41%) participants identified themselves as experts in computer usage. The distribution of responses highlights the diverse range of computer skills among the participants, indicating that a one-size-fits-all approach may not be suitable when designing interventions aimed at promoting home network security. Further investigation into the reasons behind the behaviour of those who exhibit good computer skills but fail to protect their home networking devices would be beneficial to better understand this phenomenon.

5.2 Measurement model analysis

In this study, the measurement model was examined to assess both discriminant and convergent validity of the measurement scales, as well as to evaluate the model's fit with the collected data. Following the guidelines proposed by Hair *et al.* (2010), three tests, namely, standardised factor loadings, construct reliability and average variance extracted (AVE) were used to evaluate the convergent validity of the measurement model.

5.2.1 Convergent validity. Convergent validity, as defined by Hair *et al.*, 2010, refers to the degree to which items measuring the same construct converge, thereby accounting for the shared variance among these items. In the present study, the assessment of convergent validity was conducted through the examination of factor loadings, construct reliability and the AVE, as shown in Tables 2 and 3, respectively.

Factor loading is highly recommended by researchers (Hair *et al.*, 2010; Malhotra and Dash, 2011; Woon *et al.*, 2005). The premise is that high factor loading on the construct items suggests that the items on the latent variable have a convergence. Loadings of 0.45–0.54 are considered fair; 0.55–0.62 are good; 0.63–0.70 are very good; and above 0.71 are excellent (Comrey and Lee, 2013; Woon *et al.*, 2005). These loadings are in line with the suggested values of Hair *et al.* (2010). When the factor loadings of the constructs were examined in this study, all the items used in the measurement model loaded to their distinct constructs. The overall factor loading of the items were between 0.532 and 0.926. These are well above the values suggested.

Construct items	Factor loadings	Construct items	Factor loadings
Trust in service provider		*Motivation to protect*	
TSP1	0.764	MP1	0.875
TSP2	0.852	MP2	0.9
TSP3	0.878	MP3	0.79
TSP4	0.851	MP4	0.774
Trust in technology		*Protection behaviour*	
TT1	0.865	PB1	0.657
TT2	0.904	PB2	0.81
TT3	0.653	PB3	0.638
TT4	0.616	*Perceived severity*	
Facilitating conditions		PS1	0.769
FC1	0.738	PS2	0.901
FC2	0.826	PS3	0.815
FC3	0.669	*Perceived vulnerability*	
Technology anxiety		PV1	0.652
TA1	0.794	PV2	0.801
TA2	0.889	PV3	0.746
TA3	0.898	PV4	0.691
TA4	0.914	*Social influence*	
TA4	0.833	SI1	0.849
Perceived task difficulty		SI2	0.923
PTD1	0.903	SI3	0.801
PTD2	0.925	SI4	0.725
PTD3	0.782	*Response cost*	
PTD4	0.601	RC1	0.625
Self-Efficacy		RC2	0.713
SE1	0.685	RC3	0.757
SE3	0.704		
SE4	0.607		

Source: Own work

Table 2. Standardised factor loadings of the constructs

Construct	Reliability (cronbach's alpha)	Average extracted variance (AVE)
Trust in service provider	0.902	0.701
Trust in technology	0.873	0.593
Facilitating conditions	0.784	0.558
Technology anxiety	0.937	0.751
Perceived task difficulty	0.890	0.661
Self-efficacy	0.701	0.444
Response efficacy	0.851	0.572
Response cost	0.736	0.491
Motivation to protect	0.907	0.700
Protection behaviour	0.736	0.498
Perceived severity	0.864	0.689
Perceived vulnerability	0.808	0.525
Social influence	0.892	0.685

Source: Own work

Table 3. Cronbach's alpha and average variance extracted

In addition to factor loading, construct reliability is another statistical measure that is often used to achieve convergent validity; hence, it was considered in this study. According to Hair *et al.* (2010), construct reliability refers to how consistent the measurement model is in measuring the latent variable repeatedly and in producing the same results. Furthermore, Hair *et al.* (2010) note that reliability is inversely related to measurement error, such that high reliability is associated with lower measurement error. In this study, construct reliability was assessed by examining the Cronbach's alpha and the AVE. The results are shown in Table 3.

To achieve construct reliability, the values of Cronbach's alpha for all the constructs in the measurement model should be at 0.7 or higher (Ahmad *et al.*, 2016); however, a cut-off level of 0.6 can suffice. On the other hand, the values of an AVE should be 0.5 and above. In the case of our study, the values of Cronbach's alpha were between 0.701 and 0.937, and AVE were at 0.525 and 0.751. Only the AVE values of self-efficacy (0.444), protection behaviour (0.498) and response cost (0.491) fell short of the 0.5 cut-off level. These were considered as not being a concern in this study because all the Cronbach's alpha values met and exceeded the cut-off level.

5.2.2 Discriminant validity. Once construct reliability was established, this study proceeded to examine the distinctiveness of the measurement model constructs. Discriminant validity, as defined by Hair *et al.* (2010), refers to the degree to which a construct is truly distinct from other constructs. High discriminant validity serves as evidence that a construct is unique and captures specific phenomena of interest (Malhotra and Dash, 2011). To assess discriminant validity, Hair *et al.* (2010) recommend using the AVE estimate, which should be greater than the squared inter-construct correlation estimate. This criterion is based on the assumption that a latent construct should account for more variance in its item measure than it shares with another construct (Malhotra and Dash, 2011).

Table 4 presents the correlations between the constructs of the measurement model. The AVE values were found to be greater than the maximum shared variance, providing evidence that the constructs were indeed distinct from each other. Therefore, the study achieved discriminant validity. The results of both the convergent and discriminant validity analyses support the significance of the measurement model.

Constructs	PTD	TSP	TT	SI	FC	TA	PV	PS	RE	SE	MP	PB	RC
PTD	0.813												
TSP	0.017	0.837											
TT	−0.045	0.622	0.770										
SI	0.044	0.356	0.329	0.828									
FC	−0.489	0.290	0.395	0.434	0.747								
TA	0.320	−0.167	−0.084	−0.096	−0.199	0.867							
PV	−0.083	0.047	0.127	0.173	0.153	−0.201	0.725						
PS	0.057	0.126	0.153	0.253	0.102	−0.190	0.609	0.830					
RE	0.081	0.339	0.322	0.272	0.142	−0.114	0.385	0.478	0.756				
SE	−0.281	0.366	0.331	0.318	0.566	−0.388	0.389	0.394	0.482	0.667			
MP	0.030	0.309	0.337	0.352	0.328	−0.295	0.434	0.517	0.473	0.617	0.836		
PB	−0.264	0.377	0.282	0.475	0.657	−0.220	0.207	0.182	0.114	0.458	0.391	0.706	
RC	0.345	−0.071	−0.165	−0.169	−0.324	0.467	−0.197	−0.115	−0.155	−0.220	−0.264	−0.222	0.700

Source: Own work

Table 4. Correlation analysis of the constructs

5.3 Structural model analysis

Following the validation of the measurement model, the present study proceeded to test and validate the overall fit of the structural model, using a distinct set of fit indices, as shown in Table 5.

The structural model's chi square was 2480.092 with a degree of freedom of 1,040 and a probability level of ($p = 0.000$). Hair *et al.* (2010) suggest that, to assess the goodness of fit of the structural model, at least one absolute fit index and one incremental fit index must be at an acceptable level in addition to the X^2.

5.3.1 Absolute fit index. The structural model was measured and examined by using the RMSEA index, which is one of the most commonly used measures to counteract the tendency of the chi-squared goodness-of-fit test to reject models with a large sample or large RMSEA (Hair *et al.*, 2010). In Table 5, the RMSEA index value for this study was 0.06, which is below the cut-off value of 0.08 (Hair *et al.*, 2010) indicating that the structural model fit the data well.

The normed X^2 was another absolute fit index examined. Hair *et al.* (2010) expressed the normed chi-squared as the chi-squared value divided by the degrees of freedom (X^2/df). In addition, Hair *et al.* (2010) point out that a normed chi-squared less than 2.0 is considered a very good fit, while values ranging from 2.0 to 5.0 are acceptable. Thus, the normed X^2 value of 2.3 for this study indicated an acceptable structural model fit.

5.3.2 Incremental fit index. Incremental fit indices assess how well the estimated model fits relative to some alternative baseline model (null model), assuming that all the variables are uncorrelated (Hair *et al.*, 2010). Incremental fit indices are also referred to as comparative fit indices or relative fit indices (Hooper *et al.*, 2008).

One of the most widely used incremental fit indices is the comparative fit index (CFI). The CFI value > 0.90 is regarded a good fit, according to Hair *et al.* (2010). The CFI had a value of 0.879 in this study, which was just below the suggested level (Table 5). The fit index that was below the threshold, on the other hand, was less than 0.03 short of 0.9. The structural model requires one absolute and one incremental fit index to be a successful fit. Two absolute fit indices are within the permitted ranges, and one incremental fit index is 0.879, which is acceptable given that the measurement model satisfied all of the fit indices required. As a result, the study's proposed structural model was thought to be acceptable.

5.3.3 Assessing the structural relationships. The structural model validity assessment was insufficient to confirm the structural relationships between constructs, so individual parameter estimates were taken. These estimates were used to determine whether the parameters were statistically significant. A significant parameter confirms a relationship between two constructs and confirms the validity of a hypothesis. When a parameter is not

Table 5. Structural model fit summary of the proposed model

Category	Index	Suggested levels	Structural model values	Level met? Chi-square X^2
Degree of freedom	n/a	2,480.092	n/a	
	df	n/a	1,040	n/a
Absolute fit	RMSEA	<0.08	0.06	Yes
	RMR	<0.05	0.123	No
	Normed X^2	1.9	2.3	Yes
Incremental Fit	CFI	>0.90	0.879	Marginal

Source: Adapted from Hair *et al.* (2010)

significant, the hypothesis is not accepted and the relationship between constructs is not confirmed (Hair *et al.*, 2010). SEM results in Table 6 (standardised parameter estimates) were assessed using coefficient β values and p-values.

Hair *et al.* (2010) suggest that a significant parameter estimate requires that the t-values must be greater than 1.96 and the p-value $<= 0.05$. In addition, Hair *et al.* (2010) emphasise that a significant parameter estimate value must be >0 for positive relationships and <0 for negative relationships, while the p-value must be <0.01 in both instances. Therefore, in this study, a marginal level of significance for a hypothesis to be accepted or rejected was set at p-value is <0.01 and t-values > 1.96 and p-value < 0.05 when t-values > 1.64, similar to the study of Taneja *et al.* (2014).

6. Discussion and implications

This study investigated the factors that motivate South African home fibre users to protect their home networking devices by formulating 15 hypotheses to test the proposed model. Of the 15 hypotheses, 12 were confirmed.

The findings of our study did not reveal a significant relationship between trust in the service provider and perceived vulnerability (*H1*) or severity (*H2*). Following a review of the literature, this study found no prior studies that evaluated the relationship of trust in service provider to the two PMT constructs of the threat appraisal dimension. However, a study by Touray *et al.* (2015), when determining the key trust antecedents that influence internet users' trust level towards internet service providers revealed that trust in these providers depends more on the desire to protect users than upholding acceptable standards (integrity). Furthermore, their study also supported the notion that ISPs are profit driven and that poor communication is another reason for the users not to trust in them. Therefore, in our study, a number of factors could have influenced the insignificant relationship between the constructs.

First, when asked about their exposure to technical training, 38.6% (161) of the participants said they had completed a formal qualification at a university or at a registered training provider. This could have provided them with the knowledge and skills needed to identify security threats independently, assess their level of vulnerability and determine the potential

Table 6. Results of the structural model evaluation

Hypothesis	Path	Estimate (β)	S.E.	t-value	p-value
H1	TSP → PV	−0.101	0.079	−1.278	0.201
H2	TSP → PS	−0.023	0.082	−0.281	0.779
H3	TT → PV	0.126	0.07	1.81	0.07
H4	TT → PS	0.093	0.072	1.299	0.194
H5	SI → PV	0.14	0.05	2.823	0.005
H6	SI → PS	0.209	0.052	4.022	<0.001
H7	FC → RE	0.101	0.034	2.942	0.003
H8	TA → SE	−0.25	0.048	−5.201	<0.001
H9	PTD → SE	−0.091	0.038	−2.404	0.016
H10	PV → MP	0.121	0.051	2.36	0.018
H11	PS → MP	0.269	0.046	5.812	<0.001
H12	RE → MP	0.306	0.08	3.832	<0.001
H13	SE → MP	0.474	0.073	6.531	<0.001
H14	RC → MP	−0.13	0.056	−2.333	0.02
H15	MP → PB	0.437	0.077	5.653	<0.001

Source: Own work

damage that comes with the threat (Bada and Nurse, 2019). This would then have equipped them to administer and control the threat without the need to rely on the service provider.

Second, about 53.6% (209) of the participants, when asked who is responsible for their fibre connection, said that they are in charge of their home networking devices. When responding to the question relating to the two constructs of the threat appraisal dimension of the PMT with regard to trust in the service provider, the fibre responsibility question may have introduced bias or a different interpretation. For instance, if a participant says they are in charge of their home networking devices, they will not pay attention to the questions about service provider trust, since they feel in control of the security of their home networking devices since it is under their control; not under their service provider.

We investigated the relationship between trust in technology and the perceived vulnerability (*H3*) and severity (*H4*) of home networking devices, hypothesising that trust would impact both variables negatively. Previous research by Dinev *et al.* (2006) and Gefen *et al.* (2003), has highlighted the significance of trust in predicting the adoption of new technology. A negative relationship of trust in technology by home users was predicted and partially confirmed (*H3*), suggesting that home users have confidence in the security of their home networking devices. As a result, security awareness interventions tailored for home users should recommend the implementation of the California default password law (Lee, 2023) in the case of passwords. The law states that all passwords must be unique or prompt for a password change before a home user has access to any home networking device. In addition, these awareness interventions should demonstrate scenarios of attacks to discourage home users from trusting the technology in place. This could be done through videos and, in the case of children, educational games about cybersecurity attacks could be created, similar to those discussed in the studies of Hwang and Helser (2022) and Jin *et al.* (2018).

We confirmed a positive relationship between social influence with both perceived vulnerability and severity (*H5*) and (*H6*), in line with Taneja *et al.* (2014) when researching Facebook privacy settings that social influence affects an individual behaviour positively. This relationship implies that home users trust the advice they receive from persons who are important to them. Friends, family, colleagues and community members have all been identified as having social influence in our study. The results suggest that security awareness interventions for home users should focus on these people to spread security awareness concerns to home users. For instance, community radios could be used regularly to highlight concerns about the security of home networking devices. In addition, since home security threats affect everyone in the home setting, the message can be conveyed through local churches and schools. On the other hand, because trust in the service provider could not be confirmed in this study (*H1*), home users appeared not to put their trust in the service provider that sells them these home networking devices such as routers. This suggests that security awareness interventions must not use service providers as a channel for delivering security awareness issues to home users, but rather to use the community. In other words, while the primary focus is on community channels, the service provider should be kept informed. This suggestion falls in line with the Nicholson *et al.* (2021) initiative that recruited, trained and supported older adults should become community cybersecurity educators (CyberGuardians), tasked with promoting cybersecurity best practice within their communities to prevent older adults falling victim to opportunistic cyberattacks.

In our study, facilitating conditions were defined as a home user's beliefs about the availability of resources to help them protect their home networking devices. This was also the finding of Taylor and Todd (1995), who discovered a positive relationship between facilitating conditions and perceived behavioural (self-efficacy and response efficacy) control. We also confirmed a positive relationship between facilitating conditions and

response efficacy (*H7*); however, a negative relationship for response cost (*H14*), implying that a home user will not be encouraged to take security precautions for their home networking devices if the resources to protect those devices are expensive. In many studies (Li *et al.*, 2022a, 2022b; Shaikh and Siponen, 2023; Venard, 2021), response cost supports a negative effect on individuals' behaviours with regard to taking security measures, as is the case in our study.

Considering the symbiotic relationship between *H7* and *H14*, security awareness programme interventions must point home users to resources that they can use to protect their home networking devices when developing awareness interventions (Darem *et al.*, 2022). These could include information such as where to buy cheap antivirus software for a home networking device or where to download open-source firmware updates, although open-source material may be difficult for home users owing to the lack of available assistance. Such warnings should be included in the programme as well.

Home users are not always comfortable working with their home networking devices because they may lack the skills or abilities to protect their home networking devices. As a result, a negative relationship between technology anxiety (*H8*) and perceived task difficulty (*H9*); and self-efficacy was hypothesised and confirmed. The hypotheses confirm that home users feel nervous, uncomfortable and threatened when dealing with their home networking devices (*H8*). Furthermore, home users perceived that protecting home networking devices was difficult and required more skills and abilities than they currently possessed (*H9*). Similar studies in the context of computer use by Thatcher and Perrewe (2002) and Compeau and Higgins (1995) found a negative relationship between technology anxiety and self-efficacy, implying that increased levels of anxiety can lead to lower levels of self-efficacy.

Therefore, security awareness programme creators should think about hosting free trainings via social influencers like schools, churches and community libraries using videos, demos and manuals specifically designed for home users. In doing so, home users will become better at and more comfortable working with computers.

The fact that someone must pay for trainings of this type is, of course, an issue when trying to organise them. So, in these situations, home networking device service providers could be asked to sponsor these trainings. Making these videos and training sessions as simple to follow as possible should also be considered. Perhaps local communities need first to instruct home users on how to operate computers. Furthermore, the content to be delivered should cover multiple platforms of home networking devices, so that home users can work with any home network device. As a result, technology anxiety will be reduced because home users will be able to handle the task of protecting their home networking devices.

7. Limitations

Although the study used a rigorous quantitative research process to generate reliable empirical results that can be applied to the social inquiry being examined, some potential limitations were identified. Therefore, it is essential to exercise caution when interpreting and applying the findings. The study focused on examining the factors that impact the intentions of South African home users to safeguard their home networking devices.

The primary limitation of this study may lie in the data collection process. The virtual snowball method (Baltar and Brunet, 2012) via social network services was employed to collect data. However, this approach may exclude individuals who do not use social network services. In addition, the distribution of the survey was restricted to people within the social networks of participants, which may have resulted in the exclusion of significant groups of home fibre users. To overcome this limitation, we also used the Facebook advertising paid version, which led to a wider home fibre user audience in South Africa. Furthermore,

Creswell (2002) cautions that a small sample size can significantly impact the statistical power and quality of results. In this study, 392 home users of fibre in South Africa responded to the survey. This number was deemed adequate for statistical analysis using SEM, as guided by Krejcie and Morgan (1970). However, a larger sample size could have produced more precise results and improved the generalisability of the research findings.

Finally, the sample data showed bias towards participants with higher levels of education, as most reported holding a degree. This may or may not accurately reflect the education levels of South African home fibre users.

8. Future research

This study is the first attempt to identify the factors that influence South African home users' intentions to protect their home networking devices. However, it is necessary to conduct further investigations to determine how these factors may change in response to changes in technology and home-user habits. This study only examined one point in time. The proposed PMT-based model can also be used to explore the differences between computer users and non-users at work and their subsequent home habits. Additional data collection could help to clarify behaviour patterns in other areas, such as age, experience levels and the length of time a person has owned a home computer. A more comprehensive understanding of the various home user groups and their relationship to the security of their home networking devices can further expand knowledge of the entire population of internet users. Furthermore, this study used a quantitative research approach to examine social phenomena and factors that impact the intentions of home users. While the SEM method predicted the factors, conducting interviews may provide more information about home users' behaviours and motivations, and improve the understanding of the two appraisals and the behavioural intention of PMT. Using hybrid techniques, such as mixed methods, may be beneficial in better understanding the two appraisals of PMT and the behavioural intention, as participants may relate to interviews more than to a complex statistical analysis. Finally, since this study was limited to South Africa, it would be valuable to conduct similar research in other African nations, or even in more developed countries, to evaluate how well the factors that influence home users' intentions to protect their home networking devices can be generalised to the African context and beyond.

9. Conclusion

As the threat of security breaches and cyberattacks persists, protecting the home user environment has become increasingly important. This research highlights the significance of ensuring the security of all internet-connected computers for both organisations and home users, since weak connections can impact other internet users. While service providers and security software vendors have developed various security solutions, promoting these solutions to home users remains a crucial challenge.

The study has identified several factors that influence the motivation of home users positively to protect their home networking devices. The findings indicate that the threat appraisal and coping appraisal elements of the PMT act through the motivation to protect construct to promote protection behaviour. This contribution can assist home internet service providers and security software vendors in developing strategies to encourage large groups of home users to adopt new security behaviours, making them a stronger link in security.

Overall, this research showcases the utility of the PMT in explaining the driving factors behind home users' protection of their home networks. As further research is required to examine changes in technology and home-user habits, additional investigation can clarify

patterns of behaviour in different areas, such as differences based on age, experience levels and length of computer ownership. Moreover, conducting similar research in other nations can help to assess the generalisability of the factors that influence home users' intentions to protect their home networking devices.

References

ActionFraud (2020), "COVID-19 related scams – news and resources", available at: www.actionfraud.police.uk/covid19

Ahmad, S., Zulkurnain, N.N.A. and Khairushalimi, F.I. (2016), "Assessing the validity and reliability of a measurement model in structural equation modeling (SEM)", *British Journal of Mathematics and Computer Science*, Vol. 15 No. 3, pp. 1-8.

Ahuja, M.K. and Thatcher, J.B. (2005), "Moving beyond intentions and toward the theory of trying: effects of work environment and gender on post-adoption information technology use", *MIS Quarterly*, Vol. 29 No. 3, pp. 427-459.

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

Al-Somali, S.A., Gholami, R. and Clegg, B. (2009), "An investigation into the acceptance of online banking in Saudi Arabia", *Technovation*, Vol. 29 No. 2, pp. 130-141.

Andrade, R.O., Ortiz-Garces, I. and Cazares, M. (2020), "Cybersecurity attacks on smart home during covid-19 pandemic", *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, *IEEE*, pp. 398-404.

Astrachan, C.B., Patel, V.K. and Wanzenried, G. (2014), "A comparative study of CB-SEM and PLS-SEM for theory development in family firm research", *Journal of Family Business Strategy*, Vol. 5 No. 1, pp. 116-128.

Bada, M. and Nurse, J.R. (2019), "Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMES)", *Information and Computer Security*, Vol. 27 No. 3, pp. 393-410.

Baltar, F. and Brunet, I. (2012), "Social research 2.0: virtual snowball sampling method using facebook", *Internet Research*, Vol. 22 No. 1, pp. 57-74.

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*, Vol. 39 No. 4, pp. 837-864.

Cheung, M.F. and To, V.M. (2017), "The influence of the propensity to trust on mobile users' attitudes toward in-app advertisements: an extension of the theory of planned behavior", *Computers in Human Behavior*, Vol. 76, pp. 102-111.

Compeau, D. and Higgins, C.A. (1995), "Computer self-efficacy: development of a measure and initial test", *MIS Quarterly*, Vol. 19 No. 2, pp. 189-211.

Comrey, A.L. and Lee, H.B. (2013), *A First Course in Factor Analysis*, 2nd ed., Psychology Press, New York, NY.

Creswell, J.V. (2002), "Educational research: planning, conducting, and evaluating quantitative and qualitative research", *The Journal of Educational Issues of Language Minority Students*, Vol. 15, pp. 810-881.

Crossler, R.E. (2010), "Protection motivation theory: understanding determinants to backing up personal data", *2010 43rd HI International Conference on System Sciences*, *IEEE*, pp. 1-10.

Crossler, R. and Belanger, F. (2014), "An extended perspective on individual security behaviors: protection motivation theory and a unified security practices (USP) instrument", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 45 No. 4, pp. 51-71.

Darem, A., Alhashmi, A.A. and Jemal, H. (2022), "Cybersecurity threats and countermeasures of the smart home ecosystem", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 22 No. 3, p. 303.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006), "Privacy calculus model in e-commerce-a study of Italy and the United States", *European Journal of Information Systems*, Vol. 15 No. 4, pp. 389-402.

Elie-Dit-Cosaque, C., Pallud, J. and Kalika, M. (2011), "The influence of individual, contextual, and social factors on perceived behavioral control of information technology: a field theory approach", *Journal of Management Information Systems*, Vol. 28 No. 3, pp. 201-234.

Furnell, S.M., Tsaganidi, V. and Phippen, A. (2008), "Security beliefs and barriers for novice internet users", *Computers and Security*, Vol. 27 Nos 7/8, pp. 235-240.

Gartner (2020), "Gartner forecasts global government IT spending to decline 0.6% in 2020", available at: www.gartner.com/en/newsroom/press-releases/2020-08-05-gartner-forecasts-global-government-it-spending-to-de

Gefen, D., Karahanna, E. and Straub, D.V. (2003), "Inexperience and experience with online stores: the importance of TAM and trust", *IEEE Transactions on Engineering Management*, Vol. 50 No. 3, pp. 307-321.

Gelo, O., Braakmann, D. and Benetka, G. (2008), "Quantitative and qualitative research: beyond the debate", *Integrative Psychological and Behavioral Science*, Vol. 42 No. 3, pp. 266-290.

Hair, J.F., Black, V., Babin, B. and Anderson, R. (2010), *Multivariate Data Analysis: A Global Perspective 7th ed*, Pearson Education.

Hanus, B. and Vu, Y.A. (2016), "Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective", *Information Systems Management*, Vol. 33 No. 1, pp. 2-16.

Herjavec Group (2020), "The 2020 official annual cybercrime report", available at: https://tinyurl.com/y56trmgv

Hooper, D., Coughlan, J. and Mullen, M. (2008), "Evaluating model fit: a synthesis of the structural equation modelling literature", *7th European Conference on research methodology for business and management studies*, Vol. 2008, pp. 195-200.

Howe, A.E., Ray, I., Roberts, M., Urbanska, M. and Byrne, Z. (2012), "The psychology of security for the home computer user", *2012 IEEE Symposium on Security and Privacy*, *IEEE*, pp. 209-223.

Hwang, M.I. and Helser, S. (2022), "Cybersecurity educational games: a theoretical framework", *Information and Computer Security*, Vol. 30 No. 2, pp. 225-242.

ICASA (2020), "State of the ICT sector in South Africa – 2020 report", available at: www.icasa.org.za/legislation-and-regulations/state-of-the-ict-sector-in-south-africa-2020-report

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31 No. 1, pp. 83-95.

Ishtiaq, M. (2019), "Book review", in Creswell, J.W. (Ed.), *Research Design: qualitative, Quantitative and Mixed Methods Approaches*, Sage, Thousand Oaks, CA, English Language Teaching, Vol. 12 No. 5, p. 40.

Jin, G., Tu, M., Kim, T.H., Heffron, J. and White, J. (2018), "Evaluation of game-based learning in cybersecurity education for high school students", *Journal of Education and Learning (EduLearn)*, Vol. 12 No. 1, pp. 150-158.

Kim, E., Ham, S., Yang, I.S. and Choi, J.G. (2013), "The roles of attitude, subjective norm, and perceived behavioral control in the formation of consumers' behavioral intentions to read menu labels in the restaurant industry", *International Journal of Hospitality Management*, Vol. 35, pp. 203-213.

Kopetz, H. and Steiner, V. (2022), *Internet of Things. In: Real-Time Systems: Design Principles for Distribute Embedded Applications*, Springer, Cham, pp. 325-341.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement*, Vol. 30 No. 3, pp. 607-610.

Lee, B. (2023), "What is the California default password law?", available at: https://specopssoft.com/blog/california-default-password-law/

Liang, H. and Xue, Y.L. (2010), "Understanding security behaviors in personal computer usage: a threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7, p. 1.

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*, Vol. 45, pp. 13-24.

Li, Y., Xin, T. and Siponen, M. (2022a), "Citizens' cybersecurity behavior: some major challenges", *IEEE Security and Privacy*, Vol. 20 No. 1.

Li, L., Xu, L. and He, W. (2022b), "The effects of antecedents and mediating factors on cybersecurity protection behavior", *Computers in Human Behavior Reports*, Vol. 5, p. 100165.

Malhotra, N.K. and Dash, S. (2011), *Marketing Research an Applied Orientation*, Pearson.

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

Ng, B.Y. and Rahim, M. (2005), "A socio-behavioral study of home computer users' intention to practice security", *PACIS 2005 Proceedings*, p. 20.

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L. and McGlasson, J. (2021), ""Training and embedding cybersecurity guardians in older communities", *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1-15.

Panda Security (2020), "43 COVID-19 cybersecurity statistics", available at: www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/

Ponemon Institute (2020), "Cybersecurity in the remote work era: a global risk report", available at: www.keepersecurity.com/en_GB/ponemon2020.html

Rogers, R.V. (1975), "A protection motivation theory of fear appeals and attitude change1", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rogers, R.V. (1983), "Cognitive and psychological processes in fear appeals and attitude change: a revised theory of protection motivation", *Social Psychophysiology: A Sourcebook*, pp. 53-176.

Rogers, R.V. (1985), "Attitude change and information integration in fear appeals", *Psychological Reports*, Vol. 56 No. 1, pp. 179-182.

Shaikh, F.A. and Siponen, M. (2023), "Organizational learning from cybersecurity performance: effects on cybersecurity investment decisions", *Information Systems Frontiers*, Vol. 26 No. 3, pp. 1-12.

Sommestad, T., Karlzen, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security*, Vol. 23 No. 2, pp. 200-217.

Statista (2022c), "Number of subscriptions for smart home services worldwide from 2016 to 2022, by sensor type (in millions)", available at: www.statista.com/statistics/935864/worldwide-smart-home-services-number-of-subscription-by-sensor-type/

Statista (2022a), "Global digital population as of April 2022 (in billions)", available at: www.statista.com/statistics/617136/digital-population-worldwide/

Statista (2022b), "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", available at: www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Taneja, A., Vitrano, J. and Gengo, N.J. (2014), "Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: an empirical investigation", *Computers in Human Behavior*, Vol. 38, pp. 159-173.

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: a test of competing models", *Information Systems Research*, Vol. 6 No. 2, pp. 144-176.

Thatcher, J.B., McKnight, D.H., Baker, E.V., Arsal, R.E. and Roberts, N.H. (2010), "The role of trust in postadoption IT exploration: an empirical examination of knowledge management systems", *IEEE Transactions on Engineering Management*, Vol. 58 No. 1, pp. 56-70.

Thatcher, J.B. and Perrewe, P.L. (2002), "An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy", *MIS Quarterly*, Vol. 26 No. 4, pp. 381-396.

Thompson, N., McGill, T.J. and Vang, X. (2017), "'Security begins at home': determinants of home computer and mobile device security behavior", *Computers and Security*, Vol. 70, pp. 376-391.

Touray, A., Savolainen, T., Salminen, A., Sutinen, E. and Dai, Y. (2015), "The role of trust in enhancing internet use in a high-risk society", *Journal of Systems and Information Technology*, Vol. 17 No. 2, pp. 141-166.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016), "Understanding online safety behaviors: a protection motivation theory perspective", *Computers and Security*, Vol. 59, pp. 138-150.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3/4, pp. 190-198.

Venard, B. (2021), "Cybersecurity behavior under covid-19 influence", *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, *IEEE*, pp. 1-9.

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

Verkoeyen, S. and Nepal, S.K. (2019), "Understanding scuba divers' response to coral bleaching: an application of protection motivation theory", *Journal of Environmental Management*, Vol. 231, pp. 869-877.

White, G., Ekin, T. and Visinescu, L. (2017), "Analysis of protective behavior and security incidents for home computers", *Journal of Computer Information Systems*, Vol. 57 No. 4, pp. 353-363.

Woon, I., Tan, G.V. and Low, R. (2005), "A protection motivation theory approach to home wireless security", *ICIS 2005 Proceedings*, available at: https://aisel.aisnet.org/icis2005/31/

Corresponding author
Luzuko Tekeni can be contacted at: luzukotekeni23@gmail.com