Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 11(1) 2026

Journal of Computing Research and Innovation

Cognitive Coping and Social Drivers of Internet Threat Avoidance Behaviour in Tanzania Public Sector Employees

Frank Sengati[1*], Abdulkarim M. Jamal Kanaan[2], Ramesh Kumar Ayyasamy[3], Abdelhak Senadjki[4]

[1]*Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman (UTAR), 31900 Kampar, Perak, Malaysia.*
[2,3]*Department of Information Systems, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman (UTAR), 31900 Kampar, Perak, Malaysia.*
[4]*Department of Economics, Faculty of Economics and Finance, Universiti Tunku Abdul Rahman (UTAR), 31900 Kampar, Perak, Malaysia.*

ARTICLE INFO

Article history:
Received 16 November 2025
Revised 24 December 2025
Accepted 30 December 2025
Online first
Published 1 March 2026

Keywords:
Internet Threat
Avoidance Behaviour
Cybersecurity Behaviour
Public Sector
Technology Threat Avoidance Theory

DOI:
10.24191/jcrinn.v11i1.583

ABSTRACT

This study examines how cognitive, coping, and social-attitudinal factors determine internet threat avoidance behaviour among public sector employees in a rapidly digitalising low-income setting. We draw on Technology Threat Avoidance Theory (TTAT) and the Theory of Planned Behaviour (TPB) to model avoidance intention as a proximal predictor of avoidance behaviour. Cross-section survey data were collected from 558 Tanzanian public servants across ministries, departments, and agencies, and analysed using Partial Least Square – Structural Equation Modelling. The measurement model attained conventional reliability and validity limits, and the structural model explained 60.8% of the variance in avoidance intention and 33.4% in avoidance behaviour. Avoidance intention exhibited a large positive effect on avoidance behaviour, while all the antecedents of intentions showed significant but small effects. Our findings position at the centre empowerment, low-friction, and socially embedded interventions for enhancing public sector cybersecurity in Tanzania and similar settings.

1. INTRODUCTION

The cybercrime rate is rising faster than many governments can adapt. The Federal Bureau of Investigation (FBI) has estimated that globally victims have encountered more than US$16 billion in losses in 2024 alone, a staggering 33% increase from 2023 (FBI National Press Office, 2025). Much of this impact is a result of low-tech scams that include phishing, and business email compromise that tricks the employees rather than defeating the security technology (Satter, 2025). Recent evidence has shown that approximately 60% of all data breaches involve the "human element" which includes errors, misuse, stolen credentials, or social engineering. This emphasises that the security of organisational digital resources hinges on how employees

[1*] Corresponding author. *E-mail address*: frank.sengati@gmail.com
https://doi.org/10.24191/jcrinn.v11i1.583

perceive and respond to cyber threats (Rae, 2024; Uddin & Lu, 2024; Khadka & Ullah, 2025). Surveys focusing on humans increasingly posit that psychological, organisational, and social factors have become the ultimate fault lines in cybersecurity. For that matter, a call for models that explain why, when in the face of phishing emails, malicious links, or insecure practices, some employees actively avoid threats while others do not (Khadka & Ullah, 2025).

The Tanzania public sector ecosystem is in the midst of rapid digitalisation, spearheaded by the e-Government Strategy (2022-2027) and the 2024 Government Technology Roadmap. These two seek to develop a connected government, digital public services expansion, and boost the e-government cybersecurity environment (United Republic of Tanzania, 2024; President's Office, Public Service Management and Good Governance, 2022; Economic Commission for Africa, 2025). Equally, regional policy work on data governance emphasises that sustainable digitalisation in Tanzania should factor in human behaviour, institutional culture, and technical controls (Economic Commission for Africa, 2025). Yet, little is known regarding what drives Tanzanian public servants to avoid internet-related threats in their day-to-day work. We address this gap by integrating TTAT and TPB to examine how cognitive threat appraisal factors (severity, susceptibility, and cost), coping-motivational beliefs (self-efficacy, safeguard effectiveness, avoidance motivation, and avoidance attitude), and social-contextual influences from subjective norms directly predict internet threat avoidance behaviour across the Tanzanian public sector employees.

Integrating the named theories provides a conceptual benefit of connecting threat and coping-based cognitive appraisals with socially-linked intentional processes, thereby addressing not only why employees perceive cyber threats as avoidable but also how social norms and attitudes shapes the perceptions into avoidance behaviour. In the context of Low- and Middle-Income Countries (LMIC) public sector, this integration is useful as hierarchical norms, institutional constraints, and uneven cybersecurity capacity may weaken cognitive threat models and a combination of motivational and social predictors has proved useful in explanatory and predictive power of security behaviour beyond single theory approach (Delso-Vicente et al., 2025a; Alshammari & Al-Mamary, 2025).

2. RELATED WORK

2.1 Conceptualization of cybersecurity and internet threat avoidance behaviour

Recently, a perspective of conceiving cybersecurity behaviour as a single latent trait has been dwarfed by a group of observable individual actions, which may include password practices, phishing avoidance, patching, and policy compliance. Almansoori et al. (2023) systematic review work exhibits that empirical literature operationalises behaviour as compliance or protection behaviour determined by cognitive appraisals, self-efficacy, and social influences. Furthermore, they argue that empirical literature has remained divided across theories and technologies. Following up on this, Baltuttis et al. (2024) suggest a typology to separate routine, responsive, and proactive cybersecurity behaviours in an organisational setting further cementing the premise that different predictors may instantiate different subtypes of secure behaviours.

Gerdenitsch et al. (2023) define cybersecurity behaviour in the workplace as security compliance and security participation, demonstrating that security knowledge predicts both. However, this relationship is contingent upon employees' threat appraisal (perceived severity and susceptibility) and workplace conditions, including time pressure and decision-making autonomy. Similarly, Hong et al. (2023) illustrate that job stress resulting from work overload undermines employees' cybersecurity behaviour; however, a robust corporate ethics climate helps mitigate this effect. Collectively, this research endorses the perspective that cybersecurity or internet threat avoidance behaviour is influenced by cognitive threat

https://doi.org/10.24191/jcrinn.v11i1.583

assessments, coping evaluations, and contextual workplace characteristics, emphasising the necessity to model these determinants in conjunction rather than separately.

2.2 TTAT and related threat appraisal models in cybersecurity

From an individual threat and coping perspective, Technology Threat Avoidance Theory (TTAT) first viewed avoidance of IT threats as a function of perceived threat (severity and susceptibility) and coping assessments (safeguard effectiveness, self-efficacy, and costs), with avoidance motivation mediating their effects on avoidance behaviour. More recent empirical work applies this approach to contemporary online risks. Wang et al. (2023) for example, study internet threat avoidance behaviour and find that security anxiety modulates the effects of perceived severity, susceptibility, and protection effectiveness on avoidance intention, which in turn predicts avoidance behaviour. Sulaiman et al. (2022) utilized PMT, which shares TTAT's threat–coping appraisal structure, to Malaysian government personnel and showed that higher perceived severity, vulnerability, reaction efficacy, and self-efficacy are associated with stronger cybersecurity behaviour.

Other TTAT-aligned investigations stress certain threat settings or regulatory environments. AlGhanboosi et al. (2023), for instance, show that regulatory pressure and organisational regulations strengthen the impact of threat and coping assessments on cybersecurity avoidance conduct in organisational settings. Yousuf et al. (2023) integrate PMT, TTAT, and related constructs to explain cybersecurity behaviours among mobile payment users, revealing that threat appraisal and safeguard effectiveness are significant determinants of protective intentions in high-risk financial scenarios. Overall, literature confirms that severity, susceptibility, safeguard effectiveness, self-efficacy, and costs remain highly predictive of avoidance intention and behaviour across diverse technologies, but most studies either focus on consumers or mix employee groups from different sectors and countries.

2.3 TPB and social-attitudinal determinants of cybersecurity behaviours

From social and attitudinal perspective, the Theory of Planned Behaviour (TPB), together with TTAT and PMT, is widely employed to communicate the social and attitudinal determinants of cybersecurity behaviour. Al-Shanfari et al. (2022) formulate a comprehensive model incorporating the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), General Deterrence Theory, and facilitating conditions to elucidate the information security awareness intentions and behaviours of public-sector employees; attitudes and subjective norms are identified as critical antecedents of intention, which subsequently forecast actual security behaviour. Likewise, Li et al. (2022) demonstrate that, within organisational contexts, protection motivation structures and parts of the Theory of Planned Behaviour together forecast cybersecurity protection behaviour, further emphasising the mediating function of behavioural intention.

Research indicates that positive attitudes towards security, perceived behavioural control, and perceived social expectations (Alshammari & Al-Mamary, 2025), correlate with enhanced security intentions and behaviours in the context of policy compliance, secure password usage, and secure computing practices. Recent research on cybersecurity culture and security climate indicates that subjective standards are both interpersonal (including colleagues and supervisors) (Balagopal & Saji, 2023) and institutional (AlKalbani et al., 2017), mirroring organisational expectations ingrained in policies, training, and leadership communications. Nevertheless, whereas this TPB-based research incorporates attitude and subjective norms, it typically fails to differentiate threat-related cognitions (e.g., severity from susceptibility) or clearly conceptualise "avoidance attitude" towards internet threat as separate from general security attitudes.

https://doi.org/10.24191/jcrinn.v11i1.583

2.4 Public sector and LMIC evidence

The public sector has started to receive increased attention; nonetheless, the research base is inconsistent and predominantly reflects higher-income environments. Sulaiman et al. (2022) examine cybersecurity behaviour among Malaysian government employees and demonstrate that threat and coping assessments account for substantial diversity in behaviour; however, they do not include Theory of Planned Behaviour variables such as subjective standards or avoidance attitude. An investigation of public-sector employees in Oman and Malaysia by Al-Shanfari et al. (2022), demonstrates that the Theory of Planned Behaviour variables and facilitating factors are significant for information security knowledge and behaviour, employing structural equation modelling with public-sector samples. In the Gulf setting, Alghazo et al. (2025) determine that managers' information security intelligence, employee knowledge, and protection motivation collectively predict protective cybersecurity behaviour among public-sector employees in the United Arab Emirates.

Gerdenitsch et al. (2023) provide a view of employees from four municipal organisations in Spain, Portugal, and Italy, and reported that perceived severity and susceptibility enhance the influence of security knowledge on cybersecurity compliance and participation, thereby illustrating the interaction between threat appraisal and working conditions in public organisations. However, there is still a lack of systematic evidence about public-sector cybersecurity in low- and middle-income countries (LMICs). A recent analysis of cybersecurity in local governments indicates that despite the rapid digitalisation efforts, governance and security capabilities are trailing behind wider e-government initiatives, and that evidence remains sparse and geographically inclined towards Europe and North America (Hossain et al., 2024). In Tanzania, current research emphasises organisational preparedness, regulatory and strategic frameworks, and certain areas of risk domain such as e-waste disposal. On the contrary, theory-led models of public servants' everyday internet threat avoidance behaviour, such as TTAT are lacking (President's Office, Public Service Management and Good Governance, 2022; Mtakati & Sengati, 2021; Mustapha et al., 2025).

Nonetheless, there remains a paucity of empirical research that (a) concurrently models TTAT-style cognitive and coping factors alongside TPB-based social and attitudinal variables, (b) specifically examines internet threat avoidance intention and behaviour as separate outcomes, and (c) addresses this within LMIC public-sector contexts, such as Tanzania. This study addresses the gap by investigating the direct impacts of severity, susceptibility, cost, self-efficacy, safeguard effectiveness, subjective norms, and avoidance attitude on avoidance intention, which subsequently influences avoidance behaviour among Tanzanian public-sector employees.

3. THEORETICAL BACKGROUND AND HYPOTHESES DEVELOPMENT

3.1 Integrating TTAT and TPB for internet threat avoidance

TTAT explains why and how individuals avoid information technology-related threats. It sets a demarcation between the threat appraisal process, where individuals evaluate the seriousness and likelihood of being a victim, and the coping appraisal, where an individual assesses abilities (theirs and for the measure) and costs related to carrying out avoidance behaviour. Avoidance motivation and behaviour are the outcomes. On the other hand, TPB supports TTAT by specifying behavioural intention as the most immediate determinant of actual behaviour while at the same time establishing the role of subjective norms as well as perceived behavioural control. Intention determines readiness to act, attitude establishes individual evaluative disposition regarding taking an action, and lastly, subjective norms capture perceived social expectations. Despite the conceptual overlap between perceived behavioural control and self-efficacy, our study prioritized the latter as it captures employees' confidence in carrying out a required avoidance behaviour, unlike the perceived behavioural control that is broader and further reflects

https://doi.org/10.24191/jcrinn.v11i1.583

controllability (Ajzen, 2020), limitations that may be institutionally determined in the context of the public sector.

Our study integrates TTAT and TPB to model avoidance intention as a linking factor between cognitive-motivation factors and avoidance behaviour. Threat appraisal (severity and susceptibility) and coping appraisal (self-efficacy, safeguard effectiveness, and perceived cost), as well as TPB's social attitudinal constructs (subjective norms and avoidance attitude), are established as direct antecedents of avoidance intention and ultimately avoidance behaviour. This proposition aligns with TTAT's threat-coping logic and TPB's intention-behaviour logic.

3.2 Threat appraisal and avoidance intention

Threat appraisal refers to the perceived seriousness of negative impacts (severity) and the likelihood of experiencing them (susceptibility) for a particular IT threat (Liang & Xue, 2009). When individuals believe that impacts are severe and that they are personally vulnerable, they are more likely to form strong avoidance motivations towards protective behaviours. These may include verifying URLs, using secure channels, or avoiding suspicious links (Liang & Xue, 2009; Ilany-Tzur & Fink, 2025). Recent empirical research substantiates that higher levels of severity and susceptibility perception are positively linked with security-related avoidance intentions in different contexts, such as online identity theft, cybersecurity education, and device risk-avoidance behaviour (Jibril et al., 2020; Alqahtani, 2022; Wang et al., 2023).

In line with TTAT, we conceptualise cognitive threat appraisals as a cluster of perceptions about the severity and likelihood of internet threats faced by public sector employees in their work. When a Tanzanian public servant perceives that it's likely that they can be a victim of internet threats and consequences exist for public data and service continuity, they should be more motivated to avoid risky online behaviours. We therefore hypothesize that:

H1: Perceived severity (SEV) has a positive effect on avoidance intention (AI).

H2: Perceived susceptibility (SUS) has a positive effect on avoidance intention.

3.3 Coping appraisal and avoidance intention

Coping appraisal refers to beliefs about the capability and cost of using existing safeguards. Self-efficacy refers to one's belief in their ability to perform a required protective action, such as recognising phishing emails or verifying web links, while safeguard cost addresses perceived effort, time, inconveniences, or resources required to carry out a particular protective behaviour (Liang & Xue, 2009). TTAT argues that self-efficacy and safeguard effectiveness tend to positively favour avoidance motivations, whereas a higher perception of cost discourages them. Recent empirical data on cybersecurity have consistently found that self-efficacy and response efficacy are positively linked to avoidance intentions or protection behaviours. On the other hand, response cost has a negative influence on avoidance intentions (Session & Muller, 2022; Alqahtani, 2022).

From the public sector context, employees face workload pressures and limited power over IT configurations; hence, the balance between one's belief in their capability, belief in safeguard effectiveness, and cost perceptions is likely to be important. When Tanzania public sector employees feel that they are able to execute a required security behaviour, the security measure required to be executed is effective, and the associated cost related to executing a particular behaviour is low, then they are likely to enact IT threat avoidance intention. Accordingly, we propose that:

H3: Perceived cost (CO) has a negative effect on avoidance intention.

H4: Self-efficacy (SEL) has a positive effect on avoidance intention.

H5: Safeguard effectiveness (SEF) has a positive effect on avoidance intention.

https://doi.org/10.24191/jcrinn.v11i1.583

3.4 Social and attitudinal influences and avoidance intention

The underlying principle of TPB argues that attitude, subjective norms, and perceived behavioural control together determine behavioural intention, which in turn predicts behaviour (Ajzen, 2020). In the information security and cybersecurity research domain, TPB has been extensively used to argue for policy compliance, secure password practices, and other protective behaviours. Furthermore, meta-analytic and review evidence points to the robustness of TPB in this domain (Kuppusamy et al., 2022; Almansoori et al., 2023; Ali et al., 2021) . Specifically, empirical literature shows that positive attitudes towards secure behaviour and supportive subjective norms (a perception that significant others expect one to behave securely) are strong determinants of cybersecurity intentions among young adults and employees (Alanazi et al., 2022; Parikh & Nimbekar, 2023).

Building from an integrative approach, we extend TTAT with two TPB constructs. First, we pursue an avoidance attitude to reflect an individual's overall positive or negative evaluations about engaging in internet threat avoidance behaviour. Second, we integrate subjective norms to capture perceived social pressures from supervisors, colleagues, or organisational culture to avoid risky online behaviour. Whereas in Tanzania, hierarchical structures and collective expectations are prevalent, attitudes and subjective norms are likely to be focal in shaping employees' avoidance intention. We therefore postulate that:

H6: Subjective norms (SN) has a positive effect on avoidance intention

H7: Avoidance attitude (AA) has a positive effect on avoidance intention

3.5 Avoidance intention and avoidance behaviour

Theoretically, both TTAT and TPB converge on the perception that behavioural intention is the most immediate determinant of actual behaviour. Individuals are more likely to act when they intend to do so (Ajzen, 2020). Observing this from cybersecurity and privacy research, different literature substantiates that intentions to comply with policies, use secure practices, or the protection of individual data are positively related to corresponding behaviours, despite the fact that the relationship is not always perfect (Sun et al., 2020; Ali et al., 2021). Of recent, literature addressing the intention-behaviour gap in the digital context argues that contextual limitations, habits, and affect oftentimes weaken the conversion of intention to action (Sun et al., 2020; Patronidou, 2022). However, intention has remained a paramount explanatory predictor and key design target for interventions.

Parallel to these theoretical and empirical underpinnings, we argue that internet threat avoidance intention is a proximal determinant of internet threat avoidance behaviour among public sector employees of Tanzania. We recognise that actual behaviour may diverge from observed intentions as a result of contextual and habitual factors, but we expect that higher levels of avoidance intentions will generally translate into more avoidance behaviour. We thus posit:

H8: Avoidance intention has a positive effect on avoidance behaviour (AB)

4. METHODOLOGY

4.1 Survey development, sampling, and participants

Our study employed a quantitative cross-sectional survey of public sector employees in Tanzania to examine the hypothesised structural model. We align with contemporary cybersecurity literature in applying SEM-based large-scale survey studies to model relationships among behavioural constructs (Hong & Furnell, 2021; Alsharida et al., 2023). Proportional stratified sampling was used to select targeted respondents from a sampling frame of all ministries, departments, and agencies (MDA). We targeted respondents with at least two years of work experience who routinely used internet-connected computing

https://doi.org/10.24191/jcrinn.v11i1.583

devices for their official day-to-day tasks. We adopted a procedure advocated by (Yamane, 1967) to estimate a minimum sample size required of 400 respondents from the public sector.

4.2 Measurements

Data were collected using a structured questionnaire that we adapted from prior behavioural cybersecurity literature. We revised and validated all items while retaining their theoretical meaning to fit the present study. We established a scale-level CVI/Ave of 0.95 through the content validity index (CVI) procedure (Polit et al., 2007) across six subject matter experts. We operationalised severity, susceptibility, and self-efficacy from (Wang et al., 2023), cost perception from (Liang & Xue, 2009) and safeguard effectiveness from (Carpenter et al., 2019). Subjective norms were construed from (Tsai et al., 2016) while the avoidance attitude was from (Venkatesh et al., 2003). Lastly, avoidance intention and avoidance behaviour were operationalised from (Liang & Xue, 2009). All latent predictors were measured on a 7-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). Furthermore, we captured demographic information such as gender, age group, education, formal ICT training, job tenure, and MDA type

4.3 Data analysis

To estimate the measurement and structural model, we utilised Partial Least Square Structural Equation Modelling (PLS-SEM) through SmartPLS 4. Hair and Alamer (2022) argues that PLS-SEM approach is preferred in prediction-driven models, robustness with nonnormal data, and its ability to handle complex model structures with limited sample sizes, and thus our paper aligns with this thinking to utilize PLS-SEM approach. Confirmatory Factor Analysis (CFA) verified the content validity cut-off value of ≥ 0.50 (Hair & Alamer, 2022). Discriminant validity was evaluated using the HTMT ratio of correlation and Fornell-Larcker benchmarks (Fornell & Larcker, 1981). Furthermore, we assessed convergent validity using composite reliability and average variance extracted, aiming for 0.70 and 0.50, respectively (Hair & Alamer, 2022). Reliability was assessed with a Cronbach's Alpha value of 0.70 (Hair et al., 2017).

5. RESULTS

5.1 Characteristics of respondents

A total of 558 questionnaires were usable out of 650 distributed equivalents to 85.8%. Of the usable questionnaires, 58.1% were male; most were between 26 and 49 years old, 78.4%, and 73.7% held at least a diploma. Respondents came from a broad range of ministries, authorities, and independent departments. Table 1 summarises the sample characteristics.

Table1. Demographic characteristics of the respondents

Demography	Category	f	%
Gender	Male	*324*	*58.1*
	Female	*234*	*41.9*
Age Group (years)	18 – 25 years	*51*	*9.1*
	26 – 33 years	*126*	*22.6*
	34 – 41 years	*156*	*28.0*
	42 – 49 years	*155*	*27.8*
	50 years and above	*70*	*12.5*

https://doi.org/10.24191/jcrinn.v11i1.583

Highest Education Level	O' Level	*41*	*7.3*
	A' Level	*57*	*10.2*
	Diploma or equivalent	*144*	*25.8*
	Degree or equivalent	*108*	*24.1*
	Masters' degree	*135*	*24.2*
	Doctorate degree	*48*	*8.6*
Possession of Formal ICT training	Yes	*270*	*48.4*
	No	*288*	*51.6*
Years of Job Experience	Between 2 and 4 years	*96*	*17.2*
	Between 5 and 7 years	*138*	*24.7*
	Between 8 and 10 years	*167*	*29.9*
	Over 10 years	*157*	*28.1*
MDA Type	Ministries	*76*	*13.6*
	Independent departments	*71*	*12.7*
	Authorities	*77*	*13.8*
	Agencies	*57*	*10.2*
	Funds	*28*	*5.0*
	Institutes	*46*	*8.2*
	Boards	*59*	*10.6*
	Councils	*42*	*7.5*
	Commissions	*55*	*9.9*
	Government companies	*19*	*3.4*
	Corporations	*28*	*5.0*

Source: Authors' own data

To determine global model fit, we considered Standardised Root Mean Square (SRMR), unweighted least square discrepancy (d_{ULS}), geodesic discrepancy (d_G), Chi-square, and normed fit index (NFI). Our results showed an SRMS value of 0.069, which was below the 0.08 threshold, establishing an acceptable fit (Henseler et al., 2016). Our study prioritised the predictive nature of PLS-SEM, thus positioning SRMR and predictive statistics such as Q^2 from PLSpredict over the CB-SEM comparative indices as more appropriate criteria (Henseler et al., 2016; Ogbeibu et al., 2021; Sarstedt et al., 2016) for evaluating model fit. The discrepancy measure between empirical and model-implied correlation matrices shows that the estimated model has a higher discrepancy than the saturated model (d_{ULS} = 3.006 vs 4.059) and (d_G = 1.213 vs 1.267). Chi-square findings were significant (χ^2 = 3882.88), a common occurrence with large sample sizes (Hair & Alamer, 2022). The NFI obtained was 0.80, indicating a below-convention excellent range, typically reported of $\geq$ 0.90 (Hair et al., 2022). The common model fit indices d_{ULS}, d_G, χ^2, and NFI in CB-SEM are not transferable to PLS-SEM approaches (Hair et al., 2022).

https://doi.org/10.24191/jcrinn.v11i1.583

Table 2. Descriptive statistics, factor analysis, and reliability test

Construct	Items	Factor Loading	Mean	SD	α	CR	AVE
Avoidance attitude (AA)	AA1	0.899	4.409	1.596	0.929	0.949	0.823
	AA2	0.919					
	AA3	0.902					
	AA4	0.908					
Avoidance behaviour (AB)	AB1	0.933	3.769	1.296	0.773	0.896	0.811
	AB2	0.867					
Avoidance intention (AI)	AI1	0.904	4.586	1.388	0.792	0.880	0.713
	AI2	0.916					
	AI3	0.694					
Cost (CO)	CO1	0.881	5.184	1.623	0.845	0.906	0.762
	CO2	0.858					
	CO3	0.879					
Safeguard effectiveness (SEF)	SEF1	0.762	5.399	1.306	0.909	0.927	0.645
	SEF2	0.871					
	SEF3	0.841					
	SEF4	0.786					
	SEF5	0.810					
	SEF6	0.778					
	SEF7	0.767					
Self-efficacy (SEL)	SEL1	0.784	4.215	1.268	0.930	0.943	0.702
	SEL2	0.754					
	SEL3	0.777					
	SEL4	0.896					
	SEL5	0.894					
	SEL6	0.871					
Severity (SEV)	SEV2	0.926	4.618	1.646	0.946	0.961	0.860
	SEV3	0.923					
	SEV4	0.939					
	SEV5	0.921					
Subjective norms (SN)	SN2	0.942	4.336	1.049	0.861	0.935	0.878
	SN3	0.933					
Susceptibility (SUS)	SUS1	0.836	4.765	1.247	0.856	0.911	0.774
	SUS2	0.874					
	SUS3	0.928					

Source: Authors' own data

During assessment of the measurement model, we noted low loading items from subjective norms ($SN1 = 0.208$), susceptibility ($SUS4 = 0.323$), and severity ($SEV1 = 0.593$) and these were eliminated without impairing model performance. Our final model contained 4 items for AA and SEV, 2 items for AB and SN, 3 items for AI, CO, and SUS, while SEL has 6 items, and lastly, SEF contained 7 items. As shown in Table 2, all constructs exhibited satisfactory internal consistency ($\alpha > 0.773; CR > 0.880$) and convergent validity (all loadings $\geq 0.694; AVE \geq 0.645$). Discriminant validity was supported by HTMT and Fornell-Larcker criteria, as seen in Tables 3 and 4. We examined Variance Inflation Factors (VIF) to detect multicollinearity issues among indicators, as their presence tends to inflate standard errors (Hair et al., 2022). Our results show VIF values within acceptable thresholds for both outer model (1.264 – 4.837) and the inner model (1.000 – 3.206) remaining below the conservative cut-off of 5, indicating that multicollinearity is unlikely to threaten robustness or interpretability of the estimated relationships (Hair et al., 2022). We summarize VIF observations in Table 5.

https://doi.org/10.24191/jcrinn.v11i1.583

Table 3. Heterotrait-Monotrait (HTMT) Ratio

	AA	AB	AI	CO	SEF	SEL	SEV	SN	SUS
AA	-								
AB	0.687	-							
AI	0.596	0.729	-						
CO	0.372	0.396	0.726	-					
SEF	0.356	0.400	0.727	0.853	-				
SEL	0.156	0.192	0.558	0.509	0.465	-			
SEV	0.732	0.580	0.503	0.630	0.462	0.170	-		
SN	0.772	0.672	0.627	0.385	0.392	0.169	0.527	-	-
SUS	0.481	0.365	0.614	0.533	0.512	0.428	0.445	0.425	

Source: Authors' own data

Table 4. Fornell-Larcker Criteria

	AA	AB	AI	CO	SEF	SEL	SEV	SN	SUS
AA	0.907								
AB	0.590	0.901							
AI	0.521	0.578	0.844						
CO	0.338	0.337	0.607	0.873					
SEF	0.343	0.354	0.642	0.765	0.803				
SEL	0.146	0.179	0.496	0.469	0.452	0.838			
SEV	0.690	0.501	0.444	0.575	0.450	0.162	0.927		
SN	0.690	0.557	0.520	0.334	0.356	0.155	0.479	0.937	
SUS	0.445	0.326	0.525	0.466	0.474	0.393	0.417	0.380	0.880

Source: Authors' own data

Table 5. Collinearity Statistics

	Variance Inflation Factor (VIF)	
Variable	**Inner Model**	**Outer Model**
AA	3.038	3.044 – 3.707
AB		1.658
AI	1.000	1.264 – 2.999
CO	3.206	1.952 – 2.092
SEF	2.613	1.779 – 4.718
SEL	1.395	2.679 – 3.980
SEV	2.657	3.762 – 4.837
SN	1.993	2.338
SUS	1.575	1.962 – 2.808

Source: Authors' own data

The bootstrapping procedure with 10000 samples (Streukens & Leroi-Werelds, 2016) exhibited strong structural support for the hypothesised paths. The hypothesis H7 which posits that avoidance attitude significantly influenced avoidance intention was supported ($\beta = 0.248, t = 5.028, p < 0.001$). We observed the same for H8 on the relationship between avoidance intention and avoidance behaviour ($\beta = 0.578, t = 21.591, p < 0.001$). Likewise, our hypothesis H3 was supported such that cost negatively influences avoidance intention ($\beta = 0.181, t = 3.573, p < 0.001$). Safeguard effectiveness significantly influenced avoidance intention ($\beta = 0.263, t = 6.191, p < 0.001$) and hence H5 was supported. Self-efficacy H4 strongly and positively influenced avoidance intention ($\beta = 0.206, t = 6.362, p < 0.001$). We noted that severity exhibited a negative significant influence on avoidance intention ($\beta = -0.110, t =$

https://doi.org/10.24191/jcrinn.v11i1.583

$2.440, p < 0.05$) and therefore H1 was rejected. For subjective norm H6, results indicate that the hypothesis was supported ($\beta = 0.176, t = 4.773, p < 0.001$). Lastly, susceptibility exhibited a statistically significant positive effect on avoidance intention ($\beta = 0.104, t = 2.921, p < 0.05$) and hence H2 was supported. These findings together with effect sizes, are summarised in Table 6.

Table 6. Hypotheses testing results and effect sizes

Hypothesis	Path	β	T-value	p-value	Supported	Effect size
H1	SEV → AI	-0.110	2.440	**	No	Small
H2	SUS → AI	0.104	2.921	**	Yes	Small
H3	COS → AI	0.181	3.573	***	Yes	Small
H4	SEL → AI	0.206	6.362	***	Yes	Small
H5	SEF → AI	0.263	6.191	***	Yes	Small
H6	SNO → AI	0.176	4.773	***	Yes	Small
H7	AA → AI	0.248	5.028	***	Yes	Small
H8	AI → AB	0.578	21.591	***	Yes	Large

Source: Authors' own data

Our interpretation of effect size is based on the work of (Beaudry & Pinsonneault, 2001). Findings show that for all predictors with the exception of the relationship between avoidance intention and avoidance behaviour, all effect sizes were small, ranging from 0.012 to 0.076. The largest effect size was exhibited by AI → AB relationship (0.502). Fig. 1 show the bootstrapped results.

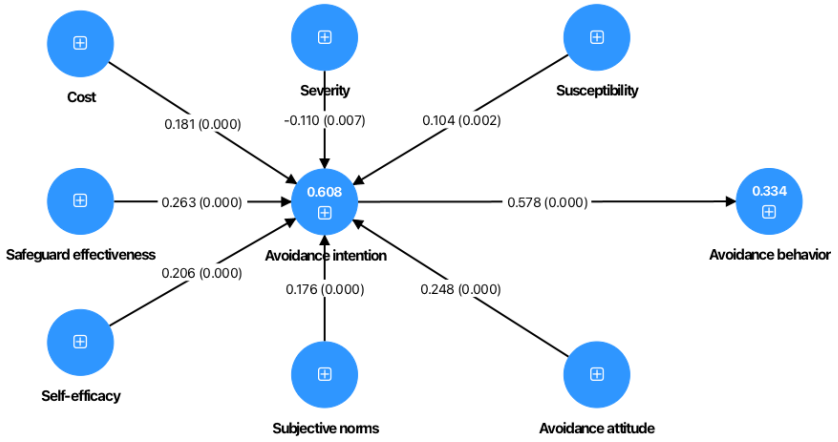

Fig. 1. Bootstrapped result (path coefficient and p-values)

Source: Authors' own data

Our analysis concluded with the examination of the model's in-sample and out-of-sample predictive power. For in-sample results, our model displayed a significant coefficient of determination for avoidance intention ($R^2 = 0.608, p < 0.001$) and avoidance behaviour ($R^2 = 0.334, p < 0.001$) indicating variance explanation of 60.8% and 33.4% respectively. Interpreting from the lens of (Hair et al., 2019) this means our proposed model exhibited between weak and moderate explanatory power. We then ran a blindfolding procedure and recorded the Q^2 values. The results were larger than zero and positive for all predictors,

https://doi.org/10.24191/jcrinn.v11i1.583

demonstrating a solid out-of-sample predictive capability. ITAB1 and ITAB2 exhibited Q^2 values of 0.280 and 0.147 respectively, while for intention ITAI1, ITAI2, and ITAI3 Q^2 values were 0.489, 0.542, and 0.239 respectively. These results are summarised in Table 7.

Table 7. Model explanatory power

Endogenous Construct	R^2	Adjusted R^2	Indicators	Q^2
Avoidance Behaviour	0.334	0.336	ITAB1	0.280
			ITAB2	0.147
Avoidance Intention	0.608	0.613	ITAI1	0.489
			ITAI2	0.542
			ITAI3	0.239

Source: Authors' own data

6. DISCUSSION

Our findings show that the proposed integrated TTAT-TPB model provides a statistically robust but modest explanatory account of the Tanzania public sector employees' internet threat avoidance behaviour. We noted the strongest result and a significant larger effect of avoidance intention on avoidance behaviour. This aligns well with the premises of TTAT and TPB, which both position intention as the proximal predictor of behaviour. Furthermore, this is a reflection of recent findings on threat avoidance, cybersecurity compliance, and privacy protective actions, where intentions account for more variance in behaviour (Han et al., 2025; Delso-Vicente et al., 2025). On the same note, avoidance behaviour has exhibited a lower explanatory power than intention, signalling the common intention-behaviour gap where individuals possess a stronger readiness to avoid internet threats than they actually do. The noted gap has been extensively documented in privacy and security studies and is oftentimes tied to situational constraints, habits, or competing performance pressures that inhibit the translation of intention to behaviour (Jenkins et al., 2021; Mayer et al., 2023). In Tanzania's public sector, where workload constraints and resource limitations are typical, strengthening intentions alone will not be enough; interventions must be put in place to reduce frictions and support habit cultivation around everyday security practices.

Results have also demonstrated that most hypothesised statements were statistically significant yet with small effects. Moderate R2 values and multiple small effects from cognitive, motivational, and coping antecedents of intentions exhibit small effects are commonly reported (Han et al., 2025; Delso-Vicente et al., 2025b). We noted that coping appraisal, specifically self-efficacy and safeguard effectiveness, is more influential than threat appraisal, aligning with TTAT and PMT premises where self-efficacy and response efficacy are strong determinants of motivation and related security intentions (Han et al., 2025). In this case, public sector employees in Tanzania who feel able to recognise different internet-based threats, feel confident responding to threats, and believe that available security measures actually work will be more likely to avoid risky online behaviours.

Oppositely, severity exhibited negative results towards avoidance intentions, even though significant. This further reverberates a common observation in behavioural cybersecurity literature (Haag et al., 2021; Han et al., 2025). Threat severity exhibits a conceptually intuitive premise yet a weak empirical variable in threat-based models, especially when individuals are too exposed or when incidents are too severe beyond their personal control (Reeves et al., 2020). In line with fear control response literature, such as Xin et al. (2022), that counters danger control actions, one possible justification is that in the context of the public sector, higher levels of severity are interpretably linked to fatalism or mass catastrophe and beyond one's sphere of influence. This tends to weaken rather than strengthen avoidance intention. On the opposite end of the spectrum, susceptibility exhibited a small yet positive relationship with avoidance intention. In line

https://doi.org/10.24191/jcrinn.v11i1.583

with TTAT, a perception of being personally at risk is more consistently linked to protective intention than a perception of catastrophic outcome (Kiran et al., 2025). From the TPB lens, avoidance attitude and subjective norms demonstrated significant and small positive effects on avoidance intention. These findings support the TPB assertion that employees with favourable attitudes towards secure behaviour and who perceive significant expectations from colleagues or supervisors are more likely to cultivate intention formation.

Perception of cost also exhibited statistically significant results, although with a small effect. TTAT commonly argues a negative influence of response cost on intention, and much behavioural cybersecurity literature reports that time and convenience barriers inhibit security intentions (Han et al., 2025). The modest effect we observed suggests that Tanzanian public servants are knowledgeable about frictions and effort required in secure practices, but they tend not to overshadow other key drivers, such as self-efficacy or safeguard effectiveness. It may be construed that these costs are interpreted as investments in security practices rather than burdensome, which may then lower the negative effect. Overall, the results of our model's in-sample and out-of-sample predictive performance demonstrate that TTAT and TPB can be resourcefully and meaningfully integrated to explain internet threat avoidance behaviour in an African public sector context. The pattern we have observed, where there is a strong intention-behaviour linkage, small multiple consistent effects, and an unexpected severity effect, echoes the wider behavioural security literature and underscores the need for intervention strategies that focus on empowering users, socially embedded, and low-friction avoidance practices.

7. CONCLUSION, IMPLICATIONS, AND LIMITATIONS

7.1 Conclusion

Our study has demonstrated that the integration of TTAT and TPB can account for meaningful aspects of the internet threat avoidance behaviour of public sector employees, with intentions emerging as a key proximal determinant of behaviour, while cognitive, coping, and social factors account for small yet meaningful effects. Our results position self-efficacy, safeguard effectiveness, avoidance attitude, and subjective norms at the centre of avoidance intention while stressing the intention-behaviour gap and the instability of severity perception in a rapidly growing digital public sector of a low-income country. The findings of the study extend the behavioural cybersecurity literature by providing evidence from an under-represented LMIC public sector setting and provide theoretically guided and empirically validated ground for designing human-focused cybersecurity interventions.

7.2 Implications

Theoretically, we provide evidence for the complementary approach between TTAT and TPB, where threat and coping appraisals, social norms, and attitudes determine avoidance intention and thus avoidance behaviour. In the future, behavioural cybersecurity models should integrate these parameters in an organisational setting. Practically, Tanzania's public sector cybersecurity programmes should focus on developing employees' self-efficacy and confidence in available security measures while also building security norms and positive avoidance attitudes through leadership communication, peer mentoring and modelling, and targeted training. Fear appeals alone are insufficient. Frictions related to executing required cybersecurity behaviour should also be minimised through procedure simplification, aligning security policies with day-to-day work practices, and offering supportive tools that cultivate translation of secure intentions to secure behaviour.

https://doi.org/10.24191/jcrinn.v11i1.583

7.3 Limitations

Our study's cross-sectional, self-reported design hinders causal inference and may be affected by common method bias and social desirability despite exhibiting above-minimum psychometric indicators. Our data was collected in a single country; hence, generalisation to other countries and cultures could be limited. Furthermore, we focused on direct effects, and thus, potential mediating mechanisms may be present but unaccounted for. These may include security climate, resource availability, or leadership support. In the future, researchers should attempt to deploy longitudinal or multi-wave studies and combine self-reported data with observational data.

8. ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge the support of the Ministry of Finance of the United Republic of Tanzania through the Institute of Accountancy Arusha (IAA) for funding the study. We extend our acknowledgement to Universiti Tunku Abdul Rahman (UTAR), Kampar, Malaysia for providing the learning environment where this study could be conceived and nurtured.

9. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial, or financial conflicts and declare the absence of conflicting interests with the funders.

10. AUTHORS' CONTRIBUTIONS

The authors were responsible for all aspects of the research, including conceptualization, investigation, formal analysis, writing the original draft, validation, and writing-reviewing.

11. REFERENCES

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. https://doi.org/10.1002/hbe2.195

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

AlGhanboosi, B., Ali, S., & Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Computers in Human Behavior*, *144*, 107702. https://doi.org/10.1016/j.chb.2023.107702

Alghazo, S. H. A., Humaidi, N., & Abdullah, N. B. (2025). Utilising manager's competency, employee's awareness and motivation for promoting cybersecurity protective behaviour. *Electronic Journal of Knowledge Management*, *23*(2), 14–40. https://doi.org/10.34190/ejkm.23.2.3895

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: an institutional perspective. *Data and Information Management*, *1*(2), 104–114. https://doi.org/10.1515/dim-2017-0006

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), 5700. https://doi.org/10.3390/app13095700

Alqahtani, H. (2022). The impact of technology threat avoidance theory constructs on cybersecurity avoidance behaviour. In *13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022)* (pp. 161–175). https://doi.org/10.54941/ahfe1002693

Alshammari, M. M., & Al-Mamary, Y. H. (2025). Bridging policy and practice: Integrated model for investigating behavioral influences on information security policy compliance. *Systems*, *13*(8), 630. https://doi.org/10.3390/systems13080630

Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. *International Journal of Advanced Computer Science and Applications*, *13*(8), 479–490. https://doi.org/10.14569/IJACSA.2022.0130855

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Balagopal, N., & Saji K., M. (2023, October 12). Information security policy violations in the work-from-home era. *WISP 2023 Proceedings*. Pre-ICIS Workshop on Information Security and Privacy (SIGSEC). https://aisel.aisnet.org/wisp2023/15

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*, 103741. https://doi.org/10.1016/j.cose.2024.103741

Beaudry, A., & Pinsonneault, A. (2001). IT-induced adaptation and individual performance: A coping acts model. *ICIS 2001 Proceedings*, *58*. https://core.ac.uk/download/pdf/301354339.pdf

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 380–407. https://doi.org/10.17705/1CAIS.04422

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & De Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, *11*(1), 28. https://doi.org/10.1186/s43093-025-00452-7

Economic Commission for Africa. (2025, August). *Tanzania's path toward a national data governance framework | United Nations Economic Commission for Africa* [Information]. Tanzania's Path toward a National Data Governance Framework. https://www.uneca.org/stories/tanzania%E2%80%99s-path-toward-a-national-data-governance-framework

https://doi.org/10.24191/jcrinn.v11i1.583

FBI National Press Office. (2025, April). *FBI Releases Annual Internet Crime Report* [Press Release]. Federal Bureau of Investigation. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal Of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *17*(4). https://doi.org/10.5817/CP2023-4-7

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, *1*(3), 100027. https://doi.org/10.1016/j.rmal.2022.100027

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (Second edition). SAGE.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *Hair A primer on partial least squares structural equation modeling pls-sem* (3rd ed.). SAGE.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. *Frontiers in Public Health*, *13*, 1677024. https://doi.org/10.3389/fpubh.2025.1677024

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20. https://doi.org/10.1108/IMDS-09-2015-0382

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Hong, Y., Kim, M.-J., & Roh, T. (2023). Mitigating the impact of work overload on cybersecurity behavior: The moderating influence of corporate ethics—A Mediated moderation analysis. *Sustainability*, *15*(19), 14327. https://doi.org/10.3390/su151914327

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501

https://doi.org/10.24191/jcrinn.v11i1.583

Ilany-Tzur, N., & Fink, L. (2025). Device and risk-avoidance behavior in the context of cybersecurity phishing attacks. *International Journal of Information Management*, *84*, 102919. https://doi.org/10.1016/j.ijinfomgt.2025.102919

Jenkins, J., Durcikova, A., & Nunamaker, J. (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), 246–272. https://doi.org/10.17705/1jais.00660

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825. https://doi.org/10.1080/23311975.2020.1832825

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security*, *149*, 104204. https://doi.org/10.1016/j.cose.2024.104204

Kuppusamy, P., Samy, G. N., Maarop, N., Shanmugam, B., & Perumal, S. (2022). Information security policy compliance behavior models, theories, and influencing factors: A systematic literature review. *Journal of Theoretical and Applied Information Technology*, *100*(5), 1536–1557.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Liang & Xue. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71. https://doi.org/10.2307/20650279

Mayer, P., Zou, Y., Lowens, B. M., Dyer, H. A., Le, K., Schaub, F., & Aviv, A. J. (2023). Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, *30*(5), 1–53. https://doi.org/10.1145/3589958

Mtakati, B., & Sengati, F. (2021). Cybersecurity posture of higher learning institutions in Tanzania. *The Journal of Informatics*, *1*(1). https://doi.org/10.59645/tji.v1i1.1

Mustapha, A., Mgawe, B. S., Mvulla, J., & Sam, A. (2025). Mitigating cybersecurity risks in e-waste: A study on secure disposal practices in Tanzania's public institutions. *Journal of Information Systems and Informatics*, *7*(2), 1354–1375. https://doi.org/10.51519/journalisi.v7i2.1100

Ogbeibu, S., Jabbour, C. J. C., Gaskin, J., Senadjki, A., & Hughes, M. (2021). Leveraging STARA competencies and green creativity to boost green organisational innovative evidence: A praxis for sustainable development. *Business Strategy and the Environment*, *30*(5), 2421–2440. https://doi.org/10.1002/bse.2754

https://doi.org/10.24191/jcrinn.v11i1.583

Parikh, V., & Nimbekar, M. (2023). Socializing the impact: An analysis of the theory of planned behavior's influence on increasing university students' cybersecurity awareness. *Journal of Community Development*, *4*(2), 139–156. https://doi.org/10.47134/comdev.v4i2.162

Patronidou, A. (2022). *Nudging Secure Digital Behavior* [Thesis]. Erasmus University Rotterdam.

Polit, D. F., Beck, C. T., & Owen, S. V. (2007). Is the CVI an acceptable indicator of content validity? Appraisal and recommendations. *Research in Nursing & Health*, *30*(4), 459–467. https://doi.org/10.1002/nur.20199

President's Office, Public Service Management and Good Governance. (2022). *Tanzania e-Government Strategy 2022*. President's Office, Public Service Management and Good Governance. https://www.utumishi.go.tz/uploads/documents/sw-1688121445-Tanzania%20e-Government%20Strategy%202022.pdf?

Rae, C. (2024, September). Time to take action: Insights from the verizon data breach investigations report 2024 [Blog]. *Isms.Online*. https://www.isms.online/information-security/time-to-take-action-insights-from-the-verizon-data-breach-investigations-report-2024/

Reeves, A., Calic, D., & Delfabbro, P. (2020). Sleeping with the enemy: Does depletion cause fatigue with cybersecurity? In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (vol. 12210, pp. 217–231). Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_15

Sarstedt, M., Hair, J. F., Ringle, C. M., Thiele, K. O., & Gudergan, S. P. (2016). Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research*, *69*(10), 3998–4010. https://doi.org/10.1016/j.jbusres.2016.06.007

Satter, R. (2025, April 23). FBI says cybercrime costs rose to at least $16 billion in 2024. *Reuters*. https://www.reuters.com/world/us/fbi-says-cybercrime-costs-rose-least-16-billion-2024-2025-04-23/

Session, W., & Muller, S. R. (2022). *Technology Threat Avoidance Factors Affecting Cybersecurity Professionals' Willingness to Share Information*. 209–213. https://doi.org/10.15439/2022M4720

Streukens, S., & Leroi-Werelds, S. (2016). Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. *European Management Journal*, *34*(6), 618–632. https://doi.org/10.1016/j.emj.2016.06.003

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413

Sun, Q., Willemsen, M. C., & Knijnenburg, B. P. (2020). Unpacking the intention-behavior gap in privacy decision making for the Internet of Things (IoT) using aspect listing. *Computers & Security*, *97*, 101924. https://doi.org/10.1016/j.cose.2020.101924

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

https://doi.org/10.24191/jcrinn.v11i1.583

Uddin, S., & Lu, H. (2024). Dataset meta-level and statistical features affect machine learning performance. *Scientific Reports*, *14*(1), 1670. https://doi.org/10.1038/s41598-024-51825-x

United Republic of Tanzania. (2024). *E-Government technology roadmap 2024* (Policy No. eGA/EXT/IRA/007; p. 37). e-Government Authority. https://www.ega.go.tz/uploads/standarddocuments/sw-1710314957-SIGNED%20e-Government%20Technology%20Roadmap%202024%20(1).pdf

Venkatesh, Morris, Davis, & Davis. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Wang, X., Li, Y., Khasraghi, H. J., & Trumbach, C. (2023). The mediating role of security anxiety in internet threat avoidance behavior. *Computers & Security*, *134*, 103429. https://doi.org/10.1016/j.cose.2023.103429

Xin, T., Siponen, M., & Chen, S. (2022). Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. *Behaviour & Information Technology*, *41*(13), 2835–2859. https://doi.org/10.1080/0144929X.2021.1954242

Yamane, T. (1967). *Statistics: An Introductory Analysis.pdf* (2nd ed.). Harper & Row and John Weatherhill Inc.

Yousuf, H., Al-Emran, M., & Shaalan, K. (2023). Evaluating individuals' cybersecurity behavior in mobile payment contactless technologies: Extending TPB with cybersecurity awareness. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (Vol. 14045, pp. 542–554). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35822-7_35

https://doi.org/10.24191/jcrinn.v11i1.583