Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666

Volume 10 Issue 41 (December 2025) PP. 440-459
DOI: 10.35631/JISTM.1041028

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

GLOBAL ACADEMIC EXCELLENCE

IT ADAPTABILITY AS A CATALYST OF PLANNED CYBER THREATS AVOIDANCE BEHAVIOUR: A MODERATED MEDIATION ANALYSIS

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

[1] Faculty of ICT, Department of Information Systems, Universiti Tunku Abdulrahman, Malaysia
Email: frank.sengati@gmail.com
[2] Faculty of ICT, Department of Information Systems, Universiti Tunku Abdulrahman, Malaysia
Email: abdulkarim@utar.edu.my
[3] Faculty of ICT, Department of Information Systems, Universiti Tunku Abdulrahman, Malaysia
Email: rameshkumar@utar.edu.my
[4] Faculty of Economics and Finance, Department of Economics, Universiti Tunku Abdulrahman, Malaysia
Email: abdelhak@utar.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 30.10.2025
Revised date: 11.11.2025
Accepted date: 21.12.2025
Published date: 31.12.2025

To cite this document:

Sengati, F., Kanaan, A. M. J., Ayyasamy, R. K. & Senadjki, A. (2025). It Adaptability as A Catalyst of Planned Cyber Threats Avoidance Behaviour: A Moderated Mediation Analysis. *Journal of Information System and Technology Management, 10* (41), 440-459.

DOI: 10.35631/JISTM.1041028

Abstract:

This study addresses the weak intention-behavior gap in dynamic threat environment such as the internet. Specifically, we examine the role of IT adaptability in enhancing the translation of cybersecurity intention to cybersecurity behavior across public sector employees. We build from the Theory of Planned Behavior (TPB), Technology Threat Avoidance Theory (TTAT), and Coping Model of User Adaptation to examines planned cyber threats avoidance behavior among 558 sampled public sector employees. A moderated mediation analysis evaluates how Avoidance Attitude (AA), Subjective Norms (SNO), and Self-efficacy (SEFF) influences Avoidance Intention (AI) and Avoidance Behavior (AB) with ITA as both a direct predictor and a moderator of AI-AB relationship. Results show that AA, SNO, and SEFF influences AI. Both AI and ITA directly predict AB. ITA strengthen the effect on AI-AB association. At higher levels of ITA, the conditional indirect effects were statistically significant. Our model explains 58.9% of variance in AB. These results extend TPB by emphasizing adaptability as a catalyst that translate security intentions into security behaviors. The findings of the study have important contribution to researchers and practitioners in the area of behavioral cybersecurity as empirical evidence for nurturing adaptive cybersecurity behaviors in an ever-changing IT environment are provided.

Keywords:

Cybersecurity Behaviour, IT Adaptability, Public Sector, Threat Avoidance, Moderated Mediation

Introduction

According to World Economic Forum (2025) and European Union Agency for Cybersecurity (2024) there is a growing trend in number, potency, and complexity of cyber threats that targets both organizations and individuals. Despite the heavy investments undertaken by organizations to secure their digital assets (World Economic Forum 2025), human behavior remains a critical weakness and oftentimes termed as “weakest link” in cybersecurity domain (Maalem Lahcen et al. 2020). This situation is critical in developing economies where public sector is characterized by insufficient resources, weak cyber security infrastructure, and low awareness (Ghelerter et al. 2022) and (Creese, Dutton, and Esteve-González 2021). In many circumstances, users hold positive intentions to avoid threats but fails to convert the intentions into consistent protective behaviors. This is a known challenge in the behavioral cybersecurity literature (Jenkins, Durcikova, and Nunamaker 2021), (Conner and Norman 2022) and (Mattson, Aurigemma, and Ren 2023). We posit that the inability to act even with intentions is attributed to individual’s IT-related inflexibility given the contemporary dynamism in cyber threats.

The Theory of Planned Behavior (TPB) argues that attitude towards behavior, subjective norms, and perceived behavioral control influence intention formation which in turn predict actual behavior (Hagger and Hamilton 2025) and (Alanazi, Freeman, and Tootell 2022). In behavioral cybersecurity literature, TPB has been used extensively to evaluate positive behavioral cybersecurity intentions as well as security policy compliance (Sommestad, Karlzén, and Hallberg 2019). However, TPB alone cannot entirely explain variances in actual cybersecurity behavior and in particular when users are faced with changing IT environment. Contemporary reviews on the utilization of TPB indicate a substantial amount of variance unexplained in behavioral cybersecurity and thus hinging on sufficiency premise that is challenged in environments that are dynamic (Sommestad et al. 2019). In behavioral cybersecurity literature, authors have oftentimes integrate the base theory with additional constructs in order to extend its explainability or capture unexplained variances (Alsharida et al. 2023), and (Prabhu and Dell 2025).

Technology Threat Avoidance Theory (TTAT) enriches the understanding of threat avoidance behavior through threat and coping appraisals as determinants of avoidance motivation and behavior. TTAT posits that users evaluate both magnitude of impact and likelihood of occurrence of a threat (threat appraisal) and their ability, cost, and efficacy of the safeguard measure (coping appraisal) before intending to avoid (Alsharida et al. 2025). Borgert *et al.*, (2024), Kiran *et al.*, (2025), and Simon *et al.*, (2025) have confirmed that self-efficacy and safeguard effectiveness of the coping appraisal are strong predictors of security behaviors.

Even with the strongest motivation, in real world scenarios behavior oftentimes falls short. In this paper, we argue that IT Adaptability serves as an important lever that bridge intention and action. We construe IT adaptability as individual’s willingness and ability to change own’s knowledge, skills, and behaviors in response to evolving IT threats (Gundu 2024). The premise of the Coping Model of User Adaptation (CMUA) argues that users’ response to IT events passes through cognitive appraisal and adaptive coping strategies (Stacey et al. 2021). Adaptation behaviors such as reconfiguring security features and learning new security routine assist users to form intentions even under changing threat landscape.

Previous behavioral cybersecurity literature emphasizes the importance of adaptation strategies. For example, Bala and Venkatesh (2016) posits that technology adaptation after implementation of IT is linked to users' coping and resource evaluation. (Gößwein and Liebherr 2025) and (Sony and Mekoth 2022) have shown that adaptation behaviors enhances effective use of IT systems. In the context of behavioral cybersecurity, this suggest that higher levels of IT adaptability are likely to avoidance intention into actual avoidance behavior even when threat parameters such as tools, tactics, and risks are evolving.

In this study we integrate TPB, TTAT, and CMUA to propose a moderated mediation model of cyber threats avoidance. Specifically, TPB provides the intention-motivation pathways that explain how individuals form readiness to act while TTAT compliment this by framing threat avoidance as an appraisal-coping process. We examine IT users' avoidance attitudes, subjective norms, and self-efficacy influences avoidance intention that predicts avoidance behavior with IT adaptability shaping both a direct interaction to avoidance behavior and moderating intention-behavior relationship. We posit that under higher levels of IT adaptability, the indirect effects of avoidance attitude, subjective norms, and self-efficacy on avoidance behavior via avoidance intention will be stronger.

Our contribution has three distinct dimensions. In the first place we extend the TPB and TTAT by including adaptability in an attempt to address the intention-behavior gap. While we agree the extent to which TPB/TTAT models intention, we argue that a threat-rich dynamic environment such as the internet requires a dynamic vigilance that translate intentions to behavior. ITA is built over individual-adaptation research as ability and willingness to adjust knowledge, behaviors, and skills in response to IT environment changes. We then empirically evaluate the dual role of IT adaptability in behavioral cybersecurity context; first as a direct driver of behavior and second as a moderator of intention-behavior gap and thus advancing the conditional process of cyber threats avoidance.

The remaining part of the paper has five sections. Section two begin by developing the theoretical basis, hypothesis derivation, and model description. Section three we present brief methodology with measures and analysis approach. Reporting of results is presented in section four while section five discusses research implications and opportunities for future work. The last section concludes with theoretical and practical recommendations and limitations.

Theoretical Framework and Hypotheses Formulation

Theory of Planned Behaviour

The Theory of Planned Behavior is firmly found on the idea that human behavior can be predicted through its intention. Furthermore, intention is determined by three antecedents namely attitude towards behavior, subjective norms, and perceived behavioral control (Ajzen 2020). Behavioral, normative, and control beliefs shape the attitude, subjective norms, and the perceived behavioral control respectively. These together forms the intentions to act and in turn predict the actual behavior. Attitude reflect individual's positive or negative evaluations of performing a required behavior, subjective norms refer to the perceived expectations from significant others about performing a required behavior, and lastly perceived behavioral control indicates to the perceived difficulty of performing a required behavior (Bosnjak, Ajzen, and Schmidt 2020). In behavioral cybersecurity literature, TPB has been used extensively to predict individual behaviors such as secure password use, security policy compliance, and phishing resistance (AlGhanboosi, Ali, and Tarhini 2023) and Hong and Furnell (2021).

Alsharida *et al.*, (2023) noted that TPB is hinged on "sufficiency assumption" and this restrictive nature has seen the theory's ability to account for unexplained variances in behavior increase. The "sufficient assumptions" asserts that only attitude, subjective norms, and perceived behavioral control are enough to account for behavioral intention and actual behaviors. In real life scenario, this premise do not account for other significant contextual, emotional, or situational predictors (Ajzen 2020) and (Sommestad et al. 2019).

In operationalization of TPB studies, self-efficacy and perceived behavioral control (PBC) are often used interchangeably. PBC is construed as a higher order construct comprising of both self-efficacy as individual confidence in own's ability and controllability related to external constraints. From the lens of (Hagger and Hamilton 2025) and (Guo et al. 2023), self-efficacy is the core arm of the PBC and many behavioral literature assess PBC from self-efficacy lens. Meta-analytic evidences have shown that PBC/self-efficacy have the ability to predict intention and behavior over attitude and norms (Armitage and Conner 2001). On the other hand, Fishbein and Ajzen (2011) highlights that in practice researchers have been emphasizing self-efficacy when evaluating PBC as capability often overpower external constraints in explaining variances in behavior.

Behavioral cybersecurity literature has shown that attitude and subjective norms predict behavioral intentions. Individual's positive assessment of avoidance actions and strong normative influence from significant others such as supervisors, professionals, and peers tends to coerce individuals to intend to comply with security policies. Moreover, individuals with higher levels of self-efficacy have strong positive intentions and actual behaviors as they believe on their ability to carry out a required security behavior (Ajzen 2020), (Borgert et al. 2024), and (Haag, Siponen, and Liu 2021). It is from this perspective we hypothesize that:

H1: Avoidance attitude has a positive effect on avoidance intention
H2: Subjective norms have positive effect on avoidance intention

Technology Threat Avoidance Theory

Proposed by Liang and Xue (2009), the Technology Threat Avoidance Theory (TTAT) explain how individuals respond to information technology-related threat through their cognitive appraisal of the threat and their coping capacity. At the beginning individuals assess the magnitude of the impact and the likelihood of threat occurrence and then evaluate their ability to effectively respond in order to eliminate or minimize the threat, the efficacy of the safeguard measure, and the related cost of executing the required behavior. These two are namely threat and coping appraisal respectively. Consequently, appraisals influence avoidance motivation which in turn predict the performance of the required protective behavior given availability of needed resources. TTAT underscores the significance of perceived severity, susceptibility, response efficacy, self-efficacy, and cost as determinants of avoidance intention (Carpenter et al. 2019).

In behavioral cybersecurity research, TTAT supplement TPB through emphasizing coping beliefs. In particular self-efficacy and perceived response efficacy as significant predictors of protective behavior. Review of recent studies has demonstrated that individuals with higher levels of own's confidence in their ability to execute a protective measure as well as a strong belief on the efficacy of the safeguard measure to be executed are more likely to avoid information technology-related threats (Kiran et al. 2025), (Borgert et al. 2024), and (Wang et al. 2023). It is from this convergent thinking we hypothesize that:

H3a: Self-efficacy has a positive effect on avoidance intention
H3b: Self-efficacy has a positive effect on avoidance behavior
H4: Avoidance intention has a positive effect on avoidance behavior

Coping Model of User Adaptation

The Coping Model of User Adaptation (CMUA) enables us to understand cognitive, relational, and process approach through which an individual go through during IT adaptation. Proposed by Beaudry and Pinsonneault (2001) the theory asserts that individual adaptation is a mental and behavioral effort exerted by user to manage consequences of IT event. We deduce therefore that during adaptation individuals can either invoke emotional focused coping or problem focused coping. Similarly, what an individual do during adaptation is a function of how much they are in control of the situation. The approach coping unlike the avoidance coping focuses on solving the problem and behaviors such as modifying IT, personalizing IT, learning new skill, or seeking social support can be manifested.

We construe IT adaptability to include cognitive, behavioral, and emotional adjustments that allow individuals to align their knowledge, skills, behaviors, and work practices with the evolving cyber risks. Recent literature has shown the extent to which adaptation enhances effective use and resilience in changing IT environments (Salo, Makkonen, and Hekkala 2020). Individuals who are more adaptable can easily enact protective behaviors and to comfortably surpasses the limitations that may hinder the execution of the required behavior. Thus, IT adaptability is expected to have direct positive influence on avoidance behavior as well as strengthening the relationship between avoidance intention and avoidance behavior. Accordingly, we postulate that:

H5: IT adaptability has a positive effect on avoidance behavior
H6: IT adaptability positively moderates the relationship between avoidance intention and avoidance behavior.

In this study, all the predictors namely avoidance attitude, subjective norms, and self-efficacy influences avoidance behavior indirectly via avoidance intention. However, the effect of these indirect influences is conditioned on IT adaptability. The proposed antecedents shape intention while at the same time IT adaptability modifies to what extent avoidance intentions translate to avoidance behavior. This conditional process model reflects the complexity of behavioral cybersecurity particularly on cyber threats avoidance where not all individuals with enough intentions will take actions unless they possess adaptive capacity (Hayes 2018). See Figure 1 for theoretical framework.

We therefore posit that the indirect influences of avoidance attitude, subjective norms, and self-efficacy on avoidance behavior through avoidance intention will be stronger when IT adaptability is higher. Specifically, we postulate that:

H7a: The indirect effect of avoidance attitude on avoidance behavior via avoidance intention is stronger when IT adaptability is higher
H7b: The indirect effect of subjective norms on avoidance behavior via avoidance intention is stronger when IT adaptability is higher
H7c: The indirect effect of self-efficacy on avoidance behavior via avoidance intention is stronger when IT adaptability is higher

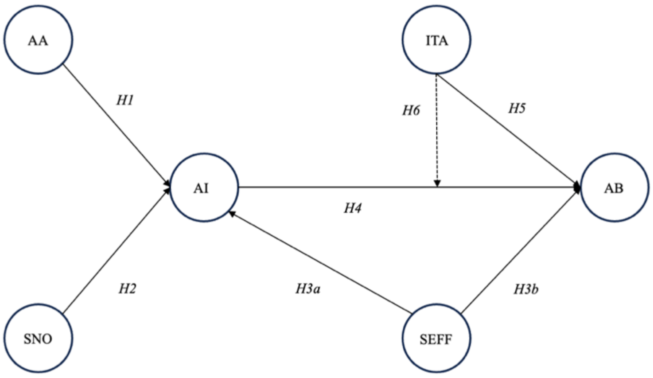

Figure 1: Theoretical Framework
Source: Authors
Note(s): AA – Avoidance Attitude; SNO – Subjective Norms; AI – Avoidance Intention; SEFF – Self-efficacy; ITA – IT adaptability; AB – Avoidance behavior
Source: Authors

Methodology

Survey Development, Sampling and Participants

This study used quantitative cross section survey approach to assess the hypothesized moderated mediation model. Research data were collected from public sector employees. The approach selected is consistent with the contemporary behavioural cybersecurity literature such as Hong and Furnell (2021) and Alsharida *et al.*, (2023) that make use of large scale survey data to evaluate structural models. The public sector is comprised of Ministries, Departments, and Agencies (MDAs) where sample was drawn and thus supporting generalizability within the public sector. Proportional stratified sampling approach was adopted to draw respondents as research participants. We targeted respondents with over two years of job experience and who uses computing devices connected to the internet for their official day to day activities.

Measurements

A structured validated questionnaire that was adapted from past behavioral cybersecurity research was employed as a survey instrument. All measurement items were adapted and adopted to suit the core tenets of this study. Avoidance attitude was operationalized from Venkatesh *et al.*, (2003) while self-efficacy and subjective norms were adapted from Wang *et al.*, (2023) and Tsai *et al.*, (2016) respectively. Measurement items for avoidance intention and avoidance behavior were adapted from the same source (Liang and Xue 2010). Lastly, IT adaptability measurement instrument were operationalized from Heijde and Van Der Heijden, (2006). The survey instrument was made up of all research constructs measured on a 7-point Likert scale ranging from 1 = strongly disagree to 7 = strongly agree. The instrument further incorporated demographic data such as gender, age group, education level, possession of formal ICT training, job experience, and MDA Type. We established content validity for the revised questionnaire as per Polit *et al.*, (2007) through computation of content validity index (CVI) across six subject matter experts. The adapted research tool achieved an S-CVI/Ave value of 0.95 above the 0.83 cut-off point.

Partial Least Square Structural Equation Modeling (PLS-SEM) analyzed the proposed associations among constructs of interest. PLS-SEM was preferred due to its ability to evaluate models with mediation and moderation paths, its ability to handle small sample size, as well as its suitability in non-normality data circumstances (Hair and Alamer 2022). The analysis was performed using SMARTPLS v 4. Confirmatory Factor Analysis (CFA) verified the content validity cut off value of >=.50 (Hair and Alamer 2022). Discriminant validity was evaluated using the HTMT ratio of correlation and Fornell Larcker benchmarks (Fornell and Larcker 1981). Furthermore, we assessed convergent validity using composite reliability and average variance extracted aiming for 0.70 and 0.50 respectively (Hair and Alamer 2022). Reliability was assessed with Cronbach's Alpha value of 0.70 (Hair et al. 2017).

Data Analysis and Results

Among the 650 questionnaires sent to respondents across all MDAs, this study managed to collect back a total of 558 completed and valid responses. This is equivalent to a response rate of 85.4%. Regarding gender, this researcher managed to collect data from 324 males that accounts for 58.1% and 234 females that accounts for 41.9% of respondents indicating a fairly well distribution of all gender across the entire sample given the sampling technique used. In terms of age group, respondents were distributed as follows: 51 (9.1%) were the youngest group aged between 18 and 25 years, 126 (22.6%) of respondents were aged between 26 and 33 years, 156 (28.0%) of respondents were between 34 and 41 years old, 155 (27.8%) of respondents aged between 42 and 49 years, and the last group that accounted for respondents with 50 years and above were 70 equivalent to 12.5%.

Most of the respondents had an educational level of diploma or equivalent qualification accounting for 144 (25.8%) followed by masters' degree holder who were 135 (24.2%). Graduates who possess first degree as their highest education level were 133 (23.8%), those with third degree as highest education level accounted for 48 (8.6%) of all respondents while for advanced secondary education and ordinary secondary education were 57 (10.2%) and 41 (7.3%) respectively. The distribution of responses from across all major educational level reflect the representation of the Tanzania public sector employees.

Data showed that respondents with formal ICT training were 270 equivalents to 48.4% of all respondents while those without formal ICT training were 288 equivalents to 51.6%. It was important that the profile of respondents to contain both categories in order to reflect different characteristics of the respondents. Of all respondents, those with between 8 and 10 years of experience in the public sector were 167 (29.9%), followed by respondents with experience of 10 years and above 157 (28.1%). Those with experience between 5 and 7 years were 138 (24.7%) and lastly between 2 and 4 years were 96 (17.2%). This kind of distribution of respondents showed that first all respondents had enough experienced to participate in the research, and second that public sector employees of varying age groups have been well represented in the sample.

The researcher collected data from all MDAs to ensure representation of the profile of the public sector. Data indicated that majority of respondents emanated from authorities, ministries and independent departments represented by 77 (13.8%),76 (13.6%), and 71 (12.7%) respectively. Further, agencies had 57 (10.2%) respondents, funds had 28 (5.0%) respondents, institutes had 46 (8.2%) respondents, boards had 59 (10.6%) of respondents, council had 42 (7.5%) of respondents, commissions had 55 (9.9%) of respondents, government companies were represented by 19 respondents equivalent to 3.4% and finally corporations had 28 respondents equivalent to 5.0%. See Table 1 for descriptive statistics

Table 1: Summary of Demographic Characteristics of the Respondents

Category	f	%	Category	f	%
Gender			*Job Experience*		
Male	*324*	*58.1*	Between 2 and 4 years	*96*	*17.2*
Female	*234*	*41.9*	Between 5 and 7 years	*138*	*24.7*
Age Group			Between 8 and 10 years	*167*	*29.9*
18 – 25 years	*51*	*9.1*	Over 10 years	*157*	*28.1*
26 – 33 years	*126*	*22.6*	*MDA Type*		
34 – 41 years	*156*	*28.0*	Ministries	*76*	*13.6*
42 – 49 years	*155*	*27.8*	Independent departments	*71*	*12.7*
50 years and above	*70*	*12.5*	Authorities	*77*	*13.8*
Education Level			Agencies	*57*	*10.2*
O' Level	*41*	*7.3*	Funds	*28*	*5.0*
A' Level	*57*	*10.2*	Institutes	*46*	*8.2*
Diploma or equivalent	*144*	*25.8*	Boards	*59*	*10.6*
Degree or equivalent	*108*	*24.1*	Councils	*42*	*7.5*
Masters' degree	*135*	*24.2*	Commissions	*55*	*9.9*
Doctorate degree	*48*	*8.6*	Government companies	*19*	*3.4*
Possession of ICT Certification			Corporations	*28*	*5.0*
Yes	*270*	*48.4*			
No	*288*	*51.6*			

Source: Authors

We followed the descriptive analysis of demographic data with research constructs. During measurement model assessment, only SNO1 loaded low at 0.206 and it was eliminated. Final outer loadings are presented in Table 2. This assessment included reliability and validity tests and examination of common method bias. We concluded the analysis with structural model evaluation and hypothesis testing and verification.

Table 2: Descriptive Statistics, Factor Analysis and Reliability Test

Construct	Items	Factor Loading	Mean	SD	α	CR	AVE
Avoidance Attitude (AA)	AITA1	0.899	4.409	1.596	0.929	0.949	0.823
	AITA2	0.919					
	AITA3	0.902					
	AITA4	0.908					
IT Adaptability (ITA)	ITA1	0.850	3.599	1.548	0.937	0.948	0.694
	ITA2	0.875					

	ITA3	0.835					
	ITA4	0.859					
	ITA5	0.839					
	ITA6	0.792					
	ITA7	0.807					
	ITA8	0.803					
Avoidance Behavior (AB)	ITAB1	0.917	3.769	1.296	0.773	0.898	0.814
	ITAB2	0.888					
Avoidance Intention (AI)	ITAI1	0.883	4.586	1.388	0.792	0.880	0.711
	ITAI2	0.898					
	ITAI3	0.739					
Self-efficacy (SEFF)	SEFF1	0.784	4.215	1.268	0.930	0.943	0.702
	SEFF2	0.754					
	SEFF3	0.778					
	SEFF4	0.896					
	SEFF5	0.894					
	SEFF6	0.875					
	SEFF7	0.871					
Subjective Norms (SNO)	SNO2	0.941	4.336	1.049	0.861	0.935	0.878
	SNO3	0.933					

Source: Authors
Note(s): Scale 1 – Strongly Disagree; 2 – Strongly Agree

To assess global model fit, we took into consideration several indices. We present both standardized root mean square residual (SRMR), unweighted least squares discrepancy (d_ULS), geodesic discrepancy (d_G), Chi-square, and normed fit index (NFI) each serving as a complimentary purpose. The SRMR (0.075) was below 0.08 threshold, indicating acceptable fit (Henseler, Hubona, and Ray 2016). Both d_ULS (1.973) and d_G (0.966) statistical values were small indicating limited differences between empirical and model implied covariance matrices. The result of Chi-square statistic were significant (χ^2 = 3139.988), a common occurrence with large sample sizes (Hair and Alamer 2022). The NFI recorded 0.763 below the required threshold of 0.90. While this result showed that the proposed model has not achieved acceptable comparative fit specifically with the NFI, our study prioritized prediction nature of PLS-SEM thus positioning SRMR and predictive statistic such as Q^2 and PLSpredict over the CB-SEM comparative indices as more appropriate criteria (Henseler 2017), (Ogbeibu et al. 2021), (Hu and Bentler 1999) and (Sarstedt et al. 2016).

Internal consistency was evaluated using Cronbach's alpha and it reflects instrument's reliability. The reliability test revealed that all Cronbach's alpha were above the threshold of 0.7 which demonstrate reliable internal consistency. These values are shown in Table 2. All Composite Reliability (CR) values exceeded 0.880 further demonstrating strong internal consistency. As it can be seen from Table 2, the measurement items' convergent validity was assessed through the item's outer loading threshold of 0.7 or 0.4 (Hair and Alamer 2022). Our results' lowest factor loading was 0.739. The square root of the Average Variance Extracted (AVE) values reported higher than its correlation with another factor (Fornell and Larcker 1981). Discriminant validity was confirmed through the results of HTMT ratios that are below 0.90 (Henseler et al. 2016). We summarize the results of HTMT ratios in Table 3.

Table 3: Descriptive Heterotrait-Monotrait (HTMT) Ratio

Construct	AA	ITA	AB	AI	SEFF	SNO
AA	-					
ITA	0.504	-				
AB	0.687	0.850	-			
AI	0.596	0.622	0.729	-		
SEFF	0.156	0.159	0.192	0.558	-	
SNO	0.772	0.552	0.672	0.627	0.169	-

Source: Authors

Structural model was assessed through bootstrapping procedure with 10000 samples (Streukens and Leroi-Werelds 2016), (Kline 2016). The results of the structural paths exhibited substantial support to the hypothesized relationships. Avoidance attitude H1 (AA) significantly influenced avoidance intention (β = 0.278, t = 6.498, p < 0.001). We noted the same positive influence with subjective norms H2 towards avoidance intention (β = 0.263, t = 6.137, p < 0.001). Self-efficacy H3a showed strongly predictive positive influence on avoidance intention (β = 0.415, t = 14.106, p < 0.001) but exhibited partial significant negative effect on avoidance behavior H3b (β = -0.051, t = 1.470, p < 0.1) suggesting a weak negative effect. On the other hand, avoidance intention H4 positively influences avoidance behavior with β = 0.322, t = 8.618, p < 0.001. IT adaptability strongly and positively predicted avoidance behavior H5 (β = 0.552, t = 15.468, p < 0.001) positioning itself as a strong determinant of avoidance behavior. We examined the moderating effect of IT adaptability and results indicated that the interaction path was positive and partial significant H6 (β = 0.066, t = 1.545, p < 0.1) hence supporting the partial moderation at the 10% confidence level (Jr et al. 2017). These results are summarized in Table 4.

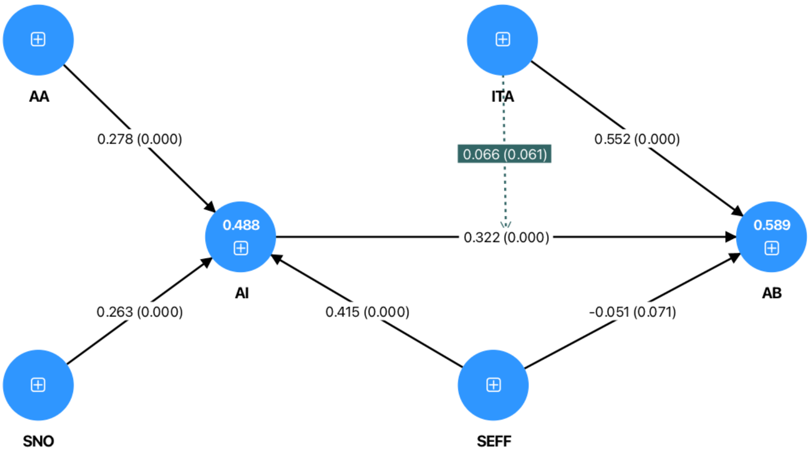

Figure 2: Bootstrapping Results (Path Coefficient and P Values)

Source: Authors

Our moderated mediation assessment show that indices value for IT adaptability mediation effect is positive. For the path avoidance attitude through avoidance intention towards avoidance behavior the values were [index = 0.019, SE = 0.012, 95%CI = (-0.000, 0.040)]. At higher levels of IT adaptability, the indirect effect of AA on AB through AI (β = 0.108, t = 4.068, p < 0.001) was stronger than at mean (β = 0.090, t = 4.861, p < 0.001) and at lower levels (β = 0.071, t = 4.242, p < 0.001). The same pattern is reported in the path subjective norms through avoidance intention towards avoidance behavior [index = 0.018, SE = 0.011, 95%CI = (-0.000, 0.038]. At higher levels of IT adaptability, the indirect effect of SN on AB through AI (β = 0.102, t = 4.070, p < 0.001) was stronger than at mean (β = 0.085, t = 4.916, p < 0.001) and at low IT adaptability (β = 0.067, t = 4.287, p < 0.001). Lastly, effect of self-efficacy on avoidance behavior via avoidance intention [index = 0.028, SE = 0.017, 95%CI = (-0.000, 0.057)] was stronger (β = 0.161, t = 5.251, p < 0.001) than both at mean levels of IT adaptability (β = 0.133, t = 6.889, p < 0.001) and lower levels (β = 0.106, t = 5.118, p < 0.001). Thus, hypothesis 7a-c are supported and corresponding conditional indirect effects and index of moderation are summarized in Table 5 and 6 respectively.

Table 4: Hypothesis Testing Results and Effect Sizes

Hypothesis	Path	β	T-value	p-value	Supported	Effect size
H1	AA → AI	0.278	6.498	***	Yes	Small
H2	SNO → AI	0.263	6.137	***	Yes	Small
H3a	SEFF → AI	0.415	14.106	***	Yes	Large
H3b	SEFF → AB	-0.051	1.470	*	No	Trivial
H4	AI → AB	0.322	8.618	***	Yes	Medium
H5	ITA → AB	0.552	15.468	***	Yes	Large
H6	ITA * AI → AB	0.066	1.545	*	Yes	Small

Source: Authors
Note(s): *** p < 0.001; ** p < 0.05; * p<0.1

We rely on the works of Beaudry and Pinsonneault (2001) to provide a classification of "small", "medium", and "large" effect size to correspond to f^2 values of 0.02, 0.15, and 0.35 respectively for direct effects while for moderation effect Hair *et al.,* (2022) classify "small", "medium", and "large" effect size to correspond to f^2 values of 0.005, 0.010, and 0.025 respectively. Results showed that effect size for ITA → AB (0.439) and SEFF → AI (0.326) were large followed by medium effect size for AI → AB (0.135) while AA → AI and SNO → AI exhibited small effect sizes of 0.079 and 0.071 respectively. Result for SEFF → AB was insignificant and trivial (0.004). For the moderation effect, even though significant the effect size was small (0.006). Consistent with behavioral cybersecurity literature, effect sizes observed were small yet significant as intentions and behaviours are determined by multiple concurrent cognitive, emotional, social, and contextual influences (Mou et al. 2022), (de Bruin and Mersinas 2024). See Table 4 above for hypothesis testing result summary.

Table 5: Conditional Indirect Effects Under IT Adaptability Moderation

Path	Level	Effect	BootSE	BootLLCI	BootULCI
AA→AI→AB	-1SD	0.071	0.017	0.045	0.100
	Mean	0.090	0.018	0.061	0.122
	+1SD	0.108	0.026	0.068	0.155
SNO → AI → AB	-1SD	0.067	0.016	0.043	0.095
	Mean	0.085	0.017	0.059	0.115
	+1SD	0.102	0.025	0.065	0.148
SEFF → AI → AB	-1SD	0.106	0.021	0.074	0.142
	Mean	0.133	0.019	0.105	0.168
	+1SD	0.161	0.031	0.113	0.215

Source: Authors
Note(s): AA – Avoidance Attitude, AI – Avoidance Intention, AB – Avoidance Behavior, SNO – Subjective Norms, SEFF – Self-efficacy; SD – Standard Deviation, LLCI – Lower Limit Confidence Interval, and ULCI – Upper Limit Confidence Interval

Table 6: Index of Moderated Mediation

Moderator	Path	Index	BootSE	BootLLCI	BootULCI
IT Adaptability	AA → AI → AB	0.019	0.012	-0.000	0.040
	SNO → AI → AB	0.018	0.011	-0.000	0.038
	SEFF → AI → AB	0.028	0.017	-0.000	0.057

Source: Authors
Note(s): AA – Avoidance Attitude, AI – Avoidance Intention, AB – Avoidance Behavior, SNO – Subjective Norms, SEFF – Self-efficacy; SE – Standard Error, LLCI – Lower Limit Confidence Interval, and ULCI – Upper Limit Confidence Interval

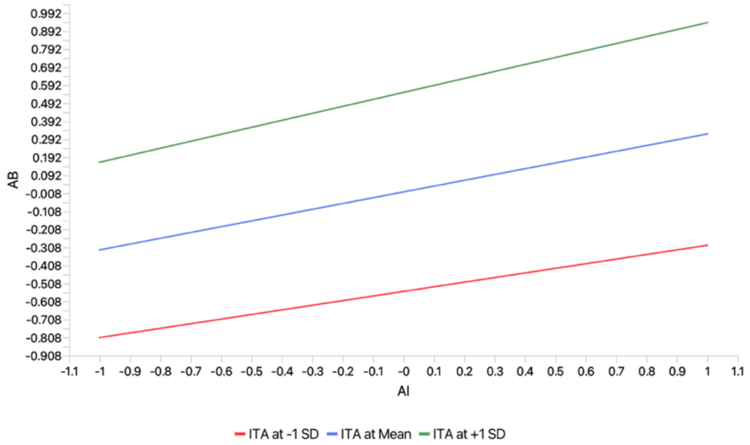

Figure 3: Moderating Effect of IT Adaptability on Avoidance Intention Towards Avoidance Behaviour

Source: Authors
Note(s): AB – Avoidance Behaviour; AI – Avoidance Intention; SD – Standard Deviation

We further examined the explanatory capability of the proposed model. The proposed model's explanatory capability recorded significant coefficient of determination for avoidance intention ($R^2 = 0.488$, $p < 0.001$) and avoidance behaviour recorded ($R^2 = 0.589$, $p < 0.001$) indicating variance explanation of 48.8% and 58.9% respectively. Interpreting from the lens of Hair *et al.*, (2019) this is a moderate explanatory power. See Table 7 for model's explanatory power.

Table 7: Model Explanatory Power

Endogenous Construct	R^2	Adjusted R^2	p value
Avoidance Intention	0.488	0.485	***
Avoidance Behavior	0.589	0.586	***

Source: Authors
Note(s): *** $p < 0.001$

Discussion

We examined how avoidance attitude, subjective norms, and self-efficacy influences cyber threats avoidance intention and behavior with IT adaptability as a moderator. Our findings have managed to demonstrate both hypothesized and nuanced results in explaining public sector employees' cybersecurity behavior.

Consistent with TPB, attitude, subjective norms, and self-efficacy meaningfully influence avoidance intention. Of all predictors of intention, self-efficacy was the strongest in congruence with Alsharida *et al.*, (2023), Almansoori *et al.*, (2023), and Chaudhary, (2024). Avoidance attitude and subjective norms likewise made notable contribution in line with the premise that both personal assessment and social pressures influence cybersecurity intentions (Gan, Lee, and Liew 2024) and (Stylianou et al. 2025). Avoidance intention remained a significant predictor of avoidance behavior (Ajzen 2020).

The role of IT adaptability is evidently highlighted influencing significantly avoidance behavior as a direct predictor. This finding concurs with CMUA's perspective that individual adaptive capacities permit problem-focused coping with dynamic information technology environment through development of adaptive behaviors, flexible skills, and knowledge (Nguyen and Ha 2021) and thus enabling effective threat avoidance. Within the boundaries of cyber threats, IT adaptability appears to function as a resource empowering employees not only to identify risks but also perform required avoidance behavior effectively. This suggests that adaptive competencies serve as critical enablers of behavior over and above the personal and social predictors identified in the TPB.

Notably, the conditional indirect effects of avoidance attitude, subjective norms, and self-efficacy on avoidance behavior through avoidance intention exhibited stronger characteristics at higher levels of IT adaptability. The moderation result revealed a more nuanced insight. The interaction role of IT adaptability on the relationship between avoidance intention and avoidance behavior appeared significant. Although modest, the interaction indicates partial moderation. However, the moderating influence of IT adaptability is likely partial in the public sector where hierarchical decision making, limited behavioural autonomy, and organizational rigidity limits employee's ability to convert intentions into actual behaviour even when adaptive capabilities are high denoting the superior role of structural controls over technology use and security practices. At higher levels of IT adaptability public sector employees' conversion of intention to behavior exhibit consistent characteristics. Recalling from Borgert *et al.*, (2024) & Klein and Zwilling, (2024a), both contextual or resource-based predictors have been documented to modify the strength of the intention-behavior relationship. This emphasizes the subtle but relevant and consistent role of IT adaptability in positively enhancing the intention-behavior relationship.

Self-efficacy exhibited negative partial significant influence on avoidance behavior. Prior literature has demonstrated how self-efficacy is able to directly shapes protective behavior (Borgert et al. 2024). Our results suggest that in the public sector context, self-efficacy functions positively through intentions and negatively through actual behavior. This can be attributed to structural constraints common in the public sector context in such a way that even though employees may feel confident in their abilities to carry out required cybersecurity behavior, they remain tied to organizational constraints such as organizational rigidity and centralized decision-making to defend their digital resources (Klein and Zwilling 2024b) and thus limiting their direct execution of behavior. Furthermore, Hagger *et al.*, (2022) & Hagger and Hamilton, (2024) indicates that belief in own's ability fuels intention more than actual behavior and in situations where frictions may emanate between employee and organization due to fatigue, workload (Kim and Kim 2024) or time pressure (Chowdhury, Adam, and Teubner 2020), self-confidence may stagnate and occasionally drift to overconfidence/inaction

(Fatoki, Shen, and Mora-Monge 2024), and (Ma and Chen 2023). This finding enriches behavioral cybersecurity literature by demonstrating that organizational settings can channel individual resources into intentions but not direct outcomes.

Finally, the modest coefficient of determination values for intention and behavior are common in social-behavioral models (Hair and Alamer 2022), (Hedayati et al. 2023), and (McEachan et al. 2016). Human behavior is influenced by multiple personal and contextual factors that may be difficult to model comprehensively. This means that the proposed model's explained variance is satisfactorily and consistent with the existing behavioral studies.

Conclusion, Implications, and Limitations

Conclusion

Our study advances the understanding of cyber threats avoidance behavior in the public sector by integrating IT adaptability into the Theory of Planned Behavior in tandem with Technology Threat Avoidance Theory and Coping Model of User Adaptation. Our results demonstrate that avoidance attitude, subjective norms, and self-efficacy significantly influence avoidance intentions. On the other hand, avoidance intentions and IT adaptability directly shapes avoidance behavior. Equally important is the moderating role of IT adaptability on the intention-behavior relationship. This moderation is further supported by robust conditional indirect effects. Together, these results demonstrate that while motivational levers are critical, IT adaptability functions as an important resource that empowers public sector employees to invoke cyber threats avoidance behavior in changing IT threat environments.

Implications

Theoretically, this study extends TPB by showing that in the context of cybersecurity behavior IT adaptability explains some intentions will likely be converted to actual behavior. This enrichment to TPB a provide coping and adaptation perspectives. Our results demonstrate that static cognitive behavioral models can be further extended through the additional of dynamic individual resources such as IT adaptability. Practically, our study emphasizes on the need to inculcate adaptability among public sector employees as their environment is characterized by structural constraints that may limit the direct effect of self-efficacy. Public sector entities can operationalize this by deploying adaptive security training modules that incorporate phishing simulations, role-based scenarios, and real-time feedback to empower employees' adaptive responses. In parallel decentralizing selected security-related decisions rights such as verification procedure, incident reporting, and access escalation may further enhance employees' intentions into concrete behavioral security actions.

Limitations

First our study utilized self-reported measures that may introduce bias and its reliance on Tanzania public sector employees may limit generalizability to other occupational or cultural dimensions. From theoretical point of view, the integration of TTAT and TPB inherits the rationality and deliberate decision-making assumptions potentially diminishing habitual or affective processes that may influence cybersecurity behavior. Furthermore, the moderating effect of IT adaptability exhibited marginal characteristic and hence its applicability in environment where employees have greater autonomy is unknown. These limitations provide plausible future endeavors through longitudinal, experimental, or intervention-based studies to further enhance the theoretical mechanisms and improve predictive validity of behavioral cybersecurity.

Acknowledgements

The authors would like to acknowledge and extended special thanks to Ministry of Planning and Finance United Republic of Tanzania through the Institute of Accountancy Arusha (IAA) and Universiti Tunku Abdulrahman Malaysia.

References

Ajzen, Icek. 2020. 'The Theory of Planned Behavior: Frequently Asked Questions'. *Human Behavior and Emerging Technologies* 2(4):314–24. doi:10.1002/hbe2.195.

Alanazi, Marfua, Mark Freeman, and Holly Tootell. 2022. 'Exploring the Factors That Influence the Cybersecurity Behaviors of Young Adults'. *Computers in Human Behavior* 136:107376. doi: 10.1016/j.chb.2022.107376.

AlGhanboosi, Basim, Saqib Ali, and Ali Tarhini. 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. doi: 10.1016/j.chb.2023.107702.

Almansoori, Afrah, Mostafa Al-Emran, and Khaled Shaalan. 2023. 'Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories'. *Applied Sciences* 13(9):5700. doi:10.3390/app13095700.

Alsharida, Rawan A., Bander Ali Saleh Al-rimy, Mostafa Al-Emran, Mohammed A. Al-Sharafi, and Anazida Zainal. 2025. 'Predicting Cybersecurity Behaviors in the Metaverse through the Lenses of TTAT and TPB: A Hybrid SEM-ANN Approach'. *Online Information Review*. doi:10.1108/OIR-08-2023-0425.

Alsharida, Rawan A., Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. 'A Systematic Review of Multi Perspectives on Human Cybersecurity Behavior'. *Technology in Society* 73:102258. doi: 10.1016/j.techsoc.2023.102258.

Armitage, Christopher J., and Mark Conner. 2001. 'Efficacy of the Theory of Planned Behaviour: A Meta-analytic Review'. *British Journal of Social Psychology* 40(4):471–99. doi:10.1348/014466601164939.

Bala, Hillol, and Viswanath Venkatesh. 2016. 'Adaptation to Information Technology: A Holistic Nomological Network from Implementation to Job Outcomes'. *Management Science* 62(1):156–79. doi:10.1287/mnsc.2014.2111.

Beaudry, Anne, and Alain Pinsonneault. 2001. 'IT-Induced Adaptation and Individual Performance: A Coping Acts Model'. in *ICIS 2001 Proceedings*. Vol. 58. International Conference on Information Systems.

Borgert, Nele, Luisa Jansen, Imke Böse, Jennifer Friedauer, M. Angela Sasse, and Malte Elson. 2024. 'Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods'. Pp. 1–32 in *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM.

Bosnjak, Michael, Icek Ajzen, and Peter Schmidt. 2020. 'The Theory of Planned Behavior: Selected Recent Advances and Applications'. *Europe's Journal of Psychology* 16(3):352–56. doi:10.5964/ejop. v16i3.3107.

de Bruin, Marten, and Konstantinos Mersinas. 2024. 'Individual and Contextual Variables of Cyber Security Behaviour -- An Empirical Analysis of National Culture, Industry, Organisation, and Individual Variables of (in)Secure Human Behaviour'.

Carpenter, Darrell, Diana K. Young, Paul Barrett, and Alexander J. McLeod. 2019. 'Refining Technology Threat Avoidance Theory'. *Communications of the Association for Information Systems* 380–407. doi:10.17705/1CAIS.04422.

Chaudhary, Sunil. 2024. 'Driving Behaviour Change with Cybersecurity Awareness'. *Computers & Security* 142:103858. doi: 10.1016/j.cose.2024.103858.

Chowdhury, Noman H., Marc T. P. Adam, and Timm Teubner. 2020. 'Time Pressure in Human Cybersecurity Behavior: Theoretical Framework and Countermeasures'. *Computers & Security* 97:101963. doi: 10.1016/j.cose.2020.101963.

Conner, Mark, and Paul Norman. 2022. 'Understanding the Intention-Behavior Gap: The Role of Intention Strength'. *Frontiers in Psychology* 13:923464. doi:10.3389/fpsyg.2022.923464.

Creese, Sadie, William H. Dutton, and Patricia Esteve-González. 2021. 'The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions'. *Personal and Ubiquitous Computing* 25(5):941–55. doi:10.1007/s00779-021-01569-6.

European Union Agency for Cybersecurity. 2024. *ENISA Threat Landscape 2024: July 2023 to June 2024.* LU: Publications Office.

Fatoki, Jimoh G., Zixing Shen, and Carlo A. Mora-Monge. 2024. 'Optimism amid Risk: How Non-IT Employees' Beliefs Affect Cybersecurity Behavior'. *Computers & Security* 141:103812. doi: 10.1016/j.cose.2024.103812.

Fishbein, Martin, and Icek Ajzen. 2011. *Predicting and Changing Behavior*. Psychology Press.

Fornell, C., and D. F. Larcker. 1981. 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error'. *JOURNAL OF MARKETING RESEARCH* 18(1):39–50.

Gan, Chin Lay, Yi Yong Lee, and Tze Wei Liew. 2024. 'Fishing for Phishy Messages: Predicting Phishing Susceptibility through the Lens of Cyber-Routine Activities Theory and Heuristic-Systematic Model'. *Humanities and Social Sciences Communications* 11(1):1552. doi:10.1057/s41599-024-04083-1.

Ghelerter, David, John Wilson, Noah Welch, and John-David Rusk. 2022. 'Cybercrime in the Developing World'.

Gößwein, Eva, and Magnus Liebherr. 2025. 'Embracing Change in the Modern Working Environment: Exploring the Role of Trust, Experimentation, and Adaptability in the Acceptance of New Technologies'. *Sage Open* 15(1):21582440241311126. doi:10.1177/21582440241311126.

Gundu, Tapiwa. 2024. 'Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model'. *International Conference on Cyber Warfare and Security* 19(1):95–102. doi:10.34190/iccws.19.1.2177.

Guo, Jong-Long, Ying-Chieh Chang, Fen-He Lin, Ching-Chih Fan, Tzu-Ming Lai, and Chiu-Mieh Huang. 2023. 'User Experience Evaluation of a 3D Virtual Reality Educational Program for Illegal Drug Use Prevention among High School Students: Applying the Decomposed Theory of Planned Behavior'. *DIGITAL HEALTH* 9:20552076231171237. doi:10.1177/20552076231171237.

Haag, Steffi, Mikko Siponen, and Fufan Liu. 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. doi:10.1145/3462766.3462770.

Hagger, Martin S., Mike W. L. Cheung, Icek Ajzen, and Kyra Hamilton. 2022. 'Perceived Behavioral Control Moderating Effects in the Theory of Planned Behavior: A Meta-Analysis.' *Health Psychology* 41(2):155–67. doi:10.1037/hea0001153.

Hagger, Martin S., and Kyra Hamilton. 2024. 'Longitudinal Tests of the Theory of Planned Behaviour: A Meta-Analysis'. *European Review of Social Psychology* 35(1):198–254. doi:10.1080/10463283.2023.2225897.

Hagger, Martin S., and Kyra Hamilton. 2025. 'Progress on Theory of Planned Behavior Research: Advances in Research Synthesis and Agenda for Future Research'. *Journal of Behavioral Medicine* 48(1):43–56. doi:10.1007/s10865-024-00545-8.

Hair, Joseph, and Abdullah Alamer. 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. doi: 10.1016/j.rmal.2022.100027.

Hair, Joseph F., G. Tomas M. Hult, Christian M. Ringle, and Marko Sarstedt. 2017. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Second edition. Los Angeles London New Delhi Singapore Washington DC Melbourne: SAGE.

Hair, Joseph F., G. Tomas M. Hult, Christian M. Ringle, and Marko Sarstedt. 2022. *Hair A Primer on Partial Least Squares Structural Equation Modeling Pls-Sem*. 3rd edn. Los Angeles London New Delhi Singapore Washington DC Melbourne: SAGE.

Hair, Joseph F., Jeffrey J. Risher, Marko Sarstedt, and Christian M. Ringle. 2019. 'When to Use and How to Report the Results of PLS-SEM'. *European Business Review* 31(1):2–24. doi:10.1108/EBR-11-2018-0203.

Hayes, Andrew F. 2018. *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. Second edition. Methodology in the Social Sciences. New York: Guilford Press.

Hedayati, Sadegh, Hossein Damghanian, Mohsen Farhadinejad, and Abbas Ali Rastgar. 2023. 'Meta-Analysis on Application of Protection Motivation Theory in Preventive Behaviors against COVID-19'. *International Journal of Disaster Risk Reduction* 94:103758. doi: 10.1016/j.ijdrr.2023.103758.

Heijde, Claudia M. Van Der, and Beatrice I. J. M. Van Der Heijden. 2006. 'A Competence-based and Multidimensional Operationalization and Measurement of Employability'. *Human Resource Management* 45(3):449–76. doi:10.1002/hrm.20119.

Henseler, Jörg. 2017. 'Partial Least Squares Path Modeling'. Pp. 361–81 in *Advanced Methods for Modeling Markets*, *International Series in Quantitative Marketing*, edited by P. S. H. Leeflang, J. E. Wieringa, T. H. A. Bijmolt, and K. H. Pauwels. Cham: Springer International Publishing.

Henseler, Jörg, Geoffrey Hubona, and Pauline Ash Ray. 2016. 'Using PLS Path Modeling in New Technology Research: Updated Guidelines'. *Industrial Management & Data Systems* 116(1):2–20. doi:10.1108/IMDS-09-2015-0382.

Hong, Yuxiang, and Steven Furnell. 2021. 'Understanding Cybersecurity Behavioral Habits: Insights from Situational Support'. *Journal of Information Security and Applications* 57:102710. doi: 10.1016/j.jisa.2020.102710.

Hu, Li-tze, and Peter M. Bentler. 1999. 'Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives'. *Structural Equation Modeling: A Multidisciplinary Journal* 6(1):1–55. doi:10.1080/10705519909540118.

Jenkins, Jeffrey, Alexandra Durcikova, and Jay Nunamaker. 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):246–72. doi:10.17705/1jais.00660.

Jr, Joe F. Hair, Lucy Matthews, Ryan Matthews, and Marko Sarstedt. 2017. 'PLS-SEM or CB-SEM: Updated Guidelines on Which Method to Use'. *International Journal of Multivariate Data Analysis* 1(2):107–23.

Kim, Byung-Jik, and Min-Jik Kim. 2024. 'The Influence of Work Overload on Cybersecurity Behavior: A Moderated Mediation Model of Psychological Contract Breach, Burnout, and Self-Efficacy in AI Learning Such as ChatGPT'. *Technology in Society* 77:102543. doi: 10.1016/j.techsoc.2024.102543.

Kiran, Uzma, Naurin Farooq Khan, Hajra Murtaza, Ali Farooq, and Henri Pirkkalainen. 2025. 'Explanatory and Predictive Modeling of Cybersecurity Behaviors Using Protection Motivation Theory'. *Computers & Security* 149:104204. doi: 10.1016/j.cose.2024.104204.

Klein, Galit, and Moti Zwilling. 2024a. 'The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home'. *Journal of Computer Information Systems* 64(3):408–22. doi:10.1080/08874417.2023.2221200.

Klein, Galit, and Moti Zwilling. 2024b. 'The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home'. *Journal of Computer Information Systems* 64(3):408–22. doi:10.1080/08874417.2023.2221200.

Kline, Rex B. 2016. *Principles and Practice of Structural Equation Modeling*. Fourth edition. Methodology in the Social Sciences. New York London: The Guilford Press.

Liang, Huigang, and Yajiong Xue. 2010. 'Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective'. *Journal of the Association for Information Systems* 11(07):394–413. doi:10.17705/1jais.00232.

Liang and Xue. 2009. 'Avoidance of Information Technology Threats: A Theoretical Perspective'. *MIS Quarterly* 33(1):71. doi:10.2307/20650279.

Ma, Shuai, and Chen Chen. 2023. 'Are Digital Natives Overconfident in Their Privacy Literacy? Discrepancy between Self-Assessed and Actual Privacy Literacy, and Their Impacts on Privacy Protection Behavior'. *Frontiers in Psychology* 14:1224168. doi:10.3389/fpsyg.2023.1224168.

Maalem Lahcen, Rachid Ait, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. 2020. 'Review and Insight on the Behavioral Aspects of Cybersecurity'. *Cybersecurity* 3(1):10. doi:10.1186/s42400-020-00050-w.

Mattson, Tom, Sal Aurigemma, and Jie Ren. 2023. 'Close the Intention-Behavior Gap via Attitudes: Case Study of the Volitional Adoption of a Two-Factor Authentication Service'. in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences.

McEachan, Rosemary, Natalie Taylor, Reema Harrison, Rebecca Lawton, Peter Gardner, and Mark Conner. 2016. 'Meta-Analysis of the Reasoned Action Approach (RAA) to Understanding Health Behaviors'. *Annals of Behavioral Medicine* 50(4):592–612. doi:10.1007/s12160-016-9798-4.

Mou, Jian, Jason Cohen, Anol Bhattacherjee, and Jongki Kim. 2022. 'A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach in Search Advertising'. *Journal of the Association for Information Systems* 23(1):196–236. doi:10.17705/1jais.00723.

Nguyen, Giang-Do, and Minh-Tri Ha. 2021. 'The Role of User Adaptation and Trust in Understanding Continuance Intention towards Mobile Shopping: An Extended

Expectation-Confirmation Model' edited by A. W. K. Tan. *Cogent Business & Management* 8(1):1980248. doi:10.1080/23311975.2021.1980248.

Ogbeibu, Samuel, Charbel Jose Chiappetta Jabbour, James Gaskin, Abdelhak Senadjki, and Mathew Hughes. 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):2421–40. doi:10.1002/bse.2754.

Polit, Denise F., Cheryl Tatano Beck, and Steven V. Owen. 2007. 'Is the CVI an Acceptable Indicator of Content Validity? Appraisal and Recommendations'. *Research in Nursing & Health* 30(4):459–67. doi:10.1002/nur.20199.

Prabhu, Sunitha, and Peter Dell. 2025. 'A Structured Review of Insider Cybersecurity Behaviour Studies'. *Information Security Journal: A Global Perspective* 1–28. doi:10.1080/19393555.2025.2543458.

Salo, Markus, Markus Makkonen, and Riitta Hekkala. 2020. 'The Interplay of IT Users' Coping Strategies: Uncovering Momentary Emotional Load, Routes, and Sequences'. *MIS Quarterly* 44(3):1143–76. doi:10.25300/MISQ/2020/15610.

Sarstedt, Marko, Joseph F. Hair, Christian M. Ringle, Kai O. Thiele, and Siegfried P. Gudergan. 2016. 'Estimation Issues with PLS and CBSEM: Where the Bias Lies!' *Journal of Business Research* 69(10):3998–4010. doi: 10.1016/j.jbusres.2016.06.007.

Simon, Joelle, Steven J. Watson, and Iris Van Sintemaartensdijk. 2025. 'Response-Efficacy Messages Produce Stronger Passwords than Self-Efficacy Messages … for Now: A Longitudinal Experimental Study of the Efficacy of Coping Message Types on Password Creation Behaviour'. *Computers in Human Behavior Reports* 17:100615. doi: 10.1016/j.chbr.2025.100615.

Sommestad, Teodor, Henrik Karlzén, and Jonas Hallberg. 2019. 'The Theory of Planned Behavior and Information Security Policy Compliance'. *Journal of Computer Information Systems* 59(4):344–53. doi:10.1080/08874417.2017.1368421.

Sony, Michael, and Nandakumar Mekoth. 2022. 'Employee Adaptability Skills for Industry 4.0 Success: A Road Map'. *Production & Manufacturing Research* 10(1):24–41. doi:10.1080/21693277.2022.2035281.

Stacey, Patrick, Rebecca Taylor, Omotolani Olowosule, and Konstantina Spanaki. 2021. 'Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study'. *International Journal of Information Management* 58:102298. doi: 10.1016/j.ijinfomgt.2020.102298.

Streukens, Sandra, and Sara Leroi-Werelds. 2016. 'Bootstrapping and PLS-SEM: A Step-by-Step Guide to Get More out of Your Bootstrap Results'. *European Management Journal* 34(6):618–32. doi: 10.1016/j.emj.2016.06.003.

Stylianou, Ioannis, Panagiotis Bountakas, Apostolis Zarras, and Christos Xenakis. 2025. 'Suspicious Minds: Psychological Techniques Correlated with Online Phishing Attacks'. *Computers in Human Behavior Reports* 19:100694. doi: 10.1016/j.chbr.2025.100694.

Tsai, Hsin-yi Sandy, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, and Shelia R. Cotten. 2016. 'Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective'. *Computers & Security* 59:138–50. doi: 10.1016/j.cose.2016.02.009.

Venkatesh, Morris, Davis, and Davis. 2003. 'User Acceptance of Information Technology: Toward a Unified View'. *MIS Quarterly* 27(3):425. doi:10.2307/30036540.

Wang, Xuan, Yaojie Li, Hanieh Javadi Khasraghi, and Cherie Trumbach. 2023. 'The Mediating Role of Security Anxiety in Internet Threat Avoidance Behavior'. *Computers & Security* 134:103429. doi: 10.1016/j.cose.2023.103429.

World Economic Forum. 2025. *Global Cybersecurity Outlook Insight Report*. World economic forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.