Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(RESEARCH ARTICLE)

Check for updates

Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach

William Vortia *

Department of Education, Westcliff University, Irvine, California, USA.

Magna Scientia Advanced Research and Reviews, 2025, 14(02), 096-111

Publication history: Received on 25 June 2025; revised on 01 August; accepted on 04 August 2025

Article DOI: https://doi.org/10.30574/msarr.2025.14.2.0094

Abstract

This study examines the interplay between cybersecurity awareness, perceived threats, and behavioral intentions to adopt secure online practices among Ghanaian university students by integrating the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT). Using Partial Least Squares Structural Equation Modeling (PLS-SEM), we analyzed survey data from 181 students with prior cybersecurity knowledge. This study used validated scales on cybersecurity awareness, perceived threats, and behavioral intentions to adopt secure online practices. The results confirm that cybersecurity awareness significantly enhances perceived threats and directly influences behavioral intentions. Perceived threats also strongly predict protective intentions. This study advances cybersecurity literature by empirically validating TPB-PMT integration in an understudied, resource-constrained setting. It highlights the primacy of threat appraisal in motivating secure behaviors among Ghanaian students and underscores the need for contextually tailored interventions.

Keywords: Cybersecurity awareness; Perceived threats; Secure online practices; PLS-SEM; Ghana

1. Introduction

The rapid digitization of educational and social activities has heightened the need for robust cybersecurity awareness and secure online practices among students (Ahamed et al., 2024; Alhogail, 2021; Fazil et al., 2023; Muasher et al., 2024). Cybersecurity encompasses the protection of digital assets and systems from unauthorised access, use, disclosure, disruption, modification or destruction. This is achieved through technical measures and procedural strategies (Amin, 2024; Clark-Ginsberg & Slayton, 2019; Cele & Kwenda, 2025; Perwej et al., 2021; Rayhan, 2024). The core objective is to ensure the integrity, confidentiality and availability of data while protecting individual and organisational interests (Clark-Ginsberg & Slayton, 2019; Cele & Kwenda, 2025). A strong cybersecurity strategy combines advanced technology, effective management and a proactive security culture to mitigate risks and prevent significant consequences (Amoo et al., 2024; Clark-Ginsberg & Slayton 2019; Wu et al., 2023). Given the dynamic nature of cyber threats, continuous improvement of cybersecurity practices through research and interdisciplinary collaboration is essential (Bada et al., 2019; Wu et al., 2023; 2025). Human factors, particularly behavioural issues, remain one of the most important vulnerabilities (Tran et al., 2024).

As information and communication technologies (ICTs) become an integral part of everyday life, we argued that secure online behaviour is increasingly important, especially for university students who regularly handle sensitive academic and personal data. As digital natives, university students rely heavily on online platforms for learning, social interaction, and research. This dependence puts them at increased risk of cybersecurity threats, highlighting the need for greater awareness and stronger safeguards. The rapid digital transformation of higher education, driven by expanded internet access and ICT adoption, has increased exposure to cyber threats such as phishing, malware, data breaches, and

* Corresponding author: William Vortia ORCID: https://orcid.org/0009-0006-2586-2303

unauthorised access to institutional databases (Cheng & Wang, 2022; Srivastava et al., 2024). In Ghana, where internet penetration continues to grow, students are increasingly exposed to cyber threats such as phishing, identity theft, and malware attacks (Agbeko, 2021; Adu & Adjei, 2018). Students in Ghana are particularly vulnerable due to limited cybersecurity awareness and sometimes risky online behaviours resulting from inadequate training on safe digital practices (Agbeko, 2021).

The Theory of Planned Behaviour (TPB), exploring factors that shape students' intentions to adopt secure online practices is crucial for developing targeted interventions that mitigate cyber risks (Alanazi et al., 2022; Almansoori et al., 2023; Jabali & Baher, 2024; Vafaei-Zadeh et al., 2019). Prior studies in Ghana have researched into cybersecurity awareness in various contexts, but few studies have explored this phenomenon in Sub, particularly Ghana (Adu & Adjei, 2018; Adu-Mensah et al., 2024; Agbeko, 2021; Kwabena-Adade & Yeboah-Boateng, 2022; Ouassini & Amini, 2021). Research on students' cybersecurity awareness and behavioral intentions adopt secure online practice remains elusive. It is also worth noting that cybersecurity awareness alone may not directly translate into secure behaviors (Hadlington, 2017). Instead, the Protection Motivation Theory (PMT) perspective, perceived threat a cognitive assessment of the severity and susceptibility to cyber threats plays a mediating role in motivating protective actions (Liang & Xue, 2009; Maddux & Rogers, 1983; Rogers, 1975). As per Maddux and Rogers (1983), PMT posits that individuals are more likely to engage in protective behaviors when they perceive significant threats and believe in their ability to respond effectively. Studies show that low cybersecurity knowledge and perceived low risk of threats often lead to risky online habits, resulting in privacy breaches, identity theft, and academic disruption (Kim et al., 2019; Lee & Kim, 2023; Mat et al., 2021; Tran et al., 2024; 2025).

Based on these insights, an evidence-based understanding of how perceived threat shape students' cybersecurity perceptions and their intentions to adopt secure practices is essential to fostering a secure digital culture in Ghanaian universities. Applying this TPB and PMT as an integrated theory, we investigate how perceived threat mediates the relationship between cybersecurity awareness and intentions to adopt secure online practices among Ghanaian students. To elaborate further, while structural equation modeling (SEM) has been widely used to analyze behavioral intentions in cybersecurity (Alanazi et al., 2022; Gombár et al., 2024; Sivarethinamohan & Sujatha, 2021; Wahid et al., 2021), its application in the Ghanaian educational context remains underexplored. This study fills this gap by employing SEM to assess the mediating role of perceived threat in the relationship between cybersecurity awareness and behavioral intentions. The findings of this study will contribute to the cybersecurity literature by: (1) providing empirical evidence on the factors influencing secure online behaviors among Ghanaian students, (2) validating the mediating role of perceived threat within the PMT framework, and (3) offering practical insights for policymakers and educators to enhance cybersecurity training programs.

2. Literature Review

2.1. Theory of planned behaviour and protection motivation theory as theoretical lenses

The theory of planned behaviour (TPB) and protection motivation theory (PMT) provide the theoretical underpinning of this study that focuses on understanding students' cybersecurity awareness and their behavioral intentions to adopt secure online practices. The Theory of Planned Behaviour (TPB) (Ajzen, 1991) is a robust framework for explaining the psychological and cognitive mechanisms behind behavioural intentions, including secure online practices (Ajzen, 2020). Within the cybersecurity context, students' attitudes may encompass their perceived benefits and risks of secure practices, while subjective norms reflect the influence of peers and institutional policies. Perceived behavioral control encapsulates their self-efficacy and access to resources for implementing secure behaviors. Attitudes, subjective norms and perceived behavioural control predict intention, which directly influences behaviour such as compliance with security policies and privacy measures (Biber et al., 2025). Recent studies confirm that these TPB constructs effectively predict intentions to protect data, with risk perception, anticipated regret and habit further strengthening the predictive accuracy of the model (Sommestad et al., 2019). Biber et al. (2025) emphasise that TPB components notably increase users' intent to protect data. Empirical studies corroborate the relevance of the TPB, demonstrating that positive attitudes and supportive norms significantly improve cybersecurity awareness and compliance among students (Li et al., 2022).

Based on these findings, we hypothesise that the core components of TPB collectively explain students' cybersecurity awareness and their behavioural intentions towards secure online practices. Furthermore, personal exposure to cyber threats increases risk perception, which in turn elevates the intention to adopt protective measures (Alanazi et al., 2022; Kostyuk & Wayne, 2021). We argue that, in addition to TPB's foundational elements, fear of cyberattacks serves as an additional motivator, reinforcing both awareness and behavioural intention. To provide a more comprehensive framework, this study integrates TPB with Protection Motivation Theory (PMT). While TPB emphasises attitudes,

norms, and perceived behavioural control, PMT complements this perspective by highlighting how threat appraisal (perceived severity and vulnerability) and coping appraisal (self-efficacy and response costs) shape cybersecurity behaviours (Debb & McClellan, 2021; De Kimpe et al., 2022). Together, these theories offer a robust lens through which to examine the interplay between cybersecurity awareness, perceived threats, and behavioural intentions. By combining TPB and PMT, this study highlights the important part played by threat perception in motivating protective online behaviours and offers a more robust framework for predicting and improving cybersecurity practices.

2.2. Conceptual model and hypothesis development

This study presents a conceptual framework for examining how cybersecurity awareness and threat perceptions influence students' intentions to engage in secure online behaviours. As illustrated in Figure 1, the proposed model outlines the relationships between three key constructs: cybersecurity awareness, perceived threat and behavioural intentions among Ghanaian university students. The model hypothesises that: (H1) Cybersecurity awareness positively influences perceived threat, (H2) cybersecurity awareness directly affects behavioural intentions, and (H3) perceived threat significantly enhances students' intentions to adopt protective online practices. It is notable that the framework positions perceived threat as a crucial mediating factor in this psychological and behavioural dynamic. The development of the hypotheses is presented as follow:

2.3. Cybersecurity awareness and perceived threats

Understanding threat perceptions in cybersecurity is crucial for designing effective awareness programmes and policies that align with psychological and organisational needs. When managed effectively, heightened threat perception can encourage proactive security measures; however, if mismanaged, it may also lead to fear or avoidance (Ali et al., 2024; Alsharida et al., 2025). Perceived threats are an individual's or organisation's subjective assessment of the likelihood and potential impact of cyber risks, such as data breaches or malware attacks. These perceptions are shaped by technical realities, as well as by factors such as vulnerability, severity, privacy concerns and awareness of cyber incidents (Debb & McClellan, 2021; Session & Muller, 2022; Vafaei-Zadeh et al., 2025). Cybersecurity awareness, defined as knowledge of risks and protective measures, plays a direct role in shaping students' responses to threats. Research confirms a strong correlation between awareness and threat perception: well-informed students are more likely to recognise risks such as phishing, malware and identity theft, and are also more inclined to adopt protective behaviours such as using stronger passwords and adjusting privacy settings (Adeshola & Oluwajana, 2024; Alanazi et al., 2022). Nevertheless, despite its significance, there is a lack of empirical research on this relationship in Ghana. This study therefore investigates the relationship between cybersecurity awareness and perceived threats among Ghanaian students. This study hypothesised that:

H1: *Cybersecurity awareness significantly shapes perceived threats among Ghanaian students*

2.4. Cybersecurity awareness and behavioural intention

In today's technology-driven world, secure online practices are essential for safeguarding against the growing threat of cybercrime. Awareness is transformative, bridging the gap between knowledge of risk and proactive mitigation (Aliyu et al., 2021; Fazil et al., 2023). In cybersecurity, awareness, or understanding security protocols and personal responsibilities, plays a pivotal role in fostering these practices. As digital platforms become increasingly prevalent in education and daily life, students are exposed to a growing number of sophisticated attacks, making awareness crucial for promoting safe behaviours. Research shows that well-designed programmes can enhance knowledge and encourage behavioural change, promoting good practices such as strong password management and cautious email use (Chaudhary, 2024; Saeed, 2023). Tailored, engaging initiatives further convert knowledge into action, reinforcing cybersecurity as a social norm and an individual duty (Zhang et al., 2021; Li et al., 2019). Empirical studies confirm that heightened awareness strengthens intentions to adopt secure practices. For example, students who are exposed to targeted interventions demonstrate greater compliance with protocols (Bognár & Bottyán, 2024; Oroni et al., 2025). Programmes that address such variables can further improve effectiveness (Adeshola & Oluwajana, 2024; Alkhdour et al., 2024). Despite these insights, however, gaps persist in Ghana, particularly with regard to the influence of cybersecurity awareness on behavioural intentions among university students. This study therefore proposes that:

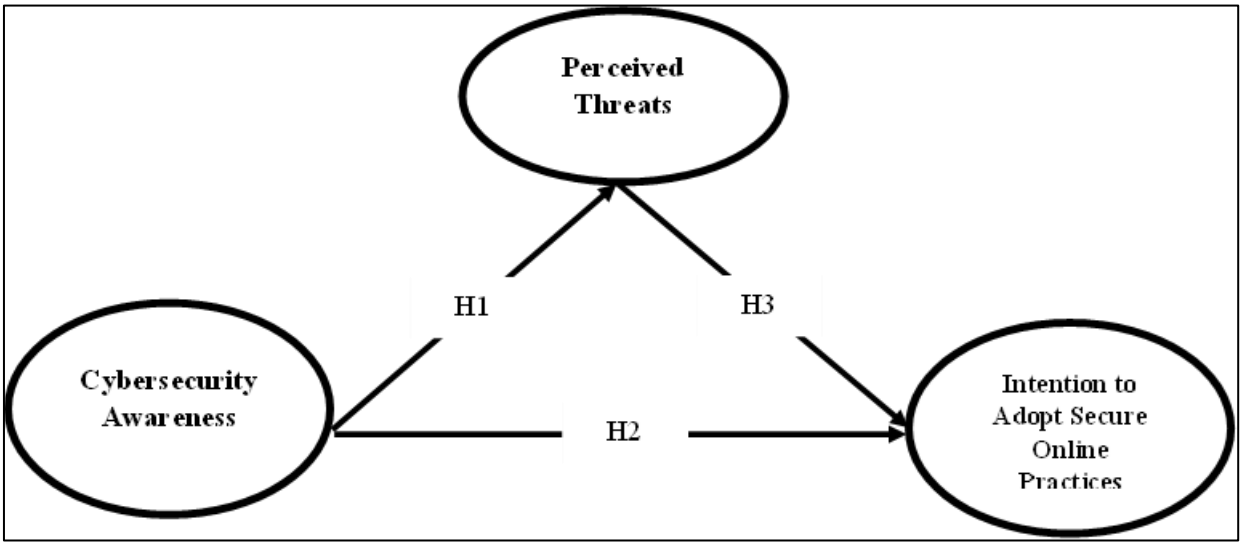
H2: *Cybersecurity awareness has a significant effect in influencing Ghanaian students' intention to adopt secure online practices*

2.5. Perceived threats and behavioural intention

In cybersecurity, perceived threat is shaped by two key dimensions: perceived susceptibility (the likelihood of experiencing a cyberattack) and perceived severity (the potential consequences of an attack). According to Protection

Motivation Theory (PMT) (Debb & McClellan, 2021; De Kimpe et al., 2022; Vafaei-Zadeh et al., 2025), these factors influence threat appraisals and motivate risk-mitigation behaviours. For example, higher perceptions of susceptibility correlate with increased caution, while greater assessments of severity emphasise the urgency of protective measures (Gerdenitsch et al., 2023; Session & Müller, 2022; Wang et al., 2023). Studies have repeatedly demonstrated a link between students' threat perceptions and their adoption of cybersecurity practices (Alanazi et al., 2022; Li et al., 2022; Yoon et al., 2012). According to PMT, heightened threat appraisals combined with coping appraisals (self-efficacy and response efficacy) drive behaviours such as enabling two-factor authentication or avoiding phishing links (Kiran et al., 2025). However, despite growing awareness, many students, particularly in regions such as Ghana, struggle to translate threat recognition into consistent secure practices due to a lack of formal training (Boateng et al., 2022). This study examines how perceived threat influences Ghanaian university students' behavioural intentions towards cybersecurity. We propose that:

H3: *Perceived threat has a significant influence on the behavioural intention to adopt secure online practices among Ghanaian university student*



Source: Authors' work

Figure 1 Conceptual framework of the study

3. Materials and Methods

3.1. Study Sample and Design

This study utilised a purposive sampling technique to recruit 181 university students who possessed prior knowledge of cybersecurity. For this study, a minimum sample size of 181 was determined on the basis of the results of an a priori analysis carried out using the G-power tool (see Appendix A). The rationale behind selecting this specific group was to ensure that participants had a foundational understanding of the topic, allowing for more reliable responses regarding cybersecurity awareness, perceived threat, and behavioral intentions. The correlational research design was employed to examine the relationships between these constructs. This design is suitable for identifying and analysing the strength and direction of associations between variables, without manipulating the study environment (Bloomfield & Fisher, 2019; Krause, 2018; Seeram, 2019). The goal was to determine the extent to which awareness of cybersecurity and perceived threat influences students' intentions to adopt secure online practices.

3.2. Measures

The study employed a survey instrument adapted from existing, validated scales to measure the three core constructs: cybersecurity awareness, perceived threat, and behavioral intentions to adopt secure online practices. The cybersecurity awareness scale was adapted from Farooq et al. (2019) and Ion et al. (2015), which assess individuals' knowledge of and familiarity with cybersecurity concepts and behaviours. Perceived threat, which captures the respondents' feelings of vulnerability and perceived risks associated with insecure online practices, was measured using a scale adapted from Macovei (2015). Finally, the behavioral intentions to adopt secure online practices were assessed using items adapted from Glanz et al. (2015), focusing on participants' readiness and intention to engage in security-

enhancing online behaviors. Each of these scales was measured using a five point Likert-type format to capture varying levels of agreement or disagreement with statements about cybersecurity and related behaviors.

3.3. Data Collection Procedure

Data collection was conducted using a structured, self-administered online survey, which was distributed to university students through institutional social media platforms. The survey included clear instructions and took approximately 15 to 20 minutes to complete. Participants were briefed on the objectives of the study and informed of their rights as respondents, including the voluntary nature of their participation. They were assured that their responses would be kept confidential and that they could withdraw from the study at any time without penalty. The online format of the survey allowed for efficient data collection while maintaining the anonymity of the participants.

3.4. Data Analysis Strategy

The collected data were analysed using Partial Least Squares Structural Equation Modeling (PLS-SEM), a robust analytical technique particularly well-suited for complex models that involve latent variables (Becker et al., 2023). PLS-SEM was chosen because of its ability to handle relatively small sample sizes while maximising predictive accuracy. It is also advantageous in exploratory studies, like this one, where the relationships between variables are being tested for the first time in Ghana. The analysis began with an assessment of the measurement model, evaluating the reliability and validity of the constructs, followed by testing the structural model to examine the relationships between cybersecurity awareness, perceived threat, and behavioral intentions to adopt secure online practices.

3.5. Ethical Considerations

The study adhered to strict ethical guidelines to ensure the protection of participants' rights and privacy. All respondents were provided with detailed information about the study's purpose and assured that their participation was entirely voluntary. Confidentiality and anonymity were prioritised, with measures in place to protect the identity of respondents throughout the data collection and analysis process. Prior to completing the survey, participants were required to give informed consent, acknowledging their understanding of the study's objectives and agreeing to participate. No personal identifiers were collected, and the data were stored securely, accessible only to the research team.

4. Results

4.1. Normality measures

Multivariate normality is an essential assumption in many multivariate analyses, where it is assumed that the variables follow a normal distribution not only individually but also jointly. In the present output, both univariate skewness and kurtosis show significant deviations from normality for the variables BIP, CBA and PT, as indicated by their z-values exceeding acceptable thresholds (e.g. z-values > |1.96| for skewness and kurtosis) [see Appendix B]. Furthermore, the Mardia multivariate skewness test (p-value = 0.000) indicates a violation of multivariate normality. Given this violation, Partial Least Squares Structural Equation Modelling (PLS-SEM) was used to analyse the data, as PLS-SEM does not require multivariate normality and is well suited to dealing with such data issues.

4.2. Common method bias

Common method bias (CMB) refers to the potential bias in statistical results when variations in responses are attributed to the measurement method rather than to the constructs being measured. Two diagnostic tests were used to assess CMB in this study. First, full collinearity variance inflation factors (VIFs) were examined and found to be below the threshold of 5 (Ringle et al., 2023), indicating no multicollinearity problems, suggesting the absence of common method bias. In addition, Harman's single factor test revealed that a single factor accounted for less than 50% of the total variance, further confirming that CMB is not an issue. These results confirm the reliability of the study's findings, free from the confounding influence of common method variance.

4.3. Measurement model assessment

The measurement model assessment reveals that the constructs exhibit high reliability and validity based on several indicators. For BIP, the indicator loadings (λ) range from 0.916 to 0.981, with Cronbach's alpha (α = 0.948), rho_A (0.958), composite reliability (CR = 0.967), and AVE (0.907), all reflecting strong internal consistency and convergent validity (Hair et al., 2019; Hair et al., 2022) [see Table 1]. Similarly, CBA demonstrates excellent reliability with loadings from 0.980 to 0.993, α = 0.986, rho_A = 0.991, CR = 0.991, and AVE = 0.973. PACT, though having a lower loading on

PACT1 (0.539), still shows acceptable reliability (α = 0.855), rho_A = 0.925, CR = 0.904, and AVE = 0.710, indicating that the construct meets the necessary criteria for validity (Hair & Alamer, 2022). All p-values are significant (***), confirming the relevance of the indicators.

Table 1 Measurement Model

Constructs	No. of Items	Item	λ	α	rho_a	CR	AVE	P value
BIP	Three	BIP3	0.916	0.948	0.958	0.967	0.907	***
		BIP4	0.981					***
		BIP5	0.959					***
CBA	Three	CBA3	0.980	0.986	0.991	0.991	0.973	***
		CBA4	0.987					***
		CBA5	0.993					***
PACT	Four	PACT1	0.539	0.855	0.925	0.904	0.710	***
		PACT2	0.967					***
		PACT3	0.915					***
		PACT4	0.882					***

Note: λ = Indicator loadings

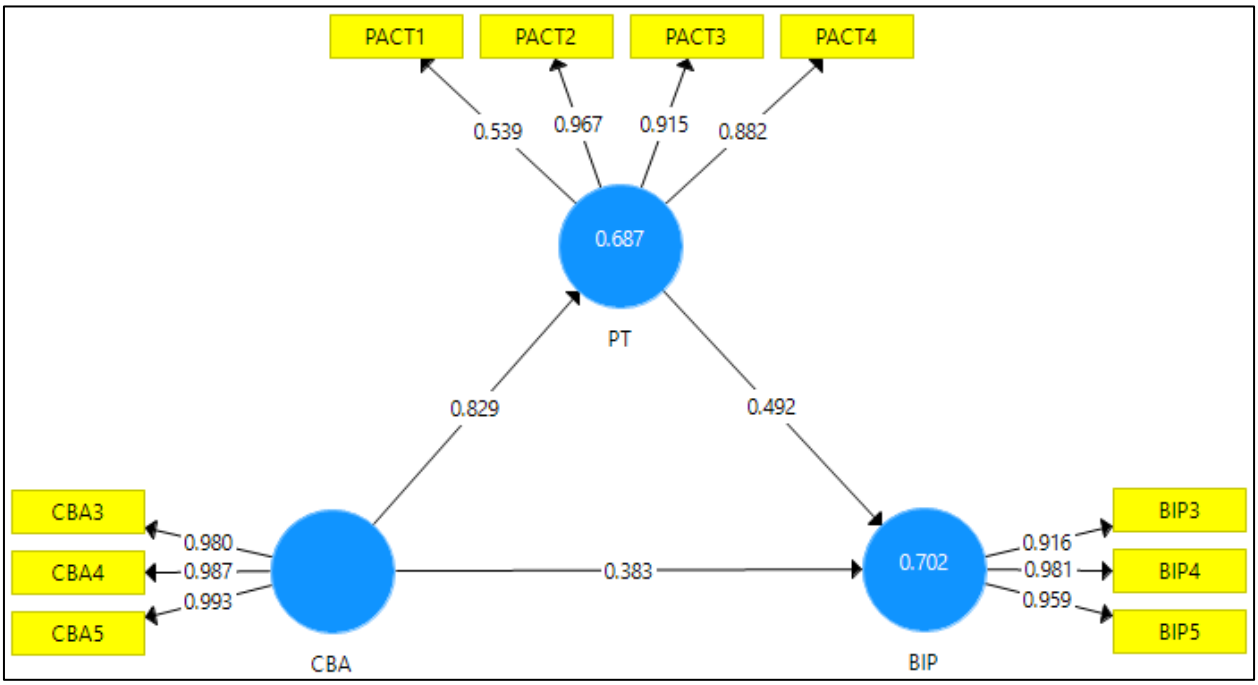


Figure 2 PLS-SEM algorithm results

4.4. Discriminant validity

Discriminant validity was assessed using the Fornell-Larcker criterion and the HTMT ratio. The Fornell-Larcker criterion indicates that each construct's square root of AVE (BIP = 0.952, CBA = 0.987, PT = 0.843) is greater than the inter-construct correlations, confirming discriminant validity (Fornell & Larcker, 1981). The HTMT ratios between constructs (BIP-CBA = 0.809, BIP-PT = 0.852, CBA-PT = 0.872) [see Table 2] are below the 0.90 threshold (Henseler et al., 2015), further supporting the distinctiveness of the constructs.

Table 2 Discriminant validity

		Fornell-Larcker criterion	
Construct	**BIP**	**CBA**	**PT**
BIP	0.952		
CBA	0.791	0.987	
PT	0.810	0.829	0.843
	HTMT ratio		
Construct	BIP	CBA	PT
BIP			
CBA	0.809 [0.741, 0.864]		
PT	0.852 [0.787, 0.900]	0.872 [0.814, 0.914]	

4.5. Structural model assessment

In assessing the structural model, multicollinearity was first assessed using the variance inflation factor (VIF). The VIF values for the model were all below the threshold of 5 (Ringle et al., 2023), indicating that multicollinearity is not a problem and that the constructs are sufficiently distinct. Subsequently, 10,000 bootstrap samples were used to test the significance and stability of the path coefficients, providing robust estimates (Becker et al., 2023). The results showed that all path coefficients were statistically significant, with the path from CBA to BIP ($\beta = 0.383$, $p < 0.001$), CBA to PT ($\beta = 0.829$, $p < 0.001$) and PT to BIP ($\beta = 0.492$, $p < 0.001$) [see Table 3] showing strong and positive relationships.

In addition to path coefficients, effect sizes (f^2) were calculated to assess the practical significance of these relationships. For example, the effect sizes for CBA's influence on PT ($f^2 = 2.194$) and PT's influence on BIP ($f^2 = 0.254$) indicate medium to large effects, indicating that these relationships contribute significantly to the variance explained in the dependent variables. In addition, the coefficient of determination (R^2) for BIP was 0.702 and for PT it was 0.687, indicating that a significant proportion of the variance in these outcomes is explained by the model. Predictive relevance (Q^2) values of 0.611 for BIP and 0.453 for PT, obtained using blindfolding, confirmed that the model has strong predictive accuracy, with Q^2 values greater than zero for all endogenous constructs. Finally, the mediation analysis revealed that PT significantly mediates the relationship between CBA and BIP ($\beta = 0.408$, $p < 0.001$), suggesting that the effect of CBA on BIP is partially channeled through PT.

Table 3 Structural Model

Relationship	**β**	**M**	**SD**	**VIF**	**t-value**	**p-values**	**2.5%**	**97.5%**	f^2	R^2	Q^2
CBA -> BIP	0.383	0.383	0.058	3.194	6.639	<.001	0.259	0.489	0.154	0.702	0.611
CBA -> PT	0.829	0.828	0.023	3.194	35.860	<.001	0.777	0.868	2.194	0.687	0.453
PT -> BIP	0.492	0.492	0.051	1.000	9.620	<.001	0.400	0.601	0.254		
Mediation											
CBA -> PT -> BIP	0.408	0.408	0.049		8.265	<.001	0.319	0.513			

Note: $R^2_{adjBIP} = 0.699$; $R^2_{adjPT} = 0.685$

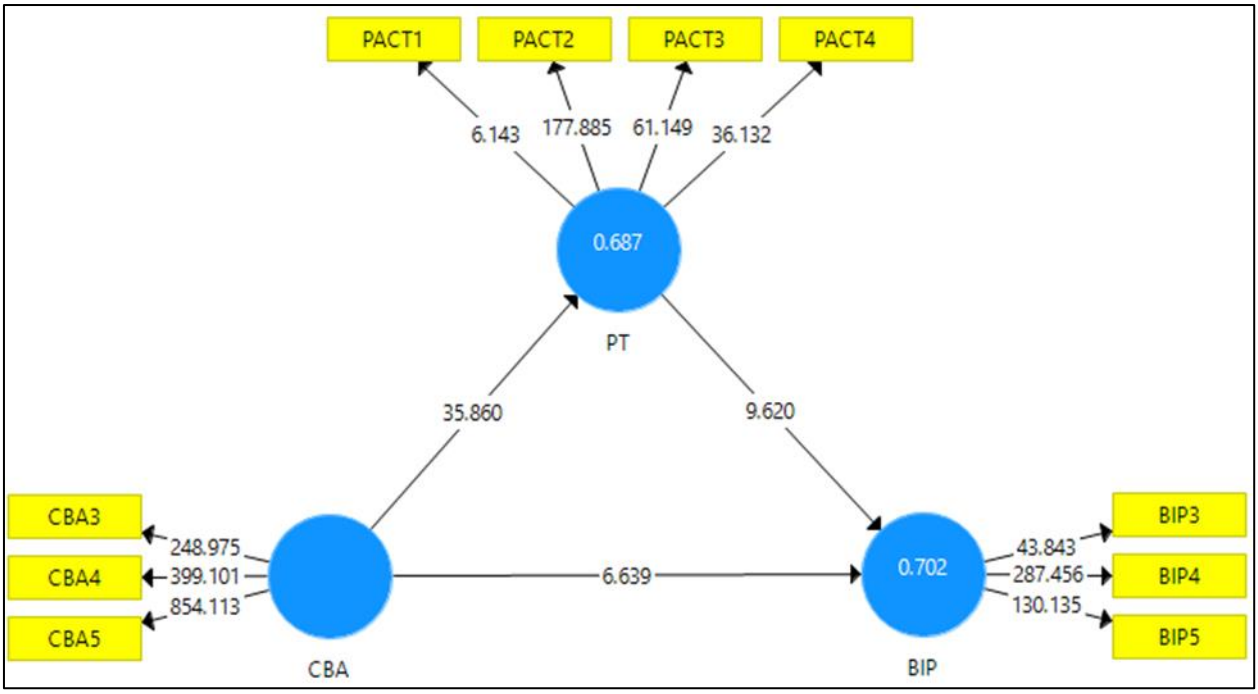


Figure 3 PLS-SEM Bootstrapping t-values

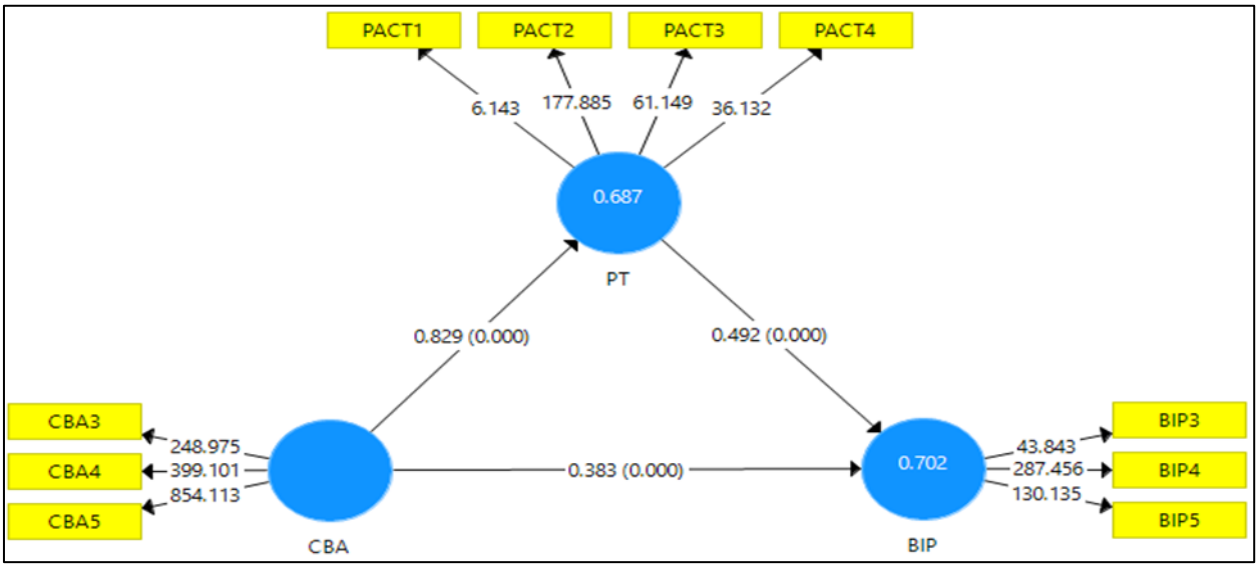


Figure 4 PLS-SEM Bootstrapping p-values

5. Discussion

This study by integrating the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT), the research provides empirical insights into the influence of awareness and threat appraisal mechanisms on cybersecurity behaviours. Using Partial Least Squares Structural Equation Modelling (PLS-SEM) the study investigates the relationship between cybersecurity awareness, perceived threats and behavioural intentions to adopt secure online practices among Ghanaian university students. The findings validate all three hypotheses, demonstrating that cybersecurity awareness significantly enhances perceived threats (H1); awareness directly increases behavioural intentions (H2); and perceived threats strongly predict protective intentions (H3).

First, cybersecurity awareness was found to have a positive influence on threat perception, thus supporting (H1). This finding is consistent with both the TPB and the PMT frameworks and also confirms with previous research (Adeshola & Oluwajana, 2024; Alanazi et al., 2022) that awareness influences the evaluation of threats, particularly with regard to the perceived severity and vulnerability of cyber risks (Debb & McClellan, 2021). This implies that Ghanaian students with greater cybersecurity awareness are more likely to recognise the associated threats such as phishing and malware. Inspite of this it is also worthy to note that their understanding often may also be derived from personal experience rather than formal training (Boateng et al., 2022). This is therefore in contrast to Western contexts, where structured education is more prevalent (Li et al., 2022; Yoon et al., 2012), suggesting that cultural and institutional factors may moderate the relationship between awareness and threat perception.

Secondly, this study found that cybersecurity awareness has a direct significant influence pn the behavioural intentions, validating (H2). This finding is also consistent with the TPB's (Ajzen, 2020) which put emphasis on knowledge as a precursor to attitudes and behavioural intentions. This also conforms with previous findings that students who understood cyber risks were more likely to implement safeguards such as strong passwords, reflecting global trends (Chaudhary, 2024; Saeed, 2023). This study also reveals that even informal awareness can prompt action in under-resourced settings, building on previous research focused on institutional training (Bognár & Bottyán, 2024). However, there are still gaps in the implementation of advanced measures, which may be due to fragmented knowledge sources compared to systematic campaigns (Zhang et al., 2021).

Thirdly, this study established that perceived threat has a significant influence in predict students' behavioural intentions to adopt secure online practices, supporting (H3). This finding reinforces the threat appraisal component of PMT (Debb & McClellan, 2021). In line with previous findings, although other threats coping appraisal (self-efficacy and response costs) may shape this relationship (De Kimpe et al., 2022), our results suggest perceived threat alone that may drive action in Ghana, and this is likely due to the heightened risk sensitivity caused by limited institutional safeguards. This may diverge from Western contexts, where coping appraisal is more influential (Session & Müller, 2022), and highlights the need for contextually tailored cybersecurity interventions.

5.1. Theoretical Implications

This study makes three key contributions to the field of cybersecurity literature. Firstly, it advances the understanding of integrating the Theory of Planned Behaviour (TPB) with Protection Motivation Theory (PMT), demonstrating the relevance of their combined application to explain cybersecurity behaviours among Ghanaian students. While these theories have been validated in Western contexts (Ajzen, 2020; Debb & McClellan, 2021), our findings confirm their applicability in developing nations with less robust safeguards. Second, the research reveals contextual nuances in behavioural drivers. Unlike in Western studies, which emphasise formal training (Li et al., 2022), we found that informal awareness can sufficiently motivate protective behaviours. This is a novel insight for settings with limited resources (Boateng et al., 2022). The mediation effect of perceived threat (H1/H3) highlights the threat appraisal mechanism of PMT, whereby heightened awareness amplifies risk perception and subsequent intentions (Debb & McClellan, 2021).

Notably, threat perception was found to be a stronger motivator than coping strategies, a finding that contrasts with those from Western studies, where self-efficacy is the dominant factor (De Kimpe et al., 2022). Third, the study sheds light on cultural-institutional contingencies. Ghanaian students rely more on personal cyberattack experiences than structured education, which aligns with socio-cognitive theories of contextual learning (Bandura, 1986). This underscores the need for culturally tailored interventions rather than universal policies. Our use of PLS-SEM addresses key challenges in exploratory behavioural research. The technique's predictive power and robustness with small samples (Becker et al., 2023) make it ideal for testing nascent frameworks. The validated measurement model provides a blueprint for future methodological approaches to examining latent psychosocial constructs, particularly in contexts where conventional sampling yields unreliable data.

5.2. Practical Implications

This study sheds light on the relationship between cybersecurity awareness, perceived threats and behavioural intentions among Ghanaian university students. The findings have important implications for policymakers, educational administrators, NGOs and students themselves. By integrating the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT), the study emphasises the need for context-specific cyber security interventions in higher education, especially in settings with limited resources, such as those in Ghana. Based on the study's key findings we therefore present actionable recommendations as follows. The study confirms that cybersecurity awareness significantly enhances threat perception (H1) and directly influences intentions to behave securely (H2). However, unlike in Western contexts where formal training is widespread, Ghanaian students predominantly rely on informal

awareness. To address this, policymakers should prioritise the integration of structured cybersecurity education into university curricula to ensure that students acquire standardised knowledge of threats such as phishing and malware.

Given the limited institutional safeguards in Ghana, national cybersecurity frameworks should mandate periodic training programmes and foster partnerships with cybersecurity firms and government agencies. In addition, educational administrators should develop localised awareness campaigns incorporating real-world cybercrime case studies to highlight the severity and vulnerability of cybercrime, which are key drivers of protective behaviour. Furthermore, non-governmental organisations (NGOs) and advocacy groups could play a pivotal role in bridging the cybersecurity awareness gap. While informal awareness can drive behavioural change, fragmented knowledge sources impede advanced protective practices. NGOs should collaborate with universities to deliver targeted workshops using peer-led training models to enhance engagement. Given the influence of perceived threats (H3), awareness initiatives should emphasise the tangible consequences of cyber risks, such as financial fraud and data breaches, to strengthen threat appraisal. Furthermore, NGOs can provide access to affordable cybersecurity tools (e.g. password managers and VPNs) to mitigate the resource constraints that may prevent students from adopting secure practices.

The study also reveals that perceived threats strongly predict behavioural intentions (H3), suggesting that risk sensitivity can motivate secure actions even without formal training. Students should proactively seek cybersecurity knowledge through open-access resources (e.g. MOOCs and webinars) and adopt basic safeguards, such as multi-factor authentication and regular software updates. Peer knowledge-sharing networks can further reinforce best practices, particularly in environments where institutional support is insufficient. Overall, this research contributes to the discourse on cybersecurity behaviour by demonstrating the applicability of TPB and PMT in under-resourced educational contexts. It challenges the assumption that formal training is the sole driver of secure behaviours, instead advocating hybrid awareness strategies combining institutional and grassroots efforts. For Ghana and similar settings, the findings suggest the need for culturally tailored interventions that consider localised threat perceptions and infrastructural limitations. Future initiatives should also explore the role of coping appraisal (e.g. self-efficacy) in reinforcing behavioural intentions to ensure a comprehensive approach to cybersecurity education. Translating these insights into policy and practice will enable stakeholders to cultivate a cybersecurity-conscious academic environment and ultimately mitigate risks in an increasingly digitalised higher education landscape.

5.3. Limitations of the Study

This study makes a significant contribution to the fields of cybersecurity and educational psychology by integrating the Theory of Planned Behaviour (TPB) and the Protection Motivation Theory (PMT) to examine cybersecurity awareness, perceived threats and behavioural intentions among Ghanaian university students. It offers novel insights from an understudied context. However, there are limitations. Self-reported data is susceptible to social desirability bias, and purposive sampling restricts generalisability. The cross-sectional design precludes causal claims, necessitating longitudinal studies. Exploring additional coping appraisal factors (e.g. self-efficacy) could provide further insight into behavioural intentions. Future research should employ mixed methods designs that combine self-reports with behavioural observations. Sampling a broader range of institutions and regions would improve generalisability. Investigations into coping mechanisms and institutional support could enhance our understanding of cybersecurity behaviours in low-resource settings. Comparative cross-cultural studies may also clarify the efficacy of formal versus informal awareness strategies. Addressing these limitations in future research will refine theoretical frameworks and strengthen cybersecurity education policies.

6. Conclusion

This study makes a contribution to the field of cybersecurity research by empirically validating the combined use of the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) on the nexus of cybersecurity awareness, perceived threats and behavioural intentions among university students in Ghana. The findings demonstrate that cybersecurity awareness significantly increases perceived threat levels and directly influences behavioural intentions to adopt secure online practices (H2). In addition, perceived threats strongly predict the intention to engage in secure online behaviours (H3). These results are theoretically significant, particularly in the Ghanaian context, as they highlight the importance of enhancing students' cybersecurity awareness and threat appraisal in order to encourage safer online practices. From a practical standpoint, the study underscores the necessity of culturally tailored interventions, such as incorporating cybersecurity education into institutional curricula, launching localised awareness campaigns, and furnishing accessible security tools. While limitations, including self-report bias and the cross-sectional design, should be acknowledged, future research could address these by expanding to more diverse populations and employing longitudinal or mixed-methods approaches. Overall, these insights provide a basis for evidence-based policies and

educational strategies that promote cybersecurity awareness in higher education, especially in under-resourced settings.

References

[1] Adeshola, I., & Oluwajana, D. I. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*, 1-23.

[2] Adeshola, I., & Oluwajana, D. I. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*, 1-23.

[3] Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *foresight*, *20*(2), 150-161

[4] Adu-Mensah, E., Odei-Appiah, S., Adjei, J. K., & Ayivor, E. (2024). The role of user awareness in the information technology and security governance nexus-evidence from Ghana's banking industry. *International Journal of Information and Computer Security*, *25*(3-4), 367-403.

[5] Agbeko, M. (2021). Understanding cyber safety behavior among teenagers in Ghana. *International Journal of Computer Science and Information Security (IJCSIS)*, *19*(6).

[6] Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. *Sage Open*, *14*(1), 21582440241228920.

[7] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.
Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human behavior and emerging technologies*, *2*(4), 314-324.

[8] Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376.

[9] Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376.

[10] Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376.

[11] Alhogail, A. (2021). Enhancing information security best practices sharing in virtual knowledge communities. *VINE journal of information and knowledge management systems*, *51*(4), 550-572.

[12] Ali, N., Alsharida, R., Al-Qaysi, N., Al-Emran, M., Iranmanesh, M., Al-Sharafi, M., & Foroughi, B. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). *Comput. Hum. Behav.*, 159, 108315.

[13] Aliyu, A., Aliyu, M., Ahmad, A., & Abdullahi, S. (2021). Investigating Cybersecurity Awareness among Tertiary Institutions Students in Nigeria. *International Journal of Advances in Engineering and Management (IJAEM)*, *3*(2), 111-118.

[14] Alkhdour, T., Mohammed, A. A., Aitizaz, A., Al-Ali, R. O. M. E. L., Lutfi, A., Al-Khasawneh, M. M., ... & Savitha, D. (2024). Real Time of Cybersecurity Risks Detection Approach for Blockchain Based Personal Medical Devices. *Journal of Theoretical and Applied Information Technology*, *102*(10).

[15] 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.

[16] Alqahtani, M. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*.

[17] Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., Al-Sharafi, M. A., & Zainal, A. (2025). Predicting cybersecurity behaviors in the metaverse through the lenses of TTAT and TPB: a hybrid SEM-ANN approach. *Online Information Review*.

[18] Amin, M. (2024). The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets. *Indian Journal of Public Administration*, *70*(3), 493-501.

[19] Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, *11*(1), 1304-1310.

[20] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

[21] Becker, J. M., Cheah, J. H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2023). PLS-SEM's most wanted guidance. *International Journal of Contemporary Hospitality Management*, *35*(1), 321-346.

[22] Biber, M., Louis, W. R., & Smith, J. R. (2025). Predicting online privacy protection for Facebook users with an extended theory of planned behavior. *The Journal of Social Psychology*, *165*(3), 313-329.

[23] Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses Association*, *22*(2), 27-30.

[24] Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, *14*(6), 588.

[25] Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31-48.

[26] Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, 103858.

[27] Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192.

[28] Clark-Ginsberg, A., & Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, *46*(3), 339-346.

[29] De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796-1808.

[30] Debb, S. M., & McClellan, M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 605-611.

[31] Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849-868.

[32] Farooq, A., Jeske, D., & Isoaho, J. (2019). Predicting students' security behavior using information-motivation-behavioral skills model. In G. Dhillon, F. Karlsson, K. Hedstrom, ¨ & A. Zúquete (Eds.), ICT systems security and privacy protection (Vol. 562). Cham: Springer. https://doi.org/10.1007/978-3-030-22312-0_17.

[33] Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. *American Journal of Education and Technology*, *2*(4), 50-61.

[34] Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. *American Journal of Education and Technology*, *2*(4), 50-61.

[35] Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

[36] 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).

[37] Glanz, K., Rimer, B. K., Orleans, C. T., & Viswanath, K. (2015). Health behavior and health education theory, research, and practice (4th ed.). USA: Jossey-Bass.

[38] Gombár, M., Vagaská, A., Korauš, A., & Račková, P. (2024). Application of structural equation modelling to cybersecurity risk analysis in the era of industry 4.0. *Mathematics*, *12*(2), 343.

[39] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7).

[40] 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.

[41] 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.

[42] Hair, J.F., Hult, G.T., Ringle, C.M. and Sarstedt, M. (2022), A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), Sage, Thousand Oaks, CA

[43] Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, *43*, 115-135.

[44] Ion, I., Reeder, R., & Consolvo, S. (2015). No one can hack my mind: Comparing expert and non-expert security practices. In Proceedings of the 11th symposium on useable privacy and security (SOUPS) 2015. July 22-24. Canada: Ottawa.

[45] Jabali, A., & Baher, N. (2024). Exploring the impact of cybersecurity knowledge and awareness on behavioral choices for protection among university students in Sweden.

[46] 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.

[47] Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, *6*(2), ogz077.

[48] Krause, M. S. (2018). Associational versus correlational research study design and data analysis. *Quality & Quantity*, *52*(6), 2691-2707.

[49] Kwabena-Adade, H., & Yeboah-Boateng, E. O. (2022). Deployment of 5G in Emerging Economies: Cybersecurity Challenges and Potentials for Ghana. In *5G, Cybersecurity and Privacy in Developing Countries* (pp. 107-130). River Publishers.

[50] Lee, C. S., & Kim, D. (2023). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*, *63*(1), 94-106.

[51] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International journal of information management*, *45*, 13-24.

[52] 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.

[53] Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

[54] Macovei, O.-I. (2015). Applying the theory of planned behavior in predicting proenvironmental behavior: The case of energy conservation. Acta Universitatis Danubius - Œconomica, 11(4), 15–32.

[55] Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

[56] Mat, N. K. N., Sulaiman, Y., Perumal, S., & Ghazi, W. (2021). The predictors of cybersecurity behavior in e-hailing services: The mediating role of perceived threat. *Malaysian Journal of Consumer and Family Economics*, *27*, 147-161.

[57] Muasher, B., Ghandour, A., & Abusaimeh, H. (2024). Enhancing Digital Transformation in Higher Education: A Study on Cybersecurity Awareness Among University Students in Jordan with a Case Study at Middle East University. In *Achieving Sustainable Business Through AI, Technology Education and Computer Science: Volume 3: Business Sustainability and Artificial Intelligence Applications* (pp. 137-149). Cham: Springer Nature Switzerland.

[58] Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. *Education and Information Technologies*, 1-40.

[59] Ouassini, A., & Amini, M. (2021). Cybersecurity in Ghana: Past, present, and future. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 564-572). Routledge.

[60] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

[61] Rayhan, A. (2024, April). Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses. In *Conference: Cybersecurity Awareness* (pp. 1-26).

[62] Ringle, C. M., Sarstedt, M., Sinkovics, N., & Sinkovics, R. R. (2023). A perspective on using partial least squares structural equation modelling in data articles. *Data in Brief*, *48*, 109074.

[63] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

[64] Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. *Sustainability*, *15*(12), 9426.

[65] Seeram, E. (2019). An overview of correlational research. *Radiologic technology*, *91*(2), 176-179.

[66] Session, W., & Muller, S. R. (2022). Technology threat avoidance factors affecting cybersecurity professionals' willingness to share information. *Annals of Computer Science and Information Systems*, *34*, 209-213.

[67] Sivarethinamohan, R., & Sujatha, S. (2021). Behavioral intentions towards adoption of information protection and cyber security (email security and online privacy): sem model. *Turkish journal of computer and mathematics education*, *12*(6), 56-68.

[68] Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*.

[69] Srivastava, A. K., Mishra, K., Kumar, R., & Mishra, B. K. (2024). A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review. *LatIA*, (2), 14.

[70] *Tassaddiq, A., & Alharbi, T. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput., 5, 23.*

[71] Tran, D. V., Nguyen, P. V., Le, L. P., & Nguyen, S. T. N. (2025). From awareness to behaviour: understanding cybersecurity compliance in Vietnam. *International Journal of Organizational Analysis*, *33*(1), 209-229.

[72] Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies*, *18*(6), 1445-1464.

[73] Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*, *43*(3), 476-505.

[74] Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes*, *48*(8), 1565-1585.

[75] Wahid, S. D. M., Buja, A. G., Jono, M. N. H. H., & Aziz, A. A. (2021). Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modeling. *International Journal of Advanced Technology and Engineering Exploration*, *8*(74), 73.

[76] 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.

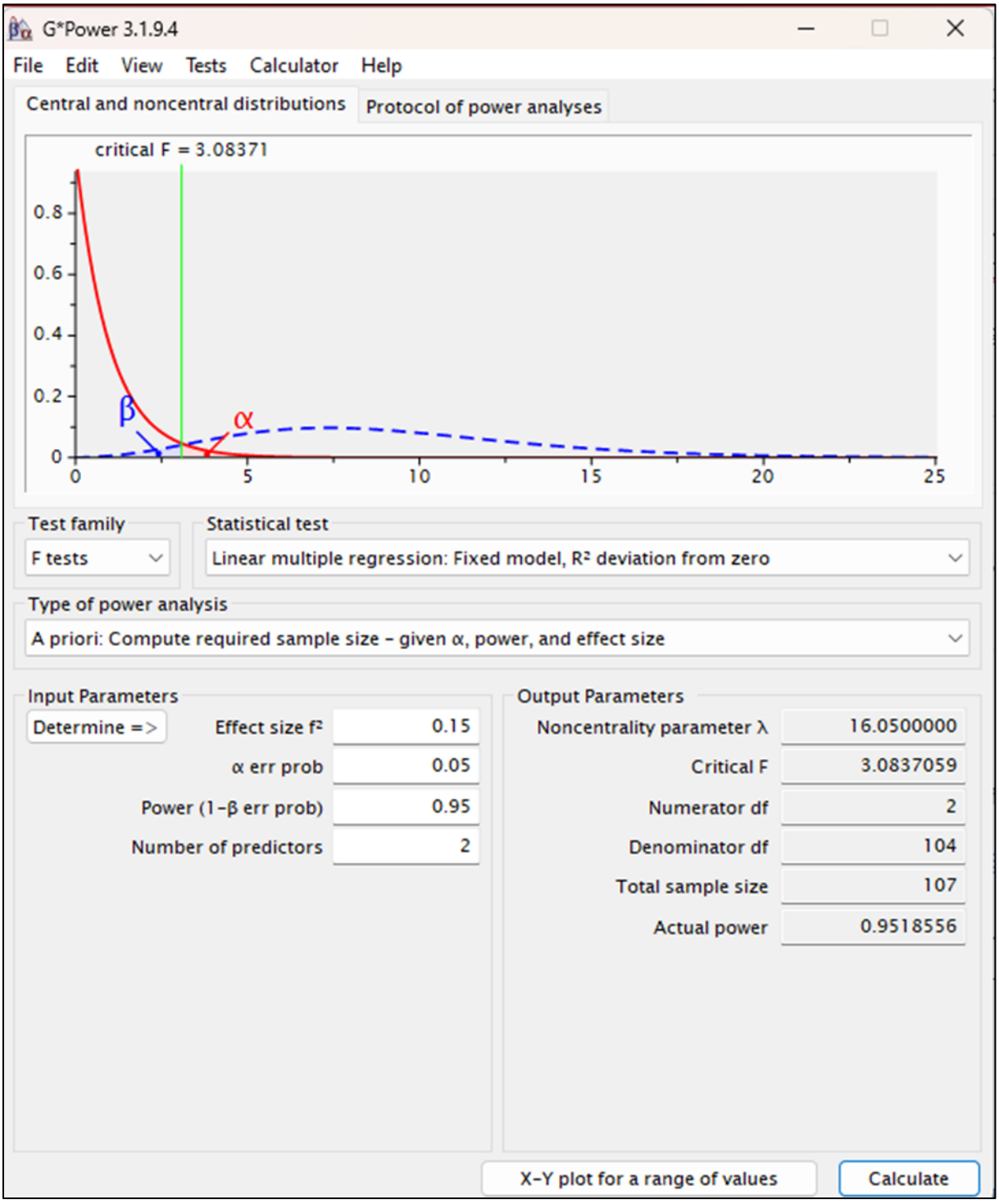
[77] Wu, J., Ji, X., He, L., Xie, Y., Niu, Y., & Zhang, F. (2025). Development Status, Trends, and Prospects of Cybersecurity Strategies and Methods. *Strategic Study of Chinese Academy of Engineering*, *27*(1), 14-27.

[78] Wu, L., Peng, Q., & Lembke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. *International Journal of Cybersecurity Intelligence & Cybercrime*, *6*(1), 5-28.

[79] Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), 407-416.

[80] Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613-636.

Appendix A


G*Power 3.1.9.4
File Edit View Tests Calculator Help
Central and noncentral distributions
Protocol of power analyses
critical F = 3.08371
0.8
0.6
0.4
0.2
0
β
α
0
5
10
15
20
25
Test family
F tests
Statistical test
Linear multiple regression: Fixed model, R² deviation from zero
Type of power analysis
A priori: Compute required sample size – given α, power, and effect size
Input Parameters
Determine =>
Effect size f²
0.15
α err prob
0.05
Power (1–β err prob)
0.95
Number of predictors
2
Output Parameters
Noncentrality parameter λ
16.0500000
Critical F
3.0837059
Numerator df
2
Denominator df
104
Total sample size
107
Actual power
0.9518556
X-Y plot for a range of values
Calculate

Appendix B

Output of skewness and kurtosis calculation

```
Sample size:  181
Number of variables:  3

Univariate skewness and kurtosis
    Skewness SE_skew Z_skew Kurtosis SE_kurt Z_kurt
BIP   -1.571   0.181 -8.697    1.444   0.359  4.020
CBA   -0.795   0.181 -4.404   -0.304   0.359 -0.846
PT    -1.195   0.181 -6.617    1.578   0.359  4.392

Mardia's multivariate skewness and kurtosis
                b           z   p-value
Skewness  4.159886 125.4898920 0.0000000
Kurtosis 14.655890  -0.4226164 0.6725752
```

Appendix C

Cross Loadings

Items	BIP	CBA	PT
BIP3	**0.916**	0.604	0.736
BIP4	**0.981**	0.828	0.782
BIP5	**0.959**	0.809	0.793
CBA3	0.720	**0.980**	0.744
CBA4	0.808	**0.987**	0.870
CBA5	0.807	**0.993**	0.831
PACT1	0.251	0.364	**0.539**
PACT2	0.730	0.794	**0.967**
PACT3	0.747	0.850	**0.915**
PACT4	0.837	0.675	**0.882**