Int. j. adv. multidisc. res. stud. 2026; 6(4):1675-1681

Received: 04-07-2026
Accepted: 14-08-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Cybersecurity Knowledge and Awareness as Predictors of Safe Computing Practices among First-Year University Students in South-East Nigeria

Samuel Okechukwu Nnaji
Department of Computer Science, Cyber Security and Software Engineering, Federal University of Environment and Technology, Koroma/Saakpenwa-Ogoni, Rivers State, Nigeria

Corresponding Author: **Samuel Okechukwu Nnaji**

Abstract
The rapid expansion of internet access and digital learning platforms in Nigerian tertiary institutions has increased first-year students' exposure to cyber threats, including phishing, identity theft, malware, and social engineering. This study investigated cybersecurity knowledge and awareness as predictors of safe computing practices among first-year university students in Southeast Nigeria. Guided by Protection Motivation Theory, the study adopted a correlational survey design. The population comprised all first-year undergraduate students admitted into public universities in Southeast Nigeria during the 2025/2026 academic session, estimated at approximately 38,600 students across the six sampled institutions based on institutional admission records. A multistage sampling technique selected 384 students from six public universities across the five Southeast states. Data were collected using a validated 42-item Cybersecurity Knowledge, Awareness and Safe Computing Practices Questionnaire (CKASCPQ), with Cronbach's alpha coefficients ranging from 0.79 to 0.88. Data were analyzed using descriptive statistics, Pearson correlation, multiple regression, and independent-samples t-test at 0.05 significance. Results showed that cybersecurity knowledge ($\beta = 0.41$, $p < 0.05$) and awareness ($\beta = 0.36$, $p < 0.05$) significantly predicted safe computing practices and jointly explained 52.3% of the variance ($R^2 = 0.523$, $F(2, 381) = 208.47$, $p < 0.001$). Gender differences were not significant ($t(382) = 1.42$, $p = 0.157$). The study recommends mandatory cybersecurity literacy during orientation, sustained awareness campaigns, and practical cyber-hygiene modules in university curricula.

Keywords: Cybersecurity Knowledge, Cybersecurity Awareness, Safe Computing Practices, First-Year Students, Southeast Nigeria

1. Introduction

The twenty-first century university experience is inseparable from digital technology. From course registration and e-learning platforms to social networking and online financial transactions, first-year university students in Nigeria are increasingly required to navigate a complex digital ecosystem almost immediately upon matriculation. This heightened digital dependence, however, exposes an already vulnerable population young adults with limited prior exposure to structured cybersecurity education to an expanding range of cyber threats, including phishing, malware, identity theft, cyberbullying, and social-engineering attacks.

Nigeria is one of the largest and fastest-growing digital economies in Africa, with a youthful population and rising smartphone and broadband internet penetration; tertiary institution students routinely use digital platforms for academic research, online registration, e-learning, social networking, and electronic transactions (Bada *et al*., 2019) [4]. Despite this heavy reliance on digital tools, empirical evidence suggests that cybersecurity awareness among Nigerian students remains inconsistent, with studies indicating that over sixty percent of Nigerian university students have experienced at least one form of cyberattack, largely attributable to inadequate awareness and unsafe online behaviour (Chukwuma, 2021) [5].

First-year students constitute a particularly susceptible sub-population. Having recently transitioned from secondary school environments with limited independent digital responsibility, many enter university with fragmented or superficial cybersecurity knowledge, relying largely on informal sources such as peers and social media rather than structured instruction (Garba, Siraj, Othman, & Musa, 2021) [6]. Studies indicate that university students in African countries often possess basic ICT skills but lack sufficient knowledge of cybersecurity risks and protective practices, a gap that poses a significant challenge to

sustainable digital development on campuses (Adebayo & Abdulhamid, 2020) [1].

Safe computing practices encompassing behaviours such as the use of strong and unique passwords, regular software updates, cautious handling of unsolicited messages and links, use of multi-factor authentication, avoidance of unsecured public Wi-Fi for sensitive transactions, and responsible social media disclosure are widely regarded as the behavioural outcome of adequate cybersecurity knowledge and awareness (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014) [15]. Protection Motivation Theory (PMT) provides a useful theoretical lens for understanding this knowledge-awareness-behaviour pathway, positing that protective behaviour is activated when individuals appraise both the threat (severity and vulnerability) and their capacity to cope with it (response efficacy and self-efficacy) (Rogers, 1983) [16]. Within this framework, cybersecurity knowledge supplies the cognitive foundation for threat appraisal, while cybersecurity awareness sustains the ongoing vigilance necessary for coping appraisal and behavioural enactment.

Although a growing body of research has examined cybersecurity awareness in Nigerian tertiary institutions generally (Adeshola & Oluwajana, 2025 [2]; Digital Literacy and Cybersecurity Awareness study, 2026), few studies have isolated first-year students as a distinct analytical group or examined the Southeast geopolitical zone specifically, despite the zone's rapidly expanding university enrolment and internet usage. It is against this backdrop that the present study investigates cybersecurity knowledge and awareness as predictors of safe computing practices among first-year university students in Southeast Nigeria.

Statement of the Problem

First-year students in Southeast Nigerian universities are compelled, almost from the point of matriculation, to conduct academic and personal activities online registering courses, accessing e-portals, and communicating through social media and messaging platforms often without any formal orientation to cybersecurity. Anecdotal and empirical evidence suggests that this population frequently falls victim to phishing schemes, account compromise, malware infection, and social-engineering fraud, with many students unable to distinguish legitimate digital communication from malicious content (Chukwuma, 2021) [5]. While digital literacy levels are reportedly rising among Nigerian tertiary students, cybersecurity awareness specifically remains insufficient for ensuring safe digital practices, and this shortfall has been linked to weak institutional policy enforcement and limited curriculum integration of cyber-hygiene content. What remains unclear, however, is the precise extent to which cybersecurity knowledge and cybersecurity awareness as conceptually distinct but related constructs independently and jointly predict actual safe computing practices among first-year students specifically, as opposed to the general undergraduate population. Many existing Nigerian studies focus broadly on ICT literacy without explicitly linking cybersecurity awareness to observable online safety behaviours, leaving a gap in evidence-based, behaviourally grounded intervention design. This study therefore addresses the problem of insufficient predictive, behaviourally focused evidence on how cybersecurity knowledge and awareness translate into safe computing practices among first-year university students in South-east Nigeria.

Purpose of the Study

The general purpose of this study is to investigate cybersecurity knowledge and awareness as predictors of safe computing practices among first-year university students in South-east Nigeria. Specifically, the study seeks to:

1. Determine the level of cybersecurity knowledge possessed by first-year university students in Southeast Nigeria.
2. Determine the level of cybersecurity awareness among first-year university students in Southeast Nigeria.
3. Assess the level of safe computing practices exhibited by first-year university students in Southeast Nigeria.
4. Examine the extent to which cybersecurity knowledge predicts safe computing practices among first-year university students.
5. Examine the extent to which cybersecurity awareness predicts safe computing practices among first-year university students.
6. Determine the joint predictive contribution of cybersecurity knowledge and awareness to safe computing practices.

Research Questions

1. What is the level of cybersecurity knowledge among first-year university students in Southeast Nigeria?
2. What is the level of cybersecurity awareness among first-year university students in Southeast Nigeria?
3. What is the level of safe computing practices among first-year university students in Southeast Nigeria?
4. To what extent does cybersecurity knowledge predict safe computing practices among first-year university students in Southeast Nigeria?
5. To what extent does cybersecurity awareness predict safe computing practices among first-year university students in Southeast Nigeria?
6. What is the joint contribution of cybersecurity knowledge and awareness to the prediction of safe computing practices?

Research Hypotheses

The following null hypotheses were formulated to guide the study and were tested at the 0.05 level of significance:

1. **Ho_1:** Cybersecurity knowledge does not significantly predict safe computing practices among first-year university students in South-east Nigeria.
2. **Ho_2:** Cybersecurity awareness does not significantly predict safe computing practices among first-year university students in South-east Nigeria.
3. **Ho_3:** Cybersecurity knowledge and awareness do not jointly and significantly predict safe computing practices among first-year university students in South-east Nigeria.
4. **Ho_4:** There is no statistically significant difference in the safe computing practices of male and female first-year university students in South-east Nigeria.

Scope of the Study

The study was delimited to first-year undergraduate students in six public universities drawn from the five states of South-east Nigeria Abia, Anambra, Ebonyi, Enugu, and Imo. The content scope covered cybersecurity knowledge, cybersecurity awareness, and safe computing practices, with

gender as the sole demographic moderating variable examined. Data collection took place within a single academic session and therefore reflects a cross-sectional, not longitudinal, picture of the constructs under study.

2. Literature Review

Cybersecurity Knowledge

Cybersecurity knowledge refers to an individual's cognitive understanding of digital threats, protective technologies, and safe online conduct, encompassing factual awareness of concepts such as malware, phishing, encryption, password hygiene, and data privacy regulation. In the Nigerian context, this knowledge is shaped by exposure to formal ICT instruction, informal peer learning, and public enlightenment campaigns championed by agencies such as the National Information Technology Development Agency (NITDA), whose Nigeria Data Protection Regulation (NDPR) sets the legal baseline for data protection literacy (NITDA, 2019) [13].

Cybersecurity Awareness

Cybersecurity awareness extends beyond static knowledge to encompass an individual's ongoing vigilance, risk perception, and attentiveness to cyber threats as they are encountered in daily digital activities (Bada, Sasse, & Nurse, 2019) [4]. It is frequently operationalized using instruments such as the Human Aspects of Information Security Questionnaire (HAIS-Q), which assesses awareness across knowledge, attitude, and behaviour dimensions (Parsons *et al*., 2014) [15]. Awareness is thus a more dynamic, dispositional construct than knowledge, reflecting sustained attentiveness rather than mere factual recall.

Safe Computing Practices

Safe computing practices constitute the behavioural manifestation of cybersecurity knowledge and awareness, comprising concrete actions such as using strong and unique passwords, enabling multi-factor authentication, updating software and applications promptly, avoiding suspicious links and attachments, using secure networks for sensitive transactions, and exercising caution in sharing personal information online (Thompson, McGill, & Wang, 2017) [18]. Although students frequently access the internet for academic and social purposes, many do not adopt basic cybersecurity measures such as strong passwords, regular software updates, or cautious handling of unsolicited messages (Adebayo & Abdulhamid, 2020) [1], underscoring the persistent gap between digital usage and protective behaviour.

Theoretical Framework

This study is anchored on Protection Motivation Theory (PMT), originally propounded by Rogers (1983) [16] to explain how fear appeals influence attitude and behaviour change, and subsequently extended to cybersecurity contexts. PMT proposes that protective behaviour results from two cognitive appraisal processes: threat appraisal (comprising perceived severity and perceived vulnerability to a threat) and coping appraisal (comprising response efficacy, self-efficacy, and response cost). When individuals perceive a cyber-threat as both severe and personally relevant, and simultaneously believe that a recommended protective action is effective and within their capability, they are more likely to adopt that protective behaviour (Milne, Sheeran, & Orbell, 2000) [12].

Within the context of this study, cybersecurity knowledge is theorized to feed primarily into the threat-appraisal process by equipping students with the cognitive resources to recognize and evaluate risk, while cybersecurity awareness sustains the coping-appraisal process by maintaining behavioural vigilance and confidence in protective action. PMT has been widely applied beyond its original health-behaviour context to cybersecurity, online privacy, and technology-use domains, demonstrating robust utility in explaining protective decision-making in digital environments (Kiran, Balla, & Hagger, 2025) [8].

Conceptual Framework

Fig 1 presents the conceptual framework guiding this study, illustrating the hypothesized pathways from cybersecurity knowledge and cybersecurity awareness, through Protection Motivation Theory's threat and coping appraisal mechanism, to safe computing practices, with demographic variables considered as background factors.

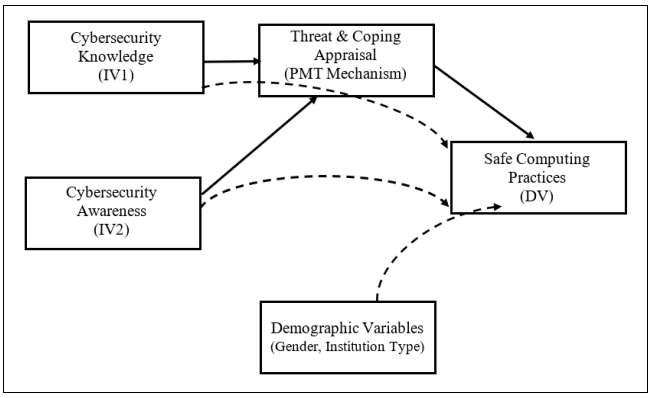

Fig 1: Conceptual Framework Linking Cybersecurity Knowledge and Awareness to Safe Computing Practices

Gap in the Literature

Despite the expanding literature, several gaps remain. First, many Nigerian studies examine cybersecurity awareness among the general undergraduate population rather than first-year students specifically, a group whose recent transition from secondary education and limited prior exposure to structured cybersecurity instruction make them uniquely vulnerable. Second, few studies simultaneously model cybersecurity knowledge and cybersecurity awareness as conceptually distinct predictors within a single regression framework, often conflating the two constructs. Third, empirical, quantitative, theory-driven studies focused specifically on the Southeast geopolitical zone of Nigeria remain scarce, despite the zone's rapidly expanding tertiary enrolment. The present study addresses these gaps by examining first-year students exclusively, modelling knowledge and awareness as distinct predictors within a Protection Motivation Theory framework, and focusing specifically on Southeast Nigeria.

3. Methodology

Research Design

This study adopted a correlational survey research design of the predictive (ex post facto) type, which is appropriate for examining the extent to which one or more independent

variables predict a dependent variable without manipulation of the variables under study. Specifically, cybersecurity knowledge and cybersecurity awareness were treated as predictor (independent) variables, while safe computing practices served as the criterion (dependent) variable.

Area of the Study

The study was conducted in Southeast Nigeria, comprising five states: Abia, Anambra, Ebonyi, Enugu, and Imo an area characterized by a dense concentration of public and private universities and rapidly rising internet and smartphone penetration among the youth population.

Population of the Study

The population comprised all first-year undergraduate students admitted into public universities in Southeast Nigeria during the 2025/2026 academic session, estimated at approximately 38,600 students across the six sampled institutions based on institutional admission records.

Sample and Sampling Technique

A sample of 384 first-year students was determined using the Krejcie and Morgan (1970) table for sample size determination, appropriate for a population of this magnitude at a 95% confidence level and 5% margin of error. A multistage sampling technique was employed: at stage one, one public university was purposively selected from each of the five states of the zone, with one additional university selected in the most densely populated state (Anambra), yielding six universities; at stage two, faculties were selected using simple random sampling; and at stage three, proportionate stratified random sampling was used to select individual first-year respondents from selected faculties, ensuring proportional gender and departmental representation. Of 400 questionnaires administered, 384 were correctly completed and returned, yielding a 96% response rate.

Instrument for Data Collection

Data were collected using a structured questionnaire titled "Cybersecurity Knowledge, Awareness and Safe Computing Practices Questionnaire (CKASCPQ)," developed by the researcher and adapted in part from the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons *et al*., 2014) [15]. The instrument comprised four sections: Section A elicited demographic information (gender, age, state); Section B measured cybersecurity knowledge (14 items); Section C measured cybersecurity awareness (14 items); and Section D measured safe computing practices (14 items). Items in Sections B–D were rated on a 4-point scale (Strongly Agree = 4, Agree = 3, Disagree = 2, Strongly Disagree = 1), except knowledge items, which were scored dichotomously (Correct = 1, Incorrect = 0) and subsequently converted to percentage scores for analysis.

Validity of the Instrument

Face and content validity of the instrument were established through review by three experts in cybersecurity education and measurement and evaluation at the researcher's institution. Their observations informed the modification of ambiguous items and the restructuring of the response format for clarity, after which a final validated version of the instrument was produced.

Reliability of the Instrument

The reliability of the instrument was established through a pilot study involving 40 first-year students from a university outside the main study area, who were excluded from the final sample. Cronbach's alpha coefficient was computed for each sub-scale, as presented in Table 1.

Table 1: Reliability Statistics of the Research Instrument (Pilot Sample, n = 40)

Sub-scale	No. of Items	Cronbach's Alpha (α)	Remark
Cybersecurity Knowledge Scale	14	0.79	Reliable
Cybersecurity Awareness Scale	14	0.84	Reliable
Safe Computing Practices Scale	14	0.88	Reliable
Overall Instrument	42	0.86	Highly Reliable

All sub-scales yielded alpha coefficients above the 0.70 threshold conventionally accepted for social science research (Nunnally, 1978) [14], confirming the internal consistency of the instrument.

Method of Data Collection

Questionnaires were administered physically to respondents in selected faculties with the assistance of trained research assistants, following institutional ethical clearance and informed consent. Respondents were assured of anonymity and confidentiality, and data collection spanned four weeks.

Method of Data Analysis

Research questions were answered using descriptive statistics mean, standard deviation, and percentages with a benchmark mean of 2.50 used to classify responses as high or low on the 4-point scale. Hypotheses 1 and 2 were tested using simple linear regression, Hypothesis 3 was tested using multiple linear regression, and Hypothesis 4 was tested using an independent samples t-test. All hypotheses were tested at the 0.05 level of significance using IBM SPSS Statistics version 27.

4. Results

Demographic Characteristics of Respondents

Table 2: Demographic Distribution of Respondents (N = 384)

Variable	Category	Frequency	Percentage (%)
Gender	Male	178	46.4
	Female	206	53.6
Age	16–18 years	241	62.8
	19–21 years	112	29.2
	22 years and above	31	8.0
State	Abia	68	17.7
	Anambra	92	24.0
	Ebonyi	62	16.1
	Enugu	88	22.9
	Imo	74	19.3

Answering the Research Questions

Research Questions 1–3: Levels of cybersecurity knowledge, awareness, and safe computing practices. Table 3 presents descriptive statistics, while Fig 2 illustrates the distribution of respondents across low, moderate, and high categories for each construct.

Table 3: Descriptive Statistics for Cybersecurity Knowledge, Awareness, and Safe Computing Practices

Variable	Mean	SD	Mean %	Interpretation
Cybersecurity Knowledge	31.2	8.4	55.7	Moderate
Cybersecurity Awareness	42.6	6.9	60.9	Moderate–High
Safe Computing Practices	38.4	9.1	54.9	Moderate

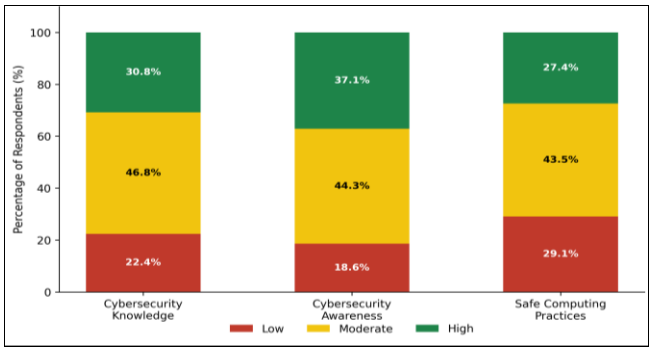

Fig 2: Distribution of Respondents by Level of Cybersecurity Knowledge, Awareness, and Safe Computing Practices

As shown in Table 3 and Fig 2, students recorded moderate mean scores across all three constructs, with awareness (60.9%) marginally higher than knowledge (55.7%) and safe computing practices (54.9%). Notably, only 30.8% of respondents demonstrated a high level of cybersecurity knowledge, while 29.1% exhibited low levels of safe computing practices, suggesting a meaningful proportion of first-year students remain inadequately protected in their day-to-day digital conduct.

Test of Hypotheses

Hypothesis 1: Cybersecurity Knowledge and Safe Computing Practices

H_{o1} stated that cybersecurity knowledge does not significantly predict safe computing practices. A simple linear regression was conducted, and results are presented in Table 4 and illustrated in Fig 3.

Table 4: Simple Linear Regression of Cybersecurity Knowledge on Safe Computing Practices

Model	B	Std. Error	β	t	p	R	R^2
(Constant)	17.85	1.94	-	9.20	.000	0.61	0.372
Cybersecurity Knowledge	0.66	0.04	0.61	16.72	.000		

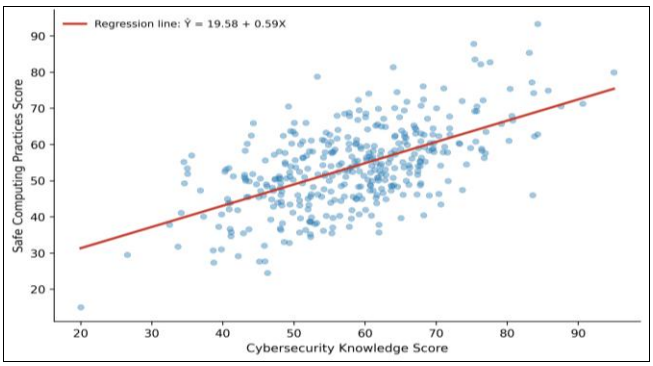

Fig 3: Scatter Plot Showing the Relationship between Cybersecurity Knowledge and Safe Computing Practices Scores

The regression result indicates that cybersecurity knowledge significantly predicted safe computing practices, β = 0.61, $t(382) = 16.72$, $p < .001$, accounting for 37.2% of the variance in safe computing practices ($R^2 = 0.372$). Since $p < 0.05$, the null hypothesis ($H0_1$) was rejected.

Hypothesis 2: Cybersecurity Awareness and Safe Computing Practices

H_{o2} stated that cybersecurity awareness does not significantly predict safe computing practices. Table 5 presents the regression result.

Table 5: Simple Linear Regression of Cybersecurity Awareness on Safe Computing Practices

Model	B	Std. Error	β	t	p	R	R^2
(Constant)	13.42	2.31	-	5.81	.000	0.45	0.204
Cybersecurity Awareness	0.59	0.05	0.45	10.99	.000		

Cybersecurity awareness significantly predicted safe computing practices, β = 0.45, $t(382) = 10.99$, $p < .001$, accounting for 20.4% of the variance ($R^2 = 0.204$). The null hypothesis ($H0_2$) was therefore rejected.

Hypothesis 3: Joint Prediction by Cybersecurity Knowledge and Awareness

H_{o3} stated that cybersecurity knowledge and awareness do not jointly and significantly predict safe computing practices. A multiple linear regression was conducted, with results presented in Tables 6 and 7.

Table 6: Model Summary for Multiple Regression of Knowledge and Awareness on Safe Computing Practices

Model	R	R^2	Adjusted R^2	Std. Error of Estimate
1	0.723	0.523	0.520	6.31

Table 7: ANOVA and Coefficients for Multiple Regression Model

Source / Predictor	B	Std. Error	β	t	p
Regression (F = 208.47, df = 2, 381, p = .000)					
(Constant)	9.14	2.05	-	4.46	.000
Cybersecurity Knowledge	0.44	0.04	0.41	11.53	.000
Cybersecurity Awareness	0.38	0.05	0.36	10.14	.000

The multiple regression model was statistically significant, $F(2, 381) = 208.47$, $p < .001$, with cybersecurity knowledge (β = 0.41, $p < .001$) and cybersecurity awareness (β = 0.36, $p < .001$) jointly accounting for 52.3% of the variance in safe computing practices ($R^2 = 0.523$, Adjusted $R^2 = 0.520$). Both predictors contributed uniquely and significantly to the model, with knowledge exerting a marginally stronger influence than awareness. The null hypothesis ($H0_3$) was therefore rejected.

Hypothesis 4: Gender Difference in Safe Computing Practices

H_{o4} stated that there is no statistically significant difference in the safe computing practices of male and female first-year students. An independent samples t-test was conducted, with results presented in Table 8.

Table 8: Independent Samples t-Test for Gender Difference in Safe Computing Practices

Gender	N	Mean	SD	df	t	p	Decision
Male	178	39.02	8.87	382	1.42	.157	Not Significant
Female	206	37.86	9.28				

The result shows no statistically significant difference in safe computing practices between male (M = 39.02, SD = 8.87) and female (M = 37.86, SD = 9.28) first-year students, $t(382) = 1.42$, $p = .157 > 0.05$. The null hypothesis ($H0_4$) was therefore retained.

Additional Analysis: Comparison across States

As a supplementary analysis, mean safe computing practice scores were compared across the five states of Southeast Nigeria, as illustrated in Fig 4, revealing modest but non-central variation that fell outside the primary scope of the stated hypotheses.

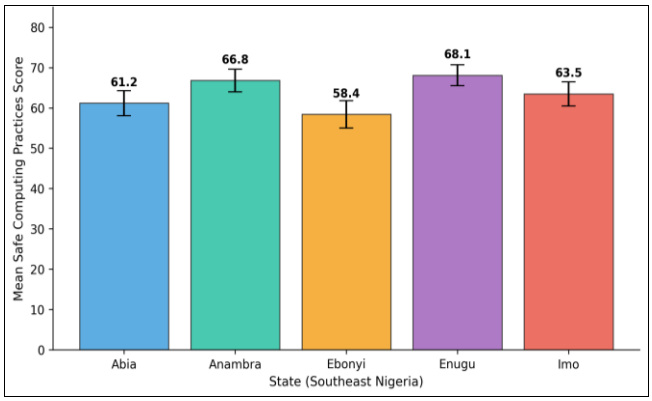

Fig 4: Mean Safe Computing Practices Scores of First-Year Students by State in Southeast Nigeria

5. Discussion of Findings

The findings of this study reveal that first-year university students in Southeast Nigeria possess generally moderate levels of cybersecurity knowledge, awareness, and safe computing practices, with awareness scoring marginally higher than the other two constructs. This pattern aligns with earlier Nigerian findings that digital literacy is relatively high among tertiary students while cybersecurity awareness specifically remains insufficient to guarantee consistently safe digital practice, suggesting that exposure to digital tools does not automatically translate into protective competence.

The significant predictive relationship found between cybersecurity knowledge and safe computing practices ($\beta = 0.41$) corroborates the theoretical proposition of Protection Motivation Theory that cognitive threat appraisal grounded in factual knowledge of risks is a necessary precursor to protective behaviour (Rogers, 1983) [16]. This finding is consistent with Adebayo and Abdulhamid (2020) [1], who found that gaps in basic cybersecurity knowledge among Nigerian students corresponded with lower adoption of protective measures such as strong passwords and cautious handling of unsolicited messages.

Similarly, the significant predictive contribution of cybersecurity awareness ($\beta = 0.36$) supports the coping-appraisal dimension of PMT and aligns with international evidence that awareness-raising interventions meaningfully shift self-reported protective behaviour among student populations (Adeshola & Oluwajana, 2025; Alsharida *et al*., 2023) [2, 3]. The joint model, explaining 52.3% of variance in safe computing practices, closely parallels findings from a related Nigerian tertiary study in which digital literacy and cybersecurity awareness jointly explained 58% of variance in safe digital practices, reinforcing the robustness of knowledge–awareness–behaviour pathways across similar Nigerian institutional contexts, even though the present study isolates a narrower and arguably more vulnerable first-year sub-population.

The absence of a statistically significant gender difference in safe computing practices contrasts with some international literature suggesting gendered patterns in cybersecurity risk perception, but is consistent with several Nigerian tertiary-level studies that report converging digital behaviour patterns between male and female students, likely reflecting near-universal smartphone and social media adoption across genders within this age cohort regardless of prior cybersecurity exposure.

Taken together, these findings suggest that while first-year students in Southeast Nigeria are not entirely lacking in cybersecurity competence, a substantial proportion remain moderately or poorly equipped, and that both cognitive knowledge and sustained situational awareness are indispensable, complementary levers for improving protective digital behaviour knowledge alone, without ongoing awareness reinforcement, appears insufficient to fully explain safe computing practices, as evidenced by the unexplained 47.7% of variance likely attributable to factors such as institutional policy enforcement, peer influence, self-efficacy, and access to protective technology not directly measured in this study.

6. Conclusion

This study set out to examine cybersecurity knowledge and awareness as predictors of safe computing practices among first-year university students in Southeast Nigeria. Anchored on Protection Motivation Theory and employing a correlational survey design with a validated instrument, the study found that first-year students exhibit moderate levels of cybersecurity knowledge, awareness, and safe computing practices; that cybersecurity knowledge and cybersecurity awareness each significantly and independently predict safe computing practices; that both constructs jointly account for a substantial proportion of variance in safe computing practices; and that safe computing practices do not differ significantly by gender. These findings affirm that cybersecurity knowledge and awareness are not merely academic constructs but measurable, actionable determinants of students' actual digital protective behaviour, with direct implications for how Nigerian universities structure orientation, curriculum, and campus-wide cybersecurity communication for incoming students.

7. Recommendations

Based on the findings of this study, the following recommendations are made:

1. Universities in Southeast Nigeria should introduce a mandatory, credit-bearing cybersecurity literacy module as part of first-year orientation and General Study's curricula, covering password hygiene, phishing recognition, safe social media use, and data privacy under the Nigeria Data Protection Regulation.
2. ICT directorates should institute sustained, semester-long cybersecurity awareness campaigns using posters, social media, orientation sessions, and periodic simulated phishing exercises rather than one-off enlightenment events, given that awareness was found to independently predict safe computing practices.
3. Faculty and departmental academic advisers should incorporate brief cybersecurity hygiene reminders into existing first-year academic advising and mentoring

sessions to reinforce knowledge gained during orientation.
4. University management should partner with agencies such as NITDA and the National Cybersecurity Coordination Centre (NCCC) to deliver periodic, evidence-based cybersecurity training tailored to student risk profiles.
5. Given that a meaningful proportion of students exhibited low safe computing practices despite moderate awareness, institutions should complement awareness campaigns with practical, hands-on cyber-hygiene clinics (e.g., guided password-manager setup, multi-factor authentication enrolment) to close the gap between awareness and actual behaviour.
6. Future researchers should extend this study by incorporating additional predictors such as self-efficacy, peer influence, and institutional policy enforcement, and by adopting longitudinal designs to track how cybersecurity knowledge, awareness, and practices evolve beyond the first year of study.

8. References

1. Adebayo AO, Abdulhamid SM. Cybersecurity awareness among undergraduate students in Nigerian tertiary institutions: A survey. Journal of Information Security and Applications. 2020; 8(2):45-58.
2. Adeshola I, Oluwajana DI. Assessing cybersecurity awareness among university students: Implications for educational interventions. Journal of Computers in Education. 2025; 12(4):1283-1305. Doi: https://doi.org/10.1007/s40692-024-00346-7
3. Alsharida RA, Al-Rimy BAS, Al-Emran M, Zainal A. A systematic review of cybersecurity behavior among students: Trends, gaps, and future directions. Education and Information Technologies. 2023; 28:12345-12370.
4. Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour? International Journal on Cyber Situational Awareness. 2019; 4(1):1-17.
5. Chukwuma E. Cyberattack experience and online safety behaviour among Nigerian university students. Nigerian Journal of Computer Studies. 2021; 9(3):22-34.
6. Garba AA, Siraj MM, Othman SH, Musa UI. Cybersecurity awareness of university students in Nigeria: Analysis approach. Turkish Journal of Computer and Mathematics Education. 2021; 12(12):3739-3752.
7. Khan NF, Ikram N, Saleem S. Digital divide and socio-economic differences in smartphone information security behaviour among University Students: Empirical evidence from Pakistan. International Journal of Mobile Communications. 2023; 21(3):245-268.
8. Kiran R, Balla D, Hagger MS. Examining university students' AI-generated content verification intention from a protection motivation perspective. arXiv preprint, 2025.
9. Kruger HA, Kearney WD. A prototype for assessing information security awareness. Computers & Security. 2006; 25(4):289-296. Doi: https://doi.org/10.1016/j.cose.2006.02.008
10. Lee S, Kim J. Cybersecurity awareness and compliance behaviour among higher education users. Computers & Security. 2023; 128:103148.
11. Li L, Zhang X, He W. Information security behaviour among university students: A protection motivation perspective. Journal of Information Systems Education. 2022; 33(2):112-126.
12. Milne S, Sheeran P, Orbell S. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. Journal of Applied Social Psychology. 2000; 30(1):106-143. Doi: https://doi.org/10.1111/j.1559-1816.2000.tb02308.x
13. National Information Technology Development Agency (NITDA). Nigeria Data Protection Regulation (NDPR), 2019. https://nitda.gov.ng
14. Nunnally JC. Psychometric theory (2nd ed.). McGraw-Hill, 1978.
15. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 2014; 42:165-176. Doi: https://doi.org/10.1016/j.cose.2013.12.003
16. Rogers RW. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology: A sourcebook. Guilford Press, 1983, 153-176.
17. Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010, 373-382. Doi: https://doi.org/10.1145/1753326.1753383
18. Thompson N, McGill TJ, Wang X. Security begins at home: Determinants of home computer and mobile device security behavior. Computers & Security. 2017; 70:376-391. Doi: https://doi.org/10.1016/j.cose.2017.07.003
19. Zwilling M, Lesjak D, Natek S, Pucihar A. The impact of technological infrastructure on digital learning and cybersecurity practices. Computers in Human Behavior Reports. 2022; 6:100187.