International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Effect of cybercrime risk on undergraduate behavioral intention in the federal universities in southwest, Nigeria

Olumide Opeyemi Babadele [1,*], Emmanuel Nimbe Olowokere [2], Modupe Olayinka Ajayi [1] and Kayode Joseph Ekundayo [1]

[1] *Department of Project Management Technology, School of Logistics and Innovation Technology, Federal University of Technology, Akure, Ondo State, Nigeria.*
[2] *Department of Business Information Technology, School of Logistics and Innovation Technology, Federal University of Technology, Akure, Akure, Ondo State, Nigeria.*

International Journal of Science and Research Archive, 2025, 17(01), 048-059

Publication history: Received on 25 August 2025; revised on 01 October 2025; accepted on 03 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2743

Abstract

Cybercrime has become one of the most pervasive threats to digital engagement globally, and undergraduates remain particularly vulnerable due to their extensive use of online platforms for financial transactions, academic activities, and social networking. In Nigeria, despite the establishment of cybercrime laws and consumer protection frameworks, weak enforcement and limited awareness continue to heighten students' exposure to online risks, thereby influencing their behavioral intentions toward digital participation. This study was conducted to evaluate the effect of cybercrime risk on undergraduate behavioral intention in South-West Nigeria. A descriptive survey design was employed, and the study population comprised undergraduates of federal universities in in the study area. Out of 900 questionnaires distributed, 653 were duly completed and returned, representing a response rate of 72.6 percent. The instrument was validated by experts in the field, while reliability was confirmed through Cronbach's alpha values above the 0.70 benchmark. Data were analyzed using descriptive statistics and inferential techniques, particularly regression analysis. The results revealed that cybercrime risk had a significant positive effect on undergraduate behavioral intention, with regression results showing $\beta = 0.401$, $R^2 = 0.177$, and $p < 0.001$. The study concluded that cybercrime risk strongly influences students' behavioral intention, either discouraging or shaping their adoption of online transactions depending on perceived levels of threat. It was recommended that cybersecurity awareness be integrated into undergraduate curricula, while universities, regulatory agencies, and financial institutions should strengthen digital literacy programs and implement effective consumer protection and redress mechanisms for students who fall victim to cybercrime.

Keywords: Cybercrime Risk; Behavioral Intention; Undergraduates; Consumer Protection; South-West Nigeria

1. Introduction

In today's interconnected world, cybercrime has become a pressing global threat with significant implications for individual users, businesses, and governments. Globally, cybercrime is estimated to cost the world economy over €300 billion annually, accounting for approximately 0.4% of the European Union's GDP alone (Cobos, 2024). The Federal Bureau of Investigation (FBI) ranks Nigeria among the top ten cybercrime hotspots worldwide, with losses running into billions of naira annually (Omobolade, 2025). These figures underscore the persistent vulnerability of consumers particularly young internet users who often lack the requisite awareness and protective mechanisms to navigate cyberspace safely.

* Corresponding author: Babadele, O. O

Developing countries, including Nigeria, face heightened exposure to cyber risks due to weak enforcement of cyber laws, limited institutional capacity, and low levels of cybersecurity awareness among consumers (Okoroafor, 2022; Sulubara et al., 2025). University undergraduates represent one of the most active groups of internet users in Nigeria, relying heavily on online platforms for academic research, financial transactions, and social networking. This exposure makes them highly susceptible to cyber threats such as phishing, identity theft, and online fraud (Okeke and Oli, 2023; Adamu et al., 2025). More critically, the perception of cybercrime risk significantly influences students' behavioral intentions toward adopting or avoiding online transactions. For instance, when undergraduates perceive online spaces as unsafe, they may reduce engagement in valuable digital activities or resort to risk adverse behaviors that hinder financial inclusion and digital learning opportunities (Wang et al., 2023).

The challenge, however, lies in the gap between existing consumer-protection frameworks and their practical effectiveness in shaping user behavior. In Nigeria, policies such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 and the Central Bank of Nigeria's Consumer Protection Framework aim to safeguard users. Yet, weak enforcement, lack of transparency, and low levels of consumer education continue to undermine trust, leaving undergraduates vulnerable and skeptical (Owuamanam, 2025). If unaddressed, this problem may perpetuate low adoption of secure e-banking practices, increase financial losses among students, and erode confidence in Nigeria's digital economy.

Studies across different contexts emphasize the behavioral consequences of perceived cyber risk. Reyns and Henson (2016) found that online routine activities directly influenced the likelihood of identity theft victimization in Canada, while Keipi et al. (2016) linked cyber risk to reduced online engagement among European youth. In the Nigerian context, Orji (2019) observed that poor liability regimes for unauthorized transactions discourage consumers from trusting digital banking platforms. These findings suggest that while global scholarship highlights the relationship between perceived risk and behavior, little is known about how this dynamic plays out specifically among Nigerian undergraduates who face unique socioeconomic and institutional realities.

The gap in literature lies in the limited empirical evidence on how undergraduates' perception of cybercrime risk influences their behavioral intentions within the Nigerian higher education setting. Most existing studies focus on general consumer groups or institutional perspectives (Nzeakor et al., 2020; Aljudaibi and Amuda, 2024), with few addressing young internet users as a distinct category of vulnerable consumers. This study therefore seeks to fill this gap by evaluating the effect of cybercrime risk on undergraduate behavioral intention in South-West Nigeria, using empirical evidence from undergraduates of federal universities.

2. Literature review

Cybercrime risk refers to the perceived likelihood that one might fall victim to online threats such as phishing, identity theft, malware attacks, and hacking during digital transactions. This perception is influenced by prior experiences of victimization, awareness of cyber threats, trust in protective mechanisms (e.g. cybersecurity laws or institutional safeguards), and sociodemographic factors such as age, gender, digital literacy, and educational level (Almaiah, AlOtaibi, Shishakly, et al., 2023; Ugwu, Ani, Ezema, et al., 2021). Among undergraduates—who frequently engage in e-learning, e-banking, social media, and other online services—high perceived cybercrime risk tends to result in reluctance or avoidance of some digital services, whereas lower perceived risk or stronger confidence in security mechanisms promotes greater adoption of such services (Garba, Kaur, and Nuraihan, 2023; Fahad and Nabeel, 2025).

Behavioral intention is a central construct in models such as the Theory of Planned Behavior and UTAUT, denoting an individual's readiness or willingness to engage in a behavior (e.g., to adopt online financial services safely). It is shaped by attitudes towards the behavior, subjective norms, perceived behavioral control, perceived risk, trust, and knowledge about security (Abawajy et al., 2022; Almaiah et al., 2023). For undergraduates, behavioral intentions carry extra significance because their online practices can influence academic integrity, financial inclusion, social interaction, and exposure to cyber harm.

Empirical investigations have repeatedly found that perceived risk is negatively associated with behavioral intention to use digital and financial technologies unless mitigated by trust, regulatory or institutional assurances, or greater digital knowledge. In Pakistan, Fahad and Nabeel (2025) found that perceived risk negatively predicted mobile-banking adoption intention among university students, but that higher digital knowledge mediated this relationship. Almaiah et al., (2023) in a study of smart m-banking users showed that perceived risk, security, and trust jointly influenced adoption intention via structural equation modelling in a Middle Eastern context. Similarly, Abikari (2024) showed that among educated young consumers, negative emotions associated with perceived risk reduce intention to adopt emerging e-banking technologies, while positive institutional trust and service quality enhance it.

Studies focused on undergraduates and ICT usage show comparable patterns The higher education environment in South Africa was studied by Goliath, Tsibolane, and Snyman (2024), who found students display a cybersecurity-resilience gap: though aware and somewhat attitudinally positive, many undergraduates' behavioral intentions do not translate into corresponding secure practices, often due to high perceived risk, low perceived control, or weak institutional support.

While there is abundant evidence that perceived cybercrime risk matters for behavioural intention in many contexts (e.g., digital banking, m-banking, IoT adoption), less work has focused specifically on undergraduates in Nigeria. Moreover, few studies have isolated the behavioral intention construct with full controls for digital knowledge, socioeconomic status, regulatory trust, or cross-faculty variation. In light of this, the present study fills this gap by empirically evaluating the effect of cybercrime risk on undergraduate behavioral intention within federal universities in Southwest, Nigeria.

From the reviewed literature, the following hypothesis was formulated for testing:

H_0: Cybercrime risk has no significant effect on undergraduates' behavioral intention in the study area

3. Methodology

This study employed a descriptive survey research design to evaluate the effect of cybercrime risk on undergraduate behavioral intention in South-West Nigeria. The research was carried out in Southwest Nigeria, which hosts federal universities with diverse student populations actively engaged in digital transactions. The target population consisted of undergraduates in these universities, and a multi-stage sampling procedure was used to select a sample size of 900 students, of which 653 questionnaires were duly completed and returned, representing a valid response rate of 72.6 percent. Data were collected using a structured questionnaire specifically designed to capture constructs relating to cybercrime risk and behavioral intention. Content validity of the instrument was established through expert review, while reliability was confirmed with Cronbach's alpha coefficients, all of which exceeded the acceptable threshold of 0.70. The data were analyzed using descriptive statistics, including frequencies, means, and standard deviations, as well as inferential statistics such as correlation and multiple regression analysis, to test the hypothesized effect of cybercrime risk on behavioral intention.

4. Results

4.1. Demographic Characteristics of Respondents

Data for this study were collected from undergraduates across six federal universities in South-West Nigeria, namely FUTA, FUOYE, UI, OAU, FUNAAB, and UNILAG. Out of the 900 questionnaires distributed, 653 were duly completed and returned, yielding a response rate of 72.5 percent, which is considered adequate for meaningful analysis. The demographic profile shows that the sample is predominantly male (57.3 percent), while females account for 42.7 percent. Most of the respondents are single (95.4 percent), with only 4.6 percent married. In terms of age, the majority fall within the traditional undergraduate bracket, with 54.7 percent between 18 and 22 years, and 29.1 percent between 23 and 25 years. Only 9.5 percent of respondents are older than 25, while 6.7 percent are below 18 years. Representation from the six universities is fairly broad. UNILAG contributed the largest share with 21.1 percent of the respondents, followed by UI with 17.8 percent, FUTA with 17.2 percent, OAU with 16.1 percent, FUNAAB with 14.4 percent, and FUOYE with 13.5 percent. This spread ensures that perspectives were drawn from different institutional contexts within the region. Academic levels of respondents show a tilt towards the upper years. Students in the 300–500 levels together make up 70.1 percent of the sample, with the 400 level alone contributing 36.0 percent. Students in the 200-level account for 20.4 percent, while those in the 100 level represent 9.5 percent. This indicates that a significant proportion of the respondents are senior undergraduates, who are more likely to have greater exposure to digital services and financial independence. Overall, the demographic characteristics reflect a respondent pool that is youthful, digitally active, and concentrated in senior levels of study, making them an appropriate group for examining issues related to cybercrime risk, consumer protection, and behavioral intention in the context of South-West Nigerian universities.

Table 1 Response rate of questionnaires

Item	Number
Questionnaires distributed	900
Questionnaires retrieved (used for analysis)	653
Response rate (%)	72.5

Source: Researcher's Field Report (2025)

Table 2 Demographic characteristics of respondents (n = 653)

Variable	Category	Frequency (n)	Percent (%)
Gender	Male	374	57.3
	Female	279	42. 7
Age	Less than 18 years	44	6.7
	18–22 years	357	54.7
	23–25 years	190	29.1
	Above 25 years	62	9.5
University	FUTA	112	17.2
	FUOYE	88	13.5
	UI	116	17.8
	OAU	105	16.1
	FUNAAB	94	14.4
	UNILAG	138	21.1
Level	100L	62	9.5
	200L	133	20.4
	300L	140	21.4
	400L	235	36.0
	500L	83	12.7
Marital status	Single	623	95.4
	Married	30	4.6

Source: Researcher's Field Report (2025)

4.2. Effect of Cybercrime Risk on Undergraduate Behavioural Intention in the Study Area

For this objective, the regression analysis (Tables 4.3 to 4.7) examined how cybercrime risk influences the behavioral intentions of undergraduates in South-West Nigeria. The dependent variable was *cybercrime risk* (avD1_7), representing students' perceptions of exposure to different forms of cyber threats. The main independent variable of interest was *undergraduate behavioral intention* (avD8_16), which reflects students' intentions regarding safe digital practices, cybersecurity compliance, and willingness to adopt protective measures online.

To account for demographic and institutional differences, several control variables were introduced and coded as dummy variables. Gender (A1) was defined such that male students were coded as 0, while female students were the reference category (1). Age (A2) was divided into students below 22 years coded as 0, and those aged 22 years and

above coded as 1 (reference). University affiliation (A3) was grouped into three categories: SW1 (UNILAG and FUNAAB), coded as 0; SW2 (UI and OAU), coded as 1 (reference); and SW3 (FUTA and FUOYE), also coded as 1 (reference). Level of study (A4) was split into junior students (100–

300 level), coded as 0, and senior students (400–500 level), coded as 1 (reference). This specification ensures that the regression analysis captures the net effect of behavioral intention on cybercrime risk while controlling for demographic and institutional variations.

The descriptive statistics in Table 4.3 show that students reported a relatively high average level of cybercrime risk (M = 3.25, SD = 0.43), alongside a slightly higher mean score for behavioral intention (M = 3.45, SD = 0.43). This indicates that while undergraduates recognize significant risks of cybercrime, they also display strong intentions to engage in protective behavior.

The correlation results in Table 4.4 reveal a strong positive and significant association between cybercrime risk and behavioral intention ($r = 0.462$, $p < 0.01$). This suggests that as students perceive greater cybercrime risks, they are more likely to adopt preventive behavioral intentions. Other demographic correlations were weak, with only slight associations observed for university affiliation (SW3: $r = 0.088$, $p < 0.05$; SW2: $r = 0.078$, $p < 0.05$), while gender, age, and level of study were not significantly correlated with cybercrime risk.

Table 3 Descriptive Statistics

Std.	**Mean**	**Deviation**	**N**
avD1_7 cybercrime risk	3.2465	0.42644	653
aGen_A1 Gender	0.4273	0.49506	653
aAge_A2 Age	0.3859	0.48718	653
aSW3_A3A_UNI FUTA FUOYE	0.3063	0.46130	653
aSW2_A3A_UNI UI OAU	0.3384	0.47354	653
aSL_A4 400_500L	0.4870	0.50021	653
avD8_16 undergraduate behavioural intention	3.4450	0.43113	653

Source: Researcher's Field Report (2025)

Table 4 Correlations

	avD1_7 cybercrime risk		**aGen_A1 Gender**	**aAge_A2 Age**	**aSW3_A3A_UNI FUTA FUOYE**	**aSW2_A3A_UNI UI OAU**	**aSL_A4 400_500L**	**avD8_16 undergraduate behavioural intention**
Pearson Correlation	avD1_7 cybercrime risk	1.000	0.022	-0.038	0.088	0.078	-0.013	0.462
	aGen_A1 Gender	0.022	1.000	-0.112	-0.278	0.095	-0.142	0.025
	aAge_A2 Age	-0.038	-0.112	1.000	0.026	-0.062	0.398	0.002
	aSW3_A3A_UNI FUTA FUOYE	0.088	-0.278	0.026	1.000	-0.475	0.124	-0.007
	aSW2_A3A_UNI UI OAU	0.078	0.095	-0.062	-0.475	1.000	-0.134	0.048

	aSL_A4 400_500L	-0.013	-0.142	0.398	0.124	-0.134	1.000	-0.029
	avD8_16 undergraduate behavioural intention	0.462	0.025	0.002	-0.007	0.048	-0.029	1.000
Sig. (1tailed)	avD1_7 cybercrime risk		0.285	0.167	0.012	0.024	0.368	0.000
	aGen_A1 Gender	0.285		0.002	0.000	0.007	0.000	0.259
	aAge_A2 Age	0.167	0.002		0.253	0.058	0.000	0.477
	aSW3_A3A_UNI	0.012	0.000	0.253		0.000	0.001	0.431
Pearson Correlation	avD1_7 cybercrime risk	1.000	0.022	-0.038	0.088	0.078	-0.013	0.462
	aGen_A1 Gender	0.022	1.000	-0.112	-0.278	0.095	-0.142	0.025
	aAge_A2 Age	-0.038	-0.112	1.000	0.026	-0.062	0.398	0.002
	aSW3_A3A_UNI FUTA FUOYE	0.088	-0.278	0.026	1.000	-0.475	0.124	-0.007
	aSW2_A3A_UNI UI OAU	0.078	0.095	-0.062	-0.475	1.000	-0.134	0.048
	aSL_A4 400_500L	-0.013	-0.142	0.398	0.124	-0.134	1.000	-0.029
	avD8_16 undergraduate behavioural intention	0.462	0.025	0.002	-0.007	0.048	-0.029	1.000
Sig. (1-tailed)	avD1_7 cybercrime risk		0.285	0.167	0.012	0.024	0.368	0.000
	aGen_A1 Gender	0.285		0.002	0.000	0.007	0.000	0.259
	aAge_A2 Age	0.167	0.002		0.253	0.058	0.000	0.477
	aSW3_A3A_UNI FUTA FUOYE	0.012	0.000	0.253		0.000	0.001	0.431
	aSW2_A3A_UNI UI OAU	0.024	0.007	0.058	0.000		0.000	0.112
	aSL_A4 400_500L	0.368	0.000	0.000	0.001	0.000		0.231
	avD8_16 undergraduate	0.000	0.259	0.477	0.431	0.112	0.231	

	behavioural intention							
N	avD1_7 cybercrime risk	653	653	653	653	653	653	653
	aGen_A1 Gender	653	653	653	653	653	653	653
	aAge_A2 Age	653	653	653	653	653	653	653
	aSW3_A3A_ UNI FUTA FUOYE	653	653	653	653	653	653	653
	aSW2_A3A_ UNI UI OAU	653	653	653	653	653	653	653
	aSL_A4 400_500L	653	653	653	653	653	653	653
	avD8_16 undergraduate behavioural intention	653	653	653	653	653	653	653

The model summary in Table 4.5 shows an R = 0.487 and R^2 = 0.237, indicating that the predictors explain 23.7% of the variance in cybercrime risk. This represents a stronger explanatory power than previous models (Objectives 3 and 4), suggesting that behavioral intention plays a substantial role in shaping perceptions of cybercrime risk among undergraduates. Table 4.6 (ANOVA) confirms the model's overall significance ($F(6, 646) = 33.515$, $p < 0.001$), demonstrating that the predictors jointly account for a significant variation in students' perception of cybercrime risk. The coefficients in Table 4.7 provide deeper insights. The strongest predictor was undergraduate behavioral intention, which had a positive and highly significant effect (B = 0.452, β = 0.457, t = 13.260, $p < 0.001$). This shows that higher levels of behavioral intention such as practicing safe online habits, avoiding suspicious links, and adopting protective software were strongly associated with students' awareness of cybercrime risk. Among the control variables, university affiliation showed significance: students in FUTA and FUOYE (SW3) reported higher perceptions of risk (B = 0.150, β = 0.163, t = 4.009, $p < 0.001$), and those in UI and OAU (SW2) also reported elevated risks (B = 0.116, β = 0.129, t = 3.290, p = 0.001), compared to the SW1 group (UNILAG and FUNAAB). Gender, age, and level of study were not significant predictors.

Overall, the regression results indicate that undergraduate behavioral intention is a strong determinant of how students perceive and respond to cybercrime risk, while institutional context (university affiliation) also influences risk perception. This suggests that both individual agency and institutional environment jointly shape the digital security outlook of undergraduates in the region.

Table 5 Model Summary

Model	R R Square	Adjusted R Square	Std. Error of the Estimate
1	.487[a] 0.237	0.230	0.37412

a. Predictors: (Constant), avD8_16 undergraduate behavioural intention, a Age_A2 Age, aSW3_A3A_UNI FUTA FUOYE, aGen_A1 Gender, aSL_A4 400_500L, aSW2_A3A_UNI UI OAU

Table 6 ANOVA[a]

Model	Sum of Squares	Mean Df Square	F	Sig.
Regression	28.146	6 4.691	33.515	.000b
Residual	90.419	646 0.140		
Total	118.565	652		

Dependent Variable: avD1_7 cybercrime risk Predictors: (Constant), avD8_16 undergraduate behavioural intention, aAge_A2 Age, aSW3_A3A_UNI FUTA FUOYE, aGen_A1 Gender, aSL_A4 400_500L, aSW2_A3A_UNI UI OAU

4.3. Unstandardized Standardized Collinearity Coefficients Statistics Std

Table 7 Coefficients[a]

Model	B	Error	Beta	T	Sig.	Tolerance	VIF
1 (Constant)	1.595	0.121		13.133	0.000		
aGen_A1 Gender	0.036	0.031	0.042	1.163	0.245	0.903	1.108
aAge_A2 Age	-0.033	0.033	-0.038	-1.002	0.317	0.836	1.197
aSW3_A3A_UNI FUTA FUOYE	0.150	0.038	0.163	4.009	0.000	0.716	1.397
aSW2_A3A_UNI UI OAU	0.116	0.035	0.129	3.290	0.001	0.764	1.309
aSL_A4 400_500L	0.015	0.032	0.018	0.476	0.634	0.819	1.221
avD8_16 undergraduate behavioural intention	0.452	0.034	0.457	13.260	0.000	0.996	1.004

a. Dependent Variable: avD1_7 cybercrime risk

5. Discussion of Findings

The results indicate that behavioral intention emerged as the strongest and most significant predictor of undergraduates' perception of cybercrime risk in South-West Nigeria. Specifically, students who expressed higher intentions to adopt protective behaviors also demonstrated greater awareness of and sensitivity to cybercrime threats. This aligns with Protection Motivation Theory, which posits that individuals' responses to threats are shaped by perceptions of vulnerability and severity, along with belief in the efficacy of preventive actions (Apaua and Lallie, 2022). In the present study, undergraduates who reported stronger intentions to engage in safe practices such as using strong passwords, avoiding phishing attempts, and keeping digital apps updated, were also more likely to recognize and report cybercrime risks.

The observed positive relationship between risk perception and behavioral intention mirrors findings from recent empirical work showing that awareness of cyber threats tends to motivate security-enhancing behavior among young people. For instance, Abikari (2024) found that emotions linked to perceive risk significantly shaped intention to adopt secure e-banking behaviors. Similarly, Abawajy et al. (2022) demonstrated that university students with higher perceived risk and stronger self-efficacy reported greater intention to adopt safe cybersecurity practices. In the Nigerian context, Garba et al., (2023) reported that awareness of cybercrime among online banking users strongly influenced their intention to adopt protective digital behaviors, while Ahmead et al (2024) highlighted that over half of surveyed undergraduates in Palestine linked their behavioral intentions directly to their perceived risk of victimization. These findings suggest that for undergraduates in Nigeria, who are frequent users of online banking, e-commerce, and social media platforms, recognizing cybercrime risks translates directly into stronger commitment to safe online practices.

Institutional affiliation was also significant: undergraduates from certain universities reported higher risk awareness than others. These differences may reflect varying levels of exposure to cybercrime education, differing institutional support for ICT security, or differing levels of digital infrastructure and awareness programs across universities. Similar to findings by Goliath, Tsibolane, and Snyman (2024), institutional context plays a critical role in shaping student risk awareness and corresponding behavioral intentions. This implies that undergraduates in institutions with stronger

digital literacy and sensitization programs may be better positioned to recognize threats and adopt preventive measures.

Interestingly, demographic variables such as gender, age, and level of study did not significantly predict cybercrime risk perception. That is, risk perception seems to be relatively uniform across these categories. This resonates with evidence from Garba et al. (2023), who found that Nigerian online banking users, regardless of demographic differences, shared similar vulnerabilities to cybercrime, largely because institutional weaknesses rather than personal traits determined exposure.

Altogether, the findings highlight two complementary drivers of cybercrime risk perception: individual behavioral intention, and institutional context. Students' willingness to engage in protective practices powerfully shapes their awareness of cyber threats, but the structural environment provided by universities also plays a decisive role. To reduce risk, both personal agency (through awareness, skills, intention) and institutional support systems (through education, policies, and access to digital security resources) are essential.

5.1. Implications of Findings

The findings from this objective have several important implications for both policy and practice in addressing cybercrime among undergraduates in South-West Nigeria.

First, the strong and positive influence of behavioral intention on cybercrime risk perception highlights the importance of fostering proactive security behaviors among students. This suggests that interventions should not only raise awareness of cyber threats but also empower students with concrete strategies for self-protection. Universities and regulators can integrate practical cybersecurity modules into general studies curricula, ensuring that students are equipped with actionable skills such as recognizing phishing attempts, safeguarding personal data, and reporting suspicious online activities. By doing so, institutions can strengthen the link between intention and actual protective behavior.

More so, the significant role of institutional affiliation implies that universities are not equally effective in shaping risk perceptions. While some institutions may provide more robust ICT training and consumer protection sensitization, others lag behind. This calls for harmonized institutional policies on cybersecurity education across Nigerian universities. The National Universities Commission (NUC) and the Federal Ministry of Education could mandate minimum standards for cybersecurity literacy programs to ensure that students in all universities receive consistent exposure to awareness and preventive measures.

Moreover, the non-significance of demographic variables such as gender, age, and academic level underscores that cybercrime risk is not limited to specific groups of students. Instead, all undergraduates are equally vulnerable. This means that interventions should adopt a universal approach, targeting the entire student population rather than tailoring programs to particular demographic subgroups. Such inclusiveness will ensure that no category of student is left unprepared against cyber threats.

Finally, the findings reinforce the urgent need for institutional and policy-driven collaboration. Universities, financial institutions, and consumer protection agencies must work together to develop responsive mechanisms that go beyond awareness to enforcement and redress. This could include confidential reporting channels within universities, stronger partnerships with law enforcement agencies, and nationwide digital safety campaigns. By addressing cybercrime at both the individual and systemic level, stakeholders can reduce students' vulnerability, build trust in digital systems, and contribute to the growth of Nigeria's digital economy.

6. Conclusion, Recommendations, Contributions to Knowledge and Suggestions for Further Studies

This study set out to evaluate the effect of cybercrime risk on undergraduate behavioral intention in South-West Nigeria, with specific focus on undergraduates of federal universities. The findings revealed that cybercrime risk significantly influences behavioral intentions, as students who perceive higher levels of risk are more likely to adopt risk-averse behaviors that limit their engagement in digital banking and online transactions. Conversely, those with lower or more manageable perceptions of risk tend to participate more confidently in digital activities. The study therefore concludes that cybercrime risk remains a critical determinant of behavioral intention among undergraduates, and that addressing it is central to building safer and more resilient digital practices within Nigerian universities.

In light of the findings, the study recommends that cybersecurity awareness programs should be systematically integrated into undergraduate curricula, enabling students to better understand and mitigate online threats. Regulatory agencies such as the Central Bank of Nigeria and the Nigeria Data Protection Commission should also strengthen enforcement of consumer protection laws while ensuring that victims of cybercrime have access to timely and transparent redress mechanisms. Furthermore, universities in collaboration with financial institutions should design targeted digital literacy and cyber-safety workshops to foster safe online practices. Policy frameworks should prioritize consumer trust through liability regimes that protect users against losses, while service providers should deploy technology-driven safeguards such as multi-factor authentication and fraud monitoring to reduce vulnerabilities in student populations.

The study makes several contributions to knowledge. It empirically demonstrates that cybercrime risk significantly predicts behavioral intention among undergraduates in South-West Nigeria, thereby extending behavioral theories such as the Theory of Planned Behavior into the domain of cyber risk. It also highlights undergraduates as a distinct category of consumers who face unique vulnerabilities, thereby expanding the existing literature beyond general populations. Importantly, the study reveals that students' perceptions of cyber risks, rather than the mere existence of regulatory frameworks, are more decisive in shaping their behavioral outcomes, which advances scholarly understanding of consumer behavior in digital environments. By providing context-specific evidence from Nigerian universities, the study further enriches the global discourse on cybercrime risk and behavioral intention in developing countries.

Although the study was limited to federal universities in South-West Nigeria, it opens avenues for further research. Future studies may extend the analysis to private and state universities, polytechnics, and colleges of education to broaden the scope of generalization. Longitudinal research designs would also be useful in capturing how cyber risk perceptions and behavioral intentions evolve over time, while qualitative approaches such as interviews and focus groups could provide richer insights into students' lived experiences of cybercrime victimisation. Moreover, further studies could investigate how socio-demographic factors such as gender, age, and income moderate the relationship between cybercrime risk and behavioral intention. Comparative studies across different regions of Nigeria or across other African countries are equally necessary to provide cross-cultural perspectives and to strengthen the evidence base on the dynamics of cybercrime risk and behavioral intention.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Statement of Ethical Approval

The University Research Ethics Committee approved the conduct of the study.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Abawajy, J., Addae, J. H., Brown, M., Sun, X., Towey, D., and Radenković, M. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, Article 107376. https://doi.org/10.1016/j.chb.2022.107376

[2] Abikari, M. (2024). Emotions, perceived risk and intentions to adopt emerging e-banking technology amongst educated young consumers. International Journal of Bank Marketing, 42(5), 1036-

[3] 1058. https://doi.org/10.1108/IJBM-01-2023-0004

[4] Adamu, U., Sarjiyus, O., and Nachandiya, N. (2025). Enhanced cybersecurity resilience model for sensitive data protection in Nigerian Tertiary Institutions: a review: a case study of Federal Polytechnic, Bali. Journal of Systematic and Modern Science Research.

[5] Ahmead, M., El Sharif, N., and Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross-sectional study. Crime Science,

[6] 13(29). https://doi.org/10.1186/s40163-024-00230-w

[7] Aljudaibi, S. A., and Amuda, Y. J. (2024). Legal framework governing consumers' protection in digital banking in Saudi Arabia. Journal of Infrastructure, Policy and Development, 8(8), 5453.

[8] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., and Alghanam, O. A. (2023). Investigating the Role of Perceived Risk, Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. Sustainability, 15(13) Article 9908. https://doi.org/10.3390/su15139908

[9] Apaua, R., and Lallie, H. S. (2022). Measuring user perceived security of mobile banking applications. arXiv preprint. https://arxiv.org/abs/2201.03052

[10] Cobos, E. V. (2024). Cybersecurity economics for emerging markets. World Bank Publications. Available at:

[11] https://books.google.com/books?

[12] hl=enandlr=andid=BfFiEQAAQBAJandoi=fndandpg=PT9anddq=Globally,+cybercrime+is+estimate d+to+cost+the+world+economy+over+%E2%82%AC300+billion+annually,+accounting+for

[13] +approximately+0.4%25+of+the+European+Union%E2%80%99s+GDP+alone+andots=Mgw Dv2qT8Vandsig=UeT8Z5kQFwx1cO3imKS_EstKwtg

[14] Fahad, A., and Nabeel, M. (2025). The Impact of Perceived Risk on Behavioral Intention toward Mobile Banking in Pakistan: The Mediating Role of Digital Knowledge. The Asian Bulletin of Big Data Management, 5(2). https://doi.org/10.62019/abbdm.v5i2.3

[15] Garba, J., Kaur, J., and Nuraihan, M. I. (2023). Awareness of cybercrime among online banking users in Nigeria. Nigerian Journal of Technology, 42(3), 406-413. https://doi.org/10.4314/njt.v42i3.14

[16] Goliath, S., Tsibolane, P., and Snyman, D. (2024). Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education. arXiv. https://arxiv.org/abs/2411.03219

[17] Keipi, T., Näsi, M., Oksanen, A., and Räsänen, P. (2016). Online hate and harmful content: Crossnational perspectives (p. 154). Taylor and Francis.

[18] Marafon, D. L., Basso, K., Espartel, L. B., and Rech, E. (2018). Perceived risk and intention to use internet banking: The effects of self-confidence and risk acceptance. International Journal of Bank Marketing, 36(2), 277-289. https://doi.org/10.1108/IJBM-11-2016-0166

[19] Moser, C. A., and Kalton, G. (2017). Survey methods in social investigation. Routledge.

[20] Nzeakor, O. F., Nwokeoma, B. N., and Ezeh, P. J. (2020). Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. International Journal of Cyber Criminology, 14(1), 283–299.

[21] Okeke, O. C., and Oli, N. P. (2023). Forms of cybercrimes perpetrated by Undergraduates in Selected Public and Private Tertiary Institutions in Anambra State, South-East, Nigeria. Social Science Research, 9(2).

[22] Okoroafor, N., Amah, J., Oyetoro, A., and Mart, J. (2022). Best Practices for Safeguarding IoT

[23] Devices from Cyberattacks. Available at: https://www.researchgate.net/profile/NneomaOkoroafor/publication/369231109_Best_Practices_for_Safegua rding_IoT_Devices_from_Cy berattacks/links/641106e166f8522c38a603b6/Best-Practices-for-Safeguarding-IoT-Devicesfrom-Cyberattacks.pdf

[24] Omobolade, I. T. (2025). Cybercrime prosecution in nigeria: challenges andprospects (doctoral dissertation, university of ibadan. Ibadan). Available at https://www.researchgate.net/profile/Timothy-

[25] Ilegbusi/publication/390941849_CYBERCRIME_PROSECUTION_IN_NIGERIA_CHALL

[26] ENGES_PROSPECTS/links/68039146d1054b0207d5813c/CYBERCRIMEPROSECUTION-IN-NIGERIA-CHALLENGES-PROSPECTS.pdf

[27] Orji, U. J. (2019). Protecting consumers from cybercrime in the banking and financial sector: an analysis of the legal response in Nigeria. Tilburg Law Review, 24(1).

[28] Owuamanam, C. I. (2025). Regulatory framework on cybersecurity in Nigeria. Polynek journal of law, technology and innovation, 1(1).

[29] Reyns, B. W., and Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International journal of offender therapy and comparative criminology, 60(10), 11191139.

[30] Sulubara, S. M., Tasril, V., and Nurkhalisah, N. (2025). Legal Protection of Cybercrime Crimes from Ransomware Attacks And Evaluation Of The Cyber Security And Resilience Bill 2025 In Indonesia'S Defense. DE LEGA LATA: Jurnal Ilmu Hukum, 10(2), 287-297.

[31] Tsai, C. Y. (2024). Is undergraduates' adoption of the Internet of Things rational? The role of risk perception. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18(4). https://doi.org/10.5817/CP2024-4-8

[32] Wang, D., Chen, Y., Tuguinay, J., and Yuan, J. J. (2023). The influence of perceived risks and behavioral intention: The case of Chinese international students. Sage Open, 13(2), 21582440231183435.