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

Cybercrime and consumer protection among undergraduates of the federal universities in southwest, Nigeria

Olumide Opeyemi Babadele *, Emmanuel Nimbe Olowokere, Modupe OlayinkaAjayi and Oluwaseyi Gabriel Sunday

Department of Project Management Technology, School of Logistics and Innovation Technology, Federal University of Technology, Akure, Ondo State, Nigeria.

International Journal of Science and Research Archive, 2025, 16(03), 1254-1262

Publication history: Received on 20 August 2025; revised on 25 September 2025; accepted on 29 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2712

Abstract

Cybercrime has emerged as a major challenge to digital security and consumer protection globally, with young people increasingly at risk due to their reliance on digital technologies. This study was therefore conducted to investigate cybercrime and consumer protection among undergraduates of federal universities in Southwest Nigeria. The specific objectives were to examine the effect of consumer protection on cybercrime. The study adopted a cross-sectional survey design. The population comprised undergraduates of six federal universities in Southwest Nigeria, with a sample size of 653 respondents selected through multistage sampling. Data were collected using a structured questionnaire and analysed using descriptive statistics, and multiple linear regression with dummy variables as controls. Regression analysis showed consumer protection had a significant effect on cybercrime experiences (R^2 = 0.178, F = 28.018, p < 0.001). Demographic controls such as gender, age, and level of study showed mixed but relatively weaker effects. The study concluded that although undergraduates are aware of cybercrime and consumer protection, mechanisms remain inadequate and ineffective, thereby exposing students to cyber risks. It was recommended, among others, that government agencies, regulatory bodies, and universities should strengthen enforcement mechanisms, promote digital literacy programmes, and implement more proactive consumer protection strategies to mitigate cybercrime among students.

Keywords: Cybercrime; Cyberattacks; Undergraduates; Consumer Trust; Consumer Protection

1. Introduction

In our digitally-driven world, cybercrime has emerged as a significant threat to industries worldwide, with the banking sector particularly vulnerable. Debarati and Jaishanka (2011) stated that cybercrimes are offences that are committed against individuals or group of individuals with criminal motive to intentionally harm the reputation of their victims or cause physical/mental harm to their victims directly or indirectly using modern telecommunication networks such as internet (chat rooms, e-mails etc.) and mobile phones (SMS/MMS). Cybercrime manifests in various forms, ranging from data breaches and phishing scams to ransomware attacks and insider threats. Each type poses unique risks and consequences for banks, their customers, and the financial ecosystem as a whole (Srijal & Batani, 2024).

The first published historical report of cybercrimes happened in the 1960s, when crimes were perpetrated by company employees, described then as computer crimes rather than cybercrimes since computers were not connected to the internet or any other computer (Maitanmi, as cited in Omodunbi et al., 2016). The growth of information technology and computer connectivity creates space for criminals to exploit security vulnerabilities in the cyber space. Unfortunately, several functionalities of the modern-day web browsers are not vulnerability-proof (Agbefu et al., 2013),

* Corresponding author: Babadele OO

thus exposing the average internet user to cybercrime victimization. Interpol (2021) argued that cybercrime affects all countries, but countries in Africa are particularly vulnerable because of their inadequate networks and security. According to Srijal and Batani (2024), fraud-related statistics show that banks in Nigeria lost N3.5 billion between July and September 2020. The need to address cybercrime in Nigeria was first noted in the Nigerian National Policy for Information Technology, 2001, which recognized the importance of establishing appropriate laws to tackle computer crimes and protect online business transactions.

The legal base of consumer protection in digital banking, in particular, includes some principles and practices consisting fairness and security of banking activities. Primordial factors include provisions on preventing fraud, ensuring data security, and mandatory disclosure. Furthermore, online conflict settlement procedures become key factors for resolution of disputes in an expedient way (Ajayi, 2018). Knowledge of consumer protection in digital banking by the concerned parties such as the policymakers, regulators, financial institutions, or even consumers themselves are regarded as important components. Regulatory mechanisms for fostering consumer trust in digital banking services in Nigeria are crucial (Ekpo, 2025).

Cybercrimes have become serious problem in Nigeria, ranking as the third out of the top ten cybercrime hot spots in the world (Federal Bureau of Investigation, 2010). Cybercrimes are experienced by people of all ages ranging from young to old, but the encountering of cybercrime among different age groups especially the undergraduates in their course of using electronic banking services is not known in Nigeria. University students are prime targets of cyberattacks as research shows frequent access to the internet compared to normal users (Adamu et al., 2021). It is therefore important to investigate the relationship between consumer protection and trust in electronic banking. This is on the ground that there exist a number of different cyber regulations in place. While Nigeria has taken legislative steps to foster consumer protection from cybercrime, gaps remain in the legal framework, necessitating further improvements.

Cyber laws do not make provisions for evolving cyber threats. The lack of satisfactory level of legislative compliance and implementation appears to reduce consumer trust in electronic banking. Lack of trust has led many customers afraid of participating electronic banking in general and electronic payments and/or fund transfers in particular (Maitanmi et al., 2013). Therefore, this study will examine the impact of cybercrime on undergraduates of the federal universities in the Southwest, Nigeria with a view to assessing the extent to which they are protected from cybercrimes in the banking sector.

2. Methods

This study employed a quantitative, cross-sectional survey design, which is well-suited for understanding the relationships between variables such as perception of cybercrime, types of threats encountered, and the effectiveness of consumer protection measures. The cross-sectional survey design collect data from a population at a single point in time, making it ideal for studies that seek to measure current behaviours, experiences, and perceptions. Given that the primary objective of this study is to understand undergraduates' fall victim of cybercrime and their respond to consumer protection mechanisms, a cross-sectional approach is appropriate. The study was conducted in Southwest Nigeria. The choice of the region is due to the educational and economic significance, hence, a strategic choice for examining cybercrimes and consumer protection among students who are highly engaged in digital activities compared to other regions, making cybercrimes a pertinent issue for its residents, particularly the younger population who frequently use online banking and digital services (National Bureau of Statistics, 2021). The population for this study comprised undergraduates enrolled in Federal Universities in Southwest Nigeria. The focus on undergraduates is justified due to their extensive use of technology in academic, personal, and financial activities, which exposes them to cyber threats. The population size for this study was estimated based on the total number of undergraduate students enrolled across selected Federal Universities in Southwest Nigeria with estimated total number of 126,825. The study employed stratified random sampling technique to ensure proportional representation from each federal university and across different academic levels and faculties. Yamane's formula (1967) was used to determine the most suitable sample size, depending on the estimated population of undergraduates in Federal Universities in Southwest Nigeria. Yamane's formula is a common approach for sample size determination in large populations and is expressed as:

$$n = N/(1+N(e)^2$$

Where:- n is the sample size; N is the population size; e is the margin of error (typically set at 5%). The calculated sample size is 399. Table 3.1 shows the study population and sample size for the study.

Table 1 Study Population and Sample Size

Universities	Population	Sample Size
University of Ibadan	15,125	48
Obafemi Awolowo University	28,498	90
Federal University of Technology Akure	18,220	57
University of Lagos	31,645	100
Federal University of Oye-Ekiti	17,371	55
Federal University of Agriculture Abeokuta	15,966	50
Total	126,825	399

NUC, 2023

The primary data collection tool for this study was a structured questionnaire designed to address the research objectives related to cybercrimes, factors hindering consumer protection and consumer protection among undergraduates in Federal Universities in Southwest Nigeria. Content validity of the questionnaire was ensured through consultation with experts in cybersecurity, consumer protection, and survey design. Following the expert review, a pilot study was conducted with a representative sample of 40 undergraduates drawn from the Federal University of Technology, Owerri (FUTO), who were not part of the main study population. The aim of the pilot study was to assess the clarity, appropriateness, and structure of the questionnaire.

3. Results and Discussion

3.1. Demographic information of Respondents

Data were drawn from the questionnaire survey administered across the six federal universities (FUTA, FUOYE, UI, OAU, FUNAAB and UNILAG) in South-West Nigeria. Of the 900-questionnaire distributed, 653 were duly completed and returned, yielding a response rate of 72.5 percent. Table 1 show information on demographic characteristics of respondents show predominantly male (57.3%) and overwhelmingly single (95.4%). A clear majority fall within the traditional undergraduate age bands: 18–22 years (54.7%) and 23–25 years (29.1%), with only 9.5% older than 25. University representation is broad across the six federal institutions, with UNILAG contributing the largest share (21.1%), followed by UI (17.8%) and FUTA (17.2%). Academic levels are tilted towards the upper years: 300–500 levels together account for 70.1%, with 400 level alone at 36.0%. This profile suggests a respondent pool with substantial exposure to digital services typical of senior undergraduates.

Table 2 Demographic information of respondents

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: Research survey, 2025

3.2. Effect of Consumer Protection on Cybercrime among Undergraduates

The analysis considered the types of cybercrime encountered by undergraduates as the dependent variable. The central explanatory factor was consumer protection, measured through students' perceptions of the adequacy and effectiveness of mechanisms designed to safeguard them against online exploitation.

As with the previous objective, control variables were incorporated to account for demographic and institutional influences. Gender was included, with male students serving as the baseline against which female students were compared. Age was also controlled, where undergraduates younger than twenty-two years represented the reference category, while those aged twenty-two years and above were contrasted with them. In terms of institutional representation, universities were grouped into three categories. The University of Lagos (UNILAG) and the Federal University of Agriculture, Abeokuta (FUNAAB) were taken as the baseline institutions, while comparisons were drawn with students at FUTA and FUOYE, and separately with those at the University of Ibadan (UI) and Obafemi Awolowo University (OAU).

These control variables ensured that the effect of consumer protection on cybercrime was examined beyond individual demographic differences and institutional contexts, thereby providing a more robust understanding of the relationship under investigation.

Table 3 presents the descriptive statistics for the variables included in the regression model. The mean score for types of cybercrime encountered was 3.18 with a standard deviation of 0.34, indicating that undergraduates experienced a moderate level of exposure to cybercrime. The mean for consumer protection was 3.10 with a standard deviation of 0.43, suggesting that students perceived consumer protection mechanisms to be fairly weak, though not completely absent. The control variables of gender, age, and university categories were also incorporated, reflecting the demographic and institutional spread of the respondents.

Table 3 Descriptive Statistics

	Mean	**Std. Deviation**	**N**
avB cybercrime TYPE	3.1776	0.34135	653
avE consumer protection	3.0960	0.42674	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

Source: Research survey, 2025

Table 4 shows the correlation results. A positive and statistically significant relationship was observed between consumer protection and the types of cybercrime encountered ($r = 0.382$, $p < 0.01$). This finding suggests that as students reported higher levels of consumer protection, they also tended to report higher levels of cybercrime experiences. This somewhat counter-intuitive outcome may reflect the possibility that students who are more aware of

consumer protection mechanisms are also more conscious of or more willing to report experiences of cybercrime. Other weak but significant correlations were noted between the dependent variable and gender as well as university categories, while the relationship with age was not statistically significant.

Table 4 Correlations

		avB cybercrime TYPE	**avE consumer protection**	**aGen_A1 Gender**	**aAge_A2 Age**	**aSW3_A3A_UNI FUTA FUOYE**	**aSW2_A3A_UNI UI OAU**
Pearson Correlation	avB cybercrime TYPE	1.000	0.382	0.073	0.001	0.037	0.118
	avE consumer protection	0.382	1.000	-0.026	-0.063	0.072	-0.014
	aGen_A1 Gender	0.073	-0.026	1.000	-0.112	-0.278	0.095
	aAge_A2 Age	0.001	-0.063	-0.112	1.000	0.026	-0.062
	aSW3_A3A_UNI FUTA FUOYE	0.037	0.072	-0.278	0.026	1.000	-0.475
	aSW2_A3A_UNI UI OAU	0.118	-0.014	0.095	-0.062	-0.475	1.000
Sig. (1-tailed)	avB cybercrime TYPE		0.000	0.032	0.490	0.170	0.001
	avE consumer protection	0.000		0.254	0.054	0.033	0.358
	aGen_A1 Gender	0.032	0.254		0.002	0.000	0.007
	aAge_A2 Age	0.490	0.054	0.002		0.253	0.058
	aSW3_A3A_UNI FUTA FUOYE	0.170	0.033	0.000	0.253		0.000
	aSW2_A3A_UNI UI OAU	0.001	0.358	0.007	0.058	0.000	
N	avB cybercrime TYPE	653	653	653	653	653	653
	avE consumer protection	653	653	653	653	653	653
	aGen_A1 Gender	653	653	653	653	653	653
	aAge_A2 Age	653	653	653	653	653	653
	aSW3_A3A_UNI FUTA FUOYE	653	653	653	653	653	653
	aSW2_A3A_UNI UI OAU	653	653	653	653	653	653

The model summary in Table 5 indicates that consumer protection, alongside the control variables, explained 17.8 per cent of the variance in the types of cybercrime experienced ($R^2 = 0.178$). The adjusted R^2 value of 0.172 confirms that the model provided a modest but reliable explanatory power in assessing the effect of consumer protection on cybercrime.

Table 5 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.422[a]	0.178	0.172	0.31067

a. Predictors: (Constant), aSW2_A3A_UNI UI OAU, avE consumer protection, aAge_A2 Age, aGen_A1 Gender, aSW3_A3A_UNI FUTA FUOYE

Table 6 which presents the ANOVA results, shows that the regression model was statistically significant, with an F-value of 28.018 at $p < 0.001$. This means that the combination of consumer protection and the control variables significantly predicted students' exposure to cybercrime in the study area.

Table 6 ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	13.521	5	2.704	28.018	.000[b]
	Residual	62.448	647	0.097		
	Total	75.969	652			

a. Dependent Variable: avB cybercrime TYPE; b. Predictors: (Constant), aSW2_A3A_UNI UI OAU, avE consumer protection , aAge_A2 Age, aGen_A1 Gender, aSW3_A3A_UNI FUTA FUOYE

The coefficients reported in Table 7 provide a more detailed understanding of the effect of each predictor. Consumer protection was found to exert a strong positive and highly significant influence on the types of cybercrime encountered ($B = 0.305$, $t = 10.632$, $p < 0.001$). This implies that, paradoxically, higher scores in consumer protection were associated with greater reported experiences of cybercrime. Among the control variables, gender showed a statistically significant effect, with female students more likely to report cybercrime exposure than their male counterparts ($B = 0.072$, $t = 2.796$, $p = 0.005$). The university categories also mattered, as students from FUTA and FUOYE ($B = 0.089$, $t = 2.860$, $p = 0.004$) and from UI and OAU ($B = 0.125$, $t = 4.274$, $p < 0.001$) reported higher exposure to cybercrime compared with those in UNILAG and FUNAAB. Age, however, did not make a significant contribution to predicting cybercrime experiences. Overall, the results indicate that consumer protection is significantly related to students' experiences of cybercrime, but the direction of the relationship suggests complex dynamics in which greater awareness or engagement with consumer protection does not necessarily translate to lower exposure to cybercrime.

Table 7 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.122	0.093		22.870	0.000		
	avE consumer protection	0.305	0.029	0.381	10.632	0.000	0.990	1.010
	aGen_A1 Gender	0.072	0.026	0.105	2.796	0.005	0.909	1.100
	aAge_A2 Age	0.031	0.025	0.044	1.228	0.220	0.980	1.021
	aSW3_A3A_UNI FUTA FUOYE	0.089	0.031	0.121	2.860	0.004	0.715	1.398
	aSW2_A3A_UNI UI OAU	0.125	0.029	0.174	4.274	0.000	0.769	1.300

a. Dependent Variable: avB cybercrime TYPE

4. Discussion of Findings

The results of this analysis reveal a significant relationship between consumer protection and students' experiences of cybercrime in federal universities in Southwest Nigeria. Contrary to what might be expected, the regression results indicated a positive association: students who reported higher levels of consumer protection also tended to report higher experiences of cybercrime. This suggests a paradox in which awareness of consumer protection measures does not necessarily translate into reduced victimisation.

One possible explanation is that students who are more knowledgeable about consumer protection frameworks are also more alert to recognising and reporting cybercrime. This aligns with findings in earlier Nigerian studies which observed that increased awareness of regulatory bodies and consumer rights often leads to heightened reporting rather than diminished incidence (Okeshola & Adeta, 2013; Ojedokun & Eraye, 2012). From this perspective, the relationship may reflect greater vigilance and exposure rather than the actual protective capacity of consumer protection mechanisms.

Institutional variation also emerged as an important factor. Students in FUTA, FUOYE, UI, and OAU reported significantly higher experiences of cybercrime compared with those in UNILAG and FUNAAB. This could be attributed to differences in the level of ICT integration, online engagement, or institutional policies related to digital safety. Previous research has shown that students in institutions with stronger digital infrastructures and broader online participation are more exposed to cybercrime risks (Adeniran, 2008). The higher exposure reported in these institutions may therefore reflect both the opportunities and risks associated with wider online interaction.

Furthermore, the analysis indicated that female students reported significantly greater exposure to cybercrime compared with their male counterparts. This aligns with empirical studies which have suggested that women may be more likely to be targeted by online scams, harassment, or identity theft due to both social and behavioural factors (Omodunbi et al., 2016). However, the lack of significant differences by age suggests that cybercrime is a pervasive threat across different stages of undergraduate life, consistent with the findings of Tade and Aliyu (2011) that cybercrime victimisation among youths cut across age categories.

In sum, these findings highlight the complexity of the relationship between consumer protection and cybercrime. While consumer protection awareness is clearly important, its current form may not be adequate to prevent cybercrime among undergraduates. Instead, it may function more as a mechanism for recognition and reporting rather than as an effective shield against victimisation.

4.1. Implications of Findings

The findings of this study carry important implications for both policy and practice. The positive association between consumer protection and reported experiences of cybercrime underscores the need to move beyond awareness creation towards the implementation of effective, enforceable protective measures. While it is encouraging that students are aware of consumer protection frameworks, the results suggest that this awareness is not yet translating into real safeguards. This highlights a critical gap between policy intent and practical enforcement.

For universities, the implication is that institutional consumer protection strategies must be strengthened, not only by providing information but also by establishing effective mechanisms for prevention and redress. For instance, clear reporting procedures, rapid response units, and student-focused digital security policies would provide undergraduates with more tangible protection against cybercrime. Integrating consumer protection education into digital literacy courses and orientation programmes would further ensure that students understand both their rights and the practical steps required to enforce them.

The observed institutional differences also suggest that interventions should be tailored to the specific contexts of individual universities. Institutions with higher reported experiences of cybercrime may need targeted programmes that combine awareness campaigns with practical tools, such as university-supported anti-phishing software, secure online portals for academic transactions, and collaborations with cybersecurity agencies.

The gender dimension of the findings points to the necessity of recognising that female students may be disproportionately affected by cybercrime. This calls for gender-sensitive protective strategies, including awareness campaigns that address the unique vulnerabilities of female students, as well as the provision of safe online reporting channels to encourage disclosure without fear of stigmatisation.

At the national policy level, the results highlight the urgent need to address the enforcement deficit in consumer protection. Agencies such as the Federal Competition and Consumer Protection Commission (FCCPC) and the Nigerian Communications Commission (NCC) must go beyond issuing guidelines to actively monitoring, enforcing, and publicising sanctions against cyber offenders. Stronger collaboration between universities, regulatory bodies, and law enforcement agencies will also be crucial in closing the gap between awareness and actual protection.

In sum, the findings imply that consumer protection must be repositioned as a proactive and enforceable system rather than a passive framework of awareness. Without this shift, undergraduates will continue to remain vulnerable despite being informed of their rights.

5. Conclusion and Recommendation

This study set out to examine cybercrime and consumer protection among undergraduates of federal universities in Southwest Nigeria. The study found that, consumer protection itself was shown to significantly influence cybercrime experiences, though in an unexpected direction. Higher perceptions of consumer protection were associated with greater reported exposure to cybercrime. This suggests that consumer protection measures are not yet functioning as effective deterrents, but may instead increase reporting and awareness of cybercrime incidents without reducing actual victimization. Consequently, the study recommends that government and consumer protection agencies should address systemic hindrances such as weak enforcement, poor awareness of consumer rights, and inadequate complaints-handling mechanisms.

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] Adamu, A. G., Maheyzah, B. S., and Siti, H. O. (2021). Cybersercurity awareness of university students in Nigeria. Analysis Approach. *Turkish Journal of computer mathemeatics Education (TURCOMAT) 12(12):3739-3752*

[2] Adeniran, I. A. (2008). The internet and emergence of Yahooboys sub-culture in Nigeria. International journal of cyber criminology (IJCC) ISSN 0974-2891 vol 2(2): 368-381

[3] Agbefu, R. E., Hon, Y., & Sakurai, K. (2013). Domain information blacklisting method for the detection of malicious webpages. *International Journal of Cyber Security and Digital Forensic, 2*(2), 36–47.

[4] Ajayi, C. B. (2018). Assessment of financial safety nets and banking sector stability in Nigeria: A study on NDIC. *Nigerian Law Review 10(4)89-105*

[5] Ekpo, E. (2025). The protection of consumer of banking services in Nigeria's cash-less Economy: Acomparative Analysis with China and U.S. Global journal of politics and law research, 13(4) 35-37, 2025

[6] Eleanya, F. (2021). Cyber fraud rises 534% as Nigerian banks lose N3.5 billion. BusinessDay. https://www.businessday.ng/banking-finance/article/cyber-fraud-rises-534-as-Nigerian-banks-lose-n3-5bn/

[7] Debarati, H., & Jaishankar, K. (2011). Cybercrime and victimization of women: Laws, rights and regulations. Hershey, PA: IGI Global.

[8] Federal Bureau of Investigation. (2010). Internet crime report. New York, NY: Federal Bureau of Investigation. https://www.fbi.gov/news/stories/2010/march/ic3031607

[9] Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. FUOYE Journal of Engineering and Technology, 1(1), 37–42.

[10] Okeshola, F. B and Adeta, A. K. (2013): The nature, causes and consequences of cybercrime in terirary institutions in Zari- Kaduna state, Nigeria. Computer Science, Law, Sociology

[11] Ojedokun, U. A and Eraye, M. C. (2012). Socioeconomic lifestyles of the Yahoo-Boys: A study of Perceptions of University students in Nigeria. International journal of cyber Criminology Vol. 6 issue 2.

[12] Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Cybercrimes and cyber laws in Nigeria. The International Journal of Engineering and Science (IJES), 2(4), 19–25.

[13] Srijal, T and Batani, R. (2024). Impact of cybercrime on the banking industry. International Jounal of Research Publication and Review. Vol (5)issue (4), April 2024, pp 4552-4558

[14] Tade, O and Aliyu, I (2011). Social organisation of internet fraud among university undergraduates in Nigeria. international journal of cyber criminology (IJCC) ISSN 0974-2891 Vol 5(2): 860-875