UKR Journal of Arts, Humanities and Social Sciences (UKRJAHSS)
Homepage: https://ukrpublisher.com/ukrjahss/
Email: submit.ukrpublisher@gmail.com
Volume 2, Issue 8, 2026
ISSN: 3107-359X (Online)

Digital Literacy and Cybersecurity Awareness as Predictors of Social Media Scam Victimization Among Tertiary Students in Anambra State, Nigeria

Victor Chukwuemelie Ilozue[1]* & Yadilichukwu Ikwuadinso[2]

[1&2] Department of Criminology and Security Studies, Chukwuemeka Odumegwu Ojukwu University, Igbariam Campus, Anambra State, Nigeria.

***Corresponding Author**: Victor Chukwuemelie Ilozue

DOI: *https://doi.org/10.5281/zenodo.21852835*

Article History

Original Research Article

Received: 09-06-2026

Accepted: 13-07-2026

Published: 08-08-2026

Citation: Ilozue, V. C., & Ikwuadinso, Y. (2026). Digital literacy and cybersecurity awareness as predictors of social media scam victimization among tertiary students in Anambra State, Nigeria. UKR Journal of Arts, Humanities and Social Sciences, 2(8), 27-38.

Abstract

The rapid shift towards online learning portals and digital platforms in Nigeria has thrown higher school students right into the path of social media fraud. This study measures if digital literacy and cybersecurity awareness predict social media scam victimization among tertiary students in Anambra State, Nigeria. Using a quantitative cross-sectional survey design, primary data were gathered via structured questionnaires from 399 undergraduate students across six public campuses within the state. The statistical findings indicate that both digital literacy and safety awareness act as major behavioral factors linked to student vulnerability, while heavy daily money struggles serve as a serious situational risk trigger. Specifically, simple linear regression shows that higher cybersecurity awareness directly lowers how vulnerable students feel to online tricks. An independent-samples t-test showed that students who had not experienced social media scams had significantly higher mean digital literacy scores than those who had experienced victimization. Finally, a chi-square test showed a significant association between financial pressure and social media scam victimization. Framed within Routine Activity Theory, these results establish that a user's personal tech skills function as an active digital shield within virtual spaces. This study shows that university heads and policymakers must stop using passive warning posters and quickly build practical, skill-based digital literacy modules within existing GST computer courses to protect students from local web predators.

Keywords: *Digital literacy, cybersecurity awareness, social media scams, victimization, tertiary students, Anambra State, Routine Activity Theory.*

1. Introduction

The way people commit, experience, and fight crime has changed completely because of digital tools. Today, the internet offers great channels for education, business, and daily communication. But this same network has handed online fraudsters clever routes to swindle unsuspecting targets. Social networks are the main playgrounds for these criminals. The apps are built to make people talk constantly, share things fast, and trust strangers easily. Because of this, scams like phishing, identity theft, fake investment setups, romance traps, and bogus job offers are everywhere online (Ajmal, 2026; Zwilling et al., 2022). Fresh records indicates that young adults, mostly university undergraduates, face the worst of these digital threats (Benson et al., 2015; Hadlington, 2017).

Undergraduates stay highly exposed because their daily school and social life forces them to stay online. Student life now revolves entirely around the internet. They pass lecture notes on WhatsApp and Telegram, run small businesses on Instagram, and pay school fees through mobile bank apps. This deep dive into the digital world comes with a heavy price, as it throws them right into the path of fraudsters. The real issue is that student victimization hardly happens because institutional firewalls broke down. Instead, it happens because criminals use social engineering. They study human choices, financial desperation, simple curiosity, and emotional weak points to wreck security from the inside (Lin et al., 2025; Ribeiro et al., 2024).

This shift shows that cybercrime has taken a new turn, moving away from core technical hacking toward psychological tricks. To build proper defenses, we must look past basic software and study how users behave. In a study covering students across 33 developing countries, Salem (2026) confirmed that basic tech literacy and high safety awareness directly stop digital harm. In another study, Ermumcu et al. (2026) found that personal privacy awareness cut down cyber victimization among Turkish undergraduates. These situations show that stopping fraud relies on building sharp critical thinking and safe habits so users can spot tricks before clicking dangerous links (Saritepeci, 2024).

In Nigeria, the situation looks worse because higher education institutions are pushing everyone online. Universities now process admissions, course forms, and tuition fees solely through internet portals. This rapid shift happened at a time when online threats are booming. The Nigerian Communications Commission (NCC, 2024) recently stated that internet scams jumped by 30% in one year, stealing billions of Naira from citizens. On campus, cheap smartphones and wider network coverage have completely changed student habits. Ezenwile and Nnoyelu (2026) showed that all types of cyber fraud are spreading across southeastern states like Imo, Abia, and Anambra. They pointed to poverty, unemployment, and sheer frustration as the main fuel. Police officers in Anambra State have openly worried about this bad trend among youths, warning that it endangers campus neighborhoods.

This state of affairs presents a serious criminological problem. In their daily tracks, students trade with unverified web sellers, seek remote jobs, and buy items on social marketplaces. Routine Activity Theory explains that these ordinary online habits accidentally bring motivated criminals and perfect targets together in the same virtual spaces (Cohen & Felson, 1979; Ngo & Paternoster, 2011). The older version of this theory focused on physical security, but modern researchers state it must cover digital environments (Leukfeldt & Yar, 2016). Recent studies show that solid digital literacy and sharp threat awareness act as vital digital shields that actively block fraud (Aningo & Nwokeoma, 2024; Lin et al., 2025).

Despite this clear reality, institutional setups in Nigeria are not balanced. Odoh and Oghuvbu (2026) pointed out at Delta State University that quick cash drives student cybercrime, yet universities care more about buying internet hardware than teaching students how to defend themselves (Garba et al., 2020). Also, older research usually looks at digital literacy, safety awareness, and victimization as single, separate issues. Solid field studies exploring how these behavioral habits work together to predict social media scams in Nigeria are still very rare (Muscanell & Guadagno, 2021).

This gap affects both academic ideas and practical rules. On the theoretical side, looking at these habits clarifies how internal protection works inside algorithm-driven spaces. On the practical side, it gives university heads and policymakers real facts to abandon useless warning posters and build interactive, skill-based digital literacy programs (Isma & Rosly, 2026; Sheng et al., 2010). To address these issues, this study measures whether digital literacy and cybersecurity awareness act as strong predictors of social media scam victimization among undergraduates inside public tertiary institutions in Anambra State, Nigeria.

2. Literature Review

Social media scams have become the main type of cybercrime because they exploit the way people behave rather than breaking into computer software (Benson et al., 2015; Vishwanath, 2015). Traditional hackers look for weak network systems, but social media fraudsters use mind tricks, lies, and fake friendships to make users give out secret information or send money. These tricks usually look like phishing mail, stolen identities, fake account profiles, unrealistic investments, bad web stores, or fake job ads (Hadlington, 2017; Muscanell & Guadagno, 2021). Because these frauds rely heavily on social engineering, experts now emphasize that studying victim habits is just as vital as tracking criminal tactics (Furnell & Clarke, 2012; Ribeiro et al., 2024). Criminology researchers have therefore stopped looking at cyber fraud as a plain technical error and now view it as a major behavioral issue (Ngo & Paternoster, 2011).

In this digital space, schools face massive cyber risks, making education the second most attacked sector regarding data theft and network hacks (Nigerian Communications Commission [NCC], 2024). Today's universities run almost entirely on web connections to handle school news, class timetables, staff work, grade sheets, and admission databases. Keeping threats like malware, spyware, viruses, and phishing away from these systems requires constant upkeep, including strong antivirus setups, fresh password changes, and tight privacy on student profiles (NCC, 2024). Standard records show that young folks between 18 and 23 years old fall into these online traps more than anyone else (NCC, 2024). In Nigeria, higher education students run high risks because they stay online all day, maintain loose browsing habits, and lack solid defense skills (Abah & Agada, 2025). This vulnerability grows alongside the country's rising digital economy, which has caused local financial fraud to transform from crude street tricks into complex web operations (Adebayo, 2025). Field data from southeastern Nigeria confirms that multiple variants of cybercrime

happen daily on campus, with phishing, identity theft, and social media fraud leading the pack (Ezenwile & Nnoyelu, 2026).

This sudden shift has made researchers focus closely on digital literacy as a tool for safety. Current studies show that digital literacy goes far beyond knowing how to click buttons on a screen. It covers the thinking patterns, critical judgment, and practical skills needed to find, check, and share information safely (Hargittai & Shaw, 2015; Saritepeci, 2024). While tracking web harassment inside AI-based study spaces, Salem (2026) found that personal tech literacy directly keeps university students safe from online harm. Field trials inside Indonesian schools also indicated that solid web skills give students a firm foundation to lock their personal data and spot online scams (Chigona & Mlotshwa, 2020; Dash & Mohanty, 2026). In southeastern Nigeria, Ugwuanyi et al. (2026) tested these patterns using a special eight-week training program sent to Economics Education undergraduates through mobile phone chats. Their records showed that targeted training caused a massive drop in student vulnerability, bad web behavior, and the urge to try cyber fraud. These results indicate that structured web training works well to guard students against online traps (Dodel & Mesch, 2019).

Cybersecurity awareness is closely tied to digital literacy, and it means how well a person understands web threats, follows safe protocols, and changes habits to avoid danger (Bulgurcu et al., 2010; McCormac et al., 2017). Even so, university data shows that merely knowing about a risk does not automatically make a student browse safely (Ajmal, 2026; Zwilling et al., 2022). For instance, tracking undergraduate habits reveals that even when students know the theoretical dangers of identity theft or phishing, many still reuse weak passwords, skip vital phone updates, and open strange links without checking them first (Dash & Mohanty, 2026). This huge gap between knowledge and action is a common topic in tech studies, proving that lasting safety happens only when theoretical awareness joins with the practical willpower to behave safely under pressure (Arachchilage & Love, 2014; Kritzinger & von Solms, 2010).

Demographics and personal habits make these safety patterns even more complex. In their study on undergraduate privacy, Ermumcu et al. (2026) discovered that while overall fraud numbers stayed low against decent privacy awareness, students showed massive differences internally. Specifically, knowing how to handle direct chats and personal posts protected students much better than basic technical password settings. Their data also showed that female students had much better privacy habits than male students, while final-year students fell victim to scams more than freshers. Crucially, spending too many hours on social apps cut down caution and raised fraud risks, proving that non-stop screen time can blunt a user's defensive habits.

At the same time, the channels used to spread safety news can cause extra issues. Looking at how social networks help teach the public, Akingbade (2023) discovered that over 65% of Nigerian internet users see cybersecurity tips online, and more than half improved their tech setups because of it. Yet, while social apps work well for quick public alerts, they can easily spread wrong tech advice, which gives students a fake sense of safety.

Recent research trends broadly back the protective power of tech skills. Salem (2026) suggested that sharp tech literacy brings safer web habits, making users much less likely to face targeted online harassment. To spread these benefits, Babadele et al. (2025) stated that schools must make cybersecurity lessons a compulsory part of university courses alongside strong tech literacy drives. Despite these clear facts, most past studies look at general web safety or device setups, leaving a big gap regarding targeted social media scams among students in developing regions (Garba et al., 2020). The Nigerian space requires deep field studies right now because fast network coverage, cheap smartphones, and online banking are changing student life much faster than school defense systems can adapt (Aningo & Nwokeoma, 2024; Balogun, 2024). Along with these global patterns, cybercrime inside Nigerian schools is becoming highly sophisticated. Phishing setups, fake financial deals, identity theft, cloned profiles, and bad social commerce web pages target young internet users daily (Odoh & Oghuvbu, 2026). Assessing cybercrime awareness among undergraduates, Garba et al. (2020) observed that a huge number of students had either personally fallen victim to digital fraud or closely knew someone who had. Their records linked risky online habits to excessive social media use, loose interactions online, and a general failure to report financial fraud to the police. Crucially, their study showed a serious lack of deep cybersecurity awareness regarding threat prevention. It suggested that while some undergraduates had a shallow knowledge of cyber threats, they lacked the practical skills to protect themselves (Garba et al., 2020).

This pattern matches the field observations of Odoh and Oghuvbu (2026), who noted that phishing, database hacking, and identity theft happen all the time within campus neighborhoods. Undergraduate vulnerability grows because students trade a lot online, search for jobs through unverified web boards, and easily share personal details across social applications. Despite this dangerous setup, structured tech training and defensive safety lessons are completely missing across Nigerian higher schools (Aningo & Nwokeoma, 2024; Babadele et al., 2025). National

setups like the Advanced Digital Empowerment Programme for Tertiary Institutions (ADEPTI) try to train thousands of workers in digital skills and security tracking, but these programs focus almost entirely on school staff instead of the students. This leaves a massive gap in student-centered safety training (Abah & Agada, 2025; NCC, 2024).

This local vulnerability is very obvious inside Anambra State. As a major center for trade and schooling in southeastern Nigeria, the state hosts a high number of higher institutions, making its student population a perfect target for web fraudsters. Local tracking across public and private universities in Anambra State confirms that internet scams, identity theft, and bank card fraud are widespread among undergraduates (Onyejiaka & Nwankwo, 2026; Onyeoziri, 2025). Police teams and federal offices see this crisis all the time. For example, the Economic and Financial Crimes Commission (EFCC) regularly raids student zones and has jailed many undergraduate fraud rings operating in places like Ifite-Awka and Onitsha (EFCC, 2025, 2026). This local emergency shows why we must stop using broad national guesses and focus on real local counts to see how specific habits protect undergraduates within Anambra's tough economic environment.

From a crime study viewpoint, Routine Activity Theory offers a solid path to explain these fraud patterns. The theory states that crime happens when a motivated criminal meets a perfect target where there is no capable guardian to stop them (Cohen & Felson, 1979). In virtual spaces, cybercriminals act as the motivated offenders, while undergraduates who lack basic digital skills or threat awareness become the perfect targets (Ngo & Paternoster, 2011). In this online setup, a capable guardian means more than just downloading a software tool. It includes the personal knowledge, sharp judgment, and safe browsing habits needed to spot and bypass lies (Lin et al., 2025). Using this theory to study online crime has caused a lot of academic debate. Leukfeldt and Yar (2016) pointed out that while web environments keep some basic structures, cyberspace is way more fluid, fast, and messy than the physical world, which challenges old ideas of physical guarding. Even so, they concluded that a fresh theoretical view that includes personal web skills and direct vigilance is necessary to fully track virtual risks.

A broad review by Ahmad and Thurasamy (2022) backed this view, proving that digital literacy and sharp risk awareness act as vital internal guardians that cut down fraud rates. On the flip side, ordinary habits—like buying things online, staying too long on social networks, and clicking strange web links—raise the chances of meeting digital predators. Similarly, Lin et al. (2025) suggested that having a guardian and being a fit target are the main reasons why fraud succeeds, while basic daily screen time only explains initial scam attempts. Because of this, the model explains clearly why students with top-tier tech and defense habits are better equipped to resist social media traps (Isma & Rosly, 2026).

Despite these clear links, real field studies measuring how digital literacy and safety awareness work together to predict social media scam victimization among Nigerian undergraduates are still very hard to find (Muscanell & Guadagno, 2021). Most local papers either talk about network hardware or measure shallow awareness without tracking real student habits or actual fraud experiences. Filling this gap is necessary for real crime prevention, which needs solid facts on what reduces target vulnerability instead of mere guesses about what users know (Arachchilage & Love, 2014; Kritzinger & von Solms, 2010). This study deals directly with this research gap by testing whether digital literacy and cybersecurity awareness act as major predictors of social media scam victimization among higher school students within Anambra State, Nigeria.

3. Methodology

This study used a quantitative cross-sectional survey design to find out if digital literacy and cybersecurity awareness predict social media scam victimization among tertiary students in Anambra State, Nigeria. This setup worked well because it allowed for gathering uniform facts from a massive pool of students at once, making it easy to run mathematical counts on how the variables link up.

The fieldwork took place across six public higher schools in Anambra State: Chukwuemeka Odumegwu Ojukwu University, Igbariam; Nnamdi Azikiwe University, Awka; Federal Polytechnic, Oko; Anambra State Polytechnic, Mgbakwu; Federal College of Education (Technical), Umunze; and Nwafor Orizu College of Education, Nsugbe. These campuses were picked because they form the core public higher education setup in the state, housing a massive student population that uses digital tools and social media apps every day.

The entire student body across these selected schools stood at 103,113 undergraduates. To find the right sample size, the standard sampling formula was applied at a 5% margin of error, giving a minimum baseline of 399 participants. To handle potential missing or ruined entries, 420 questionnaires were actually given out. In the end, exactly 399 forms were filled properly and brought back, marking a final return rate of around 95%.

A multistage sampling path was used to reach the respondents. First, the six public campuses were chosen directly due to their size and importance to the topic. Second, a proportional layout was applied to share out the

questionnaires based on the actual student population of each school. Finally, convenience sampling was used to hand out the forms to students inside lecture halls, libraries, school hostels, and common relaxation spots. Only undergraduate students who actively run at least one social media account were allowed to take part. Mixing these sampling styles gave a wide representation across all campuses while focusing strictly on users with real online habits.

The data came from a structured questionnaire built after reading past papers on web literacy, safety awareness, and social media fraud. The tool had four distinct blocks. Section A gathered basic personal details like age, gender, campus name, and daily social media habits. Section B tracked cybersecurity awareness, Section C measured digital literacy, and Section D looked at actual experiences with social media scams and daily financial pressure. The core questions used a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). To ensure the questionnaire was up to standard, face and content validity tests were done by showing the tool to experts in criminology, cybersecurity, and field research methods. Their feedback was used to reword questions, fix errors, and adjust the points before going to the field. Also, a small test run involving ten undergraduates from Nnamdi Azikiwe University, Awka, was done to see how clear the questions were, spot confusing words, test the data sharing routine, and make sure the setup fit the main study. These ten initial responses were completely left out of the final counts.

Strict ethical codes for social science research were followed from start to finish. Joining the study was entirely voluntary, and everyone gave their clear consent before taking a questionnaire. Participants were promised that their answers would stay secret and private. The forms did not collect names or ID numbers, and students were told they could stop and walk away at any moment without facing any penalty. The gathered forms were coded and loaded into statistical software for analysis. Descriptive statistics like frequencies, simple percentages, mean scores, and standard deviations were calculated to summarize the students' personal traits and social media habits. Inferential statistics dealt with the main goals of the study. A simple linear regression was run to test if cybersecurity awareness predicts how vulnerable students feel to social media fraud. An independent-samples t-test compared digital literacy scores between students who had fallen for social media scams and those who had not. Finally, a chi-square test checked the link between daily financial pressure and actual scam victimization. All decisions were evaluated at a 0.05 level of significance.

4. Results

4.1 Respondents' Characteristics

Exactly 399 properly filled forms were used for the final analysis, showing that 95.0% of the 420 distributed papers were successfully recovered. The participants came from six different public higher schools in Anambra State, giving a wide and balanced coverage of undergraduate students across the entire research zone.

Table 1: *Demographic Characteristics of Respondents (N = 399)*

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	211	52.9
	Female	188	47.1
Age (Years)	16-20	158	39.6
	21-25	199	49.9
	Above 25	42	10.5
Institution	Chukwuemeka Odumegwu Ojukwu University	68	17.0
	Nnamdi Azikiwe University, Awka	72	18.0
	Federal Polytechnic, Oko	66	16.5
	Anambra State Polytechnic, Mgbakwu	65	16.3

Variable	Category	Frequency (n)	Percentage (%)
	Federal College of Education (Technical), Umunze	64	16.0
	Nwafor Orizu College of Education, Nsugbe	64	16.0
Average Daily Time on Social Media	Less than 2 hours	39	9.8
	2-4 hours	113	28.3
	More than 4 hours	247	61.9
Most Frequently Used Platform	WhatsApp	387	97.0
	Facebook	228	57.1
	Instagram	214	53.6
	TikTok	176	44.1
	X (Twitter)	119	29.8

*Note. Percentages are based on valid responses. *Respondents could select more than one social media platform.*

The data shows a close balance between genders, with males making up 52.9% and females tracking at 47.1% of the total count. Almost all the students (89.5%) fall between 16 and 25 years old. The spread across the six campuses looks very even, which indicates that the sharing plan for the questionnaires worked correctly during the fieldwork. Looking at the hours spent online, 61.9% of the undergraduates admitted staying on social networks for more than four hours every single day. This type of non-stop screen time widens a user's digital space and gives Internet fraudsters a bigger opening to try online scams. WhatsApp turned out to be the most common app among the group at 97.0%, while Facebook scored 57.1% and Instagram followed at 53.6%. These high numbers show how deeply the students rely on social apps for their daily routines

4.2 Cybersecurity Awareness and Perceived Vulnerability to Social Media Scams

A simple linear regression test was run to see if cybersecurity awareness acts as a major predictor of how vulnerable students feel to social media fraud. The final statistical results are laid out in Table 2.

Table 2: *Simple Linear Regression Predicting Perceived Vulnerability to Social Media Scams (N = 399)*

Predictor	B	SE	β	t	p
Constant	4.21	0.28	—	15.04	< .001
Cybersecurity Awareness	-0.31	0.05	-.284	-5.91	< .001

Model Statistics

R	R^2	Adjusted R^2	F	p
.284	.081	.078	34.89	< .001

Note. Dependent variable = Perceived vulnerability to social media scams.

The regression test shows that cybersecurity awareness is a strong predictor of how vulnerable students feel to social media fraud, $F(1, 397) = 34.89$, $p < .001$. The numbers show a clear negative effect on how students see their risk (β = -.284, t = -5.91, p < .001). This indicates that undergraduates who have good safety awareness scores see themselves as far less likely to fall for social media tricks. Overall, the model explains 8.1% of the total variance regarding how vulnerable they feel (R^2 = .081), which shows that personal safety knowledge directly shrinks a user's risk profile.

4.3 Digital Literacy and Social Media Scam Victimization

An independent-samples t-test was run to check the differences in mean digital literacy scores between undergraduates who had faced social media scams and those who had never been tricked. The final figures are shown in Table 3.

Table 3: *Independent-Samples t-Test Comparing Digital Literacy Scores by Victimization Status (N = 399)*

Victimization Status	n	M	SD
Not Victimized	202	3.82	0.76
Victimized	197	3.28	0.89

Test Statistics

t	df	p
4.23	397	< .001

Note. M = Mean; SD = Standard deviation.

The statistical test shows a clear and major difference in digital literacy levels based on whether a student has been scammed or not, $t(397) = 4.23$, $p < .001$. Undergraduates who managed to avoid online fraud scored much higher on digital literacy (M = 3.82, SD = 0.76) than those who had actually fallen victim to social media tricks (M = 3.28, SD = 0.89). This gap suggests that having solid web literacy goes hand in hand with staying safe from fraud. It confirms that personal tech skills and smart online choices act as strong protective shields in virtual spaces.

4.4 Financial Pressure and Social Media Scam Victimization

A chi-square test of independence was run to see if there is a link between personal financial pressure and actually falling victim to social media fraud. The full cross-tabulation and test scores are laid out in Table 4.

Table 4: *Association Between Financial Pressure and Social Media Scam Victimization (N = 399)*

Financial Pressure	Not Victimized n (%)	Victimized n (%)
Low	78 (38.6)	33 (16.8)
Moderate	84 (41.6)	79 (40.1)
High	40 (19.8)	85 (43.1)

Chi-Square Test

Statistic	Value
χ^2	38.42
df	2
p	< .001

Note. Pearson's chi-square test of independence. Percentages are column-specific.

The chi-square test suggests that there is a clear, major link between financial pressure and undergraduate scam victimization, $\chi^2(2, N = 399) = 38.42, p < .001$. Undergraduates who face heavy money worries make up a much bigger part of the group that got scammed (43.1%). On the flip side, students with low financial pressure are mostly found in the group that never lost money to online fraud (38.6%). This big difference proves that money struggles make students far more likely to fall into online traps. It shows that heavy financial stress lowers a user's guard when they come across deceptive get-rich-quick offers.

5. Discussion of Findings

The main goal of this study was to find out if digital literacy and cybersecurity awareness predict social media scam victimization among higher school students in Anambra State, Nigeria. The findings show that a user's behavior and personal tech skills heavily affect how vulnerable they are to online fraud. At the same time, daily money struggles raise the chances of falling into these traps. Taken together, these results back the view that losing money to social media fraud does not depend on device security features alone. Instead, it happens due to a mix of personal knowledge, daily online habits, and a student's immediate economic situation.

The first major point from the field records was that cybersecurity awareness directly predicts how vulnerable students feel to social media tricks. Participants who knew a lot about phishing traps, cloned accounts, fake investment deals, and other online scams saw themselves as far less likely to get tricked. This proves that having good safety knowledge helps students spot fishy online posts before they turn into real fraud problems. Even though the regression test explained only a small part of why their risk perceptions differ, the link was statistically strong, proving that safety awareness makes a true difference in how students judge online dangers.

This match fits well with the field notes of Salem (2026), who stated that cybersecurity awareness and tech skills directly cut down digital harassment among university students in developing countries. Along the same line, Ermumcu et al. (2026) discovered a clear negative link between personal privacy awareness and cyber victimization among Turkish undergraduates. Also, Akingbade (2023) showed that over 65% of Nigerian internet users come across cybersecurity guidelines on social apps, and more than half improved their habits because of it. The present study carries these same patterns straight into the higher education setup of Anambra State. In this zone, non-stop social network use and widespread online banking give internet fraudsters more openings to launch digital crimes. Because of this issue, Babadele et al. (2025) advised that schools must push cybersecurity lessons into the compulsory courses for undergraduates across Nigerian federal universities.

Still, the small variance explained by the test (8.1%) proves that other variables left out of this study also affect how vulnerable students feel. These hidden points might include past fraud experiences, peer pressure on campus, or personal traits like how easily a student trusts strangers or views general risks. This point matches the warning from past tech papers that simply knowing about a threat does not always turn into safe browsing habits. As Garba et al. (2020) pointed out, while Nigerian undergraduates often show a decent level of awareness on paper, it is usually shallow, which proves that the depth and quality of safety knowledge matter far more than just reading basic safety tips.

The study also showed that digital literacy creates a massive gap between students who had faced social media scams and those who had managed to stay safe. Participants who avoided online fraud scored way higher on digital literacy than those who had lost money. This suggests that digital literacy means far more than just knowing how to operate a smartphone. It covers the deep critical thinking, sharp judgment, and quick decision skills needed to move around the web safely. Undergraduates with these solid skills are better equipped to double-check online ads, question strange money requests, and back away from sketchy accounts on social apps.

This outcome backs the position of Salem (2026) that good web skills help people study online posts with a critical eye, cutting down their chances of falling for digital tricks. Furthermore, Ugwuanyi et al. (2026) discovered that structured web literacy classes sent through social apps cut down fraud risks among Economics Education undergraduates in southeastern Nigeria. Their trial suggested that students who took the training showed a massive drop in fraud vulnerability, risky online habits, and the urge to try cyber fraud. Field studies inside Indonesian higher institutions similarly concluded that solid web skills are necessary to shield personal data and spot incoming threats. By establishing this clear link between digital literacy and social media scams, this study provides real field facts from Anambra State that join global research linking personal tech skills with internet safety.

Looking at past behavioral skills, the field data also pointed to financial pressure as a major variable tied directly to social media fraud. Undergraduates facing tight money situations reported falling for scams far more than those with low financial pressure. This shows that tough economic conditions push students into making bad choices online, making unverified job listings, fake investment links, and sketchy cash help setups look highly attractive.

Web fraudsters study these economic vulnerabilities and format their traps to look real, legal, and highly profitable.

This point aligns with the observations of Odoh and Oghuvbu (2026), who reported that student cyber fraud causes heavy financial losses and serious emotional pain. In the same way, Ezenwile and Nnoyelu (2026) discovered that poverty, joblessness, and frustration form the primary fuel driving student cybercrime across southeastern Nigeria. Adebayo (2025) also showed that local financial fraud heavily targets people who are searching for quick cash, with scammers flaunting crazy profit loops on investments that do not exist. Furthermore, Abah and Agada (2025) noted that socioeconomic struggles make students in developing countries easy targets for phishing mail, identity theft, and general online scams. This reality is highly visible within the Anambra State context, where recent crime tracking shows rising cases of internet fraud among young campus folks.

From a crime study perspective, these field facts heavily back Routine Activity Theory. The model explains that crime happens when a motivated criminal finds a perfect target in a space where there is no capable guardian to stop them. In digital environments, a capable guardian means more than just a software firewall. It includes behavioral skills like digital literacy and cybersecurity awareness. Undergraduates with solid web skills and safety knowledge are better at spotting tricks, verifying profiles, and blocking sketchy contacts, which leaves them looking like very poor targets for online predators. Using Routine Activity Theory to study internet crime has caused a lot of academic debate. Leukfeldt and Yar (2016) stated that this model must adapt because the digital world changes very fast. They concluded that an updated theoretical view that includes web literacy and personal caution is necessary to fully track virtual risks. A deep review by Ahmad and Thurasamy (2022) also indicated that digital literacy and sharp risk awareness act as vital internal forms of guardianship that cut down fraud rates significantly.

Lin, Wu, and Sun (2025) discovered that having a guardian and being a fit target affect whether a scam succeeds far more than simple daily screen time. This outcome suggests that Routine Activity Theory works very well to explain online crime patterns. At the same time, heavy financial worries can weaken this safety shield. It pushes students to take big risks with strange online deals even when they see clear warning signs. The field facts therefore suggest that online victimization happens due to a mix of personal knowledge, daily browsing habits, and immediate economic conditions.

These results bring out major lessons for stopping crime inside Nigerian higher schools, especially in Anambra State. Universities spend a lot of money to buy internet hardware and build digital classrooms, but they often ignore teaching students how to protect themselves from web criminals. The facts from this study show that basic safety alerts should go hand in hand with structured digital literacy programs. These classes should build real critical judgment, threat checking skills, and safe online habits. Doing this will work much better than broad warning posters because it gives undergraduates the tools to spot and block clever mind tricks. Recent programs like the Advanced Digital Empowerment Programme for Tertiary Institutions (ADEPTI) run by the Nigerian Communications Commission are good moves, but they train school workers instead of the students. This creates a massive gap in student-centered tech safety lessons.

In general, this study expands the field of cyber criminology by proving that social media fraud among students in Anambra State depends on a mix of behavioral traits and economic struggles. Instead of treating web fraud as a plain technical hardware issue, the outcomes show why schools must blend web literacy training, safety classes, and student welfare packages into their crime fighting plans. As higher education in Nigeria continues to move online, building these defense skills is the only way to shield undergraduates from social media traps.

6. Conclusion

This study tested if digital literacy and cybersecurity awareness predict social media scam victimization among Nigerian higher school students in Anambra State. Using real facts from undergraduates inside public campuses across the state, the results indicated that both digital literacy and safety awareness act as major behavioral factors linked to how vulnerable students are to social media fraud. Undergraduates with good safety knowledge saw themselves as far less likely to get scammed, while those with advanced web skills were significantly less likely to lose money to online tricks. Also, heavy money struggles turned out to be a major link to fraud, proving that tight economic situations make students far more likely to fall into online traps.These field records back the view that losing money to social media fraud goes far beyond device software setups to include personal choices and immediate situational triggers. From a crime study perspective, the results suggest that Routine Activity Theory works very well to explain online fraud dynamics. It demonstrates that solid digital literacy and safety awareness act as active internal guardians that shrink the openings online criminals use to exploit targets. At the same time, heavy financial stress makes a user a perfect target by pushing them to engage with highly risky, unverified web listings.This research expands the field of cyber fraud and victimization by providing real empirical data from Anambra State, Nigeria, where fast network expansion has brought both

great benefits and massive web risks. The outcomes show that higher institutions and policymakers must look past basic warning posters. They need to build deep plans that upgrade students' practical tech skills while dealing with the immediate economic worries that lower a user's guard. Taking these steps is the only way to build real student defense and promote a safer web space across Nigerian higher education.

7. Recommendations

Based on the study findings, the following practical and implementable recommendations are proposed for Nigerian tertiary institutions:

1. **Update General Studies (GST) Courses**: Instead of creating new expensive courses, universities in Anambra State should immediately update their existing compulsory General Studies (GST) computer or citizenship courses. They should add practical, 30-minute modules that teach students how to identify real-world social media risks, spot fake job links, verify WhatsApp broadcast messages, and recognize clone account setups. This requires zero new funding since the structures are already in place.
2. **Launch Student-Led Social Media Campaigns:** Universities should stop relying on paper posters or long seminars that students ignore. Instead, institutional media teams should partner with student union governments (SUG), campus content creators, and student influencers to share short, catchy safety videos, graphics, and text alerts on popular platforms like WhatsApp status, TikTok, and Instagram. These updates should showcase common local fraud tricks using everyday language that students relate to.
3. **Train Security Staff to Handle Cyber Complaints:** Campus security divisions should assign and train at least two officers to serve as a mini-digital safety desk. Since setting up high-tech tech support hubs is expensive, this desk will simply act as a safe first-point-of-contact where students can quickly walk in to report online scams, get immediate guidance on how to block fraud accounts, and receive help tracking down stolen digital assets without facing shame or judgment from the school.
4. **Partner with Local Banks and Telecoms for Orientation:** During annual orientation weeks for fresh students, university management should bring in regional compliance officers from local commercial banks and telecommunications providers. These firms can deliver direct, practical lectures on how mobile banking fraud occurs, warn students against leasing their bank accounts or SIM cards to "Yahoo Yahoo" syndicates, and provide direct hotlines for emergency account freezing.
5. **Utilize Work-Study and Entrepreneurship Grants:** To directly reduce the extreme financial pressures that make students look for risky online get-rich-quick deals, university administrations must expand and aggressively publicize their campus work-study programs. Giving vulnerable undergraduates part-time jobs within campus libraries, laboratories, or administrative offices—and providing small micro-grants through the school's entrepreneurship centers—will give students safe, legitimate income options.
6. **Encourage Localized Academic Studies:** Future researchers should focus on small-scale, field-based studies that track how fast local online fraud methods change across different campus settings in Nigeria. Rather than writing long, abstract theories, future works should use brief surveys to map out active campus scam trends every session. This will provide school heads with fast, accurate feedback to upgrade their campus safety rules before students fall victim.

References

1. Abah, JA, & Agada, SA (2025). Students' vulnerability to cybercrime: implications for cybersecurity in the global south. *International Journal of Didactic Mathematics in Distance Education* , *3* (2), 1-15
2. Adebayo, M. (2025). Role of social media in facilitating financial scams in Abuja, Nigeria: Development communication interventions for prevention. *African Journal of Stability and Development*, *17*(1), 32–45. doi.org
3. Ahmad, R., & Thurasamy, R. (2022). A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber Security and Mobility* , 11(3), 393–424. doi.org
4. Ajmal, I. (2026). *Cybersecurity awareness and online safety practices among university students* [Thesis, Metropolia University of Applied Sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-202603315394
5. Akingbade, K. O. (2023). Cybercrime involvement and awareness among undergraduate students in southwestern Nigeria. *African Journal of Cyber Criminology* , 8(2), 45–59.
6. Aningo, I. B., & Nwokeoma, B. N. (2024). Understanding individual victims' contribution in the

predicting factors of cybercrime victimization experiences in Abia State, Nigeria. *Fuoye Journal of Criminology and Security Studies, 3*(1), 44–58. https://fjcss.fuoye.edu.ng/index.php/fjcss/article/view/82

7. Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

8. Babadele, O. O., Olowokere, E. N., Ajayi, M. O., & Ekundayo, K. J. (2025). Effect of cybercrime risk on undergraduate behavioral intention in the federal universities in southwest, Nigeria. *International Journal of Science and Research Archives* , 17(1), 48–59. https://doi.org/10.30574/ijsra.2025.17.1.2743.

9. Balogun, NA (2024). Exploring the prevalence of internet crimes among undergraduate students in a Nigerian university: A case study of the University of Ilorin. *Nigerian Journal of Technology* , 43(1), 112–125.Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control matter? Computers in Human Behavior, 51, 351-360.

10. British Educational Research Association. (2018). Ethical guidelines for educational research (4th ed.). London: BERA.

11. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.

12. Chigona, W., & Mlotshwa, N. (2020). Cybercrime awareness among university students in developing countries. Information Technology for Development, 26(4), 745-764.

13. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

14. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

15. Dash, S., & Mohanty, S. (2026). Awareness of digital evidence and cyber-laws among students: An analytical study. *International Journal of Cyber Criminology* , 18(1), 114–128.

16. DeVellis, R. F. (2017). Scale development: Theory and applications (4th ed.). SAGE Publications.

17. Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security* , 86, 141–148.

18. Economic and Financial Crimes Commission [EFCC]. (2025). EFCC arrests 37 suspected internet fraudsters in Awka. EFCC Official Directorate Report. https://efcc.gov.ng

19. Ermumcu, G., Uğur, SB, & Yasan-Ak, N. (2026). Online privacy awareness and cyber victimization among university students in Turkey: A social work perspective. *Acta Psychologica* , 269, Article 107419. doi.org

20. Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1-4.

21. Ezenwile, U. S., & Nnoyelu, C. V. (2026). Forms of cybercrimes perpetrated by undergraduates in selected public and private tertiary institutions in Anambra State, South-East Nigeria. *Social Sciences Review* , 15(1), 102–118.

22. Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE Publications.

23. Furnell, S., & Clarke, N. (2012). Power to the people? The evolving role of humans in cybersecurity. Computer Fraud & Security, 2012(6), 5-9.

24. Garba, A., Ahmed, M., & Umar, A. (2020). Cyber security awareness among university students: A case study. Journal of Information Security and Applications, 52, 102-115.

25. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Journal of Cybersecurity, 3(3), 191-199.

26. Hargittai, E., & Shaw, A. (2015). Mind the skills gap: The role of internet know-how and gender in differentiated contributions to Wikipedia. Information, Communication & Society, 18(4), 424-442.

27. IBM Corp. (2015). IBM SPSS Statistics for Windows, Version 23.0. Armonk, NY: IBM Corp.

28. Isma, N., & Rosly, M. (2026). What leads to online financial fraud victimization among consumers: An empirical analysis. *International Journal of Cyber Criminology* , 18(1), 45–62

29. Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840–847.

30. Leukfeldt, ER, & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* , 37(3), 263–280.

31. Lin, K., Wu, Y., & Sun, IY (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice* , 23(1). Advance online publication.

32. Mburaimoh, A., & Samuel, O. (2025). Social media's influence on cybersecurity awareness among Nigerian users. African Journal of Information Systems, 16(2), 112-130.

33. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151-156.

34. Muscanell, N. L., & Guadagno, R. E. (2021). Online social networking and cybercrime: A review of the literature. Social Science Computer Review, 39(2), 182-199.

35. Nigerian Communications Commission. (2024). *2023 annual report and accounts* . NCC Abuja. https://ncc.gov.ng/market-data-reports/annual-reports

36. Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773-793.

37. Odoh, F. A., & Oghuvbu, E. A. (2026). Cybercrime among Delta State University students, Abraka, Nigeria, from 2015 to 2024. *Islamic University Journal of Social Sciences* , 5(1), 45–62. http://journals.iuiu.ac.ug/index.php/iujss/article/view/1106 [1, 2]

38. Oladehin, R. O. (2025). Cybercrime among undergraduate students: Problems and solutions. A case study of Nigeria. *International Journal of Research and Innovation in Social Science* , 9(2), 4569–4589. doi.orgPallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS (7th ed.). Open University Press.

39. Onyejiaka, C. I., & Nwankwo, O. B. (2026). Forms of cybercrimes perpetrated by undergraduates in selected public and private tertiary institutions in Anambra State, South-East, Nigeria. Social Sciences Review, 14(2), 112–128. https://journals.aphriapub.com/index.php/SSR/article/view/2417

40. Onyeoziri, C. U. (2025). Influence of peer pressure on youth involvement in cybercrime in commercial nerve centers: A case study of Onitsha North, Anambra State. Nigerian Journal of Social Sciences, 19(4), 45–59.

41. Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). SAGE Publications.

42. Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. Computers & Security, 137, 103612. doi.orgSalem, M. A. (2026). Reshaping digital social reality in the AI era: A data-driven analysis of university students' exposure to digital harassment in emerging countries. Societies, 16(2), 71.

43. Salem, M. A. (2026). Reshaping digital social reality in the AI era: A data-driven analysis of university students' exposure to digital harassment in emerging countries. Societies, 16(2), Article 71. https://doi.org

44. Saritepeci, M. (2024). Modeling the relationship between learning motivation, digital literacy, and data security awareness. Journal of Computer Assisted Learning, 40(3), 890–905. https://doi.org

45. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). 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, 373-382.

46. Ugwuanyi, C. K., Onuoha, J. C., Eneogu, N. D., & Ugwonna, G. O. (2026). Impact of social media based-digital literacy on reduction of internet fraud among Economics Education undergraduates in South East Nigeria. Journal of Economics and Social Sciences Education Research (JERCPT), 6(2).

47. Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. Journal of Computer-Mediated Communication, 20(1), 83-98.

48. Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.

49. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.