

CYBER CRIMINALITY AWARENESS AND RISK PERCEPTION AMONG SECONDARY SCHOOL STUDENTS IN SELECTED GOVERNMENT SCHOOLS IN ABUJA

Akor, P. E & Dr. Hassan Abdulazeez

Department of Sociology, Faculty of Social Science, University of Abuja, Abuja

DOI: <https://doi.org/10.57233/gujos.v6i1.19>

Abstract

Cybercrime as a growing threat in Nigeria, particularly among young people, amid the rapid digitalization, weak ethical awareness, and socioeconomic pressures. This study assessed cyber criminality in relation to its awareness and risk perception among secondary school students in selected government schools in Abuja. Using a mixed-methods approach involving questionnaires administered to 380 students and focus group discussions with 16 participants, the research examined students' perceptions of the impacts of cybercrime and the influence of demographic factors on their practices toward cyber offenses. Findings showed that most respondents were highly aware of the harmful effects of cybercrime, with a strong agreement that it tarnishes Nigeria's international image, affect victims financially as well as emotionally, erodes trust in digital systems, and also promotes moral decay among Nigerian youths. However, knowledge of specific legal provisions and certain non-financial offenses was limited. A very small number of students in the study area reported moral disengagement, which was characterised by viewing less harm when victims were distant or wealthy. The chi-square analysis showed a statistically significant association between gender and practices towards cybercrime ($p = 0.040$), with males being more likely to hold permissive or neutral attitudes than females. There were no statistically significant effects of age and class level. Qualitative data revealed limited understanding, peer influence, and the glamorization of "Yahoo Yahoo" lifestyles on social media. The research finds that although students acknowledge various dangers of cybercrime, deficiencies in legal knowledge and ethical comprehension remain, with gender significantly influencing behavior tendencies. The paper suggests the need to incorporating cybersecurity education and digital ethics into the secondary school curriculum, also to focus on awareness initiatives with organizations like National Information Technology Development Agency (NITDA) and Economic and Financial Crimes Commission (EFCC), including the need for gender-sensitive measures to tackle peer pressure among male students. These initiatives are vital to reduce youth participation in cybercrime and encourage responsible digital citizenship.

Key words: Digital technology, cybercrime, secondary school students

Introduction

Cyber criminality is the perpetration of a range of illegal activities via computer systems, digital devices and the Internet, such as illegal access to data, manipulation of systems, fraud, identity theft, cyberbullying and dissemination of malicious software (Goni, 2022). The Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 of Nigeria provides for the official definition and prosecution of cybercriminal offences (including hacking, online fraud, cyberstalking, cyber terrorism, identity theft and child pornography). These offenses are classified as crimes and are punishable by fines and imprisonment based on the nature and scope of the crime. This legislation protects critical national infrastructure, encourages cybersecurity knowledge, and provides a legal basis for prosecuting offenses within the cyber domain (Okibe&Olebara, 2022). It has transcended national borders, affecting individuals, organizations, and governments alike. The growth of cyber-dependent crimes across the world is evidence of how cybercriminals exploit technological vulnerabilities and human ignorance to commit crimes for financial, political, or psychological gains (United Nations Office on Drugs and Crime [UNODC], 2021). Cybercrimes commonly perpetrated by adolescents include phishing, online impersonation, social media scams, illegal downloads, and participation in financial fraud (e.g., “Yahoo Yahoo”). Young people can also be involved in cyberbullying and digital harassment, sometimes without fully understanding the legal and ethical consequences of their actions.

According to research by Odinka et al (2023), peer pressure, a lack of digital ethics, and the perception of socioeconomic advantages are all contributing factors to the growing number of Nigerian teenagers engaging in cyber fraud. Because juveniles are less likely to incur severe legal penalties, adult cybercriminals may utilize teenagers as pawns or train them to carry out illegal actions covertly. The scope of cybercrime extends beyond well-known offenses like hacking and cyberterrorism. Less evident but no less harmful practices include disseminating false information, transmitting personal information without authorization, and exploiting school networks to download illicit content

A recent study by Akanbi and Gbadamosi (2021), on cybercrime Knowledge among Nigerian students revealed that a significant percentage of secondary school students were familiar with various cyber fraud techniques and did not necessarily perceive them as criminal. This suggests a worrying gap in ethical understanding and legal Knowledge among this age group. The influence of social media, where fraudsters sometimes display their lavish lifestyles, further encourages others to emulate these behaviours. This normalization of digital fraud not

only undermines moral values but also threatens the future of a generation that sees cybercrime as a viable alternative to legitimate career paths. Given this alarming trend, it becomes crucial to investigate how much students especially those in government secondary schools understand the legal, moral, and social consequences of cybercrime. Their perceptions could either reinforce the problem or serve as a foundation for intervention. Understanding these dynamics will aid in designing school-based programs and national strategies to counteract the growing wave of youth cybercriminality. Understanding the knowledge and perception of cyber criminality among secondary school students is a critical element in addressing the rising involvement of youths in cybercrime (Abah & Inalegwu, 2025).

Statement of Problem

The use of technology has greatly increased among secondary school students. This exposes them to types of cybercrimes. These include cyber fraud, identity theft, cyberbullying and hacking into computer systems. A study by Adebayo and Olasunkanmi in 2020 found that many Junior Secondary School 3 students in Ibadan knew about computer ethics. However, many still did not follow these ethics online. This shows a difference between what they know and what they do. Another study by Olofinbiyi in 2021 found that urbanization, unemployment, peer pressure and weak laws against cybercrime contribute to cybercrime among people in Lagos. There are not studies on secondary school students in Abuja who are involved in cybercrime. Two schools Government Secondary School Lugbe and Government Secondary School Pyakasa are places to study this issue. They are in an diverse area of Abuja. These schools have students from backgrounds. This makes them ideal for studying what students know and think about cybercrime. The digital world is a part of students lives in these schools. It is like this in public schools in Nigeria. Government Secondary School Lugbe and Government Secondary School Pyakasa are examples of this. They can help us understand the issue of cybercrime, among secondary school students. . Their strategic location, high access to digital devices, and exposure to urban influences make them a representative microcosm of urban public secondary schools in the country. Furthermore, existing literature has not adequately examined how demographic variables such as age, gender, and educational level influence students' knowledge, perceptions, and practices regarding cyber criminality. Against this background, the present study seeks to assess the level of cyber criminality awareness and risk perception among secondary school students in selected government schools in Abuja,

Objective of the study

The study is aimed to assess Cyber Criminality Awareness and Risk Perception among Secondary School Students in Selected Government Schools in Abuja. on cyber criminality and its implications. The following objectives guided the study:

- i. To assess the perceptions of students on the impact of cyber criminality.
- ii. To examine the influence of demographic factors on students' practices towards cyber-crimes among secondary school students in Abuja

Literature Review

The Perceptions of Students on the Impact of Cyber Criminality

Odeyemi and Aluko (2023) examined the effects of internet fraud on students at Adeyemi Federal University of Education, Ondo State. The researchers surveyed 250 students and found that cybercrime negatively affected their academic performance by reducing their concentration and commitment to their studies. Many respondents believed that involvement in "Yahoo Yahoo" activities contributed to poor study habits. The study provides valuable insight into the impact of cybercrime on students; however, it focused only on university students and did not include secondary school students.

Usman et al. (2022) investigated the effects of cyberbullying on students in tertiary institutions in Yobe State using questionnaires and focus group discussions. The findings revealed that cyberbullying had significant emotional effects on students, causing them to withdraw from social interactions and experience reduced self-confidence. Although the study provides useful information on students' experiences with cyberbullying, it was limited to university students and did not consider secondary school students. Okeke and Abiola (2021) conducted a study on secondary school students in Lagos State to examine their perceptions of cybercrime. The researchers surveyed 210 students and found that many believed cybercrime encouraged immoral behaviour and reduced trust among peers. However, some respondents did not consider cybercrime to be a serious issue. The study is valuable because it focused on secondary school students, but it relied only on students' opinions without exploring the underlying reasons for their perceptions.

Balogun and Musa (2023) examined the effects of cybercrime on the economy and the perceptions of Nigerian youths in Ilorin, Kwara State. The researchers surveyed 300 students, who reported that cybercrime negatively affected the Nigerian economy and damaged the country's international reputation. The study concluded that cybercrime is a major societal problem with adverse consequences for both students and the national economy. Chukwuma and Ibrahim (2022) conducted a survey involving 198 secondary school students in Enugu State to investigate their perceptions of the social effects of cybercrime. The findings showed that students believed involvement in internet fraud tarnished the reputation of their families and schools. Although the study effectively captured students' views, including the perspectives of parents and teachers would have provided a more comprehensive understanding of the issue.

Madu, Eze, and Onyekachi (2021) investigated university students' perceptions of the social effects of cyber-fraud in Imo State. The findings indicated that students believed cybercrime created a negative image of Nigerian youths both nationally and internationally. While the study highlighted the reputational consequences of cybercrime, it was limited to university students in one state and did not include secondary school students. Oli (2024) examined the influence of moral disengagement on Nigerian university students' perceptions of cybercrime using Bandura's theory as the study's theoretical framework. The findings showed that students with higher levels of moral disengagement were more likely to perceive cybercrime as less harmful. Although the study was strengthened by its theoretical foundation, it did not directly investigate the perceptions of secondary school students.

Adeleke and Lawal (2023) conducted a survey of 180 secondary school students in Ibadan to examine their perceptions of cyberbullying. The findings revealed that cyberbullying made students fearful of attending school, anxious about interactions with their peers, and emotionally distressed. Although the study provided important insights into the effects of cyberbullying in schools, it did not examine other forms of cybercrime, such as internet fraud or hacking. According to UNICEF (2024), Nigerian adolescents perceive cybercrime, including internet fraud and cyberbullying, as a threat to their safety, education, and trust in online platforms. Although the report provides comprehensive information on the effects of cybercrime among young people, it is based on a broader national context rather than focusing specifically on secondary schools in Abuja.

Lo Cricchio et al. (2021) investigated adolescents' perceptions of cyberbullying and online theft among participants from Nigeria, South America, and Korea. The study found that many adolescents perceived online victimization as less harmful than face-to-face victimization, making them more likely to justify harmful online behaviour. Although the study provides valuable international perspectives, its findings may not fully reflect the unique experiences and perceptions of Nigerian secondary school students.

The Influence of Demographic Factors on Students' Practice Towards Cyber-Crimes

Okoro and Adebisi (2022) examined how age and class level influence secondary school students' perceptions of cybercrime in Lagos State. The researchers surveyed 210 students and found that older students were more likely to perceive certain forms of cybercrime as acceptable. The study suggests that students' perceptions of cybercrime change with age; however, it did not explain the factors responsible for these differences. Similarly, Yusuf and Adeyemi (2023) investigated whether male and female students differed in their perceptions of cybercrime. The researchers surveyed 300 secondary school students in Ilorin, Kwara State, and found that male students were more likely to perceive cybercrime as acceptable, whereas female students considered cyberbullying to be more harmful and unacceptable. Although the study provides useful insights into gender differences, it did not examine the influence of students' socioeconomic backgrounds.

Furthermore, Johnson et al. (2021) examined the influence of family socioeconomic status on students' perceptions of cybercrime. The researchers surveyed 400 secondary school students in Anambra State and found that students from higher-income families were less likely to perceive cybercrime as acceptable, whereas those from lower-income families were more likely to justify cybercrime because of financial challenges. These findings highlight the role of economic factors in shaping students' perceptions; however, the study did not examine the influence of peer pressure. Likewise, Musa and Ibrahim (2022) investigated whether students in public and private secondary schools differed in their perceptions of cybercrime. The researchers surveyed 250 students in Kano State and found that students in public schools were more likely to perceive cybercrime as acceptable. They attributed this finding to limited digital literacy education and lower levels of parental supervision. Nevertheless, the study focused only on school type and did not consider other demographic variables such as gender and age.

In addition, Adebayo, Oladipo, and Ajayi (2024) examined differences in the perceptions of cybercrime among students living in urban and rural communities. The findings revealed that students in urban areas had greater awareness of both online safety practices and cybercrime activities, whereas students in rural areas had lower levels of digital exposure but viewed cybercrime more negatively. While the study demonstrates that place of residence influences perceptions of cybercrime, it did not explore the unique challenges faced by students in rural communities. Similarly, Lo Cricchio et al. (2021) investigated demographic differences in perceptions of cybercrime across several countries. The study found that older students and male participants were more likely to perceive cybercrime as acceptable. Although the study provides valuable cross-cultural evidence, it did not examine the influence of socioeconomic status on these perceptions.

Moreover, Nwachukwu and Nwankwo (2023) assessed the influence of parental education on students' perceptions of cybercrime in Enugu State. The researchers surveyed 280 students and found that children of educated parents were less likely to perceive cybercrime as acceptable because their parents emphasized moral values and responsible internet use. However, the study did not examine the influence of gender, thereby limiting a broader understanding of students' perceptions. Furthermore, Usman et al. (2022) examined the influence of age, gender, and digital technology use on students' perceptions of cyberbullying in Yobe State. The findings showed that male students were more likely to consider cyberbullying acceptable and that frequent use of digital devices influenced students' attitudes toward online bullying. However, one limitation of the study is that it relied on self-reported data, which may have affected the accuracy of the findings.

At the national level, UNICEF (2024) reported that demographic factors such as age, socioeconomic status, and place of residence influence adolescents' online safety and perceptions of cybercrime in Nigeria. The report found that younger adolescents had lower levels of online safety awareness, while those from economically disadvantaged backgrounds were more susceptible to engaging in risky online behaviours due to peer influence. Although the report is based on extensive national data, its findings may not accurately represent the experiences of adolescents in specific locations such as Abuja. Similarly, Adeola and Okeke (2025) examined the influence of gender and socioeconomic status on students' involvement in internet fraud in Ogun State. The findings revealed that male students from low-income families were more likely to perceive internet fraud as acceptable.

Therefore, the study supports the view that demographic characteristics influence students' involvement in cybercrime. However, it focused only on internet fraud and did not examine other forms of cybercrime.

In another study, Nwaogwugwu and Ulu-Eke (2024) conducted a survey in Ukwaiia, Abia State, to examine the relationship between age, educational level, and involvement in cybercrime. The findings indicated significant relationships among these variables. Although the study involved adults rather than adolescents, it provides useful insights into demographic factors associated with cybercrime. Likewise, Olubode et al. (2023) surveyed 400 Nigerian adolescents using questionnaires to examine the influence of age and gender on cyberbullying and internet addiction. The findings showed that age significantly influenced involvement in cyberbullying, while gender was strongly associated with internet addiction. Although the study is relevant because it focused on adolescents, the inclusion of participants from different educational levels may have influenced the findings.

In a related study, Obaweiki, Njoroge, and Kanga (2021) surveyed individuals imprisoned for cybercrime offences in Lagos and Edo States. The findings revealed that age, gender, and educational level were significantly associated with involvement in cybercrime. Although the respondents were adults, the study provides useful evidence regarding demographic factors linked to cybercrime. Furthermore, Molokwu (2023) conducted a survey involving 150 participants in Ibadan to examine the influence of peer relationships, socioeconomic status, and access to digital devices on cybercrime. The findings indicated that these demographic factors were significantly associated with involvement in cybercrime. However, the participants were older than the secondary school students targeted in the present study.

Similarly, Oli (2024) surveyed over 1,000 university students to examine the influence of age and field of study on perceptions of cybercrime. The study found that younger students and those enrolled in technology-related disciplines were more likely to perceive cybercrime as acceptable. Although the large sample size strengthens the study, its findings are limited to university students and may not be applicable to secondary school students.

Additionally, Adigwe (2024) conducted a survey involving 1,050 secondary school students in Lagos State to examine the influence of gender and parental mediation on online behaviour. The findings showed that male students were more likely to engage in risky

online behaviours, such as communicating with strangers and online gaming, whereas female students used social media more frequently. Consequently, the study is highly relevant because it focused on secondary school students, although it examined online behaviour rather than perceptions of cybercrime.

Finally, Ekwochi, Asije, Agbo, James, Famodimu, and Obiajunwa (2025) surveyed 100 youths in southeastern Nigeria to examine the influence of age, gender, and socioeconomic status on perceptions of and involvement in cybercrime. The findings indicated that unemployment and peer influence were major factors associated with favourable attitudes toward cybercrime. Although the study had a relatively small sample size, it provides valuable theoretical and demographic insights into factors associated with cybercrime among Nigerian youths.

Theoretical Framework

Theoretical frameworks provide the intellectual scaffolding for interpreting students' knowledge, practices, and perceptions of cyber criminality. They help explain why cybercrimes happen among teenagers. It also shows how things around them their friends and what they think influence how they behave online. This study uses two theories: Routine Activity Theory and Differential Association Theory. Differential Association Theory is used as the framework for this research. This is because it directly relates to how the environment, around secondary school students shapes their knowledge, practices and views on cybercrime. The environment includes their peers, the media and the community.

Routine Activity Theory (Cohen & Felson, 1979)

The Routine Activity Theory says that a crime happens when three things come together at the time and in the same place: someone who wants to commit a crime a target that is easy to attack and no one to stop them.

These people who want to commit a crime are called offenders. A suitable target can be a person or something that can be stolen. A capable guardian is someone or something that can prevent a crime from happening like a security system. The internet is a place where the Routine Activity Theory's very important. There are targets on the internet that can be easily attacked like personal accounts and financial information. There are not enough capable guardians, like strong security measures to protect these targets. This means that people who want to commit crimes like students or groups of hackers can easily attack these targets.

For students in school doing things online without supervision like using social media or browsing the internet late at night can create opportunities for crimes to happen. These students may encounter targets like their classmates' profiles without anyone to protect them. Foreexample if students are not supervised at home or at school they may be more likely to fall victim to phishing scams or try to hack into their peers accounts. The Routine Activity Theory helps us understand why students commit cyber crimes and where and when these crimes are most likely to happen. The Routine Activity Theory is useful, for understanding the patterns of student cyber wrongdoing. It can help us figure out how to prevent these crimes from happening in the future by looking at the Routine Activity Theory and how it applies to secondary school students and their online activities.

Differential Association Theory (Edwin Sutherland, 1939) – Adopted Framework

The Differential Association Theory, which Edwin H. Sutherland introduced in 1939 is still an important idea about how people behave in a criminal way. The Differential Association Theory says that people are not born to be criminals. They learn how to be criminals from the people they interact with especially their friends and family. The Differential Association Theory is a way of understanding how people learn to do things and it is based on the idea that we learn by being around other people, especially the people we are close, to. The Differential Association Theory is important because it helps us understand why people do things and it says that the Differential Association Theory is a key part of understanding criminal behavior. . Individuals learn criminal techniques, motives, rationalizations, and attitudes from others primarily through communication and association. Consequently, crime results from socialization processes in which a person is exposed to more definitions favorable to law-breaking than definitions unfavorable to it (Sutherland & Cressey, 1947). Sutherland formulated nine key propositions (assumptions) of the theory, which together explain how criminal behavior is learned:

1. **Criminal behavior is learned:** This means that individuals are not inherently deviant; they acquire criminal tendencies through interaction and communication, not through biological inheritance or mental disorder.
2. **Criminal behavior is learned in interaction with other persons in a process of communication:** Learning occurs primarily through verbal and non-verbal exchanges, discussions, and shared experiences within social networks.

3. **The principal part of the learning of criminal behavior occurs within intimate personal groups:** Close-knit groups such as peers, classmates, or online communities have the greatest influence on an individual's behavior.
4. **When criminal behavior is learned, the learning includes techniques of committing the crime and the specific direction of motives, drives, rationalizations, and attitudes:** Individuals learn not only *how* to commit crimes (e.g., methods of hacking or fraud) but also *why* such acts are justifiable or rewarding.
5. **The specific direction of motives and drives is learned from definitions of the legal codes as favorable or unfavorable:** People develop attitudes that view certain laws as either acceptable to break ("favorable") or important to obey ("unfavorable"), depending on their social environment.
6. **A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law:** When individuals are more frequently exposed to attitudes that justify or reward law-breaking than to those that condemn it, they are more likely to engage in deviant behavior.
7. **Differential associations may vary in frequency, duration, priority, and intensity:** The likelihood of adopting criminal behavior depends on how often (frequency), how long (duration), how early in life (priority), and how emotionally significant (intensity) those associations are.
8. **The process of learning criminal behavior by association with criminal and anti-criminal patterns involves all the mechanisms involved in any other learning:** Learning criminal behavior is no different from learning any other behavior it follows normal psychological and social learning processes.
9. **While criminal behavior is an expression of general needs and values, it is not explained by those needs and values because non-criminal behavior is an expression of the same needs and values:** People commit crimes not simply because of needs like money or status, since legitimate means could satisfy the same needs; the difference lies in what they have *learned* from their environment.

Application of the Theory to the Present Study

Sutherland's Differential Association Theory provides a strong theoretical foundation for this study on secondary school students' knowledge, perceptions, and attitudes toward cybercrime in Government Secondary School Garki and Government Secondary School Wuse, Abuja. The theory shows how friends, media and online interactions affect students

views and behaviorstowards cybercrime. In Nigeria cybercrime is often seen as normal among school students. This happens through talks with friends, social media posts and local stories that make "Yahoo Yahoo" or online fraud look like a way to succeed. These stories make it seem like a fix. Students hear about it from friends. See it online. It is an issue, in schools. Cybercrime is something students think about because of their friends and what they see online. It is portrayed as a way to get fast. Adebayo and Olanokun also wrote about it in 2020. According to the theory, students acquire both the practical techniques (such as creating fake profiles, phishing, and hacking) and the accompanying rationalizations (e.g., "it's not real stealing," "foreigners can afford it") from peers and online communities that present cyber-offending as clever or victimless. The frequency, duration, priority, and intensity of these associations particularly on social media determine the extent to which these pro-crime definitions are internalized. For example, when students regularly talk to friends who think it is okay to commit cybercrime and do not care about the police, they are more likely to think that way. On the hand if students do not learn about digital ethics or what it means to be a good citizen; they are less likely to stand up against bad behavior. The idea behind this is that things like how old studentsre what grade they are in and whether they are a boy or a girl can affect what they think. Students who are younger and use media a lot tend to be more easily influenced and more likely to think that cybercrime is not so bad. This study uses something called Differential Association Theory because it helps us understand how students in school in Abuja might start to think that cybercrime is okay just because of what they learn from their friends and the people, around them not because they are born to be criminals. It highlights the critical influence of social context, peer networks, and communication processes in forming students' awareness, perceptions, and potential involvement in cybercrime.

Methodology

This study adopted a mixed-method research design, combining a descriptive quantitative survey with qualitative Focus Group Discussions (FGDs), to assess secondary school students' knowledge and perceptions of cyber criminality. The study was conducted in the Abuja Municipal Area Council (AMAC) of the Federal Capital Territory, focusing on Government Secondary School Pyakasa and Government Secondary School Lugbe, two urban schools selected for their diverse and digitally exposed student populations. The population comprised approximately 2,400 SS1–SS3 students, from which a sample size of

343 was derived using the Taro Yamane formula; this was increased to 380 targeted respondents, with 420 questionnaires distributed proportionately across both schools to allow for non-response. Data were collected using a self-developed instrument, the Knowledge and Perception of Cyber Criminality among Secondary School Students Questionnaire (KPCSSQ), comprising a demographic section and five Likert-scaled clusters of seven items each, alongside a semi-structured FGD guide covering four thematic areas. Both instruments were validated by experts in criminology, cybersecurity, and educational measurement, who refined item wording for clarity, age-appropriateness, and reduced social-desirability bias. Reliability testing through a pilot study of 30 students yielded Cronbach's alpha coefficients ranging from 0.78 to 0.86 across clusters, with an overall coefficient of 0.83, indicating good internal consistency, while the FGD guide was assessed for trustworthiness using credibility, dependability, confirmability, and transferability criteria. Questionnaires were administered in person by trained research assistants under informed consent, and four FGD sessions of 8–10 participants each were conducted, recorded, and transcribed verbatim. Quantitative data were analyzed using descriptive statistics and Chi-square tests of independence at a 0.05 significance level via SPSS version 25, while qualitative data were subjected to thematic analysis following Braun and Clarke's (2006) six-phase framework, with findings from both strands triangulated to produce a comprehensive interpretation of students' cybercrime-related knowledge, perceptions, and practices.

Data Analysis and Discussion of Findings

Objective one: Students' Perceptions on the Impact of Cyber-Criminality

To achieve this objective, students were asked to indicate their level of agreement with statements about the consequences of cyber-crime on individuals, society, and the nation. Their responses are presented in Table 1.

Table 1: Students' Perceptions of the Impact of Cyber-Criminality

Perception Statement	Strongly Agree	Agree	Disagree	Strongly Disagree	Mean (x̄)	Decision
Cyber-crime ruins the reputation of Nigeria internationally.	160 (42.1%)	150 (39.5%)	40 (10.5%)	30 (7.9%)	3.16	Positive
Victims of cyber-crime usually suffer serious financial and emotional harm.	170 (44.7%)	140 (36.8%)	40 (10.5%)	30 (7.9%)	3.18	Positive
Cyber-crime reduces trust in online systems and digital services.	150 (39.5%)	140 (36.8%)	60 (15.8%)	30 (7.9%)	3.08	Positive
Cyber-crime can provide opportunities for young people to become rich quickly.	60 (15.8%)	90 (23.7%)	140 (36.8%)	90 (23.7%)	2.32	Negative
Cyber-crime contributes to moral decay among Nigerian youths.	180 (47.4%)	130 (34.2%)	40 (10.5%)	30 (7.9%)	3.18	Positive

The results in Table 1 suggest that students largely perceive cyber-crime as having negative consequences for individuals, society, and the nation. A majority (81.6%) agreed that cyber-crime damages Nigeria's international reputation (mean = 3.16), while 81.5% agreed that victims of cyber-crime suffer serious financial and emotional harm (mean = 3.18).

Similarly, 76.3% believed that cyber-crime reduces trust in online systems and digital services (mean = 3.08). A strong 81.6% also perceived cyber-crime as contributing to moral decay among Nigerian youths (mean = 3.18).

Conversely, only a minority (39.5%) saw cyber-crime as a means of quick wealth, with the majority (60.5%) disagreeing (mean = 2.32). This reflects a general rejection of cyber-crime as a viable or acceptable pathway to success.

On the reputational damage to Nigeria, participants expressed strong negative sentiments. A female SS3 student from Government Secondary School Pyakasa stated:

When I tell people online that I am from Nigeria, some of them immediately think I want to scam them. It is embarrassing. Yahoo Yahoo has spoiled our name everywhere."

This narrative corroborates the quantitative finding that 81.6% of students agreed cybercrime ruins Nigeria's international reputation (mean = 3.16).

Regarding victim impact, FGD participants showed high empathy toward financial fraud victims but displayed differential concern for non-financial offenses.

A male SS2 student from Government Secondary School Lugbe remarked:

"If someone loses money to a scammer, that is really bad. But if someone is just insulted on Instagram, they can block the person. It is not that serious."

Regarding trust in digital systems, a female SS2 student noted:

"I don't feel safe buying things online anymore. Even Jumia and Konga, I am afraid they might be fake."

This supports the quantitative finding that 76.3% of students believe cybercrime reduces trust in online systems (mean = 3.08). The qualitative data reveals that this erosion of trust extends to legitimate e-commerce platforms, potentially hampering digital economic participation among Nigerian youth.

On the pathway to quick wealth, the qualitative findings strongly reinforced the quantitative rejection. A male SS2 participant stated:

"Yahoo Yahoo is fast money, but it is not real success. My father says anything built on lies will collapse."

Another female SS3 student added: "I would rather suffer and make honest money than have EFCC knock on my door one day."

These narratives help explain why only 39.5% of survey respondents saw cybercrime as a means of quick wealth (mean = 2.32), suggesting that anti-cybercrime messaging and parental socialization have influenced student attitudes.

Objective One

The findings highlight that students in Abuja recognize the far-reaching consequences of cyber-crime, particularly in terms of reputational harm, victimization, and erosion of trust in digital platforms. The quantitative data established that the majority of students (76.3%--81.6%) perceive cybercrime as damaging to Nigeria's reputation, harmful to victims, erosive

of digital trust, and contributory to moral decay. The qualitative narratives enriched these statistics by revealing the mechanisms and lived experiences behind these perceptions. This aligns with Alabi et al. (2023), who reported that Nigerian youths increasingly acknowledge the damaging effects of cybercrime on national reputation and trust in technology. Similarly, Mundt and Baier (2021) stressed that cyber-crime syndicates such as “Yahoo boys” have contributed to a global stereotype of Nigeria as a hub of digital fraud, a view confirmed by these students.

The perception that cyber-crime causes moral decay among youths resonates with findings by Aborisade (2023), who linked the glamorization of “Yahoo Yahoo” to declining values among adolescents. However, the relatively lower endorsement of the idea that cyber-crime provides opportunities for quick wealth suggests that anti-cybercrime campaigns and increasing Knowledge of legal risks may be influencing perceptions.

The FGD data suggest that anti-cybercrime campaigns and increasing media coverage of EFCC arrests may be influencing student attitudes beyond what the quantitative items alone could reveal.

Overall, these findings indicate that while students recognize the destructive impact of cyber-crime, sustained educational and policy interventions are needed to further strengthen their rejection of cyber-crime as a legitimate option for economic advancement.

Objective Two: Influence of Demographic Factors on Students’ Practices Toward Cyber-Crimes

To address this objective, students’ demographic variables (gender, age, and class level) were cross-tabulated with their responses on practices toward cyber-criminality. Chi-square tests were applied at the 0.05 significance level to determine whether significant associations existed. The results are presented in Tables 2 to 4.

Table 2: Influence of Gender on Practices Toward Cyber-Crime

Practice Category	Male (n=190)	Female (n=190)	χ^2 (df)	p-value	Decision
Positive Practice	60 (31.6%)	40 (21.1%)	6.42(2)	0.040	Significant
Neutral Practice	50 (26.3%)	55 (28.9%)			
Negative Practice	80 (42.1%)	95 (50.0%)			

Table 2 shows a significant association between gender and students' practices toward cyber-crime ($\chi^2 = 6.42$, $p = 0.040$). Male students were more likely to express positive or neutral practices toward cyber-crime compared to females, who were more strongly represented among negative practices.

The FGD data provided rich narrative explanations for the significant gender differences observed in Table 2.

Male participants consistently reported greater exposure to peer networks where cybercrime was normalized or glamorized.

A male SS2 student from Government Secondary School Lugbe explained:

"In my area, if you are not doing Yahoo or you don't know someone who is doing it, people think you are dull. Some boys even teach each other how to do it. It is like a normal thing now."

This account illustrates how criminal techniques and pro-crime definitions are transmitted within male peer networks, directly supporting Sutherland's Differential Association Theory.

In contrast, female participants described peer environments that discouraged cybercrime.

An SS3 female student from Pyakasa stated:

"Among my friends, we talk about going to university and getting good jobs. Nobody talks about doing Yahoo because our parents would be ashamed."

Another female SS2 participant added:

"My mother always tells me that whatever you do online stays forever. She says a good name is better than money. That is why I would never do Yahoo or support anyone who does it."

These narratives suggest that gendered socialization patterns and parental mediation contribute to the significant difference in practices between male and female students. Social media glamorization was identified as a particularly powerful influence on male students. Interestingly, a small number of male participants expressed awareness of the legal risks but remained ambivalent. One SS3 male student said:

"I know EFCC is arresting people, but many still get away with it. The risk is there, but the money is tempting."

This ambivalence among a subset of male students helps explain the neutral practice category (26.3% male vs. 28.9% female), where students neither fully endorse nor reject cybercrime.

The qualitative narratives explained these differences through three key mechanisms: (1) differential peer network exposure, where male students were more likely to interact with peers involved in or glamorizing cybercrime; (2) gendered socialization, where female students received stronger parental guidance against cybercrime and were socialized to prioritize reputation and long-term goals; and (3) differential media consumption, where male students were more exposed to music and social media content that normalized "Yahoo Yahoo."

Table 3: Influence of Age on Practices Toward Cyber-Crime

Age Group	Positive Practice	Neutral Practice	Negative Practice	χ^2 (df)	p-value	Decision
12–13 yrs	15 (25.0%)	20 (33.3%)	25 (41.7%)			
14–15 yrs	35 (26.9%)	40 (30.8%)	55 (42.3%)			
16–17 yrs	40 (28.6%)	45 (32.1%)	55 (39.3%)	4.85(4)	0.303	Not Significant
18–19 yrs	10 (20.0%)	15 (30.0%)	25 (50.0%)			

Table 3. shows no statistically significant association between age group and practices toward cyber-crime ($\chi^2 = 4.85$, $p = 0.303$). While older students (18–19 years) tended to hold slightly more negative practices, the overall differences were not significant across age groups.

The FGD data in Table 3.

Participants across all age groups expressed remarkably similar attitudes toward cybercrime, suggesting that the shared digital environment in Abuja's urban public schools homogenizes perceptions regardless of age.

A 13-year-old SS1 student from Government Secondary School Pyakasa stated: "I know Yahoo Yahoo is bad because my elder brother was arrested by EFCC. I will never do it."

In contrast, an 18-year-old SS3 student from the same school expressed a nearly identical sentiment: "My cousin went to prison for Yahoo Yahoo. It destroyed our family. I hate cybercrime because of what it did to us."

These parallel narratives from opposite ends of the age spectrum illustrate that personal and family experiences with cybercrime consequences transcend age boundaries.

This comment highlights the homogenizing effect of shared digital culture, which may override age-related developmental differences that other studies have found. Interestingly, some older students (18--19 years) expressed more cynical views about the legitimacy of anti-cybercrime efforts. One SS3 male student commented: "The government says cybercrime is bad, but politicians steal more than Yahoo boys. Why should we listen to them?"

This cynicism, however, did not correlate with higher rates of positive cybercrime practices in the quantitative data, suggesting that disillusionment with government does not necessarily translate into criminal behavior.

Table 4: Influence of Class Level on Practices Toward Cyber-Crime

Class Level	Positive Practice	Neutral Practice	Negative Practice	χ^2 (df)	p-value	Decision
SS1	30 (25.0%)	40 (33.3%)	50 (41.7%)			
SS2	50 (33.3%)	45 (30.0%)	55 (36.7%)	7.12(4)	0.068	Not Significant
SS3	25 (22.7%)	30 (27.3%)	55 (50.0%)			

Table 4. shows that although SS3 students had the highest proportion of negative practices toward cyber-crime (50.0%), the chi-square test revealed no statistically significant association between class level and practices ($\chi^2 = 7.12$, $p = 0.068$).

From the FGD data

Participants from SS1, SS2, and SS3 expressed broadly similar attitudes, with minor variations that did not reach statistical significance.

An SS1 male student from Government Secondary School Lugbe stated:

"In my class, we hear about Yahoo Yahoo from older students and from social media. Even though we are in SS1, we know what is happening. Some boys already talk about trying it when they get older."

This comment reveals that cybercrime awareness and temptation permeate all class levels, not just senior students.

An SS2 female student from Pyakasa offered a similar perspective:

"Class does not matter for knowing about cybercrime. In SS1, SS2, and SS3, we all use the same phones and apps. The

difference is that SS3 students are more careful because they are about to write WAEC and JAMB."

This observation aligns with the quantitative finding that SS3 students had the highest proportion of negative practices (50.0%), suggesting that examination pressure and impending graduation may serve as temporary protective factors.

However, an SS3 male student from Lugbe complicated this narrative:

"Some SS3 students think they need quick money before university because their parents cannot afford school fees. That is why some of them are attracted to Yahoo."

This account suggests that while SS3 students may express more negative attitudes in surveys, the socioeconomic pressures of transitioning to higher education could create vulnerability among a subset of senior students.

Discussion of findings

The findings indicate that gender is the only demographic factor that significantly influences students' practices toward cyber-criminality, with male students more inclined toward permissive or neutral practices than females. This supports the findings of Okafor et al. (2025), who observed that male students were more involved in cyber-crime than students in Enugu State.

On the hand the study found that age and class level did not really affect how students behave towards cyber-crime. This is different from what Ojedokun et al. (2021) Found, which was that older teenagers had negative views of cyber-crime than younger ones.

The reason for this difference might be that students in schools in Abuja are influenced by the same social environment and friends which makes their views on cyber-crime similar no matter how old they are or what class they are in. These results show that we need to focus on gender when trying to stop cyber-crime because male students seem likely to think it's okay to do cyber-crime.

On students' perceptions of cybercrime impact (Objective One), both data strands converged strongly. The quantitative data showed high agreement (76.3%--81.6%) that cybercrime damages Nigeria's reputation, harms victims, erodes digital trust, and promotes moral decay.

On demographic influences (Objective Two), the quantitative chi-square tests identified gender as the only significant factor ($p = 0.040$), while age ($p = 0.303$) and class level ($p = 0.068$) were non-significant. The qualitative data provided explanatory depth for each result. For gender, male students' greater exposure to peer networks glamorizing cybercrime, combined with gendered socialization patterns, explains the significant difference. For age and class level, the shared digital environment and peer culture in Abuja's urban public schools homogenize attitudes across these boundaries.

Similarly, the identification of social media glamorization and music culture as drivers of pro-crime attitudes points to the need for media literacy components in prevention programs. The ambivalence expressed by some male students who recognized legal risks yet remained tempted by financial rewards would have been missed without the FGD component.

Conclusion

Findings from the research showed that students are very aware of cybercrime especially when it comes to things like online fraud and hacking. They do not know much about other types of cybercrime such as cyberbullying and digital piracy. The research also found that students do not really understand what cybercrime is and they have a time telling what is legal and what is not when they are online. Students also do not know much about the Cybercrimes Act of 2015 which means they are not very good at understanding the law when it comes to cybercrime.

When it comes to how students think about cybercrime the research found that they know it can cause problems like hurting people damaging Nigeriasreputation. Some students do not think cybercrime is a big deal especially if the people who are hurt are rich or far away. The

research also found that whether a student is a boy or a girl can affect how they think about cybercrime but how old they are or what class they are in does not make a difference.

Recommendations

Based on what the research found here are some things that can be done to help students in Abuja understand cybercrime better:

- a) Cybersecurity and digital ethics should be taught in school.
- b) These lessons should include not technical skills, but also the social and legal consequences of cybercrime.
- c) Government agencies like the National Information Technology Development Agency and the Economic and Financial Crimes Commission should work with schools to have workshops that teach students about cybercrime.
- d) These workshops should talk about the punishments for cybercrime. Encourage students to behave responsibly online. Because the research found that male students are more okay with cybercrime special programs should be made to help them understand why cybercrime is bad and to stop them from feeling pressure, from their friends to do things that're not right.

References

- Abah, J. A., & Inalegwu, P. (2025). Understanding the knowledge and perception of cyber criminality among secondary school students. *International Journal of Digital Media and Digital Engagement*, 2(2), 141-164.
- Adebayo, A. M., & Olasunkanmi, I. A. (2020). Youth and Cybercrime in Nigeria: An Emerging Trend in the Digital Age. *Journal of African Studies and Sustainable Development*, 3(2), 51-65.
- Adebayo, S., Oladipo, M., & Ajayi, F. (2024). Urban-rural differences in adolescents' perceptions of cybercrime in Ekiti State, Nigeria. *Journal of Digital Youth Studies*, 5(1), 22-41.
- Adeleke, O., & Lawal, K. (2023). Perceptions of cyberbullying among secondary school students in Ibadan, Nigeria. *Journal of Child and Adolescent Studies*, 18(2), 45-57.

- Akanbi, M. A., & Gbadamosi, O. (2021). Knowledge and Perception of Cybercrime among Secondary School Students in Ibadan, Nigeria. *African Journal of Criminology and Justice Studies*, 14(1), 1–17.
- Balogun, J., & Musa, A. (2023). Youth perceptions of the economic implications of cybercrime in Nigeria. *African Journal of Criminology and Justice Studies*, 16(1), 88–104.
- Chukwuma, E., & Ibrahim, M. (2022). Social consequences of youth involvement in cybercrime: Perspectives from secondary school students in Enugu State, Nigeria. *International Journal of Cybersecurity and Youth Studies*, 4(1), 55–72.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015*. Government Press.
- Johnson et al. (2021). Socioeconomic status and adolescents' practices toward cybercrime in Anambra State. *Journal of Social and Developmental Studies*, 8(3), 88–102.
- Lo Cricchio et al. (2021). Moral disengagement and adolescents' perceptions of cyberbullying: A cross-cultural study in Nigeria, South America, and Korea. *Computers in Human Behavior*, 114, 106562.
- Musa, H., & Ibrahim, T. (2022). School type and adolescents' attitudes toward cybercrime in Kano State. *International Journal of Cybersecurity and Youth Development*, 2(2), 77–92.
- Nwachukwu, J., & Nwankwo, U. (2023). Influence of parental background on adolescents' practices toward cybercrime in Enugu State. *Journal of Behavioral and Social Sciences*, 17(1), 65–81.
- Odeyemi, A., & Aluko, T. (2023). Perceived academic impact of internet fraud on undergraduates in Ondo State, Nigeria. *Nigerian Journal of Education and Social Sciences*, 12(1), 75–90.
- Odinka, G. E., Okpa, J. T., Ushie, E. A., Ekpenyong, B. E., & Echu, S. N. (2023). Exploring the Socio-economic Dynamics of Youths' Involvement in Internet Fraud in Nigeria. *Journal of Public Administration, Policy and Governance Research*, 1(3), 83-91.
- Okeke, C., & Abiola, R. (2021). Secondary school students' perceptions of the consequences of cybercrime in Lagos, Nigeria. *Journal of Youth Risk Behavior Studies*, 9(2), 34–49.
- Okibe, E. S., & Olebara, O. P. E. (2024). An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks, Challenges, and Prospects for Combating Cybercrime. Alex-Ekwueme Federal University Faculty of Law LL.B Projects.

- Okoro, A., & Adebisi, R. (2022). Age and class level differences in cybercrime practices among secondary school students in Lagos, Nigeria. *Journal of Adolescent Criminology*, 14(2), 50–66.
- Olofinbiyi (2021). [Full details as cited: Urbanization, unemployment, peer pressure, and weak enforcement of cybercrime laws as drivers of cybercriminal activities among youths in Lagos Metropolis].
- Okafor et al. (2025). [As cited in discussion: Higher cyber-crime involvement among male students compared to females in Enugu State].
- Sutherland, E. H. (1939). *Principles of Criminology* (3rd ed.). J.B. Lippincott.
- UNICEF Nigeria (2024). Adolescent online safety and perceptions of cybercrime in Nigeria. United Nations Children’s Fund (UNICEF).
- Usman, A., Ibrahim, T., & Gambo, A. (2022). Age, gender, and ICT exposure as predictors of practices toward cyberbullying among Nigerian students. *Journal of Educational Psychology and Cybersecurity*, 14(2), 99–118.
- Yusuf, R., & Adeyemi, K. (2023). Gender differences in adolescents’ attitudes toward cybercrime in Ilorin, Nigeria. *African Journal of Youth and Criminology Studies*, 6(1), 45–60
- UNODC (2021). *Global report on cybercrime*. United Nations Office on Drugs