ABNUS JOURNAL
Your Research Partner

Legal Systems, Justice, and Governance
in Contemporary Society (LSJG)
E-ISSN: 3164-3434 | Vol. 1, No. 2 (2026) | pp. 117-129

Internet Fraud and Cybersecurity in Nigeria: Yahoo Boys, Youth Vulnerability, Social Conditions, and Crime Prevention

Adams Adah Otakwu[1*]

Centre for Civil-Military Cooperation (CIMICO), Abuja, Nigeria[1]

***Corresponding author:** cimicocentre@gmail.com

Received: 22 March 2026 | Revised: 19 May 2026 | Revised: 24 May 2026 | Published: 30 June 2026

Abstract

Purpose: This study examines the relationship between internet fraud, cybersecurity, and the social conditions associated with youth participation in cybercrime in Nigeria. It specifically analyzes how unemployment, economic insecurity, peer influence, conspicuous consumption, social exclusion, digital opportunities, and changing perceptions of illicit wealth contribute to vulnerability to internet fraud.

Research Methodology: The study adopts a qualitative documentary research design. Data were obtained from contemporary academic literature, Nigerian legislation, institutional reports, and international assessments. The collected evidence was analyzed thematically across four dimensions: social conditions, criminal opportunity, cybersecurity vulnerability, and institutional response.

Results: The findings indicate that socioeconomic conditions may increase vulnerability to cybercrime recruitment but do not independently explain offending behavior. Internet fraud participation is shaped by the interaction of peer networks, social learning, perceived rewards, technological accessibility, weak deterrence, and economic pressures. The study also finds that cybercrime affects digital trust, financial integrity, Nigeria's international reputation, and the development of the digital economy.

Conclusions: Effective prevention requires an integrated approach combining cybersecurity strengthening, law enforcement, digital literacy, youth economic inclusion, community-based prevention, and responsible social-value transformation.

Limitations: The study relies on documentary evidence and does not include primary data from cybercrime offenders, victims, or cybersecurity practitioners.

Contributions: This study contributes to cybercrime and cybersecurity literature by providing a multidimensional explanation of internet fraud in Nigeria and proposing a prevention framework that integrates technological, social, economic, and institutional dimensions.

Keywords: *Cybersecurity, Internet Fraud, Nigeria, Social Conditions, Yahoo Boys, Youth*

How to Cite: Otakwu, A. A. (2026). Internet Fraud and Cybersecurity in Nigeria: Yahoo Boys, Youth Vulnerability, Social Conditions, and Crime Prevention. *Legal Systems, Justice, and Governance in Contemporary Society (LSJG)*, 1(2), 117-129.

1. Introduction

The expansion of the internet and digital technologies has fundamentally transformed contemporary social and economic life. Digital platforms now support banking, commerce, education, communication, employment, government services, and international transactions, making cyberspace an increasingly important component of national economic infrastructure. However, greater connectivity has also created opportunities for criminal exploitation. Cybercrime encompasses various technology-enabled offences, including unauthorized access to computer systems, data interference,

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

identity theft, phishing, online fraud, and other forms of digital financial crime. The United Nations Office on Drugs and Crime (UNODC) recognizes cybercrime as an increasingly transnational phenomenon that requires coordinated legal, technological, institutional, and international responses (Sumadinata, 2023). Nigeria cybersecurity framework similarly acknowledges that internet-enabled criminal activities can affect economic development, social stability, national security, and public trust in digital systems (Khan, Zakir, Tayyab, & Ibrahim, 2024).

Nigeria represents an important case in discussions of cybercrime in Africa due to its large digital population, expanding financial technology ecosystem, extensive mobile connectivity, and significant youth demographic. These developments have created substantial opportunities for digital entrepreneurship and economic participation while simultaneously providing criminal actors with opportunities to exploit technological platforms and social networks. Therefore, Nigeria cybercrime challenge cannot be understood solely as a technological problem (Sule, Sambo, & Yusuf, 2023). It reflects the interaction of social, economic, cultural, institutional, and behavioral factors that shape how individuals perceive and engage with digital opportunities. Previous research involving Nigerian tertiary students indicates that socioeconomic background, peer influence, and demographic characteristics may influence youth vulnerability to cybercrime, although the phenomenon cannot be explained by a single factor alone (Ikwuadinso & Ilozue, 2026).

The development of internet fraud in Nigeria should also be understood within the broader historical evolution of fraud. Advance-fee fraud existed before the widespread adoption of the internet and was previously conducted through traditional communication channels. The expansion of telecommunications and digital platforms has transformed these activities by providing faster, cheaper, and geographically unrestricted methods of targeting victims (Rossy & Ribaux, 2020). Thus, internet technology did not necessarily create fraudulent behavior but expanded the scale, speed, and reach of existing criminal practices. This historical perspective demonstrates that cybercrime involves both technological opportunities and underlying social conditions that influence criminal adaptation (Chen, Hao, Ding, Jiang, Dong, Zhang, & Gao, 2023).

Within Nigerian society, the term “Yahoo Boys” has become widely associated with individuals involved in internet-enabled fraud. The expression has gained recognition through popular culture, social media, and everyday discourse. However, academic analysis requires caution because the label does not represent Nigerian youth generally, nor does it describe every individual involved in digital activities. Evidence from interviews with Economic and Financial Crimes Commission personnel suggests that although young men are frequently identified among suspected cyber-fraud offenders, perpetrators may originate from diverse socioeconomic and demographic backgrounds. Therefore, “Yahoo Boys” should be understood as a socially constructed label associated with a category of cyber-fraud activities rather than as a general characterization of Nigerian youth (Wariboko, & Nwanyanwu, 2024; Omokhabi, Atoyebi, & Omokhabi, 2024).

Socioeconomic conditions remain an important dimension in understanding internet fraud because criminal opportunities are influenced by broader social environments. Economic insecurity, limited employment opportunities, unequal access to legitimate income sources, and social exclusion may increase vulnerability to illicit alternatives for some individuals (Akinyetun, 2021). Research on Nigerian tertiary students identifies relationships between socioeconomic characteristics, peer influence, and cybercrime engagement, while UNODC assessments highlight unemployment, social pressure to achieve wealth, peer networks, and perceptions of rapid financial success as factors associated with cybercrime vulnerability. Nevertheless, socioeconomic disadvantage should not be interpreted as a direct cause of cybercrime because many individuals experiencing economic hardship do not participate in criminal activities. Instead, social conditions interact with peer influence, technological skills, perceived opportunities, expected rewards, moral justification, and perceptions of enforcement in shaping individual decisions (Park, Cho, Lee, & Lee, 2019).

The role of conspicuous consumption has also received increasing attention in discussions of Nigerian internet fraud. Social media platforms have amplified the visibility of luxury lifestyles, expensive

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

possessions, travel, and other symbols of material success. When illicit wealth is publicly displayed and interpreted as evidence of achievement, financial gain may become associated with social recognition and status. Research on internet fraud in Nigeria suggests that aspirations for rapid wealth accumulation and social prestige contribute to the attractiveness of cybercrime among some individuals. Consequently, prevention strategies must consider not only legal enforcement but also the social meanings attached to wealth, success, and status (Orhero & Nwoke, 2025).

Cybersecurity represents another essential dimension of internet fraud prevention. Digital fraud frequently exploits vulnerabilities in technology, human behavior, and information exchange. Phishing, impersonation, identity theft, social engineering, and fraudulent electronic communication often rely on manipulating human trust rather than exploiting technological weaknesses alone. Nigeria has developed legal responses through the Cybercrime Act and related institutional mechanisms to address computer-related fraud, identity theft, and electronic deception. However, cybersecurity challenges continue to evolve as offenders adopt increasingly sophisticated techniques and exploit emerging digital systems (Amoo, Atadoga, Abrahams, Farayola, Osasona, & Ayinla, 2024).

The economic consequences of internet fraud extend beyond individual victims. Cybercrime affects financial institutions, businesses, government agencies, telecommunications providers, and public confidence in the digital economy. The UNODC Cybercrime Assessment for Nigeria highlights substantial financial losses and increasing sophistication in cyberattacks, including the use of cryptocurrency-related mechanisms for illicit financial activities. These developments demonstrate that internet fraud is not merely a criminal justice issue but also a broader challenge affecting economic integrity, digital trust, and national development (Oladipupo, 2025).

Addressing internet fraud requires coordinated responses involving multiple stakeholders. Law enforcement agencies must investigate and prosecute offenders, cybersecurity institutions must reduce technological vulnerabilities, financial institutions must strengthen transaction monitoring, educational institutions must promote digital ethics, and communities must discourage criminal recruitment. Government policies must also address structural conditions that may increase vulnerability to cybercrime. Therefore, effective prevention requires an integrated approach that combines cybersecurity enhancement, institutional enforcement, youth empowerment, digital literacy, and social transformation (Ibegbu, Osita-Njoku, & Nwabuaku, 2026; Anser, Ali, Chen, & Nazar, 2026).

Despite increasing attention to cybercrime in Nigeria, several research gaps remain. Existing discussions often emphasize technological vulnerabilities or law enforcement responses while providing limited integration of the social conditions, behavioral factors, and institutional challenges that shape internet fraud participation. Furthermore, the “Yahoo Boys” phenomenon requires careful analysis that avoids both stereotyping Nigerian youth and reducing cybercrime solely to economic hardship. A comprehensive understanding requires examining how digital opportunities interact with social aspirations, peer networks, economic pressures, and cybersecurity vulnerabilities.

This study therefore examines internet fraud and cybersecurity in Nigeria through a social-structural perspective. It analyzes how economic insecurity, peer influence, material aspirations, digital access, and institutional conditions interact with opportunities for cybercrime while also assessing legal, cybersecurity, and preventive responses. The study seeks to contribute to a broader understanding of internet fraud by demonstrating that effective prevention requires simultaneous attention to digital infrastructure, social environments, institutional capacity, and the factors that influence criminal opportunity formation.

2. Literature Review and Hypothesis/es Development

2.1 Internet Fraud

Internet fraud refers to fraudulent activities in which digital technologies, online platforms, electronic communication systems, or computer networks are used to deceive individuals, organizations, or

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

institutions for unlawful financial or personal benefits (Ali & Mohd, 2024). It includes various forms of deception such as phishing, identity theft, impersonation, advance-fee fraud, fraudulent electronic transactions, and social engineering-based schemes. Unlike traditional fraud, internet fraud is characterized by greater speed, anonymity, scalability, and the ability to target victims across geographical boundaries. Therefore, internet fraud represents a significant challenge within the contemporary digital environment because offenders can exploit technological accessibility and information asymmetry (Abubakari & Oseh-Ovarah, 2025).

In Nigeria, internet fraud has developed as a prominent form of cyber-enabled criminal activity associated with the broader phenomenon of online deception. Although technology provides the tools through which fraud is conducted, participation in internet fraud is also influenced by social, economic, cultural, and behavioral factors (Chinecherem, 2025). Understanding internet fraud therefore requires attention not only to digital vulnerabilities but also to the social environments that shape criminal opportunities, motivations, and networks. This perspective allows internet fraud to be examined as a multidimensional phenomenon involving technology, individual decision-making, and broader societal conditions.

2.2 Cybercrime

Cybercrime refers broadly to criminal activities involving computers, digital systems, networks, or information technologies. Cybercrime may involve offences where digital systems are the direct target, such as unauthorized access, malware attacks, and data interference, as well as offences where technology functions as a tool for committing traditional crimes, including fraud, identity theft, and financial deception. This distinction is important because internet fraud represents one form of cybercrime but does not encompass the entire range of technology-related offences (Ibegbu, Osita-Njoku, & Nwabuaku, 2026).

The expansion of digital connectivity has increased both the opportunities and challenges associated with cybercrime prevention. Criminal actors continuously adapt their methods by exploiting technological developments, online platforms, and human vulnerabilities. Consequently, effective cybercrime responses require more than technical solutions; they require legal frameworks, institutional capacity, cybersecurity awareness, law enforcement capability, and cooperation among public and private stakeholders. In Nigeria, the Cybercrime Act provides a legal foundation for addressing various technology-enabled offences, including computer-related fraud and identity-related crimes (Sumadinata, 2023; (Anser, Ali, Chen, & Nazar, 2026)).

2.3 Cybersecurity

Cybersecurity refers to the protection of digital systems, networks, devices, applications, and data from unauthorized access, disruption, manipulation, exploitation, and other malicious activities. Contemporary cybersecurity is no longer limited to technical protection mechanisms such as encryption, access control, and system security. It also includes human awareness, organizational governance, risk management, incident response, institutional coordination, and resilience against evolving digital threats (Ikwuadinso & Ilozue, 2026).

In the context of internet fraud, cybersecurity is closely connected with both technological and human factors. Many fraudulent activities do not rely solely on sophisticated technical attacks but also exploit human trust, limited digital awareness, weak security practices, and social engineering techniques (Uroko, 2022). Therefore, strengthening cybersecurity requires an integrated approach that combines technological protection, public education, institutional preparedness, and effective regulatory responses. In Nigeria, improving cybersecurity capacity is essential not only for protecting digital infrastructure but also for maintaining confidence in financial systems and digital economic development (Ibegbu, Osita-Njoku, & Nwabuaku, 2026).

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

2.4 "Yahoo Boys"

The term "Yahoo Boys" is a popular Nigerian expression commonly associated with young individuals involved in internet-enabled fraud. The term emerged within Nigerian popular culture and social discourse and has become widely used to describe a recognizable category of cyber-fraud actors. However, it is not a legal classification and should be distinguished from formal definitions of cybercrime offences established under Nigerian law (Ajayi, Adesope, & Oso, 2025).

Academic analysis of the "Yahoo Boys" phenomenon requires careful interpretation because the term may create social assumptions about Nigerian youth generally. Not all young Nigerians involved in digital activities participate in cybercrime, and cyber-fraud offenders do not necessarily share identical socioeconomic backgrounds (Ajah, Onyejegbu, Isife, Enweonwu, Chinweze, Anyadike, Ilo, Omaliko, Asadu, Ugwu, Okemini, Chukwuemeka, Ohabuenyi, Uzoigwe, Iloma, Madubuko, & Ngwu, 2026). Therefore, the concept should be understood as a socially constructed identity associated with a particular form of cyber-enabled offending rather than as a representation of Nigerian youth as a whole. Studying the phenomenon requires examining the social networks, cultural meanings, economic aspirations, and digital opportunities that contribute to participation in internet fraud (Wariboko, & Nwanyanwu, 2024; Okosun, & Ilo, 2023).

2.5 Social Conditions

Social conditions refer to the economic, institutional, cultural, and relational environments that influence individual experiences, opportunities, and decision-making processes. In relation to internet fraud, relevant social conditions include employment opportunities, economic insecurity, educational experiences, peer relationships, family circumstances, perceptions of social mobility, and expectations regarding material success. These conditions do not directly determine criminal behavior but may influence individuals' exposure to risks, opportunities, and motivations (Muhar, Raymond, Bauer, Böck, Braito, & Van, 2018).

The relationship between social conditions and cybercrime is therefore complex and multidimensional. Economic pressures and limited legitimate opportunities may increase vulnerability for some individuals, but they do not automatically lead to criminal participation. Instead, social conditions interact with peer influence, technological access, perceived rewards, moral justification, and individual choices. Understanding these interactions is essential for developing prevention strategies that address both cybersecurity vulnerabilities and the broader social factors associated with cybercrime engagement (Hesketh & Robinson, 2019).

2.6 Theoretical Framework

2.6.1 General Strain Theory

General Strain Theory (GST), developed by Agnew, provides an important framework for understanding how social pressures and perceived disadvantages may influence engagement in deviant behavior. The theory proposes that individuals may experience strain through failure to achieve valued goals, loss of positive conditions, or exposure to negative circumstances. When individuals perceive legitimate pathways to success as limited or inaccessible, some may seek alternative means, including deviant adaptations, to achieve desired outcomes.

Within the Nigerian cybercrime context, GST helps explain how unemployment, economic insecurity, social inequality, and blocked aspirations may contribute to vulnerability to internet fraud. However, the theory does not suggest that disadvantaged conditions automatically cause criminal behavior. Rather, strain interacts with individual coping mechanisms, social environments, available opportunities, and perceptions of acceptable behavior. This perspective is consistent with research indicating that socioeconomic factors may influence cybercrime vulnerability while remaining insufficient as a single explanation for participation.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

2.6.2 Social Learning Theory

Social Learning Theory explains criminal behavior through processes of interaction, observation, and reinforcement within social environments. According to this perspective, individuals may learn techniques, motivations, rationalizations, and attitudes that support criminal activities through relationships with peers, groups, and social networks. This framework is particularly relevant to internet fraud because digital knowledge, fraudulent techniques, and justifications for offending can be transmitted through both offline and online communities.

In Nigeria, peer networks and social environments have been identified as important factors influencing youth engagement with cybercrime. Individuals may become exposed to cyber-fraud practices through interactions with others who normalize or promote illicit activities as acceptable pathways to financial success. Social Learning Theory therefore complements General Strain Theory by explaining how social conditions are transformed into actual criminal behavior through learning processes, group influence, and shared definitions favorable to cybercrime.

3. Research Methodology

The study adopts a qualitative documentary research design. It relies on secondary materials including peer-reviewed academic articles, Nigerian legislation, government and law-enforcement publications, international assessments and relevant scholarly literature. Materials were purposively selected according to their relevance to internet fraud, cybercrime, youth participation, socioeconomic conditions, cybersecurity and prevention. The analysis is thematic and focuses on four interconnected dimensions: social conditions, criminal opportunity, cybersecurity vulnerability and institutional response. The documentary approach is appropriate because the study seeks to integrate legal, sociological, criminological and cybersecurity perspectives rather than generate primary prevalence estimates (Bowen, 2009; Nowell, Norris, White, & Moules, 2017).

4. Results and Discussions

4.1 Evolution of Internet Fraud in Nigeria

Internet fraud in Nigeria developed from earlier forms of advance-fee fraud that relied on letters, postal communication, telephone calls and other forms of interpersonal deception. The emergence of affordable internet access and telecommunications transformed the operational environment by reducing geographical barriers and enabling fraudsters to communicate simultaneously with large numbers of potential victims (Rossy & Ribaux, 2020). The historical evolution demonstrates that internet fraud is partly a technological adaptation of an older fraudulent practice.

The transformation became particularly significant as cybercafés, mobile telecommunications and internet-enabled devices became increasingly accessible. Digital platforms created opportunities for anonymity, rapid communication, false identities and international targeting. The development of social media and online financial services further expanded the range of platforms through which fraud could occur. Consequently, internet fraud has moved beyond the traditional email-based advance-fee model into increasingly diverse forms of digital deception (Conde, 2020).

Contemporary cyber-fraud may involve romance scams, business-email compromise, investment deception, impersonation, phishing, fraudulent online sales, identity theft and other forms of social engineering. Some offenders operate individually, while others operate through networks in which different participants perform specialised roles. This organisational dimension makes internet fraud a law-enforcement challenge rather than merely an issue of individual dishonesty.

4.2 The "Yahoo Boys" Phenomenon and Youth Culture

The "Yahoo Boys" phenomenon has acquired significance beyond the commission of internet fraud because it has become connected with identity, peer networks and perceptions of social status. The

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

term is frequently used in Nigerian popular discourse to describe young men associated with online fraud and conspicuous wealth. Academic research, however, demonstrates that the social characteristics of cyber-fraudsters are more diverse than the popular stereotype suggests. Interviews with EFCC personnel found that although young men were commonly represented, cyber-fraudsters could come from affluent as well as economically disadvantaged backgrounds.

The phenomenon can therefore be examined as a form of deviant subculture in which certain behaviours and symbols may acquire social meaning. Where expensive vehicles, clothing, travel and other displays of wealth become visible markers of success, illicit income can potentially be interpreted by some observers as a route to social mobility. Recent UNODC analysis similarly identifies societal pressure for rapid and conspicuous wealth accumulation and peer networks as factors associated with vulnerability to cybercrime recruitment (Bemgba, 2025).

The cultural dimension should not, however, be overstated. Nigerian society contains strong social, religious and community norms against fraud, and many young Nigerians actively reject cybercrime. The existence of a visible cyber-fraud subculture therefore does not mean that internet fraud is culturally accepted by Nigerian society as a whole. The more analytically useful question is how specific peer groups and social environments may normalise or rationalise offending (Wariboko & Nwanyanwu, 2024).

4.3 Social Conditions and Youth Vulnerability

Economic conditions constitute an important part of the context within which cybercrime may develop. Youth unemployment, underemployment, rising living costs, inequality and difficulties in transitioning from education to stable employment can create frustration and uncertainty. These conditions may increase the appeal of income-generating opportunities that appear faster or more accessible than conventional employment. Recent research among Nigerian tertiary students found associations between socioeconomic characteristics and cybercrime engagement, with peer influence identified as an important factor (Adewuyi, Odutayo, Opesemowo, & Jacob, 2024).

However, the existence of socioeconomic hardship does not establish a direct causal relationship with internet fraud. If unemployment alone caused cybercrime, all unemployed individuals would be expected to participate in cybercrime, which is not the case. Moreover, research involving law-enforcement personnel indicates that suspected cyber-fraudsters may originate from diverse socioeconomic backgrounds. Social conditions should therefore be conceptualised as risk environments that may interact with opportunity, peer networks, individual choices and perceptions of enforcement (Alabi, Bamidele, & Oladimeji, 2023).

Educational institutions constitute another important environment. Universities and other tertiary institutions provide large concentrations of young people with digital literacy and social networks. Digital competence can generate legitimate economic opportunities, but it can also facilitate cybercrime when combined with criminal motivation and peer influence. The 2026 study of Nigerian tertiary students identified online scams, hacking and phishing among reported forms of cybercrime and found significant associations between selected demographic factors and engagement.

4.4 Peer Influence, Social Learning and Criminal Recruitment

Peer networks can facilitate cybercrime by providing technical knowledge, contacts, encouragement and opportunities. A young person who has no prior experience of online fraud may encounter peers who demonstrate techniques, display financial rewards or provide access to criminal networks. Social learning can consequently reduce the psychological and practical barriers to participation. The importance of peer networks is supported by recent Nigerian research identifying peer pressure as a significant influence among tertiary students. The broader literature on Nigerian cyber-fraud also indicates that cybercriminal behavior can involve shared meanings and social networks rather than isolated individual decisions.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

This has implications for prevention. Interventions directed only at individuals after arrest may not disrupt the social networks through which knowledge and recruitment occur. Prevention should therefore include educational institutions, youth organizations, families, community leaders and digital platforms. The objective should be to interrupt recruitment pathways while creating legitimate networks through which young people can acquire digital skills, employment opportunities and entrepreneurship support.

4.5 Conspicuous Consumption and the Social Meaning of Wealth

The display of wealth is an important dimension of the social discourse surrounding internet fraud. Social media enables individuals to publicly display possessions and lifestyles that were previously visible only within limited physical communities. Where luxury becomes a marker of achievement, young people may be exposed to highly visible representations of success without equally visible information about the source of the wealth.

Research on Nigerian internet fraud has identified the pursuit of rapid wealth and social recognition as part of the broader phenomenon. UNODC's recent analysis similarly discusses social pressure to attain wealth quickly and the visibility of luxury lifestyles associated with some cybercriminal networks. The policy implication is not that material ambition should be discouraged. Economic aspiration is an important driver of entrepreneurship and innovation. The challenge is to distinguish legitimate wealth creation from criminal acquisition and to create social environments in which competence, innovation, professional achievement and community contribution are also recognized as meaningful forms of success.

4.6 Cybersecurity and the Architecture of Internet Fraud

Internet fraud exploits weaknesses across three interconnected environments: technology, institutions and human behavior. Technical vulnerabilities may include compromised accounts, insecure systems and inadequate authentication. Institutional vulnerabilities may involve weak controls, poor information sharing and insufficient incident response. Human vulnerabilities may include inadequate awareness, excessive trust, poor password practices and susceptibility to social engineering.

The Nigerian Cybercrime Act provides statutory responses to several of these threats. Its provisions address computer-related fraud and identity theft, including fraudulent impersonation and deceptive electronic communications (Amoo, Atadoga, Abrahams, Farayola, Osasona, & Ayinla, 2024). Nigeria's national cybersecurity policy also recognises that cyber threats affect economic and national-security interests and calls for coordinated responses involving relevant stakeholders. Cybersecurity therefore requires a whole-of-society approach. Banks, telecommunications companies, technology platforms, educational institutions, government agencies and citizens each control part of the environment within which cybercrime occurs. Security agencies alone cannot prevent every fraudulent transaction because many incidents originate from human interactions and rapidly changing digital platforms.

4.7 Internet Fraud, Financial Integrity and the Digital Economy

The economic consequences of cybercrime extend beyond the immediate financial losses suffered by victims. Fraud can increase transaction costs, require financial institutions to invest more heavily in security, undermine consumer confidence and complicate cross-border digital commerce. Businesses may also face reputational risks when customers associate Nigerian digital transactions with fraud (Alabi, Bamidele, & Oladimeji, 2023).

UNODC's 2025 Nigeria Cybercrime Assessment reports substantial financial losses associated with cybercrime and identifies increasing sophistication in cyberattacks and the use of cryptocurrency in laundering illicit proceeds. These developments demonstrate the growing relationship between cybercrime and financial crime.The implications are particularly significant for Nigeria's digital transformation. Digital finance and online commerce depend fundamentally upon trust. If citizens become reluctant to use digital platforms because of perceived fraud risks, the benefits of

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

digitalisation may be reduced. Cybersecurity is therefore not simply a security-sector concern; it is an economic-development requirement.

4.8 Legal and Institutional Response

Nigeria has developed a substantial legal and institutional framework for responding to cybercrime. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 established a dedicated statutory framework covering computer-related offences, identity theft and other cybercrime categories. The legislation provides criminal sanctions for computer-related fraud and fraudulent impersonation.

The Economic and Financial Crimes Commission plays a central role in investigating and prosecuting economic and financial crimes, including internet fraud. Its public institutional statistics indicate extensive investigative, prosecutorial and conviction activity across its mandate. The Commission also continues to publicize arrests, prosecutions and convictions involving alleged internet fraudsters. The institutional response nevertheless requires coordination because cybercrime does not respect institutional boundaries. Financial intelligence, digital forensics, telecommunications information, banking records, international cooperation and prosecutorial expertise may all be necessary in a single investigation. Effective enforcement consequently depends upon timely information sharing and technically competent investigators (Khan, Zakir, Tayyab, & Ibrahim, 2024).

4.9 Limitations of an Enforcement-Centre Response

Law enforcement remains indispensable because cybercrime produces identifiable victims and unlawful financial benefits. Arrest, investigation, prosecution, conviction and asset recovery provide accountability and deterrence. Nevertheless, enforcement alone cannot eliminate the social processes through which cybercrime is learned and reproduced.

The recruitment of new participants can continue if the underlying social networks remain intact. Similarly, where young people perceive cybercrime as a faster route to economic mobility than legitimate employment, arresting individual offenders may not remove the perceived incentives. Prevention therefore requires complementary interventions directed at education, employment, digital ethics, community values and youth entrepreneurship. A balanced response should also distinguish between prevention and stigmatization. Excessive generalization about young people can produce distrust and undermine legitimate digital entrepreneurship. The appropriate objective is to identify specific criminal behavior and risk factors while simultaneously expanding lawful opportunities for young Nigerians.

4.10 Social Prevention and Youth Economic Inclusion

Youth economic inclusion should form part of a comprehensive cybercrime-prevention framework. Digital skills can generate legitimate employment through software development, cybersecurity, digital marketing, financial technology, online commerce and other sectors. The same technological knowledge that can be exploited for fraud can therefore be redirected towards productive economic activity.

The relationship between digitalization and employment is complex. Recent African evidence suggests that digital technologies can reduce unemployment in some circumstances while also producing displacement or skills-mismatch effects depending on the technology and labor market context. Consequently, simply providing internet access or technical training is insufficient. Digital skills program should be connected to market demand, apprenticeships, entrepreneurship finance and credible employment pathways. Educational institutions should also incorporate digital ethics into ICT education. Students should understand not only how to use digital technologies but also the legal, social and economic consequences of misuse. Such program can combine cybersecurity awareness, digital citizenship, financial literacy and professional ethics (Ikwuadinso & Ilozue, 2026).

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

4.11 Community and Family-Based Prevention

Communities play an important role in determining what forms of behavior receive approval, criticism or indifference. Families, religious institutions, traditional institutions, youth organisations and civil society can contribute to prevention by discouraging the social celebration of illicit wealth and supporting lawful pathways to economic advancement. Community-based prevention should not rely upon moral condemnation alone. Young people require credible alternatives. Mentorship, entrepreneurship networks, career guidance, technical training and access to legitimate digital work can provide practical alternatives to criminal recruitment. The community approach is also relevant to reporting. Citizens who encounter suspicious online activities should have accessible channels for reporting incidents. The EFCC's digital reporting mechanisms illustrate the importance of making reporting accessible to citizens. Similar reporting pathways should exist across relevant cybersecurity and law-enforcement institutions.

4.12 International and Cross-Border Dimensions

Internet fraud is inherently transnational because offenders can operate from one jurisdiction while targeting victims in another and moving proceeds through multiple financial systems. Effective investigation may therefore require international cooperation, electronic evidence sharing, asset tracing and extradition or mutual legal assistance mechanisms. Nigeria's cybercrime response should consequently remain connected to regional and international cybersecurity frameworks. UNODC emphasizes international cooperation, electronic evidence, specialized investigative techniques and coordinated law-enforcement responses as important dimensions of cybercrime control. Cross-border cooperation should also extend to financial institutions and technology companies. Fraudulent accounts, digital wallets, cryptocurrency addresses and social-media profiles may involve service providers located outside Nigeria. Timely cooperation is therefore essential for identifying offenders and recovering proceeds (Rossy & Ribaux, 2020).

4.13 Discussion

The evidence reviewed in this study demonstrates that internet fraud in Nigeria is simultaneously a technological, economic, social and institutional phenomenon. The emergence of the “Yahoo Boys” phenomenon illustrates how criminal behavior can become connected with youth identity, peer networks and social perceptions of wealth. However, the evidence does not support a simplistic conclusion that unemployment or poverty directly causes internet fraud. Research identifies socioeconomic conditions as relevant contextual factors, while other evidence demonstrates that cyber-fraudsters may originate from different social backgrounds.

General Strain Theory helps explain how economic pressure and blocked aspirations may create vulnerability, while Social Learning Theory explains how peer networks can transmit criminal knowledge and rationalizations. Neither theory alone provides a complete explanation. The Nigerian phenomenon is better understood as the interaction of structural conditions, individual choices, social learning, technological opportunity and perceptions of reward and risk.

The cybersecurity implications are substantial. Internet fraud undermines confidence in digital transactions, imposes financial costs on institutions and may facilitate broader forms of financial crime. The UNODC assessment demonstrates that Nigeria's cybercrime losses are significant and that criminal methods are becoming increasingly sophisticated. The response must therefore integrate cybersecurity with financial regulation, criminal investigation and social prevention.

The analysis further indicates that prevention should move beyond an exclusively punitive framework. Enforcement remains essential, but sustainable prevention requires reducing recruitment opportunities, improving digital ethics, expanding legitimate youth economic opportunities and challenging social environments that normalize illicit wealth. This approach does not excuse criminal conduct; rather, it recognizes that effective crime prevention requires intervention at multiple points in the causal and opportunity structure.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

5. Conclusions

Internet fraud represents an important component of Nigeria's contemporary cybercrime and economic-security environment. The phenomenon popularly described as “Yahoo Boys” reflects a particular social expression of internet-enabled fraud involving predominantly young people, although the available evidence indicates that cyber-fraudsters are not socially homogeneous. The phenomenon must therefore be studied without stereotyping Nigerian youth or attributing cybercrime exclusively to poverty, unemployment or any single social condition.

The study finds that socioeconomic insecurity, peer influence, material aspirations, digital opportunity and perceptions of enforcement can interact in ways that make cybercrime attractive to some individuals. At the same time, the presence of these conditions does not inevitably result in offending. This distinction is essential for developing evidence-based interventions.

Nigeria's cybersecurity and criminal justice response should consequently combine enforcement with prevention. Effective measures should address digital vulnerabilities, improve institutional coordination, disrupt criminal networks, enhance financial monitoring, provide cybersecurity education and expand legitimate economic opportunities for young people. Community and educational institutions should also contribute to reducing the social normalization of illicit wealth.

Ultimately, the challenge is not to restrict Nigeria's digital transformation but to make that transformation safer, more inclusive and more ethically grounded. Digital technologies can provide pathways to employment, innovation and economic development. The task of public policy is to ensure that these opportunities are not displaced by criminal networks while maintaining a criminal justice response capable of holding offenders accountable.

Acknowledgement

The author would like to acknowledge the contributions of researchers, institutions, and organizations whose academic publications, policy documents, and cybersecurity reports provided valuable insights for this study. The author also appreciates the efforts of institutions involved in cybersecurity development, cybercrime prevention, and digital governance in Nigeria, whose work supported the understanding of internet fraud, social conditions, and prevention strategies.

Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this article. The research was conducted independently, and no financial, commercial, institutional, or personal relationships influenced the research design, data analysis, interpretation of findings, or preparation of the manuscript. The author has no competing interests that could affect the objectivity and integrity of this study.

References

Abubakari, Y., & Oseh-Ovarah, V. (2025). The gamification of online romance fraud through offenders’ cards. *Digital Threats: Research and Practice*, *6*(4), 1-20. https://doi.org/10.1145/3773289

Adewuyi, H. O., Odutayo, A. O., Opesemowo, O. A., & Jacob, U. S. (2024). Peer pressure, socio-economic status and gender difference on cybercrime tendencies of undergraduates. *Journal of Pedagogical Sociology and Psychology*, *7*(1), 42-53. https://doi.org/10.33902/jpsp.202528154

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

Ajah, B. O., Onyejegbu, D. C., Isife, C. T., Enweonwu, O. A., Chinweze, U. C., Anyadike, N. O., Ilo, K. O., Omaliko, J. C., Asadu, N., Ugwu, C. C. O., Okemini, O. O., Chukwuemeka, L. K. C., Ohabuenyi, J., Uzoigwe, C. O., Iloma, D. O., Madubuko, J. C., & Ngwu, G. E. (2026). Narrative accounts, feelings, and perceptions of yahoo-plus offenders in Enugu and Abakaliki correctional centers, Nigeria. *International Journal of Law, Crime and Justice, 84, 100823*. https://doi.org/10.1016/j.ijlcj.2025.100823

Ajayi, T. M., Adesope, O. A., & Oso, I. O. (2025). Yahooism to ritualism: Ideological motivations for cyber fraud in selected Yoruba films. *Southern African Linguistics and Applied Language Studies*, *43*(1), 102-116. https://doi.org/10.2989/16073614.2024.2341708

Akinyetun, T. S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2), 86-109. https://doi.org/10.19184/csi.v1i2.24188

Alabi, A., Bamidele, A. H., & Oladimeji, A. B. (2023). Cybercrime in Nigeria: Social influence affecting the prevention and control. *Lafia Journal of Economics and Management Sciences, 227-241*. https://doi.org/10.64290/gjam.v5i1.1137

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101-121. https://doi.org/10.1177/10567879221082966

Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World journal of advanced research and reviews*, *21*(2), 205-217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Anser, M. K., Ali, S., Chen, Y., & Nazar, R. (2026). Crisis-driven cyber risk: Evaluating the cybercrime landscape in the face of pandemic uncertainty. *Computers & Security, 169, 104973*. https://doi.org/10.1016/j.cose.2026.104973

Bemgba, P. T. (2025). Evaluating Public Perception and Awareness of Internet Fraud among Residents in Nigeria. *African Journal of Stability and Development (AJSD)*, *17*(2), 903-933. https://doi.org/10.53982/ajsd.2025.1702.06-j

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 71. https://doi.org/10.1057/s41599-023-01560-x

Chinecherem, A. M. (2025). Cybercrime and National Security: A Critical Study of Online Fraud and State Vulnerabilities in West Africa. *Sciences (UKRJAHSS)*, *1*(6), 245-256. https://doi.org/10.5281/zenodo

Conde Solares, C. (2020). The Moral Dimensions of Sufism and the Iberian Mystical Canon. *Religions*, *11*(1), 15. https://doi.org/10.3390/rel11010015

Hesketh, R. F., & Robinson, G. (2019). Grafting:“The boyz” just doing business? Deviant entrepreneurship in street gangs. *Safer Communities*, *18*(2), 54-63. https://doi.org/10.1108/sc-05-2019-0016

Ibegbu, C. M., Osita-Njoku, A., & Nwabuaku, K. W. (2026). Socioeconomic determinants of cybercrime engagement among youths in Nigerian tertiary institutions: Insights from Imo State. *African Journal of Social Issues*, *9*(1), 185-198. https://doi.org/10.4314/ajosi.v9i1.11

Ikwuadinso, Y. T., & Ilozue, V. (2026). Behavioural and Socioeconomic Profiles of Cybercrime Offenders: Implications for Cybersecurity in Anambra State Correctional Centres. *Sciences*, *2*(8), 152-166. https://doi.org/10.5281/zenodo.22048281

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co

Khan, S. H., Zakir, M. H., Tayyab, A., & Ibrahim, S. (2024). The role of international law in addressing transnational organized crime. *Journal of Asian Development Studies*, *13*(01), 283-294. https://doi.org/10.62345/jads.2024.13.1.24

Muhar, A., Raymond, C. M., Van Den Born, R. J., Bauer, N., Böck, K., Braito, M., ... & Van Riper, C. J. (2018). A model integrating social-cultural concepts of nature into frameworks of interaction between social and natural systems. *Journal of Environmental Planning and Management, 61(5-6), 756-777*. https://doi.org/10.1080/09640568.2017.1327424

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria International Journal of Qualitative Methods, 16, 1–13. *DOI:*. https://doi.org/10.1177/1609406917733847

Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, *30*(6), 1653-1663. https://doi.org/10.1108/JFC-08-2022-0185

Oladipupo, A. O. (2025). The dark web of cryptocurrency: Unpacking the nexus between digital currencies, Cybercrime, and Global Governance. *Journal of Contemporary International Relations and Diplomacy*, *6*(2), 46-59. https://doi.org/10.53982/jcird.2025.0602.04-j

Omokhabi, A. A., Atoyebi, V. O., & Omokhabi, U. S. (2024). An Analysis of young adults engagement in cyber-criminal activities in Nigeria. *FUOYE Journal of Criminology and Security Studies*, *3*(1). https://doi.org/10.21107/sml.v6i1.18239

Orhero, M. I., & Nwoke, C. (2025). Theorizing the hypeman in Nigerian popular culture: Poetics, performance, and the e-fraud economy. *Canadian Journal of African Studies/Revue canadienne des études africaines*, *59*(3), 497-516. https://doi.org/10.1080/00083968.2025.2462217

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The economics of cybercrime: The role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems (TMIS)*, *10*(4), 1-23. https://doi.org/10.1145/3351159

Rossy, Q., & Ribaux, O. (2020). Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms: Q. *Rossy, O. Ribaux. European Journal on Criminal Policy and Research*, *26*(3), 335-356. https://doi.org/10.1007/s10610-020-09438-3

Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, *30*(6), 1557-1574. https://doi.org/10.1108/JFC-07-2022-0157

Sumadinata, W. S. (2023). Cybercrime and global security threats: A challenge in international law. *Russian Law Journal*, *11*(3), 438-444. https://doi.org/10.52783/rlj.v11i3.1112

Uroko, F. C. (2022). Proverbs 4:10–19 And the growing spate of Internet fraud amongst Nigerian youths. *HTS Theological Studies*, *77*(4). https://doi.org/10.4102/hts.v77i4.6776

Wariboko, O. P. C., & Nwanyanwu, F. C. (2024). The dark side of connectivity: A socio-ethical exploration of internet fraud and Nigerian youth. *Àgídìgbo: ABUAD Journal of the Humanities*, *12*(1), 89-104. https://doi.org/10.53982/agidigbo.2024.1201.06-j

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co