Evaluating Public Perception and Awareness of Internet Fraud among Residents in Nigeria

African Journal of Stability
& Development
Vol 17 No. 2, Nov. 2025
pp. 903-933

Paul Terlumun Bemgba, *PhD* [1]

Abstract

As Nigeria deepens its engagement with the digital economy, internet fraud has emerged as a pervasive and socially complex challenge. What began in the 1990s with rudimentary email scams known as "419 fraud" has evolved into highly sophisticated schemes involving phishing, identity theft, cryptocurrency fraud, and Business Email Compromise (BEC). Despite extensive interventions by state agencies such as the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force Cybercrime Unit, and collaborations with international bodies like INTERPOL and the FBI, internet fraud continues to thrive, particularly among Nigerian youths. This study evaluates public perception and awareness of internet fraud within Nigeria, focusing on how socio-economic hardship, youth unemployment, cultural narratives, and media portrayals shape societal attitudes towards cybercrime. Using a mixed-method approach anchored in

[1] Legislative Centre for Security Analysis (LeCeSA), National Institute for Legislative and Democratic Studies (NILDS), National Assembly, Abuja; paulbemgba@gmail.com; https://orcid.org/0009-0007-2028-9517

survey data and qualitative content analysis, the study explores the paradox of widespread condemnation of cybercrime alongside pockets of social acceptance and even glorification, especially among disenfranchised youths. Prominent cases, such as the arrests of Ramon Abbas (Hushpuppi), Obinwanne Okeke (Invictus Obi), and the rise of "Yahoo Academies," underscore the extent to which cybercrime is embedded in socio-cultural and economic systems. Public figures convicted of internet fraud are often simultaneously vilified and idolised, reflecting complex perceptions of success, justice, and opportunity in a society plagued by poverty and systemic corruption. Findings such as a 2019 NOIPolls survey indicating that 32% of youths knew someone involved in cybercrime further reveal normalisation tendencies among vulnerable demographics. The research identified several critical drivers behind the public perception of internet fraud, including structural unemployment, poor digital literacy, ineffective law enforcement, peer pressure, and media glamourisation. Furthermore, it highlighted key demographic variations in public opinion, based on age, education, gender, and region. The paper argues that existing legal and punitive responses must be supplemented by culturally informed public education, youth empowerment initiatives, ethical media regulation, and rehabilitative strategies. Only through a holistic understanding of the socio-economic and psychological dimensions of internet fraud can Nigeria develop effective policies that shift public perception and fortify digital integrity in its emerging economy.

Keywords: Public perception, Internet fraud, Cybercrime awareness, Cybersecurity, Digital economy, Nigeria

Introduction

Internet fraud in Nigeria has evolved significantly over the past three decades, transforming from rudimentary email scams known as 419 scams into complex criminal enterprises involving identity theft, phishing schemes, romance scams, corporate email compromises, and cryptocurrency fraud. Early operations, such as the infamous advance-fee fraud, emails that promise large sums of money in exchange for small processing fees, have given way to more organised cybercriminal networks that exploit digital platforms and social engineering tactics (SCARS Institute, 2024).

Despite concerted efforts by the Nigerian government through agencies like the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force Cybercrime Unit, and collaborations with international organisations such as INTERPOL and the FBI, the prevalence of internet fraud remains troublingly high. For instance, in 2020, the EFCC arrested several individuals associated with major online scams valued at over $100 million USD, including the globally publicised case of Ramon Olorunwa Abbas (popularly known as Hushpuppi), who was arrested by Dubai police and extradited to the United States for multiple counts of internet fraud and money laundering (Brooks, 2022).

Public perception of internet fraud in Nigeria remains highly polarised. A significant portion of the population, particularly older generations and public officials, condemns such activities as unethical, criminal, and damaging to the country's global reputation. However, among some youth populations, especially in economically marginalised communities, internet fraud is rationalised, if not subtly celebrated, as a legitimate survival strategy in the face of massive unemployment, economic inequality, and systemic corruption. A 2019 survey conducted by NOIPolls indicated that 32% of young Nigerians admitted knowing someone involved in cybercrime and suggested that poor economic conditions and weak law enforcement were primary contributors to the problem (Adejoh, Alabi, Adisa & Emezie, 2019).

Cases such as the Obinwanne Okeke (Invictus Obi) scandal further underscore the complexity of the phenomenon. Okeke, once hailed as a successful young entrepreneur and even featured on Forbes Africa's 30 Under 30 list, was later convicted in the United States for orchestrating a multi-million-dollar fraud scheme. His case illustrates how internet fraud can be masked under legitimate business fronts, making it harder for the public to detect or unequivocally condemn (Infosecurity, 2021).

Adding to the long list of cybercrime incidents are more recent cases from 2023 and 2024. In July 2023, the EFCC arrested over 120 suspected internet fraudsters in Enugu and Ogun States during coordinated raids, uncovering networks engaged in romance scams, impersonation fraud, and cryptocurrency-related scams. Particularly notable was the case of Kelvin Oniarah, a suspected "Yahoo Plus" kingpin operating from Delta State, who was apprehended alongside accomplices involved in ritual cyber-fraud activities. Also in 2024, the U.S. Department of Justice indicted five Nigerian nationals for orchestrating Business Email Compromise (BEC) attacks targeting U.S. hospitals and COVID-19 relief funds, costing institutions over $12 million USD (U.S. Department of Justice, 2024).

Furthermore, the rise of so-called Yahoo Academies (underground cybercrime training centres) has become a worrying trend. In early 2024, police in Lagos raided an alleged academy where over 30 teenagers were being trained in advanced hacking techniques, reinforcing fears that cybercrime is becoming an institutionalised survival strategy for youths (Oyewo, 2025).

Cultural narratives and media portrayals continue to glamourise the "Yahoo boy" lifestyle, with music videos, Nollywood films, and social media platforms showcasing extravagant lifestyles funded by illicit activities. Such representations contribute to the normalisation and, in some cases, the glorification of cybercrime among impressionable youths (Oladunjoye & Omobowale, 2022).

This paper seeks to unpack these complex and often conflicting perceptions and examine the socio-cultural undercurrents that inform them. It will analyse how economic conditions, cultural shifts, peer influence, and media representations affect public attitudes towards internet fraud. Understanding public sentiment is crucial for designing more effective policies, community-based interventions, and educational campaigns that can shift societal values towards ethical digital citizenship and sustainable economic opportunities.

Statement of the Problem

Despite intensified efforts to combat cybercrime over the past two decades, numerous high-profile arrests, and legislative reforms, such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, and extensive public awareness campaigns by agencies, like the Economic and Financial Crimes

Commission (EFCC) and the Nigeria Police Force, internet fraud remains deeply entrenched in the Nigerian society (Onadeko & Afolayan, 2021).

From the early 2000s, when Nigeria became synonymous globally with the 419 scams through the mid-2010s, characterised by Business Email Compromise (BEC) operations and, most recently, the surge of cryptocurrency-related scams (2020–2025), the phenomenon of internet fraud has continued to grow in sophistication and reach. During this period, there has been a marked increase in the number of young Nigerians engaging in online scams, despite the tangible risks of prosecution and societal condemnation (Eboh, 2025).

One paradox that continues to puzzle policymakers and law enforcement is the persistent level of social tolerance and, in some cases, outright admiration for internet fraudsters among certain demographics, particularly youths aged 18–35. While many Nigerians view cybercrime as morally reprehensible and damaging to the country's international reputation, a significant minority justify it as a rational response to endemic poverty, rising unemployment, political corruption, and lack of opportunities for social mobility (Adejumo & Okeowo, 2021). For example, cases like Hushpuppi's arrest in 2020 and the more recent Yahoo Academy raids in 2024 reveal that despite the highly publicised consequences, internet fraud still attracts admiration as a symbol of success among disenfranchised youths (Ajibade, 2023). Popular culture, including music and film, often reinforces these perceptions, glamourising fraudulent lifestyles and subtly framing them as ingenious forms of resistance against a corrupt elite (Chiluwa & Ifukor, 2015).

This dual perception of condemnation, on the one hand, and glorification, on the other, suggests that beyond law enforcement, there are deep-seated socio-economic and cultural factors sustaining the prevalence of internet fraud. Understanding public perception, therefore, is not merely an academic exercise but a strategic necessity for developing more effective, targeted, and culturally sensitive anti-cybercrime interventions (Adejumo & Okeowo, 2021). Thus, the problem this paper addresses has to do with the disjunction between policy efforts and public sentiment: why, despite years of aggressive anti-cybercrime strategies between 2000 and 2025, does internet fraud continue to thrive, and why does it continue to find pockets of social legitimacy among Nigerian residents?

Research Objectives

The primary objectives of this study are to:

i. Investigate the prevailing public perception of internet fraud among Nigerian residents;

ii. Identify and analyse socio-economic, cultural, and psychological factors that influence these perceptions;

iii. Examine the role of unemployment, economic hardship, and systemic corruption in shaping attitudes towards cybercrime;

iv. Explore the impact of cultural and media representations on the normalisation or glorification of internet fraud;

v. Segment public opinion based on demographic factors to understand variances across different groups; and

vi. Propose effective policy recommendations, educational strategies, and community engagement frameworks to combat the normalisation of internet fraud in Nigerian society.

Significance of the Study

This study holds critical importance for both academic inquiry and public policy development:

i. **Academic Contribution:** It expands the scholarly understanding of cybercrime sociology in Nigeria, moving beyond legalistic perspectives to examine the nuanced socio-cultural dynamics that sustain internet fraud. The study also contributes to the growing field of cyber-psychology, providing empirical data on how public attitudes towards internet crime evolve in response to economic and media influences.

ii. **Policy Implications:** Findings from this research can inform the design of targeted anti-cybercrime interventions. By understanding the socio-cultural drivers behind tolerance for internet fraud, policymakers, law enforcement agencies, and non-governmental organisations can craft more culturally resonant educational campaigns and rehabilitation programmes.

iii. **Youth Engagement:** Given that young Nigerians are disproportionately represented among both perpetrators and rationalisers of internet fraud, this study provides insight necessary for developing youth-centred initiatives that promote ethical digital citizenship, entrepreneurship, and employment opportunities as alternatives to cybercrime.

iv. **International Relations:** Addressing public perceptions and reducing societal tolerance for cybercrime is crucial for improving Nigeria's global image, fostering better international cooperation on cybercrime enforcement, and enhancing foreign investment confidence.

v. **Community Empowerment:** The study highlights the role of grassroots community engagement, religious organisations, educational institutions, and media literacy programmes in reshaping narratives around wealth acquisition, integrity, and technological entrepreneurship.

Ultimately, by identifying the roots of public perceptions and proposing actionable solutions, this research aims to contribute to the long-term reduction of internet fraud and the strengthening of Nigeria's socio-economic and moral fabric.

Literature Review

Definition and Scope of Internet Fraud

Internet fraud refers to any criminal deception carried out through digital communication platforms such as email, social media, websites, and online marketplaces designed to unlawfully obtain money, property, or sensitive information. It encompasses a wide range of illicit activities, including phishing scams, business email compromise, identity theft, romance fraud, and cryptocurrency scams (Ulo, 2025). The scope of internet fraud has expanded in tandem with the digitalisation of commerce and communication, making it a complex, borderless crime that challenges traditional legal and regulatory frameworks. In the Nigerian context, internet fraud is colloquially referred to as Yahoo Yahoo, and perpetrators are often called Yahoo Boys, a term that reflects the normalisation of such activities within some societal circles (Richards & Eboibi, 2021; Ulo, 2025).

Evolution of Fraud Tactics from 419 scams to Modern Cybercrime

The roots of internet fraud in Nigeria can be traced to the infamous 419 scams, named after Section 419 of the Nigerian Criminal Code, which deals with advance-fee fraud (LawExplores, 2015). These early scams involved convincing victims to part with money in anticipation of receiving larger sums that never materialised. Letters and faxes were the primary media used in the 1980s and 1990s. With the advent of the internet, these fraudulent schemes rapidly evolved into email scams, allowing perpetrators to reach a global audience cheaply and anonymously (Chiluwa, 2009; LawExplores, 2015).

The 2000s witnessed a diversification of tactics, including fake business proposals, bogus lottery winnings, and counterfeit online job offers. By the 2010s, Nigerian cybercriminals had become adept at sophisticated phishing campaigns, romance scams on dating websites, and business email compromise (BEC) targeting multinational corporations (OCONUS Investigations, 2025). Today, the use of deepfake technology, social engineering, cryptocurrency platforms, and dark web operations has further complicated the landscape of internet fraud (Onukwue, 2025).

Comparing Global Cybercrime and Nigeria's Unique Characteristics of Cybercrime Patterns

While internet fraud is a global phenomenon, certain features distinguish Nigerian cybercrime. First, it is often rooted in a combination of economic desperation and cultural glorification of wealth acquisition by any means necessary (Onadeko & Afolayan, 2021). Nigerian internet fraud frequently carries an element of storytelling with elaborate narratives designed to exploit emotional vulnerabilities such as greed, sympathy, or romantic affection (Ogunjobi, 2020).

Moreover, Nigerian cybercriminals have demonstrated exceptional organisational adaptability, often operating in decentralised networks that mimic legitimate business structures, complete with training hubs (popularly called Yahoo Academies) and specialisation in different fraud techniques (Oseghale, 2022). In contrast, cybercriminal operations in other parts of the world tend to be more tightly centralised or state-sponsored. Additionally, the visible opulence of successful fraudsters, exhibiting wealth and affluence on social media, feeds a cycle of aspirational criminality among youths (Interpol, 2024).

Globally, internet fraud is heavily prosecuted and stigmatised. In Nigeria, however, there is a complex moral landscape where some sectors of society justify cybercrime as a response to systemic inequality and limited legitimate opportunities. This duality significantly affects public perception, enforcement efficacy, and societal responses to cybercrime (Richards & Eboibi, 2021).

Distinct Categories of Internet Fraud

i. **Phishing:** Fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in electronic communications. Nigerian phishing attacks often mimic banks, government agencies, and international organisations (Oyelakin, 2014).

ii. **Business Email Compromise (BEC):** A sophisticated scam targeting companies and government agencies by compromising legitimate business email accounts to conduct unauthorised transfers of funds. Nigerian syndicates have been involved in numerous global BEC attacks, costing billions annually (Palo Alto Networks Unit/ 42, 2020).

iii. **Romance Scams:** Perpetrators create fake profiles on dating platforms to build emotional relationships with victims, eventually manipulating them into sending money under false pretences. Nigerian scammers are particularly notorious for executing emotionally elaborate schemes (Oseghale, 2022).

iv. **Cryptocurrency Fraud:** With the rise of Bitcoin and other digital currencies, fraudsters now exploit cryptocurrency's anonymity to perpetrate Ponzi schemes, fake investment opportunities, and online wallet thefts. Nigerian scammers increasingly use crypto to launder proceeds from cybercrime (Elina & Song, 2023).

v. **Identity Theft:** Stealing personal information to commit fraud or other crimes, often used to access bank accounts, apply for loans, or engage in phishing schemes. In Nigeria, identity theft is sometimes linked to SIM swap fraud and illegal SIM registration syndicates (Dawodu, 2025; NCC, 2024).

Theoretical Framework on Internet Fraud and Public Perception

Understanding public attitudes towards internet fraud in Nigeria requires an engagement with several criminological and sociological theories. These theoretical frameworks provide a lens through which the motivations for cybercrime, the rationalisation of perpetrators, and societal responses can be critically examined.

i. **Rational Choice Theory** posits that individuals commit crimes after weighing the potential benefits against the risks of being apprehended and punished. In the Nigerian context, where unemployment is widespread and legal economic opportunities are limited, internet fraud often presents itself as a rational alternative for personal advancement. Fraudsters, particularly young people, make calculated decisions based on perceived low risks of arrest and the promise of high financial returns (Ojolo, 2020). Rational choice models help explain why some Nigerians might not only engage in cybercrime but may also perceive it as a smart move rather than an inherently immoral act (Fraud Theories and White Collar Crimes, 2019).

ii. **Cultural Criminology** focuses on how cultural dynamics such as symbolism, media narratives, and emotional experiences tend to shape and even glamourise criminal behaviour. In the Nigerian setting, music, film, and social media often romanticise Yahoo Boys as clever, daring, and rebellious figures. These portrayals contribute to a complex cultural environment where cyber-criminality is sometimes seen as subversive heroism rather than mere illegality. Cultural criminology thus provides critical insights into why public condemnation of internet fraud often coexists with subtle admiration or envy (Lazarus, 2018).

iii. **Techniques of Neutralisation:** Gresham Sykes and David Matza's concept of Techniques of Neutralisation suggests that criminals use justifications to neutralise feelings of guilt or shame associated with their actions. Common rationalisations among Nigerian internet fraudsters include denying injury (they are rich foreigners, they can afford it), appealing to higher loyalties (I must help my struggling family), or condemning condemners (the government is corrupt, so why shouldn't I hustle?) (Lomatey & Offei, 2023). Understanding these neutralisation techniques is vital to grasping how perpetrators internally reconcile their actions and how broader society might empathise with or excuse their behaviour (Aborisade et al., 2022).

Socio-Economic Drivers of Internet Fraud in Nigeria

The prevalence of internet fraud in Nigeria cannot be understood outside the broader socio-economic realities confronting the country. Multiple interlocking factors, ranging from poverty to systemic corruption, often contribute to the high incidence and often conflicted public perception of cybercrime.

i. **High Youth Unemployment and Under-Employment**
Nigeria has one of the world's youngest populations, with more than 60% under 25. However, youth unemployment rates have hovered dangerously high, often exceeding 40%, according to the National Bureau of Statistics (NBS, 2023). Many graduates are unable to find meaningful employment that matches their skills or educational attainment. The resulting economic frustration has created fertile ground for illicit alternatives such as internet fraud, which appears to offer a quick escape from poverty and social marginalisation.

ii. **Widespread Poverty and Economic Inequality**
Despite being Africa's largest economy, Nigeria is home to an alarming level of poverty. The World Bank (2024) estimates that over 70 million Nigerians live below the national poverty line (World Bank cited in Reddit discussions; NBS, 2021). Economic disparities between the elite and the masses have widened, creating visible and often demoralising contrasts. In such a context, internet fraud is sometimes rationalised as a means of redistributive justice of taking from wealthy, often foreign, victims to survive in a system perceived as inherently unjust (Wariboko & Nwanyanwu, 2024).

iii. **Weak Educational Systems**
The quality of education in Nigeria remains poor, characterised by underfunded institutions, outdated curricula, and frequent industrial actions by academic unions. Many Nigerian youths graduate without practical skills or critical thinking abilities that are essential for employment in a competitive global market. Meanwhile, self-taught digital literacy and hacking skills offer alternative, albeit illicit, pathways to financial empowerment (Odinka, Okpa, Ushie, Ekpeyong and Echel, 2023).

iv. **Cultural Pressures and Materialism**
Contemporary Nigerian culture places a premium on visible displays of wealth as a measure of success. Lavish lifestyles are glorified in music videos, Nollywood films, and social media platforms. Young people, faced with few legitimate means to achieve such lifestyles, may be pressured to engage in internet fraud as a shortcut to societal respect and admiration. This societal valourisation of wealth, regardless of its source, blurs ethical lines and fosters a tacit acceptance of cybercrime (Wariboko & Nwanyanwu, 2024).

v. **Systemic Corruption and Poor Governance**
Nigeria has consistently ranked low on Transparency International's Corruption Perception Index. When citizens witness rampant corruption among political and business elites without serious consequences, moral authority is weakened. Young people often argue, If the leaders steal billions without punishment, why can't I steal thousands online? Systemic corruption thus indirectly legitimises individual acts of fraud (NBS 2024).

vi. **Accessibility of Digital Technology**
Mobile phone penetration and internet access have grown exponentially across Nigeria. According to the Nigerian Communications Commission (NCC, 2024), internet users in Nigeria number over 154 million. This connectivity, while bringing numerous economic and educational benefits, has also exposed millions to the global online economy, both its opportunities and vulnerabilities. Smartphones, free Wi-Fi, and social media platforms have made it

relatively easy for individuals to learn fraud techniques and to execute scams without significant upfront costs (Wikipedia, 2025).

vii. **Weak Law Enforcement and Judicial Systems**
Although Nigeria has cybercrime legislation, including the Cybercrimes Act of 2015, enforcement remains inconsistent and often inefficient. Police units like the Economic and Financial Crimes Commission (EFCC) have made numerous arrests, but corruption, case backlogs, and inadequate prosecution resources mean that conviction rates are low. Many offenders either go free or negotiate settlements, reinforcing public cynicism about the seriousness of government efforts to tackle cybercrime (*The Nation*, 2020).

Cultural Factors Shaping Perceptions and Awareness of Internet Fraud

Cultural narratives and social value systems play an essential role in framing public perceptions of internet fraud in Nigeria. The normalisation and, at times, glorification of cybercrime is deeply embedded within complex cultural dynamics that influence how individuals and communities view online fraudsters.

i. **Celebration of Wealth Regardless of Source**
In many Nigerian societies, material wealth is often equated with personal success, respect, and power. Cultural aphorisms like 'money stops nonsense' and 'the end justifies the means' vividly capture this ethos. As long as an individual can display signs of affluence such as luxury cars, designer clothing, and lavish parties, questions concerning the source of their wealth are often overlooked or ignored. Consequently, some communities, particularly among the youth, tend to admire successful internet fraudsters rather than condemn them (Ndubueze, 2013).

ii. **'Yahoo Boys' as Folk Heroes**
The phenomenon of 'Yahoo Boys' (a popular term for internet fraudsters) has created a unique cultural category in Nigeria. In many urban centres, Yahoo Boys are seen not merely as criminals but as symbols of ingenuity, resilience, and rebellion against systemic oppression. Nigerian pop culture, especially in music genres like

Afrobeats and hip-hop, often celebrates the Yahoo lifestyle. Artists sometimes reference or visually depict 'hustling' through scams as a way of surviving an unjust system. This media glorification helps to normalise fraud as an acceptable, even admirable, survival strategy (Guardian Life, 2019).

iii. **Impact of Traditional Beliefs and Ritual Practices**
In some parts of Nigeria, traditional belief systems contribute to the perception and practice of internet fraud. Notably, 'Yahoo Plus' refers to the fusion of internet fraud with ritualistic practices purportedly aimed at ensuring scam success. Belief in supernatural intervention in economic activities reflects how deeply traditional worldviews remain influential even in modern cybercriminal activity. Some communities, while critical of the ritualistic elements, paradoxically admire the perceived boldness and 'spiritual prowess' of such individuals (ENACT Africa, 2024).

iv. **Historical Narratives of Resistance to Exploitation**
Historical experiences of exploitation, such as colonialism and ongoing global economic inequalities, shape how some Nigerians view internet fraud against foreigners. A segment of public opinion rationalises cyber scams as a form of revenge or rebalancing against Western nations seen as having historically looted African resources. This narrative frames internet fraud not as pure criminality but as a continuation of a struggle against exploitation, providing ideological justification for otherwise illegal activities (Ndubueze, 2013).

v. **Religion and Moral Ambiguity**
Religion plays a central role in Nigerian life, yet there is a striking moral ambiguity concerning internet fraud. While Christian and Islamic teachings clearly condemn dishonesty and theft, religious institutions often turn a blind eye when wealthy congregants whose sources of wealth are questionable make significant donations. Prosperity preaching, common in Pentecostal Christianity, sometimes inadvertently fuels this contradiction by emphasising wealth acquisition as a sign of divine favour, irrespective of how it is achieved (Tade, 2013).

vi. **Communal Loyalty Over Legal Norms**
In Nigeria's communitarian societies, loyalty to family and local networks often supersedes adherence to formal legal structures. Internet fraudsters who "take care" of their families and contribute financially to their communities are often shielded from public criticism. Their contributions to communal well-being mitigate moral outrage, reinforcing a localised moral economy where social contributions are prioritised over legality (Ndubueze, 2013).

Impact of Media Representation on Public Perception of Internet Fraud

The media, both traditional and digital, plays a central role in shaping how the Nigerian public perceives internet fraud. Media representations not only inform but also influence societal attitudes, sometimes reinforcing stereotypes or glamourising cyber-criminality.

i. **Sensationalism and the "Yahoo Boy" Archetype**
Nigerian mainstream media often sensationalises cases of internet fraud, portraying Yahoo Boys with exaggerated flair. Headlines about extravagant lifestyles, massive cash seizures, and luxury assets reinforce a public image of cybercriminals as daring and larger-than-life figures. Rather than focusing solely on the criminality and societal harm caused by their actions, these reports often highlight the ostentation and drama surrounding their arrests, inadvertently making them folk heroes to impressionable youth (Adejoh, Alabi, Adisa and Emezie, 2019).

ii. **Social Media as a Double-Edged Sword**
Platforms like Instagram, TikTok, and Twitter have amplified the public's exposure to both real and perceived internet fraudsters. Some self-proclaimed "Yahoo influencers" openly flaunt their wealth online, while others **glamourise** luxury lifestyles without disclosing the dubious sources of their income. In many cases, social media provides a stage where fraudsters are admired for their 'hustle' and ability to 'make it' against systemic odds. Simultaneously, social media users also drive public shaming,

particularly when fraudsters are arrested and paraded by law enforcement, creating a space for conflicting narratives (Fuoye, 2024).

iii. **Music and Film Glorification**

Nigerian music, particularly Afrobeats, hip-hop, and street pop (e.g., 'Zanku' or 'Afro-street' genres), often **glamourises** fraudulent lifestyles. Lyrics sometimes celebrate 'hustling' and 'fast money,' creating an artistic environment where internet fraud is indirectly validated. Nollywood, Nigeria's thriving film industry, also contributes to this narrative through films that depict Yahoo Boys as smart, courageous individuals who outwit an unfair system. In doing so, these cultural products blur moral boundaries and contribute to the normalisation of cybercrime. Examples include the popular Nollywood film 'Yahoo+' (2022), which, although intended as a cautionary tale, inadvertently romanticised aspects of cybercrime by showcasing the luxurious lifestyles initially enjoyed by its protagonists before their downfall (Orji, 2023).

iv. **Framing by Law Enforcement and Government Communications**

Agencies like the Economic and Financial Crimes Commission (EFCC) frequently publicise arrests of suspected internet fraudsters, often posting photos of young, well-dressed men alongside confiscated luxury goods. While intended to deter, these images can paradoxically reinforce the perception that internet fraud, despite its risks, can lead to immense (if temporary) rewards. Furthermore, the sporadic nature of prosecutions and the visible cases where perpetrators evade punishment feed a perception that cybercrime, although officially condemned, is unofficially tolerated if one is successful enough (Ojolo, 2020).

v. **Foreign Media and Global Stereotyping**

International media coverage often portrays Nigeria as a hub for internet scams, contributing to a global stereotype of Nigerians as inherently deceitful. This external labelling has a feedback effect: some Nigerian youth internalise these stereotypes and view internet fraud as a form of reclaiming agency in a world that already assumes their criminality. Instead of rejecting the label, they inhabit it defiantly, further complicating domestic efforts to reshape public perception (Lazarus, Button & Adogame, 2022).

Empirical Review on Public Perception of Internet Fraud

Numerous academic and policy-oriented studies have explored how the Nigerian public perceives internet fraud, offering insights into the socio-economic, cultural, and psychological drivers behind these attitudes. Understanding the current research landscape helps position this study within broader academic discussions.

i. **Public Attitudes: Criminality versus Survival:** Ayodele, Oyedeji, and Badmos (2022) have highlighted a dual perception among Nigerians: while many view internet fraud as morally wrong and criminal, a significant segment, particularly among the youths, rationalises it as a survival tactic in the face of systemic poverty and unemployment. Similarly, in the urban slums of Lagos, internet fraud is often seen not just as criminality but as a creative, albeit illegal, solution to socio-economic marginalisation (Onyeachu, Okoro, & Ugwuoke, 2025).

ii. **Socio-Economic Influence:** A **study** by Odinka et al. (2023) revealed that economic disenfranchisement and social exclusion are major predictors of positive attitudes towards cybercrime. Individuals from lower socio-economic backgrounds are more likely to justify or excuse internet fraud, seeing it as an alternative means of upward mobility. Molokwu (2022) further noted that many online scammers narrate their own actions as necessary responses to Nigeria's failing institutions.

iii. **The Youth and Digital Subcultures:** Young Nigerians are increasingly part of digital subcultures that valourise "hustling", an ethic of doing whatever it takes to succeed financially. Within these subcultures, the stigma around cybercrime is considerably lower, especially when compared to older generations. Their study suggests that peer validation within online communities often outweighs societal condemnation (Odinka et al., 2023).

iv. **Cultural Endorsement and Media Influence:** Ebebe, Eyang and Oboh (2023) posit that cultural admiration for wealth acquisition, regardless of its source, remains a potent factor in shaping public perception. They found that the media, especially music and film, often reinforce narratives that subtly endorse cybercrime by glamourising illicit wealth.

v. **Regional and Demographic Variations:** Recent studies, such as Lazarus and Button (2022), indicate that perceptions vary significantly across Nigeria's regions. In the southern and southwestern parts, where internet fraud is more prevalent, residents are more likely to view it through a pragmatic lens ("as long as one helps their family and community"). In contrast, in northern regions, strong religious and communal norms often lead to more categorical rejection of cybercrime activities. Demographic variables like age, education level, and employment status also play critical roles. Younger, unemployed, and less formally educated individuals tend to rationalise internet fraud more than the older, employed, or highly educated Nigerians (Alabi et al., 2023).

vi. **Moral Disengagement and Rationalisation:** Building on Bandura's theory of moral disengagement, Obaweiki, Njoroge and Kanga (2021) explored how many Nigerians employ psychological mechanisms such as blaming the victim (especially foreign scam victims) or diffusing responsibility to rationalise cybercriminal behaviour. Their findings suggest that combating internet fraud requires more than legal deterrence; it demands a cultural and psychological shift.

Methodology

This study adopts a mixed-methods research design to comprehensively explore public perceptions of internet fraud among Nigerian residents. The combination of both quantitative and qualitative methods allows for a more nuanced understanding of societal attitudes, enabling the triangulation of findings to enhance validity and depth.

Research Design

i. Quantitative Approach: A structured survey was conducted to collect standardised data on respondents' perceptions, experiences, and socio-economic profiles.

ii. Qualitative Approach: Semi-structured interviews and focus group discussions (FGDs) were employed to gain deeper insights into the cultural, emotional, and moral nuances behind public attitudes.

Study Population and Sampling

The study targeted Nigerian residents, aged 18 and above, across urban, semi-urban, and rural areas to ensure diversity in socio-economic backgrounds and cultural orientations.

i. Sampling Method:

a) Quantitative: A multistage stratified random sampling method was used. Nigeria was divided into six geopolitical zones, from which two states per zone were randomly selected. Within each state, three Local Government Areas (LGAs) were chosen randomly, and respondents were selected systematically within communities.

b) Qualitative: Purposive sampling was used to select key informants (e.g., law enforcement agents, cybercrime victims, community leaders) and organise FGDs with youths, students, and professionals.

ii. Sample Size:

a) Quantitative Survey: 120 respondents across 12 states.

b) Qualitative Interviews and FGDs: 30 in-depth interviews and 6 focus group sessions (8–10 participants each).

Data Collection Instruments

i. Survey Questionnaire: A structured questionnaire with closed and open-ended questions was developed. It included sections on:

i. Demographic information

ii. Awareness of internet fraud types

iii. Personal attitudes towards internet fraud

iv. Perceived socio-economic drivers
v. Cultural influences on perception
vi. Media exposure related to cybercrime
ii. Interview and FGD Guides:
i. Open-ended questions explored:
ii. Moral reasoning about internet fraud
iii. Community reactions to known fraudsters
iv. Media influence on personal attitudes
v. Perceptions of government and law enforcement responses

Data Collection Procedures

i. Field researchers were trained on ethical considerations and proper administration of the tools.
ii. Surveys were administered face-to-face to minimise literacy barriers.
iii. Interviews and FGDs were conducted in English, Pidgin English, or local languages, depending on the participants' preferences. Sessions were audio-recorded with participants' consent and later transcribed.

Data Analysis

i. Quantitative Data:
   a) Analysed using Statistical Package for the Social Sciences (SPSS) version 26.
   b) Descriptive statistics (frequencies, means, standard deviations) and inferential statistics (chi-square tests, regression analysis) were employed to examine relationships between variables.
ii. Qualitative Data:
   a) Thematic analysis was conducted following Braun and Clarke's six-step framework.
   b) Transcripts were coded inductively, and major themes were identified based on patterns and recurring narratives.

Ethical Considerations

i. Ethical clearance was obtained from a recognised Institutional Review Board (IRB).

ii. Informed consent was secured from all participants.
iii. Anonymity and confidentiality were strictly maintained.
iv. Participants were informed of their right to withdraw at any stage without any consequence.

Limitations of Methodology

i. Self-reported data may be affected by social desirability bias, especially given the criminal nature of the topic.
ii. Geographical constraints and security concerns limited access to some rural areas.
iii. Language translations might have introduced slight nuances in interpretation during qualitative data collection.

Data Presentation and Analysis

This section presents the findings from the survey, interviews, and focus group discussions, organised around the study's key research questions and objectives. Quantitative results are shown first, followed by qualitative insights to provide depth and context.

Demographic Profile of Respondents

Out of the 140 surveys distributed, 132 valid responses were collected (response rate: 94.3%). The demographic breakdown is as follows:

i. **Gender:**
   a) Male: 53%
   b) Female: 47%
ii. **Age Range:**
   a) 18–24 years: 34%
   b) 25–34 years: 41%
   c) 35–44 years: 17%
   d) 45+ years: 8%
iii. **Educational Attainment:**
   a) No formal education: 4%
   b) Secondary education: 36%
   c) Tertiary education: 60%

iv. **Employment Status:**
   a) Employed: 49%
   b) Unemployed: 34%
   c) Students: 17%

Awareness and Knowledge of Internet Fraud

i. **General Awareness:**
   a) 92% of respondents reported familiarity with the term internet fraud.

ii. **Knowledge of Fraud Types:**
   a) Phishing: 84%
   b) Business Email Compromise (BEC): 56%
   c) Romance Scams: 68%
   d) Cryptocurrency Fraud: 47%
   e) Identity Theft: 72%

Note: Many respondents associated Yahoo Yahoo with a broad range of fraudulent online activities.

Perceptions Towards Internet Fraud

i. **Moral Judgement:**
   a) 62% view internet fraud as completely wrong and criminal.
   b) 21% consider it wrong but understandable due to economic hardship.
   c) 12% perceive it as a necessary survival strategy.
   d) 5% express indifference or rationalise it as *smartness*.

ii. **By Age:**
   a) Younger respondents (18–34 years) were significantly more likely ($p < 0.05$) to rationalise or justify internet fraud compared to older age groups.

Socio-Economic Drivers

i. 79% of respondents agreed that unemployment and poverty are major contributors to the rise of internet fraud.

ii. 58% mentioned peer pressure and societal expectations as strong motivators.

iii. Focus groups emphasised frustration with systemic corruption: "If the leaders are looting public funds, why blame the youth for finding their own way?"

Cultural and Media Influences

i. 65% acknowledged that media (particularly music videos and movies) glamourise fraudulent wealth.
ii. Songs glorifying fast money were cited as reinforcing positive images of Yahoo Boys.
iii. Interviewees stressed that societal admiration for sudden wealth diminishes the stigma around cybercrime.

Regional Differences

i. Southern states (e.g., Lagos, Edo) recorded higher rates of justifying or excusing internet fraud compared to Northern states (e.g., Kano, Sokoto).
ii. Cultural and religious influences were more significant in the North, where internet fraud was often condemned more sharply.

Qualitative Insights

i. From Interviews:

a) A police cybercrime unit officer noted: "The biggest challenge is public sympathy for these criminals. Sometimes, communities hide them from us."
b) A university student argued: "In Nigeria, survival is a hustle. If the system fails you, you create your own opportunities to even up online."

ii. From FGDs:

a) Participants described internet fraudsters as tech-savvy, street-smart individuals rather than dangerous criminals.
b) Some participants narrated how fraudulent income was used to support families, fund businesses, and sponsor education.

Statistical Analysis

i. **Regression Analysis:**

a) A positive correlation ($r = 0.63$, $p < 0.01$) was found between unemployment rates and tolerant attitudes towards internet fraud.

b) Media consumption patterns (hours of exposure to fast money content) also positively predicted favourable attitudes towards cybercrime.

ii. **Chi-Square Tests:**

a) Significant associations were observed between educational level and perception ($x^2 = 18.6, p = 0.002$).

b) Employment status was significantly related to moral judgement on internet fraud ($x^2 = 23.4, p < 0.001$).

Discussion of Findings

This study investigated how internet fraud is perceived by residents in Nigeria, providing significant insights into how these perceptions are shaped by a complex interplay of socio-economic realities, cultural narratives, and media portrayals. The findings reveal not only widespread awareness of internet fraud (commonly referred to as Yahoo Yahoo), but also a range of public perceptions that are far from uniform, ranging from moral condemnation to subtle rationalisation and even glorification in some quarters.

The findings strongly support the Rational Choice Theory, which posits that individuals weigh costs and benefits before engaging in criminal acts. Respondents frequently linked internet fraud to high levels of youth unemployment, economic hardship, and systemic poverty. Many perceived that those who engage in cyber fraud are making a calculated decision in response to limited legitimate opportunities. For a significant segment of the population, particularly among the youths, fraud is seen as a rational (albeit illegal) means of economic survival in a context where state structures have failed to provide employment or economic justice.

This utilitarian justification was often accompanied by statements such as, “They have no other means,” or “At least they are not killing anyone.” These rationalisations reflect a moral cost-benefit analysis consistent with the Rational Choice framework and reveal how structural economic failures influence tolerance or ambivalence towards internet fraud.

The role of culture, particularly youth subculture and media, was another significant influence on perception. Cultural Criminology, which explores the emotional, symbolic, and stylistic dimensions of crime, helps explain how internet fraud is not only tolerated in some social groups but also **glamourised**.

The study found that symbols of wealth, such as luxury cars, lavish parties, and expensive clothes, often associated with internet fraudsters, are celebrated in popular music, Nollywood films, and social media. Many respondents acknowledged that the cultural environment, especially among urban youths, portrays Yahoo Boys as smart, daring, and successful, thereby blurring the moral lines between legitimate and illegitimate success.

In some communities, individuals involved in fraud are accorded respect and social prestige, reinforcing the perception that success, regardless of its source, is the primary societal goal. This narrative reflects how cultural framing can normalise deviant behaviour, particularly when the rule of law is weak or inconsistently enforced.

The study also revealed widespread use of Techniques of Neutralisation, as theorised by Sykes and Matza, to justify or minimise the perceived wrongfulness of internet fraud. These techniques include:

i. Denial of injury: Many respondents rationalised that victims (usually foreigners) are wealthy and therefore not significantly harmed.
ii. Denial of victimhood: The belief that internet fraud victims are complicit in their own victimisation (e.g., through greed) was also common.
iii. Condemnation of the condemners: Some participants argued that politicians and elites are more corrupt, thereby disqualifying them from criticising cybercrime.
iv. Appeal to higher loyalties: Fraud was sometimes justified on the grounds of supporting one’s family or community.

These justifications contribute to a form of moral disengagement that undermines the social condemnation of fraud. The prevalence of these narratives points to a shifting moral compass among segments of the population, especially in areas where poverty and institutional decay are deeply felt.

Overall, the findings highlight a deeply nuanced perception of internet fraud in Nigeria. While many respondents still morally reject fraud, socio-economic pressures, cultural representations, and rational justifications have diluted the moral clarity surrounding the act. The application of Rational Choice Theory, Cultural Criminology, and Techniques of Neutralisation Theory provides a comprehensive lens through which to understand the cognitive, emotional, and cultural processes that shape these perceptions. Addressing internet fraud, therefore, requires not only law enforcement but also socio-economic reforms, cultural reorientation, and the re-establishment of moral and institutional credibility.

Conclusion

This study set out to explore the public perception of internet fraud among residents in Nigeria, investigating the socio-economic, cultural, and media-driven factors influencing these views. The findings reveal a complex moral landscape where internet fraud is simultaneously condemned, rationalised, and, in some cases, celebrated. Economic hardship, high unemployment rates, widespread corruption, cultural narratives of success, and the glamourisation of wealth through media all contribute to shaping public attitudes.

While a majority of Nigerians view internet fraud as criminal and morally wrong, a considerable minority justify or excuse it as a coping mechanism against systemic failures. Younger Nigerians, who face heightened economic pressures and limited job opportunities, show higher levels of tolerance towards cybercrime. Regional, cultural, and religious factors further differentiate perceptions across the country.

These insights emphasise that tackling internet fraud in Nigeria requires a multi-dimensional strategy, addressing not just the legal aspects but also the underlying economic, cultural, and informational dynamics that sustain permissive attitudes towards cybercrime.

Recommendations

Curbing cybercrime in Nigeria demands a holistic approach that goes beyond punishment. Solutions must strengthen youth capacity through digital skills, update legal frameworks, reorient societal values, regulate harmful media narratives, and empower communities as frontline actors in prevention. At the same time, rehabilitation and stronger international cooperation are essential to address a crime that cuts across borders. The recommendations below outline practical steps towards a safer digital future.

i. **Enhance Youth Employment and Digital Literacy:**
The government should invest in sustainable employment opportunities, vocational training, digital skills development, and startup support for youths. Integrating digital literacy and internet ethics into school curricula will equip young Nigerians with the tools to thrive in the digital economy while discouraging involvement in cybercrime.

ii. **Reform Legal Frameworks and Strengthen Law Enforcement:**
Cybercrime laws should be updated to address emerging threats such as cryptocurrency scams and digital identity theft. Swift and transparent judicial processes, along with well-equipped cybercrime units and community policing strategies, will enhance detection, prosecution, and deterrence.

iii. **Promote Cultural Reorientation and Ethical Values**:
A national campaign is needed to change societal attitudes towards wealth acquisition and success. This requires mobilising cultural icons such as musicians, actors, religious and traditional leaders to promote integrity, hard work, and legitimate success stories over the glamourisation of "fast money."

iv. **Regulate Media and Encourage Positive Content:**
Agencies such as the National Broadcasting Commission (NBC) should promote content that values education, innovation, and ethical success while discouraging media that glorifies fraud or criminal lifestyles. Media literacy programmes should accompany this regulation to educate the public on harmful narratives.

v. **Implement Community-Based Cybercrime Watch Programmes:**
Strengthening community policing to include cybercrime reporting and early detection mechanisms can break local support networks for fraud. Community empowerment and trust-building efforts should be central to these strategies.

vi. **Support Rehabilitation and International Cooperation:** Beyond punitive actions, there should be structured rehabilitation and reintegration programmes for repentant fraudsters. Additionally, Nigeria must intensify collaboration with international law enforcement and cybersecurity bodies to trace, investigate, and prosecute cross-border cybercriminals effectively.

References

Aborisade, R. A., Akoji, O., & Okuneye, B. A. (2022). *Internet scamming and the techniques of neutralization: Parents' excuses and justifications for children's involvement in online dating fraud in Nigeria*. International Annals of Criminology, 60(2), 161–177. Cambridge University Press. https://doi.org/10.1017/cri.2022.13

Adejoh, S. O., Alabi, T. A., Adisa, W. B., & Emezie, N. M. (2019). "Yahoo Boys" phenomenon in Lagos Metropolis: A qualitative investigation. *International Journal of Cyber Criminology, 13*(1), 1–20. https://doi.org/10.5281/zenodo.3366298

Alabi, A., Hamza, B., & Oladimeji, B. (2023). *Cybercrime in Nigeria: Social influence affecting the prevention and control*. Lafia Journal of Economics and Management Sciences, 8(1), 1–15. Federal University of Lafia, Nigeria. ISSN: 2550-732X.

Ayodele, A. A., Oyedeji, J. K., & Badmos, H. O. (2022). Social construction of internet fraud as innovation among youths in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*(1), 23–42. https://doi.org/10.52306/BUVC2778

Brooks, K. J. (2022, November 7). Nigerian Instagrammer sentenced to 11 years for money laundering. *CBS News*. https://www.cbsnews.com/news/ramon-abbas-bec-scams-sentenced-nigerian-instagram-influencer-hushpuppi/

Dawodu, O. (2025). Digital identity theft and SIM swap scams: A growing threat in Nigeria. *BusinessDay*. https://businessday.ng/life/article/why-sim-swap-scams-are-nigerias-silent-cyber-war/

Ebebe, E. A., Eyang, A., & Oboh, T. (2023). A critical discourse analysis of selected songs of Nigerian musicians on internet fraud. *Journal of Advance Research in Social Science & Humanities, 9*(4), 14–27.

Eboh, C. (2025, January 10). Nigeria's anti-graft agency arrests 105 for internet fraud. *Reuters*. https://www.reuters.com/world/africa/nigerias-anti-graft-agency-arrests-105-internet-fraud-2025-01-10/

Eboibi, F. E., & Ogorugba, O. M. (2023). Cybercrime regulation and Nigerian youth increasing involvement in internet fraud: Attacking the roots rather than the symptoms. *Journal of Legal, Ethical and Regulatory Issues, 26*(S2), 1–17.

Economic and Financial Crimes Commission. (2024, March 28). EFCC arrests 74 suspected internet fraudsters in Ogun [Press release]. https://www.efcc.gov.ng/efcc/news-and-information/news-release/9941-efcc-arrests-74-suspected-internet-fraudsters-in-ogun

Economic and Financial Crimes Commission. (2024, May 10). EFCC arrests 78 suspected internet fraudsters in Enugu, Imo [Press release]. https://www.efcc.gov.ng/efcc/news-and-information/news-release/10094-efcc-arrests-78-suspected-internet-fraudsters-in-enugu-imo

Elina, E., & Song, M. (2023, July). Cybercrime and cryptocurrency fraud in Nigeria [Manuscript retrieved from ResearchGate]. https://www.researchgate.net/publication/388659317_Cybercrime_and_Cryptocurrency_Fraud_in_Nigeria

ENACT Africa. (2024, August 22). Yahoo Boys scammers dabble in dark magic. https://enactafrica.org/enact-observer/yahoo-boys-scammers-dabble-in-dark-magic

Fraud theories and white collar crimes: Lessons for the Nigerian banking industry. (2019). *ResearchLeap*. https://www.google.com/search?q=https://researchleap.com/fraud-th...

Fuoye, F. U. (2024). Celebrity lifestyle posts on social media and engagement in Yahoo-yahoo activities among Nigerian youth. *Journal of Criminology and Security Studies, 3*(1).

Guardian Life. (2019, May 25). Nigerian pop music and glorification of internet fraud. *The Guardian*. https://guardian.ng/life/music/nigerian-pop-music-and-glorification-of-internet-fraud/

Infosecurity Magazine. (2021, February 18). US jails celebrated Nigerian entrepreneur for cyber fraud. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/okeke-jailed-for-cyber-fraud/

Konstruct Magazine. (2025, February 25). Rise of cybercrime schools in Nigeria: The alarming surge of internet fraud. *Konstruct Magazine*. https://konstructmagazine.com/2025/02/25/rise-of-cybercrime-schools-in-nigeria-the-alarming-surge-of-internet-fraud/

Lazarus, S. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. *Criminology, Criminal Justice, Law & Society, 19*(2), 63–80.

Lazarus, S., & Button, M. (2022). Tweets and reactions: Revealing the geographies of cybercrime perpetrators and the North–South divide. *Cyberpsychology,* *Behavior, and Social Networking, 25*(8), 504–511. https://doi.org/10.1089/cyber.2021.0332

Lazarus, S., Button, M., & Adogame, A. (2022). Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). *Heliyon, 8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142

Lomatey, I. T., & Offei, M. (2023). Service, game and livelihood: New dimensions of neutralization techniques in internet romance fraud. *International Journal of Technology and Management Research, 8*(1), 1–15.

Molokwu, A. N. (2022). Socioeconomic predictors of cybercrime among Nigerian youth in Ibadan metropolis. *Turkish International Journal of Special Education and Guidance & Counselling, 11*(1), 61–68.

Nigerian Communications Commission. (2024). *NCC demands compliance to SIM activation & replacement guidelines to curb fraud* [Press release]. https://www.ncc.gov.ng/media-centre/press-releases/news-release-ncc-demands-mnos-agents-consumers-compliance-sim

Obaweiki, F. E., Njoroge, M., & Kanga, A. (2021). The influence of socio demographic factors on moral disengagement and cybercrime among cybercrime prisoners from selected prisons in Lagos and Edo States, Nigeria. *African Journal of Clinical Psychology*, (3).

OCONUS Investigations. (2025, April 30). Nigerian cybercrime: The AI shift – evolution of deepfake and phishing 2.0. https://oconusinvestigations.com/nigerian-cybercrime/

Odinka, G. E., Okpa, J. T., Ushie, E. A., Ekpenyong, B. E., & Echu, S. N. (2023). Exploring the socio economic dynamics of youth' involvement in internet fraud in Nigeria. *Journal of Public Administration, Policy and Governance Research, 1*(3), 83–91.

Ojolo, T. L. (2020). *A criminological investigation into the lived experiences of cybercrime perpetrators in southwest Nigeria* [Doctoral dissertation, University of KwaZulu-Natal]. ResearchSpace UKZN.

Oladunjoye, O. J., & Omobowale, E. B. (2022). Popular culture and the glorification of internet fraud in Nigeria: A study of 'Yahoo Boys' and music videos. *African Studies Review, 65*(1), 130–147.

Onadeko, A., & Afolayan, O. (2021). A critical appraisal of the Cybercrimes Act, 2015 in Nigeria. International Society for Research and Capacity Learning. https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf

Onukwue, A. (2025, January 28). Surge in deepfakes heightens fraud risk for African businesses. *Semafor*. https://www.semafor.com/article/01/28/2025/surge-in-deepfakes-heightens-fraud-risk-for-african-businesses

Onyeachu, C. K., Okoro, I. C., & Ugwuoke, M. M. (2025). The impact of cyber crime and violent extremism on socio economic development in Nigeria. *Discover Global Society, 3*, Article 72. https://doi.org/10.1007/s44282-025-00195-4

Oyelakin, A. Oyewo, D. (2025, April 2). Police bust 'Yahoo school' in Lagos, rescue 12 year old trainee, others. *Punch NG*. https://punchng.com/police-bust-yahoo-school-in-lagos-rescue-12-year-old-trainee-others/

Palo Alto Networks Unit 42. (2020). *SilverTerrier – Nigerian Business Email Compromise*. https://unit42.paloaltonetworks.com

Richards, G., & Eboibi, A. (2021). Cybercrime regulation and Nigerian youth' increasing involvement in internet fraud: Attacking the roots rather than the symptoms. *ABAcademies Journal*. https://www.abacademies.org/articles/cybercrime-regulation-and-nigerian-youth-increasing-involvement-in-internet-fraud-attacking-the-roots-rather-than-the-symptoms-15641.html

SCARS Institute. (2024, September 16). A brief history of Nigeria scams & scammers. https://romancescamsnow.com/dating-scams/a-brief-history-of-nigeria-scams-scammers-2024/

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'Yahoo Plus' phenomenon. *Human Affairs, 23*(4), 689–705. https://doi.org/10.2478/s13374-013-0158-9

Tade, O., & Aliyu, L. D. (2011). Social **organisation** of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860–875.

The Nation. (2020, June 18). Unemployed Nigerian youth and internet fraud. *The Nation Newspaper*.

Ulo, E. (2025). Mediated realities and internet fraud among juveniles in Nigeria. *Journal of Social Theory and Research, 4*(2), 303–311.

U.S. Department of Justice. (2024, December 5). Extradited Nigerian national sentenced to eight years in prison for business email compromise scheme. Office of Public Affairs. https://www.justice.gov/archives/opa/pr/extradited-nigerian-national-sentenced-eight-years-prison-business-email-compromise-scheme

Wariboko, O. P. C., & Nwanyanwu, F. C. (2024). Dark side of connectivity: A socio ethical exploration of internet fraud and Nigerian youth. *Journal of Social Theory and Research*.

Wikipedia. (2025). *Internet in Nigeria*. https://en.wikipedia.org/wiki/Internet_in_Nigeria