Research Article

Causes, Consequences and Control of Online Advance Fee Fraud in Ilorin Metropolis, Nigeria

Abayomi Abdulquadir Ajibade

Thomas Adewumi University, Oko-Irese, Nigeria

Abstract

In this mixed-method study, which employed strain theory and routine activities theory (RAT) as the theoretical framework, surveys and interviews were conducted with 382 respondents and 10 participants, respectively. The research explored the causes, consequences, and solutions related to online advance fee fraud (OAFF), also known as "419 scams." The primary drivers identified by respondents were unemployment (33.8%), poverty (21.2%), and the allure of easy money, as well as low detection risks, weak regulatory oversight, peer pressure, and poor societal values. It is estimated that victims suffer substantial financial losses (64.1%), emotional trauma (46.6%), and a loss of trust (52.6%), whereas governments suffer financial losses (63.6%), tainted law enforcement (60.7%), and reputational damage (71.4%). As a result of these incidents, companies suffer financial losses (99.5%), reputational losses (74.8%), and customer trust losses (78.7%). Youth empowerment, employment opportunities, awareness raising, partnership with stakeholders, and increased EFCC monitoring were identified as key interventions by respondents. The importance of public vigilance, self-control, avoiding greed, and whistleblowing was emphasised as preventative measures. The study highlighted the evolving nature of OAFF, presently amplified by artificial intelligence and deep-fake technology, which calls for not only socio-economic remedies, but also strong technological, legal, and collective action to counter its increasing impact on individuals, governments, and businesses.

Keywords: cybercrime; EFCC; Ilorin metropolis; online advance fee fraud; yahoo-yahoo

De-centre: Journal of Interdisciplinary Studies (DJIS) 1(1) 2025
ISSN: 3105-3300

Received: 12 March 2025 | **Revised**: 7 May 2025 | **Published**: 2 September 2025

1. Introduction

Online Advance Fee Fraud (OAFF), commonly known as "419 scams" or "Nigerian Prince scams," is a prevalent form of cybercrime that has gained significant attention globally (Tade and Aliyu, 2011; Lazarus and Okolorie, 2019). Online Advance Fee Fraud is characterised by deceptive schemes in which fraudsters initiate contact with potential victims through various online channels, such as emails, social media platforms, or online classes. These fraudsters often present themselves as wealthy individuals, government officials, or representatives of reputable organisations, enticing victims with promises of financial gains, business opportunities, or charitable endeavours (Chiluwa and Ifukor, 2015; Tade and Aliyu, 2011; Lazarus and Okolorie, 2019). The core mechanism involves convincing victims to make upfront payments or disclose sensitive personal information with the false promise of receiving a greater reward in return. Online Advance Fee Fraud has far-reaching consequences that affect not only individual victims but also the broader society and economy (Lazarus and Okolorie, 2019). OAFF is a global phenomenon that transcends national borders and affects individuals from various countries.

Nigerian Advance Fee Fraud (AFF) or "419" originated from previous frauds, such as the 18th-century Spanish prisoner scam, which relies on emotional manipulation and the promise of concealed wealth (Scannell, 2014; Chiluwa and Ifukor, 2015). These trends were also observed in 19th-century frauds such as the "Letter from Jerusalem" (Lazarus and Okolorie, 2019). Nigerian OAFF scammers globalised these during the 1980s and 1990s via fake documents by mail and fax and then shifted to email during the internet era (Tade and Aliyu, 2011). AFF still takes advantage of socioeconomic weakness and borrows from traditional folklore practices to appear authentic (Chawki, 2009). Throughout the late 1990s and early 2000s, the introduction of the internet led to the development of advanced online versions of the AFF known as sophisticated online fraud. The internet introduced three crucial aspects of anonymity combined with quick functions and worldwide accessibility, which enabled criminals to commit fraud through email scams and phony websites as well as social platforms (Ulo, 2023, Danquah et al., 2022). OAFF identity, location, and behavioural anonymity. Identity anonymity is exploited by scammers with pseudo-profiles to impersonate real individuals (Ulo, 2023), whereas location anonymity through the VPN hides their origin and makes prosecution more difficult (The Police Foundation, 2023). Behavioural anonymity allows them to execute multiple scams without linking activities to actual identities (Danquah et al., 2022). These aspects, along with the immediacy of the internet and its worldwide reach, facilitate the implementation of OAFF and veil its trail (Rainie et al., 2013).

Nigeria has legislated a number of legal instruments aimed at fighting Advance Fee Fraud, namely, Section 419 of the Criminal Code, the Advance Fee Fraud and Other Related Offences Act (2006), and the Cybercrimes Act (2015). Section 419 prescribes a maximum penalty of imprisonment for 14 years but is limited by low conviction rates due to late trials and inadequate resources (Obuah, 2010; Chawki, 2009). The 2006 Act increased penalties (up to 20 years) and promoted international cooperation, particularly by empowering the Economic and Financial Crimes Commission (EFCC) to work with agencies such as the FBI and Interpol. However, the EFCC reported that out of thousands of reported AFF cases, only a few have been investigated in depth because of their low capacity (Adesina, 2020). The Cybercrimes Act of 2015 challenged cyber fraud more proactively, criminalising web-based scams and enhancing evidence collection. The EFCC secured more than 300 cybercrime and AFF-related convictions during 2019 alone, yet cross-border cyber fraud and weak digital forensic capability continue to impede enforcement (Okeshola and Adeta, 2013; Tade and Aliyu, 2011).

According to the internet Crime Complaint Center (IC3), in 2022, IC3 received 801,000 complaints, resulting in $10.3 billion in losses. Notably, phishing schemes were the most reported cybercrimes, whereas investment schemes caused the highest financial losses (IC3, 2023). This highlights the widespread nature of the problem and the financial impact it has on victims, organisations and governments. A study conducted by the Australian Competition and Consumer Commission (ACCC) revealed that OAFF scams were the most financially devastating form of scam reported in Australia, with losses exceeding AUD$86 million in 2020 (ACCC, 2020). These findings highlight the high prevalence of OAFFs even in developed countries with robust law enforcement and consumer protection systems. The Nigerian Communications Commission (NCC) reported that, in 2020 alone, there were over 11,000 reported cases of cybercrime, including OAFF, in Nigeria (NCC,2021). However, because of the scale of the problem, states such as Lagos, Oyo and Ilorin Metropolis, as prominent urban centres have experienced a surge in Online Advance Fee Fraud cases (Ojedokun and Ilori, 2021; Ajibade et al., 2024).

Understanding the specific causes, consequences, and control of OAFFs in this local context is crucial for developing effective countermeasures tailored to the region. Factors such as socioeconomic conditions, technological penetration, and cultural dynamics may influence the prevalence and manifestation of OAFFs in the Ilorin Metropolis. By examining the causes of Online Advance Fee Fraud in Ilorin Metropolis, this research can shed light on the root factors that contribute to its occurrence. This knowledge can aid policymakers, law enforcement agencies, and other relevant stakeholders in developing targeted strategies to mitigate risks and prevent the victimisation of individuals in the local community. While extensive research has been conducted on Online Advance Fee Fraud at a global level, context-driven studies that examine specific dynamics are needed. By filling this knowledge gap, this study provides insights that are relevant to the study context, allowing for a more comprehensive understanding of OAFF and its implications.

2. Conceptual clarification

Online Advance Fee Fraud (OAFF)

Online Advance Fee Fraud (OAFF) represents a digital crime where the scammers deceive victims to pay in advance by making deceptive promises about goods, services or money payouts. The scammers create fake identities of officials or businessmen so that they can befriend victims before requesting payments for processing fees or taxes and documentation. The growth of technology now features OAFF as mobile communication through electronic mail and social media platforms while expanding its scope and enhancing its hiding capabilities (Ladegaard, 2019). This Nigerian internet swindle continues to spread at a high rate throughout Nigeria because it causes major financial damage and societal consequences (Chiluwa and Ifukor, 2015).

Yahoo Yahoo (Yahoo Boys)

“Yahoo Yahoo" and "Yahoo Boys" are slang terms that denote the prevailing culture of youth-based internet-enabled fraud in Nigeria, especially with Online Advance Fee Fraud (OAFF) (Doppelmayr, 2013). "Yahoo Yahoo" is derived from the use of Yahoo! In the early 2000s, mail became the primary means through which cybercriminals interacted with prospective victims. Over the years, however, the term has come to describe a broader subculture of cybercrime, including romance scams, phishing, job and lottery scams, and especially OAFF (Tade, 2013; Ojedokun and Eraye, 2012). The perpetrators, popularly known as "Yahoo Boys," are typically unemployed or underemployed, and they use digital technologies and false identities to defraud victims both inside and outside Nigeria (Ogayi, 2025). Empirical studies indicate that the rise of Yahoo Yahoo is not just a crime trend but a response to socioeconomic disadvantage, peer pressure, parental encouragement, and the glamourisation of cybercrime in youth culture (Adejoh et al., 2019). It is legitimised in some communities as a way of becoming rich and gaining social status, and it creates a criminogenic environment where deviance becomes culturally accepted.

3. Nature and prevalence of online advance fee fraud

Online Advance Fee Fraud typically involves deceptive schemes where fraudsters initiate contact with victims through emails, social media, or other communication channels. They pretend to be wealthy individuals, government officials, or representatives of organisations, enticing victims with promises of financial gain, business opportunities, or charitable endeavours (Ojedokun and Eraye, 2023). The fraudsters exploit the victims' trust, greed, or desperation, eventually convincing them to make upfront payments or disclose sensitive personal information. Previous studies have identified common tactics used in Online Advance Fee Fraud, such as impersonation, fake lottery or inheritance claims, and bogus investment proposals (Bhutta, 2012). These scams often employ psychological manipulation, urgency, and secrecy to maintain the illusion of credibility and exploit victims' vulnerabilities (Oluwatobi et al., 2017).

OAFF has become a widespread and persistent issue in Nigeria, with significant consequences for individuals, businesses, and the country's reputation. Extensive studies have shed light on the nature, dynamics, and prevalence of OAFF in Nigeria, providing valuable insights into the scope of this fraudulent activity. Nigeria has gained a notorious reputation as a global hotspot for OAFF, accounting for a significant portion of scams reported worldwide (Ogbebor, 2023). Fraudsters operating within Nigeria employ various tactics and schemes to defraud unsuspecting victims, including impersonation, fake investment opportunities, and fraudulent inheritance claims. The prevalence of OAFF in Nigeria can be attributed to factors such as high levels of internet connectivity, economic disparities, and a lack of effective law enforcement mechanisms (Aloba et al., 2015; Akintunde et al., 2018). Within Nigeria, Kwara State has also witnessed a notable prevalence of OAFF. Kwara State is in the North Central region of the country and is home to the city of Ilorin, which serves as the capital and a major economic centre. The presence of economic activities and a relatively high level of internet penetration has made Ilorin an attractive target for fraudsters seeking to perpetrate OAFF scams. Research has documented the prevalence of OAFF in Ilorin and its impact on individuals and businesses in cities (Adegoke et al., 2018; Aloba et al., 2015). A study conducted by Aloba, Olusola, and Adagunodo (2015) specifically focused on the prevalence of online scams in Kwara State, including Ilorin. The study highlighted that Kwara State, like other regions in Nigeria, has experienced a significant increase in OAFF cases in recent years. Fraudsters in Ilorin often exploit online platforms, such as email, social media, and fraudulent websites, to engage with potential victims and deceive them into parting with their money or personal information.

The prevalence of OAFFs in Kwara State, particularly in Ilorin, can be attributed to various factors. The proliferation of internet access and the ease of creating fake online identities have enabled fraudsters to operate with relative anonymity and target individuals on a global scale. The lack of cybercrime awareness and limited enforcement capacity in Kwara State contribute to the challenges faced in combating OAFF effectively (Aloba et al., 2015; Adegoke et al., 2018). Overall, Online Advance Fee Fraud is a prevalent form of fraud with significant consequences for individuals, societies, and economies. Its nature, causes, and consequences are multidimensional and influenced by socioeconomic factors, technological advancements, and psychological manipulation. Combating Online Advance Fee Fraud requires constant public awareness, robust law enforcement efforts, and collaboration between governments, financial institutions, and international organisations.

4. Causes of online advance fee fraud (OAFF)

OAFF is driven by a complex web of interconnected causes that illuminate the motivations behind individuals engaging in fraudulent activities. Unemployment and poverty, as extensively explored in prior research, stand as pivotal drivers. Economic difficulties and aspirations for socioeconomic improvement increase susceptibility to OAFF, allured by the prospect of easy money and substantial financial gains with minimal effort (Ajiboye, 2020; Anifowose, 2016). Moreover, economic disparities amplify the appeal of OAFFs, as they widen the chasm between individuals' aspirations and the limited opportunities accessible to them. This gap motivates some to seek alternative avenues for financial gain, even if it involves fraudulent activities (Nwafor and Emeh, 2019). The rapid advancement of technology and the widespread use of the internet provide fertile ground for OAFF. Rapid technological advancements, along with global internet usage, create perfect conditions for OAFF attacks. Cybercriminals employ artificial intelligence along with deepfakes and automated bots to create authentic-seem scams that prove difficult to detect and prevent (Ladegaard, 2019; Buchanan and Imran, 2021). Recent reports suggest that deepfake and AI technologies are increasingly being used to enable OAFF in Nigeria. AI is utilized by fraudsters to automate phishing and create counterfeit identities, and deepfakes allow them to convincingly impersonate public figures, leading to successful fraud (Mondaq, 2021; Nwakanma, 2023). King and Aggarwal (2020) suggest the need for updates, as current legal frameworks fail to address these advanced methods adequately in the fight against contemporary cybercrime.

The lack of awareness and education about OAFF is another contributing factor. Limited knowledge about the nature and risks of OAFF renders individuals more vulnerable to fraudulent schemes, as those with low awareness and education levels are more likely to be targeted by fraudsters (Akintunde et al., 2018). Cultural and societal factors further complicate the landscape. Societal pressures to achieve wealth and status, coupled with the erosion of moral values and ethical standards, add to the allure of OAFFs, according to various studies (Anifowose, 2016; Nwafor and Emeh, 2019). These causes are intricately interwoven, and individuals' involvement in OAFFs often results from the convergence of multiple factors. Understanding these causes is crucial for the development of effective strategies by policymakers, law enforcement agencies, and other stakeholders to prevent OAFF and safeguard potential victims.

5. Consequences of online advance fee fraud

The consequences of OAFF reverberate through individuals, governments, and businesses, encompassing a spectrum of effects, as observed in prior research. Foremost among these consequences is the substantial financial loss suffered by victims of OAFF. Studies indicate that victims can incur significant financial losses, often leading to severe financial distress, sometimes even causing the loss of homes and life savings (Ajiboye, 2020). Beyond the realm of finances, OAFF inflicts profound emotional distress upon its victims. Research emphasises the emotional turmoil experienced by victims, encompassing feelings of betrayal, anger, shame, and embarrassment (Oluwatobi et al., 2017). Such emotional trauma may also extend to a loss of trust in others, impeding their ability to form new relationships (Akintunde et al., 2018).

Furthermore, OAFFs influence the reputation of individuals, governments, and businesses alike. Victims may bear the weight of reputational damage and the stigma associated with falling prey to fraudulent schemes (Anifowose, 2016). For governments and businesses, the association with OAFF can erode their credibility and trustworthiness in the eyes of the public (Akintunde et al., 2018). The burden of addressing OAFF is also borne by law enforcement agencies, as studies illustrate that investigating and prosecuting OAFF cases necessitate significant resources and effort (Ajiboye, 2020). The intricate nature of OAFF, which often involves international networks, further complicates these law enforcement efforts. Additionally, OAFF can disrupt the normal operations of businesses and organizations, resulting in financial losses (Akintunde et al., 2018). The need to invest in enhanced security measures to prevent OAFF can impose additional costs on these entities.

In sum, these consequences underscore the far-reaching impact of OAFF on individuals, governments, and businesses. Financial losses, emotional distress, damage to reputation, law enforcement burdens, and business disruptions represent significant challenges associated with OAFF, necessitating comprehensive efforts to mitigate and prevent its adverse effects.

6. Theoretical framework

This study adopts strain theory and routine activity theory (RAT) as two theoretical explanations for the occurrence of OAFF in Ilorin. Strain theory, initially put forward by Merton (1938), contends that individuals may turn to crime if they are unable to access desired social aims through legitimate channels. In Nigeria, chronic youth unemployment, poverty, and social inequality present tensions that compel some youths into cybercrime as a substitute for success (Tade, 2013; Adewunmi, 2018). Social glamorisation of money, especially on social media, usually supports fraudulent inclinations among those who are socioeconomically stressed; thus, OAFF is a viable but illegitimate adjustment. Routine activity theory, formulated by Cohen and Felson (1979), is the opposite of strain theory because it explains situational conditions that enable criminal offenses to occur. In the RAT, crime occurs if and only when a motivated offender encounters an accessible target with no effective guardianship. In OAFF, economically hard-pressed youths are motivated offenders, innocent users of the internet are potential targets, and a lack of effective cybersecurity control or police presence represents weak guardianship (Yar, 2005; Chiluwa and Ifukor, 2015). These theories provide a strong explanation of OAFF by linking more generalised structural pressures to more specific environmental and technological liabilities, which facilitate crime in Ilorin.

7. Method

The research utilised a research design that combines a questionnaire survey and in-depth interviews to gather data from multiple perspectives. This mixed-methods approach allows for a more holistic understanding of OAFF. A total of 382 respondents was selected through referrals for the questionnaire survey. However, for the in-depth interviews, a total of 10 participants were selected via a purposive sampling technique. The participants were selected based on their expertise and experience related to OAFF. The 10 participants included (3) inmates convicted of OAFF-related offenses, (3) legal practitioners, (2) NGO staff members working with fraud victims, and (2) personnel from the Economic and Financial Crimes Commission (EFCC). The quantitative data from the questionnaire survey was analysed as frequencies, percentages, and charts via statistical software. On the other hand, the qualitative data from the in-depth interviews were transcribed verbatim. Thematic analysis was employed to identify recurring themes and patterns in participants' narratives. By employing a mixed-methods approach, this study provides a comprehensive understanding of the causes, consequences, and prospects of OAFF. This methodology ensured a rigorous and nuanced examination of OAFFs, contributing to the existing body of knowledge and informing effective strategies to combat this global issue.

8. Results

Demographic & socioeconomic characteristics of the respondents

Table 1: Demographic & Socio-Economic Characteristics of the Respondents

Sex:			**Age:**		
Male	217	56.8	18-29	289	75.7
Female	165	43.2	30-39	45	11.8
Total	382	100	40-49	22	5.8
			50-59	22	5.8
			60 & Above	4	1.0
			Total	382	100
Marital Status:			**Occupational Status:**		
Single	293	76.7	Employed	134	35.1
Married	85	22.3	Unemployed	46	12.0
Divorced	2	0.5	Student	179	46.9
Widowed	2	0.5	Apprentice	15	3.9
Total	382	100	Others	8	2.1
			Total	382	100
Educational Background:					
No Formal Education	4	1.0			
Primary Certificate	2	0.5			
Secondary Certificate	62	16.2			
Tertiary Certificate	297	77.7			
Others	17	4.5			
Total	382	100			

The data provided in Table 1 above offer insights into the characteristics of the respondents in the study of online advance fee fraud. Most of the respondents were male (56.8%), while females constituted 43.2% of the sample. The age distribution of the respondents, with the highest percentage (75.7%), fell within the 18--29 age range. This suggests that the research population primarily consists of young individuals, particularly Nigerian youths, who are often involved in online advance fee fraud activities. In terms of marital status, many of the respondents (76.7%) were single, whereas 22.3% were married. This indicates that many participants in the study were unmarried and likely still pursuing their education. Additionally, Table 1 provides information on the occupation and educational background of the respondents. A substantial portion (46.9%) of the respondents were students, followed by 35.1% who were employed and 12.0% who were unemployed. With respect to education, 77.7% of the respondents were graduates of higher institutions, indicating that the study population is predominantly well educated. Overall, the findings from the tables indicate that the study population consists mostly of young, unmarried, and well-educated individuals, predominantly male. While this demographic composition may influence the study's results to some extent, it also suggests that

the selected sample is well suited to provide insights into the subject of online advance fee fraud, given their potential involvement as perpetrators, victims, or familiarity with the issue.

Factors that pull or push individuals into online advance fee fraud (OAFF)

Table 2: Causes of Online Advance Fee Fraud

	Frequency	Percent
Unemployment	129	33.8
Poverty	81	21.2
Greed	44	11.5
Poor Regulatory Oversight	4	1.0
Corruption among Security Agencies	10	2.6
Peer Influence	46	12.0
Quick Money Syndrome	61	16.1
Nature of the Victims	5	1.3
	2	0.5
Total	382	100.0

Table 2 shows that unemployment (33.8%) and poverty (21.2%) are the factors with the highest percentages. Therefore, this finding indicates that many of the respondents believe that the reasons behind the perpetration of online advance fee fraud are unemployment and poverty. These findings are connected to the fact that socioeconomic factors are the major factors that push people to perpetrate online advance fee fraud and influence the rate of victimization.

In line with the causal factors mentioned above, a key informant interview conducted with a respondent in one of the study areas revealed that:

> With a musical career, yahoo is a means to increase capital and focus more on developing oneself in the fast-growing competitive music industry. (KII with an Inmate, Medium Security Custodial Service, Oke-Kura, Ilorin)

In related development, some respondents revealed the following:

> No other alternative is available to obtain money or survive. The country's situation has worsened daily. Therefore, yahoo yahoo is a better means to earn a good living. (KII with an Inmate, Medium Security Custodial Service, Oke-Kura, Ilorin)

> The allure of easy money is a significant factor that pulls individuals into OAFF. Fraudsters exploit the promise of significant financial gains with minimal effort, attracting those facing financial difficulties or seeking socioeconomic improvement. (KII with EFCC personnel, Ilorin, Kwara State)

The findings revealed that unemployment and poverty are the major factors that push people into engaging in online advance fee fraud (yahoo yahoo). On the other hand, an EFCC personnel gave a different view:

> The perceived low risk of detection and prosecution in online operations is another factor that draws people into OAFF. Fraudsters believe that their anonymity online makes it challenging for law enforcement agencies to track them, resulting in a sense of impunity and emboldening their engagement in fraudulent activities. (KII with EFCC personnel, Ilorin, Kwara State)

Nevertheless, different opinions have also been given aside with respect to socioeconomic factors. In an interview with a court registrar, she revealed that:

> The causes of online advance fee fraud can be attributed to both systemic and individual factors. Weak financial regulations, loopholes in the legal system, and gaps in cybersecurity infrastructure contribute to the proliferation of these scams. On an individual level, some perpetrators may lack moral values, whereas others may be driven by financial desperation or a desire for wealth without considering the consequences. (IDI with a Court Registrar, Ilorin, Kwara State)

Additionally, a nongovernmental organization member of staff submitted in an in-depth interview that

> The causes of online advance fee fraud are often rooted in a lack of awareness and understanding of the risks associated with engaging in fraudulent activities. Insufficient education on cybersecurity and digital literacy leaves individuals susceptible to falling victim to scams or being lured into perpetrating fraud themselves. Addressing these knowledge gaps is crucial in preventing these crimes. (IDI with an NGO staff member, Ilorin, Kwara State)

However, a barrister gave a more robust submission:

> The causes of online advance fee fraud are multifaceted. In addition to economic factors, psychological motivations such as greed, opportunism, and a lack of empathy can contribute to individuals engaging in fraudulent activities. It is essential to address both underlying systemic issues and individual accountability to effectively combat this form of fraud. (IDI with a legal practitioner, Ilorin, Kwara State)

Consequences of online advance fee fraud on the public, government, and businesses

Table 3: Consequences of OAFF on the Public

	Frequency	Percent
Financial Loss	245	64.1
Identity Theft	112	29.3
Emotional Distress	178	46.6
Trust Damage	201	52.6
Legal Troubles	67	17.5
Damage of Reputation	132	34.6
Relationship Strain	89	23.3
Loss of Personal Information	93	24.3

Based on the findings in Table 3 above, although all the above are viewed as the main effect of OAFF on the public, only financial loss (64.1%) and trust damage (52.6%) are the main consequences of this menace on Ilorin metropolitan areas. This was also in line with the view of legal practitioners during an in-depth interview. He revealed that:

> The consequences of online advance fee fraud (OAFF) are far-reaching and can have devastating effects on both individuals and society as a whole. Victims of OAFFs often suffer significant financial losses, as fraudsters deceive them into making upfront payments or divulging sensitive financial information. These losses can have long-lasting implications, causing financial distress, bankruptcy, and even the loss of homes or life savings. (IDI with a legal practitioner, Ilorin, Kwara State)

Furthermore, another participant gave a similar note.

> In addition to financial losses, OAFFs can also lead to emotional and psychological trauma for victims. The realization that they have been deceived and manipulated can result in feelings of shame, guilt, and a loss of trust in others. Victims may experience anxiety, depression, and posttraumatic stress disorder (PTSD) as a result of victimization, which impacts their overall well-being and quality of life. (IDI with a legal practitioner, Ilorin, Kwara State)

Additionally, a participant in an in-depth interview revealed the following:

> As someone who was involved in OAFF, I can attest to the severe consequences it has on one's life. Engaging in fraud not only carries the risk of imprisonment but also damages personal relationships and societal standing. Upon conviction, individuals face stigmatization, making it challenging to reintegrate into society and secure employment opportunities in the future. (KII with Inmate, Medium Security Custodial Service, Oke-Kura, Ilorin, Kwara State)

As such, the above findings reveal that the consequences of OAFF and cyber frauds mostly revolve around the financial and psychological implications for victims.

Table 4: Consequences of OAFF on the Government

	Frequency	Percent
Financial Loss to Government	243	63.6
Diversion of Resources	89	23.3
Decrease Public Trust	178	46.6
Burden on Law Enforcement	232	60.7
Increased Cybercrime	201	52.6
Measures	67	17.5
Impact on Economic	76	19.
Development	43	11.3
Reputation Damage	273	71.4
International Relations Impact	297	77.7

According to the findings in Table 4 above, the Ilorin metropolitan area feels that the government also feels the impact of fraud. They suggested that OAFFs primarily result in financial loss to the government, a burden on law enforcement, a continuous increase in cybercrime, damage to government reputation, and negative impacts on international relations.

Furthermore, based on the qualitative data from the interviews, a participant presented a similar view:

> Furthermore, the prevalence of OAFFs tarnishes the reputation of affected countries or regions. Nigeria, in particular, has gained notoriety as a hub for OAFF, which can have negative implications for legitimate businesses, tourism, and foreign investments. The perception of widespread fraud can undermine economic growth and hinder international partnerships. (KII with EFCC personnel, Ilorin, Kwara State)

Table 5: Consequences of OAFF on Businesses and Organizations

	Frequency	Percent
Financial Loss	380	99.5
Damage to Reputation	286	74.8
Disruption of Operations	178	46.6
Increased Security Costs	156	40.8
Loss of Customer Trust	301	78.7
Legal Proceedings and Lawsuits	90	23.5
Business Closure or Bankruptcy	198	51.8
Productivity and Efficiency Loss	284	74.3
Intellectual Property Theft	46	12.0

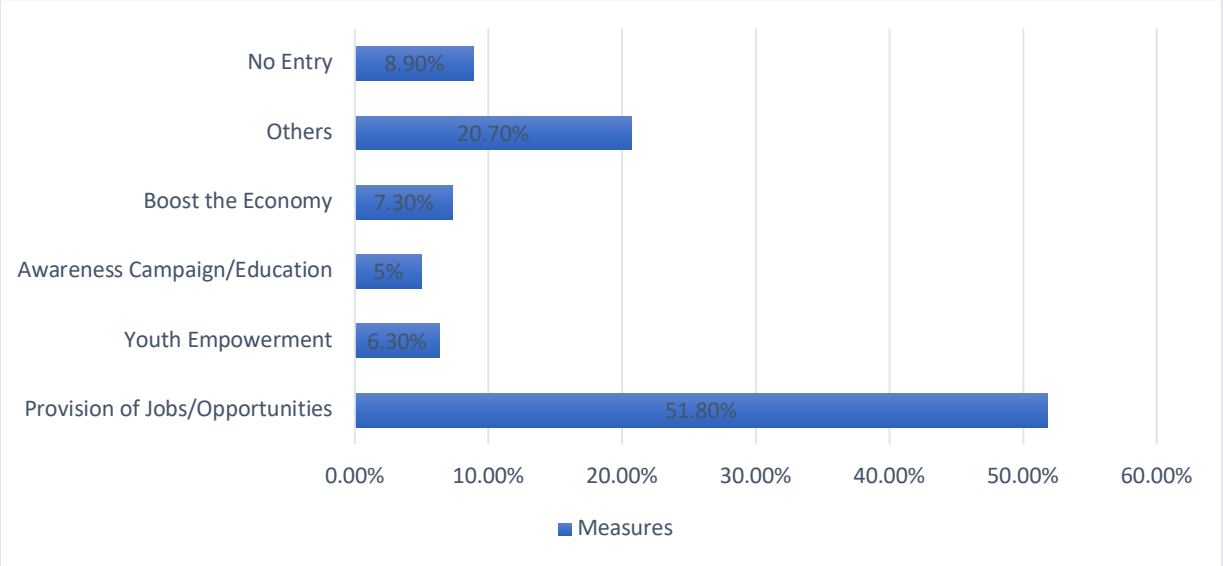
According to the findings presented in Table 5, while the menace of cybercrimes and OAFF reflects on the public and the government, Ilorin metropolitans still believes that businesses and organisations also feel the negative impact of malicious acts. They revealed that because of the OAFF, businesses/organisations mostly face financial loss, damaged reputation, loss of customers' trust, business closure or bankruptcy, and productivity and efficiency loss. To reinforce these quantitative data, the findings from the interviews also fall in the same line, as two NGO staff members gave the following submissions:

> As an NGO staff member, I have witnessed the detrimental consequences of OAFF for vulnerable individuals and communities. Moreover, OAFF undermines the credibility and trustworthiness of NGOs, as fraudsters may impersonate or exploit the reputation of legitimate organizations. (KII with an NGO staff member, Ilorin, Kwara State)

> OAFF has significant consequences for vulnerable individuals and the credibility of NGOs. It undermines trust in legitimate businesses and communities. In terms of NGOs, cyber fraud has negative impacts on some NGOs because of identity theft, which tends to affect their missions and visions. (KII with an NGO staff member, Ilorin, Kwara State)

Measures to reduce the menace of online advance fee fraud

Figure 1: Public perceptions of how to curb the rate of yahoo yahoo



According to Figure 1, majority of the respondents emphasise the issue of youth empowerment, i.e., that the state should make available programs, grants, and opportunities that can empower youth towards achieving their goals, as fundamental to curbing cybercrime. This was also reinforced by the responses obtained from the in-depth interviews and the key informant interviews. They revealed that:

> Good jobs, they should create jobs for everyone. If people are working, they would not think of doing yahoo yahoo or stealing. (KII with Inmate, Medium Security Custodial Service, Oke-Kura, Ilorin, Kwara State)

> Societal help from the government. Like the provision of employment and reducing the rate of poverty in Nigeria. Additionally, with respect to security and a good economy that pays well, young people do not have time to press a phone and think of defrauding people. (IDI with a Court Registrar, Ilorin, Kwara State)

Nevertheless, some participants feel the need for advocacy for enlightenment and awareness, as personnel at the EFCC in a key informant interview submitted that:

> Yes, number one in the public enlightenment on how to use the internet, the laws guiding usage, and the consequences attached to usage. Additionally, this should be imposed on the learning institution, which is at all levels (primary, secondary and tertiary). (KII with EFCC personnel, Ilorin, Kwara State)

On the other hand, while the above recommendations have been made, a legal practitioner recommended the following:

> Has always been an advocate of receiving a policy that will police the police. Therefore, we should have an institution whereby police will be policed by another police officer. The government should find a means of regulating, controlling, monitoring, and checking the activities of the EFCC. (IDI with a legal practitioner, Ilorin, Kwara State)

The above explanation implies that the government should avail itself of a system that will encourage policing of the EFCC. Additionally, an EFCC personnel at the Ilorin Zonal Command believed that the government should encourage synergy between all institutions in the country, as he revealed:

> There should be synergy between the various stakeholders. Law enforcement companies, financial institutions, learning institutions, religious institutions, judiciaries, parents, and other government institutions should collaborate with the EFCC, as this collaboration will improve the fight against online advance fee fraud. (KII with EFCC personnel, Ilorin, Kwara State)

Measures the public can take to avoid being victimized by yahoo yahoo Boys

Figure 2: Public perceptions of measures the public can take to avoid being victimized by yahoo yahoo boys

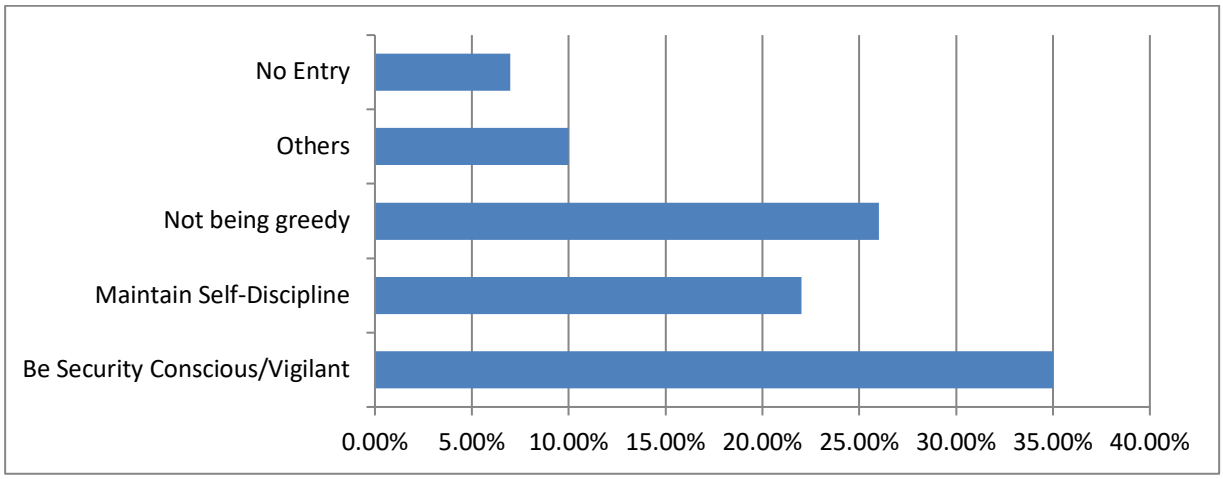
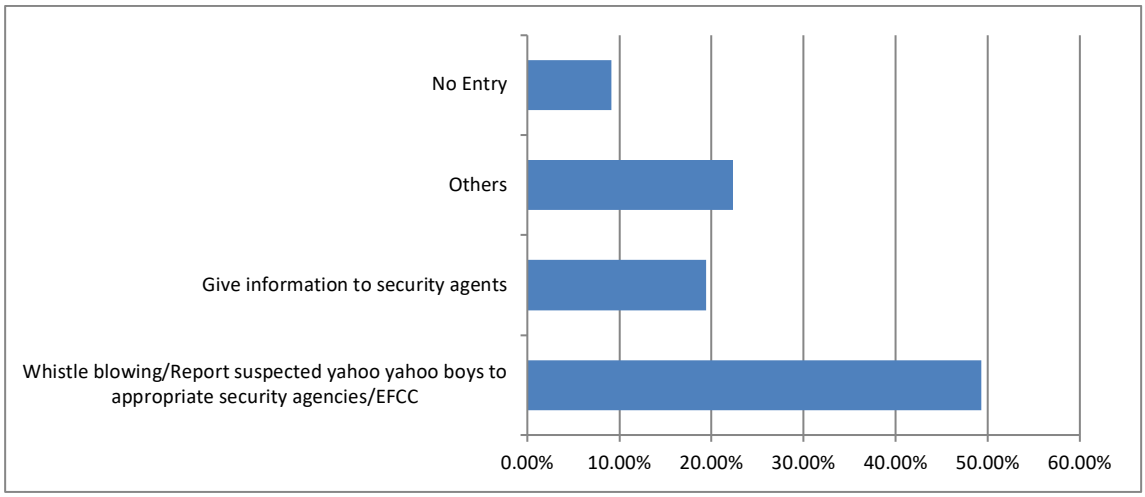


Figure 2 depicts the proactive measures the public can take in place to avoid victimisation. However, when respondents are asked about their perceptions of this, the majority believe that the public can avoid being victimised by yahoo yahoo boys only if they are vigilant and securely conscious in their daily activities. Additionally, while some respondents indicated that the public should be disciplined, some emphasised the issue of greediness. That is, if the public is disciplined and not greedy, they will not fall prey or be easily lured into fraudulent acts or transactions. On the other hand, other recommendations include protecting sensitive personal information, being careful with the use of social media, and moral-dressing to avoid harassment.

Figure 3: Public perception of the role the public can play in assisting the EFCC in combating yahoo yahoo



Based on the findings in Figure 3 above, the respondents were asked what role the public can play in assisting the EFCC in combating online advance fee fraud (yahoo yahoo). According to the results, more than half of the respondents advocated for whistling blowing and the reporting of suspected yahoo yahoo boys to the appropriate security agencies. Nevertheless, some of the respondents believe that the public can only assist the EFCC by providing credible information that can assist them in their legal, operational, and administrative processes.

Personnel of the EFCC also emphasized the role of the public in the fight against online advance fee fraud and revealed the following:

> Additionally, the issues of societal values, parental guidance, and all. If the value system is still in order, parents should be the first people to investigate the source of their children's wealth and report, but they should embrace and accept money from them. (KII with EFCC personnel, Ilorin, Kwara State)

Meanwhile, some indicated that the EFCC should assist their selves in being assisted by the public. Additionally, recommendations were given on the aspect of the public frowning at the act of yahoo yahoo; in essence, the public should stop celebrating the act and discourage its perpetration through sensitizations and campaigns.

9. Discussion of findings

Based on the analyses of the causes of OAFF, unemployment, poverty, and the allure of easy money were identified as the primary factors driving individuals to engage in OAFF. This is in line with the findings of Bhutta (2012), who suggested that high levels of poverty, unemployment, and economic inequality create an environment conducive to engaging in fraudulent activities. Additionally, while research has shown that the low risk of detection and prosecution attracts people to OAFF, Oluwatobi et al. (2017), on the contrary, noted that the widespread availability of internet access and digital communication platforms has facilitated the expansion of Online Advance Fee Fraud. However, understanding these factors is essential for developing effective strategies to address OAFF and protect potential victims. OAFF has severe consequences for the public, the government, and businesses. Victims suffer significant financial loss, emotional distress, and a loss of trust in others. Governments face financial loss, burdened law enforcement, and damage to their reputation and international relations. Businesses experience financial loss, reputation damage, disruption of operations, and increased security costs. All the negative effects of OAFFs revealed by the Ilorin metropolitan area tend to be general in nature, as several studies have revealed similar results. For example, several studies suggest that victims of OAFF face physical, social and psychological trauma (Anifowose, 2016; Ajiboye, 2020; Oluwatobi et al., 2017; and Bhutta, 2012). In other words, addressing these consequences requires preventive measures, awareness-raising, and enhanced law enforcement efforts.

As such, this research examines measures that can be put in place to curtail the menace of OAFF. According to the analyses above, to reduce OAFF, youth empowerment through job creation, grants, and programs is crucial to steer individuals away from fraudulent activities due to unemployment and poverty. These are in line with the strategies profiled in the empirical review (Ene and Oluku, 2024; Ogbebor). Advocacy for enlightenment and awareness should educate the public about internet usage, associated laws, and the consequences of fraudulent activities. Establishing an institution to oversee and regulate law enforcement agencies such as the EFCC is recommended. Synergy and collaboration among stakeholders, including law enforcement, financial and educational institutions, religious bodies, judiciaries, parents, and government entities, are vital in combating OAFF. Following the assumption of routine activity theory, to avoid victimisation, the study recommends that the public be vigilant, security conscious, and disciplined. Avoiding greed, being cautious with personal information, and practicing responsible social media use are recommended. Whistleblowing and reporting suspected OAFF perpetrators to appropriate security agencies are ways in which the public can assist the EFCC. Providing credible information and encouraging societal values and parental

10. Conclusion

Online advance fee fraud is a widespread and pervasive form of fraud that poses significant challenges in Ilorin Metropolis and beyond. The study sheds light on the factors driving individuals to engage in this fraudulent activity, such as unemployment, poverty, the allure of easy money, and the perceived low risk of detection and prosecution. The consequences of OAFF are severe and impact individuals, governments, and businesses. Victims suffer financial losses, emotional distress, and a loss of trust, whereas governments face financial burdens, reputational damage, and strained law enforcement resources. Businesses experience financial losses, reputation damage, operational disruptions, and increased security costs. Addressing OAFF requires focusing on preventive measures and raising awareness among the public. While previous studies have often focused on socioeconomic factors such as unemployment and poverty as primary drivers of OAFF, this study places additional emphasis on the role of the internet, AI and emerging technologies such as automated bots and deepfakes because they strengthen OAFF victimisation methods. The digital tools assist fraudsters with individualized attacks that change victims' digital identity information, thus making detection between real and fake transactions more difficult. Technological advancements have dramatically expanded OAFF operations while creating new barriers to detect and prevent crimes. This highlights the evolving nature of online fraud and its adaptation to the digital age.

This study highlights the burden OAFF places on governments, including financial losses, reputational damage, and strained law enforcement resources. While previous studies have often focused on the consequences for individuals and businesses, this research assesses the broader policy implications and challenges for governments in effectively combating OAFF. These differences in findings provide a more comprehensive understanding of OAFF and suggest the need for updated policy responses that address both the socioeconomic and technological aspects of this issue. Encouraging the reporting of suspected fraudsters, providing credible information to support law enforcement, and promoting responsible online behaviour can help individuals avoid falling victim to OAFF schemes. Nevertheless, strengthening technology infrastructure, enhancing international cooperation, and sharing best practices can further assist in combating OAFF. However, OAFF is a pervasive form of fraud with significant consequences for individuals, governments, and businesses. By implementing preventive measures, raising awareness, promoting responsible behaviour, enhancing collaboration among stakeholders, and addressing root causes, it is possible to mitigate the occurrence of OAFF and protect individuals and society from its harmful effects in Ilorin Metropolis and beyond.

Declarations:

- **Originality Statement:** I, Abayomi Abdulquadir AJIBADE, confirm that this manuscript is original, has not been previously published, and is not under review elsewhere.
- **Author Approval Statement:** I, Abayomi Abdulquadir AJIBADE, confirm that all authors have read and approved the submitted manuscript, and the author order has been agreed upon by all co-authors.
- **Conflict of Interest Disclosure:** The authors declare that there are no conflicts of interest associated with this research. No financial, personal, or institutional relationships influenced the study's design, data collection, analysis, or interpretation. This disclosure affirms the objectivity and academic integrity of the work presented in this paper.
- **Funding Information:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. All expenses associated with the study were personally covered by the authors.
- **Authors Contributions:** AA: conceptualisation, pilot systematic literature review, and synthesis, AA: methodology, data analysis. AA: review-editing and writing, original manuscript preparation. Author have read and approved the published on the final version of the article.

References

ACCC, 2020. Targeting scams: ACCC Scamwatch report 2020. Available at: https://www.accc.gov.au/system/files/Targeting%20scams%20report%202020.pdf [Accessed 25 April 2025].

Adegoke, T., Oluwatayo, T.A. and Oluwatobi, S.O., 2018. Digital crimes and digital divide: A study of cyber fraud victimization in Nigeria. Journal of internet and Information Systems, 11(2), pp.107-124.

Adesina, O.S., 2020. Cybercrime and law enforcement in Nigeria: The role of the EFCC and ICPC. Journal of Financial Crime, 27(1), pp.218–234.

Adesina, O.S., 2020. Cybercrime and law enforcement in Nigeria: Challenges and prospects. African Journal of Criminology and Justice Studies, 13(1), pp.24-39.

Aloba, O.S., Akinsola, M.K. and Olajide, O.A., 2015. Personality factors as correlates of cybercrime involvement among Nigerian undergraduates. Psychology, 6(1), pp.47-52.

Adewunmi, F., 2018. Youth Unemployment and Cybercrime in Nigeria: A Sociological Perspective. Nigerian Journal of Social Sciences, 14(2), pp.112–126.

Ajibade, A. A., Ndubueze, P. N., & Hussein, M. D. (2024). Patterns of Online Advance Fee Fraud in Ilorin Metropolis, Kwara State, Nigeria. POLAC International Journal of Economics & Management Science, 10(1), pp.1-11.

Ajiboye, T., 2020. The dynamics of cybercrime in Nigeria: Causes, challenges, and policy implications. International Journal of Innovation, Creativity and Change, 13(8), pp.600-613.

Akintunde, A.O., Odeyemi, T., Olawoye, O.O. and Oloyede, O.A., 2018. Cybercrime victimization and psychological distress among undergraduates in Nigeria: The moderating role of coping strategies. African Journal of Criminology and Justice Studies, 11(2), pp.148-166.

Aloba, O.S., Akinsola, M.K. and Olajide, O.A., 2015. Personality factors as correlates of cybercrime involvement among Nigerian undergraduates. Psychology, 6(1), pp.47–52.

Anifowose, M., 2016. The impact of cybercrime on national security: The Nigerian perspective. Journal of internet and Information Systems, 7(2), pp.48-56.

Bhutta, N.M., 2012. Towards understanding the dynamics of online fraud victimization. International Journal of Cyber Criminology, 6(1), pp.789-801.

Buchanan, B. and Imran, A., 2021. Deepfakes and synthetic media: Proving identity in a post truth world. Survival, 63(1), pp.107-126.

Chawki, M., 2009. Nigeria tackles advance fee fraud. Journal of Information Law & Technology, 1(1), pp.1-20.

Chiluwa, I. and Ifukor, P., 2015. Online religion in Nigeria: The internet and 'Yahoo Yahoo' scam. Journal of Asian and African Studies, 50(1), pp.60-73.

Cohen, L.E. and Felson, M., 1979. Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), pp.588-608. https://doi.org/10.2307/2094589

Danquah, P., Kani, J.A. and Bibi, D., 2022. Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity. East African Journal of Information Technology, 5(1), pp.39–52. https://doi.org/10.37284/eajit.5.1.673

Doppelmayr, M., 2013. Internet-based fraud schemes: An analysis of the Nigerian Advance Fee Fraud (419) and Yahoo Yahoo scams. Master's thesis, University of Oslo. Available at: https://www.duo.uio.no/bitstream/handle/10852/41667/Master-Doppelmayr.pdf?sequence=1 [Accessed 7 May 2025].

Felson, M. and Boba, R.L., 2010. Crime and everyday life (4th ed.). Thousand Oaks, CA: Sage Publications. https://doi.org/10.4135/9781483349299

IC3, 2023. Internet Crime Report 2021. Available at: https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics [Accessed 22 April 2025].

King, J. and Aggarwal, N., 2020. AI crime: An emerging challenge for cybersecurity law. Journal of Law and Technology, 33(4), pp.529-552.

Ladegaard, I., 2019. Wealth by deception: Online scams in the context of political instability. British Journal of Criminology, 59(1), pp.158-176.

Lazarus, S. and Okolorie, G.U., 2019. The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telematics and Informatics, 40, pp.14–26. https://doi.org/10.1016/j.tele.2019.04.009

Mondaq, 2021. Deepfakes in Nigeria: Protection and legal framework against deepfake attacks in Nigeria. Available at: https://www.mondaq.com/nigeria/security/1114750/deepfakes-in-nigeria-protection-and-legal-framework-against-deepfake-attacks-in-nigeria [Accessed 7 May 2025].

NCC, 2021. Nigeria Communications Commission Annual Report 2021. Available at: https://www.ncc.gov.ng/docman-main/legal-regulatory/ncc-publications/annual-reports/1858-ncc-annual-report-2021/file [Accessed 7 May 2025].

Ndubueze, I.M., 2017. Cybercrime in Nigeria: Implications and prevention strategies. Journal of Internet and Information Systems, 7(1), pp.60-68.

Nwafor, C. and Emeh, I.E., 2019. An analysis of cybercrime and cyber security awareness in Nigeria. Journal of Engineering Research and Reports, 4(3), pp.1-12.

Nwakanma, A., 2023. Legal gaps in addressing AI-facilitated cybercrime under Nigerian law. African Journal of Law and Human Rights, 9(1). Available at: https://journals.ezenwaohaetorc.org/index.php/AJLHR/article/view/2864 [Accessed 7 May 2025].

Obuah, E., 2010. Combating corruption in a "failed" state: The Nigerian Economic and Financial Crimes Commission (EFCC). Journal of Sustainable Development in Africa, 12(1), pp.27–53.

Ogbebor, O.V., 2023. Advance Fee Fraud on the Increase: The Shield of Support Over the Victims. [Dissertation] Liberty University.

Ojedokun, U.A. and Eraye, C.M., 2012. Socioeconomic lifestyles of youth involved in cybercrime in Nigeria. Journal of Financial Crime, 19(1), pp.20-33.

Ojedokun, O. and Ilori, M.O., 2021. Yahoo-Boy tools, techniques, and underground networks: A study of internet fraud in Ibadan, Nigeria. African Criminology and Justice Studies, 14(1), pp.76–98. https://doi.org/10.36889/IJCJ.2021.003

Okeshola, F.B. and Adeta, A.K., 2013. The nature, causes and consequences of cybercrime in tertiary institutions in Zaria–Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), pp.98–114.

Oluwatobi, S.O., Oyebisi, T.O. and Adesesan, Y.A., 2017. Perception and victimization of online fraud among Nigerian undergraduate students. Journal of internet and Information Systems, 8(1), pp.41–51.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S. and Dabbish, L., 2013. Anonymity, privacy, and security online. Pew Research Center. Available at: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/ [Accessed 7 May 2025].

Scannell, J., 2014. The '419 scam': An unacceptable 'power of the false'? Portal: Journal of Multidisciplinary International Studies, 11(2), pp.36–51. https://doi.org/10.5130/portal.v11i2.3220

The Police Foundation, 2023. Online anonymity and fraud: Understanding the implications for the problem and the solutions. Available at: https://www.police-foundation.org.uk/online-fraud-research-hub/online-anonymity-and-fraud-understanding-the-implications-for-the-problem-and-solutions/ [Accessed 7 May 2025].

Tade, O. and Aliyu, I.A., 2011. Social Organization of internet Fraud among University Undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), pp.860–875.

Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: The 'Yahoo Plus' phenomenon. Human Affairs, 23(4), pp.689–

705. https://doi.org/10.2478/s13374-013-0158-9

Ulo, E., 2023. Cyberspace anonymity: The root cause of internet fraud among Nigerian youths. Ilorin Journal of Criminology and Security Studies, 1(2), pp.77–88.

Yar, M., 2005. The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), pp.407–427. https://doi.org/10.1177/147737080556056