ALKEBULAN
A Journal of West and East African Studies

Volume 5, Issue 2

Alkebulan: A Journal of West and East African Studies
http://gnosipublishers.com.ng/index.php/alkebulan/index
ISSN (Online): 2971-6187

The Youth and Cybercrime in Nigeria: Cross River State Experience, 2001-2023

Effiong, Eke Nta, Festus Nwankwo Ongele, Eke, Effefiong Nta
University of Calabar, Calabar, Nigeria.

ABSTRACT

The rapid growth of digital technology and internet access has led to a rise in cybercrime, particularly among Nigerian youths. This study investigates youth involvement in cybercrime in Nigeria, focusing on Cross River State between 2001 and 2023. It examines the various forms of cybercrime, historical trends, and the socio-economic and psychological factors driving youth participation. Using a qualitative research approach, the study draws on primary sources, including interviews and field reports, as well as secondary sources such as official records and scholarly literature. Findings reveal that unemployment, peer influence, a lack of digital ethics, and weak enforcement mechanisms have significantly contributed to the rise in cybercrime in the state. The study further highlights the impact of cybercrime on youth development, societal values, and economic stability. While some government policies and cybersecurity initiatives exist, their implementation remains inadequate. The study recommends strengthening legal frameworks, implementing digital literacy campaigns, promoting youth empowerment programs, and enhancing cybersecurity training for law enforcement agencies. It concludes that a holistic approach addressing both social and institutional gaps is essential to curbing cybercrime and redirecting youth energy toward productive digital engagements in Cross River State and Nigeria at large.

Keywords: Youth; Crime; Cybercrime; Nigeria; Security.

Corresponding author:
Lilian Sanga
Received: *23 July 2024*
Accepted: *22 July 2025*
Published: *30 September 2025*

This is an open access article distributed under the Creative Commons Attribution License CC-BY-NC-4.0 ©2025 by author (https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

In Nigeria, cybercrime, also known as internet-based crime, is becoming an increasingly significant problem, particularly among young people. Due to financial strain, unemployment, and the pursuit of quick wealth, many youths have turned to cybercrime as a means of earning a living, facilitated by the widespread use of technology and easier internet access. Nigeria is not alone in facing cybercrime; other countries with significant cybercrime activities include the United States, China, Russia, India, Brazil, South Africa, and Kenya (Chigad & Madzinga, 2021).

Research indicates that cybercrime has damaged Nigeria's economy and its international reputation, prompting international sanctions and restrictions in certain areas (Adewale & Olorunfemi, 2020). The Nigerian government has attempted to curb this trend through legislative and regulatory frameworks like the Cybercrimes (Prohibition, Prevention) Act of 2015, which aims to address cyber offences and establish penalties for offenders. Despite these measures, cybercrime—especially among youth—continues to rise.

In Cross River State, the issue of cybercrime among youths has been prominent over the years. Several socio-economic factors, including high youth unemployment, poverty, and a lack of viable alternatives for income generation, have driven young people toward cybercrime as a means of survival. In recent years, technological advancements and widespread internet access have made cybercriminal activities such as phishing, online scams, identity theft, and hacking more prevalent in the state. Like many other regions in Nigeria, youths in Cross River State face numerous obstacles to social mobility, employment, and education. Consequently, some have turned to cybercrime—often referred to as “yahoo-yahoo”—as a way to cope with these challenges. This trend has significantly impacted the individuals involved, their communities, and the state at large. Cybercrime has raised security concerns, caused social unrest, and strained relationships between local law enforcement and youth, endangering the state's socio-economic stability. This study examines the factors influencing youth participation in cybercrime in Cross River State between 2001 and 2023, exploring the technological, cultural, and socioeconomic dimensions of this pressing issue.

WHAT IS CYBERCRIME?

Cybercrime, sometimes referred to as computer-based crime, encompasses unlawful activities carried out through networks, computers, or the internet. It is a significant problem in the digital age that impacts individuals, businesses, and governments globally. Different fields have varying definitions for it, and different schools of thought offer different perspectives on its nature and impact.

The legal school defines cybercrime as activities that violate laws specifically designed to regulate electronic and digital domains. Goodman and Brenner (2002) describe cybercrime as offences “where a computer is a tool, target, or means for committing the offence” (p. 45). This perspective emphasizes the need for specialized legal frameworks to address crimes such as hacking, online fraud, and identity theft. The legal approach also underscores the complexities of prosecuting offenders who exploit the borderless nature of cyberspace.

The technological school of thought views cybercrime through the prism of the instruments and systems used to commit it. Parker (1984) emphasizes that cybercrime entails unlawful acts that compromise data integrity, system functionality, or the

dependability of electronic communication. This school highlights the technological prowess of cybercriminals, who often exploit vulnerabilities in software, networks, or digital infrastructures. Consequently, combating cybercrime necessitates advanced technical expertise and constant innovation (Jakobsson & Myers, 2006).

The sociological school views cybercrime as an issue resulting from the misuse of technology in the modern environment, emphasizing societal elements. Wall (2007) defines cybercrime as "criminal acts conducted online, typically assisted by anonymity" (p. 12). This viewpoint examines how social and human factors, such as a lack of digital literacy, unequal access to technology, and moral failings, contribute to cybercrime. It also emphasizes how the anonymity provided by the internet emboldens perpetrators, making accountability more challenging.

As observed by scholars like Broadhurst Roderic (2017), cybercrime takes many forms, often categorized by the target. Crimes against individuals exploit personal vulnerabilities, such as phishing, identity theft, and online harassment. Crimes against property, such as hacking and ransomware attacks, target corporate or organizational systems to steal data or disrupt operations. Financial crimes, like online banking fraud, exploit digital financial networks, while crimes against governments, such as cyberterrorism and espionage, threaten national security (Okonkwo, 2019).

HISTORICIZING CYBERCRIME IN NIGERIA

The history of cybercrime in Nigeria is closely linked to the global development of the internet and the country's socio-economic challenges. Cybercrime in Nigeria gained prominence through a particular type of fraud known as "419 scams," named after Section 419 of the Nigerian Criminal Code, which addresses fraud and deception (Odumesi, 2014). These activities began with conventional communication techniques like letters and faxes but became more sophisticated with technological advancement. With the advent of personal computers and rudimentary internet services in the late 1980s and early 1990s, a new form of criminal activity evolved. Initially constrained by analogue tools, scammers quickly adapted to the opportunities provided by the internet.

In the 1990s, young Nigerians, referred to as "Yahoo Boys," began using online resources to carry out fraudulent operations. Their actions often involved sending false emails to potential victims worldwide, featuring fake business proposals, fictitious personal connections, or inheritance claims that demanded upfront payments for non-existent prizes. The anonymity and global reach of the internet made these scams successful and hard to detect. During this time, individual scams gave way to more coordinated cybercrime efforts, driven by economic hardships like high unemployment and a lack of legitimate opportunities (Oladipo & Ogundele, 2021). As internet access became more widespread in the 2000s, the scale and complexity of cybercrime operations increased dramatically. Cybercafés, popular during this period, became hubs for criminal activities. One of the most infamous scams was the "Nigerian Prince" email fraud, where perpetrators impersonated wealthy individuals or officials seeking assistance to transfer large sums of money, promising victims a share in return for financial help. The prevalence of such scams drew international attention, making Nigeria a focal point in discussions on cybercrime (Aghatise, 2020).

Recognizing the rising threat, the Nigerian government took steps to address the problem. In 2003, it established the Economic and Financial Crimes Commission (EFCC) to investigate and prosecute financial crimes, including cybercrime. The EFCC achieved

notable successes, including arrests and convictions in high-profile cases, and launched public awareness campaigns. Despite these efforts, its effectiveness was hindered by limited resources, systemic corruption, and the ingenuity of cybercriminals (Emmanuel & Adedeji, 2013).

Nigeria enacted the comprehensive Cybercrimes (Prohibition, Prevention, Etc.) Act in 2015, criminalizing a wide range of activities like hacking, identity theft, and phishing. While this act represented significant progress, enforcement remained challenging due to the complex, borderless nature of cybercrime. In recent years, cybercrime in Nigeria has evolved beyond traditional email scams to include more advanced tactics like Business Email Compromise (BEC), phishing schemes, and ransomware attacks. Some syndicates operate on a global scale, targeting corporations and governments. International collaboration has been effective, as seen in the 2019 arrest of Obinwanne Okeke ("Invictus Obi"), whose multi-million dollar fraudulent activities spanned several countries (EFCC, 2016). Such cases underscore the growing sophistication of Nigerian cybercrime and its global implications. The history of cybercrime in Nigeria highlights the intersection of socio-economic challenges and technological advancements, emphasizing the need for sustained efforts in cybersecurity infrastructure, public education, and international collaboration.

CYBERCRIME IN CROSS RIVER STATE

The proliferation of cybercafés in Cross River State during the mid-2000s significantly contributed to the emergence and growth of cybercrime. These establishments, initially intended for educational research, communication, and business, soon became hotspots for fraudulent activities. In Calabar, cybercafés in areas like Marian Road and Etta-Agbor became hubs where young individuals, mostly men, experimented with internet fraud. These venues were often packed with patrons, some engaged in legitimate browsing, while others conducted dubious activities like phishing and email fraud targeting international victims (Ojong, personal interview, November 25, 2024). Economic hardship and limited employment opportunities created an environment where cybercrime became a perceived alternative to poverty. In areas such as Akim Qua Town and Eight Miles, groups of young men, often called "Yahoo boys," operated discreetly in their neighborhoods, spending long hours online engaged in fraudulent schemes. The lack of affordable cybersecurity education and public awareness campaigns exacerbated the situation, leaving many susceptible to online scams.

In Calabar South, where the bustling Watt Market serves as a centre for both legal and illegal transactions, locals have expressed concern about the normalization of cybercrime. A shopkeeper in the area noted, "Many of these boys flaunt their wealth openly; they drive flashy cars and throw lavish parties. It's hard to tell them apart from legitimate businesspeople" (Samuel, personal interview, January 4, 2025). This societal acceptance of quick wealth, regardless of its source, has contributed to the allure of cybercrime, particularly among impressionable youths. However, community leaders in areas like Ikot Ishie have criticized this trend as a moral decay that undermines traditional values of honesty and hard work.

In Cross River State, cybercrime is viewed differently by various segments of society. Some see it as a response to systemic unemployment, while others regard it as damaging to the state's reputation. The EFCC has made high-profile arrests in Calabar, targeting neighborhoods such as Ediba, Satellite Town, Marian, Ekorinim, Lemna, and 8 Miles.

Despite these initiatives, cybercrime persists, raising questions about the effectiveness of punitive versus preventative strategies. Critics argue that addressing underlying causes like poverty and unemployment is more critical than enforcement alone (Inakefe & Bassey, 2023).

PATTERNS OF CYBERCRIME

As technology advances and internet accessibility increases, cybercriminals in Cross River State have adapted their strategies, employing more sophisticated methods and expanding their operations. In recent years, cybercrime in Calabar has evolved significantly, with perpetrators shifting from primarily targeting foreign victims to exploiting local and regional opportunities. This transformation reflects broader trends in the digitalization of economies and the growing reliance on online platforms. Among the most alarming developments are the rise in Business Email Compromise (BEC), the persistence of romance scams, and the emergence of ransomware attacks, each showcasing the adaptability of cybercriminals in the region. Business Email Compromise (BEC), a cybercrime that has increased globally, primarily targets small and medium-scale enterprises (SMEs). Due to increased economic activity and internet access, Calabar has become a desirable location for local cybercriminals operating BEC scams. These schemes are particularly harmful as they exploit trust in corporate procedures. Criminals infiltrate business email correspondence, alter invoices, and divert payments to fictitious accounts, often leaving victims with few options for recourse (Jakobsson & Myers, 2006).

BEC schemes involve careful preparation and in-depth investigation of targets. Cybercriminals in Calabar often pose as reliable organizations, such as suppliers or senior company personnel, using spear-phishing emails or spoofed websites to appear legitimate. They monitor email exchanges to identify payment schedules, timing their attacks to coincide with legitimate transactions. The Internet Crime Complaint Centre (IC3) reported global losses from BEC scams exceeding $1.8 billion in 2021, with a growing portion attributed to actors in cities like Calabar. Many local SMEs lack robust cybersecurity frameworks, such as two-factor authentication or email encryption, making them vulnerable. The economic implications are severe, leading to financial losses, disrupted operations, and eroded trust between companies (Chigad & Madzinga, 2021).
Romance scams, a form of online fraud, have also become a significant issue in Calabar. These scams exploit the emotional vulnerabilities of individuals seeking companionship through fake profiles on social media and dating apps. Cybercriminals, often tech-savvy youths, pose as attractive or successful professionals to build trust with victims over time (Aghatise, 2020).

The process typically begins with a false identity, using stolen photographs and elaborate backstories. Scammers engage with targets through messaging and video calls, weaving tales of personal hardship to foster empathy. Once an emotional bond is formed, they introduce fabricated financial crises, such as medical emergencies or investment opportunities, persuading victims to send money. Romance scams inflict not only financial losses but also significant emotional and psychological harm, causing embarrassment and deterring victims from reporting the crime. This erodes trust in online platforms and tarnishes the city's reputation.

FACTORS ENHANCING CYBERCRIME AMONG YOUTHS IN CROSS RIVER STATE

Cybercrime among youths is a major global concern, driven by a combination of factors ranging from socio-economic challenges to peer influence and technological advancements.

a) Socio-Economic Challenges

In developing countries like Nigeria, unemployment and poverty are significant drivers of cybercrime. The lack of traditional economic opportunities pushes technologically inclined youths to use their skills for illegal purposes. Cybercrime promises quick financial gains that often exceed potential earnings from legitimate work, increasing its allure (Oladipo & Ogundele, 2021). The case of Ramon Abbas ("Hushpuppi"), arrested in 2020 for masterminding multi-million-dollar cyber fraud, exemplifies how financial difficulties can lead to criminal activity. In environments with structural poverty and limited access to quality education, many youths see cybercrime as an escape. This is further encouraged by weak cybercrime legislation and enforcement in some regions (Abdulrahman, 2022).

Underlying socio-economic disparities resulting from poor governance, corruption, and a failure to build sustainable economic infrastructures create a vicious cycle. Addressing these issues requires substantial reforms, including investment in education, skill-building initiatives, and robust cybercrime laws. Promoting an ethical digital culture through awareness programs can also help prevent the normalization of cybercrime as a profitable profession. Mitigating cybercrime necessitates not only punitive measures but also addressing the socio-economic vulnerabilities that drive such behaviours.

b) Peer Pressure and Social Influence

Peer pressure significantly contributes to youth involvement in cybercrime in Cross River State. Adolescents and young adults are susceptible to peer influence due to a strong desire for acceptance and social validation. Peer groups that glamorize fraudulent lifestyles create a narrative associating cybercrime with wealth and success, normalizing illegal activities. This dynamic is potent in urban settings with pronounced economic disparities (Ajayi, 2020).

Social media exacerbates peer pressure by providing a platform to display wealth acquired through illegal activity. The visibility of opulent lifestyles creates a framework of comparison, pressuring others to engage in similar practices. Peer networks often provide the technical know-how and equipment needed for fraudulent actions. These networks act as echo chambers, downplaying the risks of cybercrime while exaggerating its rewards, which hinders moral reasoning and fosters justification for illegal activities. This aligns with Bandura's (1999) theory of moral disengagement, which explains how individuals rationalize unethical behaviour by diffusing personal responsibility.

c) Lack of Ethical Guidance

Family structures significantly shape a child's ethical framework. Weak family units, characterized by parental negligence or insufficient moral guidance, are correlated with delinquent behaviours. In contemporary society, broken homes and dysfunctional dynamics contribute to a lack of supervision, leaving youths vulnerable to influences that promote unethical conduct like cybercrime (Ajayi, 2020). Limited parental awareness of

digital tools often results in a laissez-faire approach to monitoring online activities, allowing harmful behaviours to flourish.

In an interview, Mrs. Ada Obi, a mother of two teenagers in Uyo, noted: "Parenting is hard, especially with technology. I work long hours, and it's difficult to monitor their every move online. I only realize they've done something wrong when the damage is already done. We also weren't taught how to handle this digital age, so it's overwhelming" (personal interview, May 26, 2025). This experience underscores the gap in parental education and involvement. Without intentional efforts to instil ethical values, youths are left to navigate complex societal influences alone.

d) Lack of Adequate Cybercrime Legislation and Enforcement

The inadequacy of cybercrime legislation and enforcement mechanisms remains a significant challenge in Nigeria. Loopholes in legal frameworks, combined with weak enforcement capacity, create a conducive environment for cybercrime. Nigeria grapples with outdated laws that fail to address modern cybercrimes like phishing and ransomware clearly, deterring effective prosecution and fostering a culture of impunity (Okonkwo, 2019).

Law enforcement agencies often lack the expertise and resources needed to trace and monitor cybercriminal activities. In Cross River State, enforcement efforts are hampered by limited funding and poorly trained personnel. This institutional weakness emboldens perpetrators, many of whom are technologically adept youths exploiting digital vulnerabilities with little fear of consequences.

EFFECTS OF CYBERCRIME ON YOUTHS IN CROSS RIVER STATE

Impact on Youth Development and Employment

The involvement of youths in cybercrime has significant effects on their personal growth and employment prospects. While some view cyber fraud as a path to financial stability, the long-term consequences are detrimental, leading to stalled career development, lower employment rates, and negative societal attitudes. Many youths engaged in online fraud abandon formal education or vocational training, diminishing their ability to contribute positively to the workforce and leaving them vulnerable if law enforcement crackdowns intensify (Oladipo & Ogundele, 2021).

Furthermore, involvement in cybercrime hampers career opportunities. Individuals caught engaging in these acts often acquire criminal records that restrict employment options. As employers conduct more frequent background checks, those with cybercrime-related offences find it difficult to secure stable jobs, leading to extended unemployment and social alienation. This perpetuates a cycle where they revert to cybercrime due to a lack of alternatives.

Another major repercussion is the reinforcement of negative stereotypes about youths in Cross River State. As cybercrime becomes widespread, businesses and investors grow sceptical of young professionals from the area. Financial institutions and international firms may impose stricter regulations on individuals and enterprises from Cross River out of concern over fraud. These stereotypes not only impact those directly involved but also hinder opportunities for law-abiding youths, who struggle to access financial and employment avenues due to widespread mistrust.

Legal and Ethical Implications

The rise of cybercrime in Cross River State carries serious legal and ethical implications. Nigerian laws, such as the Cybercrimes Act of 2015, criminalize cyber fraud, hacking, and identity theft; however, enforcement within the state remains challenging. Ethical concerns arise as many youths fail to appreciate the long-term impact of their actions on victims and society. A primary legal challenge is the difficulty in prosecuting cybercriminals effectively. Although the EFCC has made arrests in Calabar and Ikom, conviction rates remain low due to resource constraints, judicial delays, and corruption. Many cases face prolonged court delays or end with plea bargains, undermining deterrence. The lack of dedicated cybercrime units in Cross River hampers investigations, making it harder to track sophisticated fraud rings (Omoniyi, 2020).

Jurisdiction presents another challenge. Cybercrimes often target victims across borders, complicating prosecution due to differences in national laws and limited international cooperation. Nigeria has struggled to extradite cybercriminals because of complex diplomatic procedures, enabling offenders to continue their activities. This has made Cross River a hub for cybercriminals exploiting legal loopholes. Ethically, the normalization of online fraud among youths is a profound concern. Many young people see cybercrime as a practical way to make money, sometimes framing it as a form of "reparations fraud" against wealthy foreigners who have historically exploited Africa. This mindset distorts moral values and fosters a culture where deception is acceptable (Aghatise, 2020). Another ethical issue is the erosion of trust in digital transactions. When companies fall prey to cyber fraud, it stifles economic growth and damages consumer confidence. The role of social media in promoting cybercrime is also significant, as young cybercriminals flaunt illicit earnings online, glorifying fraudsters as role models and deepening unethical behaviour.

ADDRESSING CYBERCRIME IN CROSS RIVER STATE

Addressing cybercrime in Cross River State requires robust government policies, legal frameworks, and active law enforcement. Cybersecurity agencies must play a key role in preventing and prosecuting offences while promoting public awareness.

Government Policies and Legal Framework

The Cross River State government, in line with national regulations, has implemented policies to combat cybercrime. However, enforcement at the local level remains challenging due to limited resources, inadequate technical expertise, and corruption. A key initiative is the collaboration between local security agencies and the EFCC in tackling "Yahoo Yahoo." The EFCC has conducted raids in Cross River, resulting in arrests of individuals involved in financial scams. In 2021, for instance, multiple suspects were apprehended in Calabar for operating fraudulent online businesses targeting overseas victims. These actions serve as a deterrent but also highlight the persistent nature of the problem (EFCC, 2016).

The Cross River State Government has also initiated the Digital Economy and E-Governance Initiative to bridge the digital divide and enhance governance through technology. In partnership with private firms, the state has developed digital platforms, such as mobile applications and web portals, to improve efficiency and transparency across government agencies. For example, the Cross River Pay Self-Service Portal allows residents to manage taxes online, streamlining administration and enhancing revenue

collection (Inakefe & Bassey, 2023). These initiatives aim to equip youths with legitimate digital skills and promote safe internet practices, reducing their vulnerability to cybercrime.

Role of Law Enforcement and Cybersecurity Agencies

In Cross River State, law enforcement and cybersecurity agencies are crucial for safeguarding the community from digital threats. They work together to investigate cybercrime, protect digital infrastructure, and educate the public. Despite facing significant challenges, their efforts are essential for mitigating the impact of cybercrime. The Nigerian Police Force (NPF), with specialized cybercrime units, plays a central role in responding to incidents of hacking, online fraud, and identity theft. For example, in 2020, the NPF apprehended a group of youths involved in internet fraud in Calabar, demonstrating growing efforts to combat cybercrime locally. The NPF collaborates with the EFCC, which has a mandate to investigate financial crimes. However, these agencies are often limited by a lack of resources and technical expertise (Omoniyi, 2020).

Cybersecurity agencies like the National Information Technology Development Agency (NITDA) focus on enhancing national cyber defenses. In Cross River, NITDA conducts training sessions for government institutions and private organizations to improve their ability to detect and respond to cyber threats. The Nigerian Communications Commission (NCC) works to ensure that internet service providers adhere to cybersecurity best practices. While the role of these agencies is vital, continued investment in resources, training, and inter-agency collaboration is needed to address the growing digital threats facing the state effectively.

CONCLUSION

The issue of youth engagement in cybercrime in Cross River State highlights the urgent need for effective interventions. The troubling rise in cybercrime activities poses significant risks to the state's economy, security, and development. The persistence of this issue despite existing laws points to the inadequacy of current strategies. Addressing cybercrime requires coordinated efforts from law enforcement agencies, community leaders, educational institutions, and the government. Key actions include strengthening legal frameworks, providing cyber education and awareness programs, offering alternative livelihood opportunities for youths, and promoting digital literacy. Empowering young people with the skills to thrive in legitimate sectors can reduce their involvement in cybercrime. A comprehensive, multi-stakeholder approach is essential for tackling this problem, ensuring a safer digital environment and a brighter future for the youths of Cross River State.

REFERENCES

Abdulrahman, M. (2022). *Cybersecurity challenges in Africa: Legislative and enforcement gaps*. Alpha Publications.

Adewale, T., & Olorunfemi, S. (2020). Digital crime and governance: The African experience. *Journal of Contemporary African Studies, 38*(3), 45-62.

Aghatise, J. (2020). The role of social media in cybercrime normalization among Nigerian youths. *African Journal of Cyber Ethics, 5*(2), 112-125.

Ajayi, A. (2020). *Youth delinquency and family dynamics in Nigeria*. Sunshine Press.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review, 3*(3), 193–209.
Chigad, J., & Madzinga, T. (2021). Cybersecurity threats and socio-economic challenges in developing nations. *Journal of Information Systems in Developing Countries, 5*(2), 1-15.
Economic and Financial Crimes Commission (EFCC). (2016). *Annual report*. EFCC.
Ekwutosi, O., & Eke, N. (2021). The role of information technology in enhancing national security in Nigeria, 2001-2020. *Pinisi Journal of Art, Humanity and Social Studies, 1*(1), 55-67.
Emmanuel, A., & Adedeji, T. (2013). Cybercrime and law enforcement in Nigeria: Challenges and opportunities. *International Journal of Cyber Criminology, 7*(1), 12-25.
Goodman, S., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Review of Law, Computers & Technology, 16*(1), 45-60.
Inakefe, G., & Bassey, V. (2023). Evaluation of the policy and institutional implications of digital tools in E-governance reforms implementation for service delivery in Cross River State Civil Service, Nigeria. *International Journal of Electronic Government Research, 4*(2), 1-18.
Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. John Wiley & Sons.
Odumesi, J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(2), 45-53.
Ojong, T. (2024, November 25). Personal interview [Personal interview].
Okonkwo, C. (2019). *Cybercrime and legal challenges in Nigeria: Enforcement and jurisdictional issues*. Legal Perspectives Press.
Oladipo, T., & Ogundele, K. (2021). Youth and cybercrime in Nigeria: Socio-economic implications. *African Journal of Criminology, 3*(2), 78-95.
Omoniyi, S. (2020). Law enforcement's role in combating cybercrime in Nigeria: A case study of the Nigerian Police. *Journal of Cybersecurity and Law, 7*(2), 34-50.
Onomrerhinor, F. A. (2023). Universal jurisdiction for transnational cybercrimes? *UCC Law Journal, 3*(1), 101-120.
Parker, D. (1984). *The many faces of data vulnerability*. Spectrum Books.
Samuel, O. N. (2025, January 4). Personal interview [Personal interview].
Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.