Economics, Business, Accounting & Society Review
Volume 3, Nomor 3, p. 208 – 216
ISSN 2810-0115

The Relationship Between Cybercrime and the Nigerian Economy: Causes, Implications and the Path Forward

Nathan Udoinyang[1], Reuben Daniel[2], Abroad E. David[3]

[1] *Ignatius Ajuru University of Education, Rumuolumeni, Nigeria*
[2,3] *College of Education Warri, Delta, Nigeria*
Corresponding Author: Nathan Udoinyang
Corresponding Email: nathannathanudoinyang@gmail.com

ARTICLE INFO
Article history:
Received 28 October 2024
Revised 20 November 2024
Accepted 27 November 2024
Available Online 03 December 2024

Keywords:
Cybercrime, Nigerian economy, Causes, Implications and Path forward.

Cite as:
Udoinyang, N., Daniel, R., & David, A. (2024). The Relationship Between Cybercrime and the Nigerian Economy: Causes, Implications and the Path Forward. Economics, Business, Accounting & Society Review, 3(3), 208–216. https://doi.org/10.55980/ebasr.v3i3.148

ABSTRACT
This study investigates the intricate relationship between cybercrime and Nigeria's economic landscape, focusing on its causes, implications, and potential mitigation pathways. Cybercrime has evolved into a systemic challenge in Nigeria, fueled by socio-economic disparities, institutional weaknesses, and behavioural tendencies, threatening financial stability and economic development. The primary objective of this research is to identify the dominant drivers of cybercrime and assess its economic consequences, with the goal of proposing collaborative strategies for mitigation. A survey-based quantitative approach was employed, targeting five major Nigerian banks—Access Bank, First Bank, GT Bank, UBA, and Zenith Bank—and academic institutions, including the University of Port Harcourt and Ignatius Ajuru University of Education. A structured questionnaire (C.N.E.C.I.P.F.) was administered to a randomly selected sample of 300 individuals, of which 260 valid responses (86.7%) were analyzed using descriptive statistics and percentage analysis, with a 50% aggregate agreement threshold. Findings reveal that unemployment, poor law enforcement, urbanization, and corruption are primary contributors to cybercrime. The economic implications include loss of revenue, business disruption, and decreased investor confidence. While cybercrime cannot be fully eradicated, the study emphasizes the potential for reduction through synergistic collaboration between government, businesses, and citizens. This research contributes to the growing body of literature on cybercrime by offering empirical insights specific to the Nigerian context and proposes an inclusive, multistakeholder framework for mitigating its socio-economic effects.

1. Introduction

The growth of the Internet and seamless access to computer-aided technology has created various opportunities for work and business activities, as well as for those taking advantage of the Internet revolution to engage in illegal activities (Aldridge, 2019; Marttila et al., 2021; Razaque et al., 2021).

The introduction of information communication technology and online communication has led to a dramatic increase in incidents as well as the emergence of new trends and patterns of Internet-enabled criminal activities (Brinck et al., 2023; Raza et al., 2024). However, the rise of the Internet in Nigeria has come with an unintended consequence: global notoriety as a haven for cybercrime. In the 90s, fraud in Nigerian society was popularly referred to as 419 in reference to the penal code that framed the criminal justice system in Nigeria. At the time, individuals arrested in connection with that law were labelled '419ers' (Bello & Griffiths, 2021). Then came the Internet, shortly after which a number of tech-savvy contrarians successfully exported the 419 concepts. While the popular 419 reference has been expanded to include cybercriminals, the name 'Yahoo-Yahoo' is the most familiar informal usage in Nigeria to refer to people who commit online (cybercrime) scams.

In the 1990s, the term 419 was popular in Nigeria to refer to advanced fraud, referring to an article of criminal law that prohibits the practice. With the advent of the Internet, this scheme evolved into cybercrime and became known as Yahoo-Yahoo, referring to the use of Yahoo emails to deceive victims through fake relationships, fictitious inheritances, or business offers (Akanle & Shadare, 2019; Soares et al., 2025). Another popular mode is phishing, where the perpetrator sends a fake email that looks official to steal personal data (Lyon, 2024). This crime is increasingly threatening, especially as the digitalization of banking increases, making cybercrime a serious obstacle to Nigeria's economic stability. In recent years, several empirical studies have highlighted that the level of public literacy and awareness of the risks of cybercrime has not been commensurate with the complexity of the threats faced by financial institutions and individuals (Ahmead et al., 2024; Lee & Chua, 2024).

Garba et al. (2023) emphasized that despite the rapid growth of digital banking services in Nigeria, the gap in public understanding of cybercrime risks remains high. This unpreparedness creates systemic vulnerabilities that can shake public confidence and threaten the stability of the national financial system. Furthermore, Akazue et al. (2022) identified that phishing attacks are the most common form of cybercrime among student smartphone users in various universities in Nigeria. These findings confirm that educational institutions are also the main targets of cyberattacks, so the potential disruption to the digital capacity building of the young generation is enormous, with long-term implications for the behaviour and resilience of the national economy. From a regulatory perspective, Nte et al. (2020) expose the weak governance of cybercrime in the higher education environment and the lack of effective law enforcement. This condition is the main inhibiting factor in mitigating the escalation of cybercrime. Therefore, the author recommends strengthening the legal framework and mainstreaming digital literacy in the education sector as an essential prevention strategy.

In the context of macroeconomics, research by Adeyemo et al. (2020) observed that the adoption of a cashless payment system by the Central Bank of Nigeria has actually posed new challenges, especially related to data security and digital transactions. Inadequate technological infrastructure increases exposure to cyberattacks, which in turn can weaken public trust in the banking system. In response to this challenge, Adebayo et al. (2022) offer innovative solutions through the development of cryptographic-based cybersecurity frameworks. This approach emphasizes the central role of technology in mitigating economic losses due to cybercrime, particularly in the financial sector. The model also shows the potential for adaptation in improving national digital resilience as a whole (Orbaningsih et al., 2022).

The increasing adoption of digital services in Nigeria, particularly in the banking and communications sectors, has not been accompanied by an adequate increase in cybersecurity literacy among the public. Garba (2023) suggests that this unpreparedness increases vulnerability to cybercrime and erodes trust in the financial system. This condition is exacerbated by socio-economic factors such as unemployment, poverty, and an instant mentality that encourages some individuals, especially young people, to engage in digital-based illegal activities. Akazue et al. (2022) and Nte et al. (2020) highlight that students and young graduates are easy targets for crimes such as phishing amid weak regulations and a lack of digital security education in educational institutions. Moreover, Okosun and Ilo (2023) trace the evolution of the "Nigerian prince scam" scam as part of a crime scheme rooted in the practice of 419, which has now evolved into a more complex and digital form.

In terms of law and policy, Abdulkadir and Abdulkadir (2019) highlighted the inconsistency between the implementation of the Nigerian Cybercrime Act and international human rights standards, which creates ambiguity in legal protection and enforcement effectiveness. This

challenge is further complicated by the presence of new technologies such as artificial intelligence, which, according to Kanu et al. (2024), requires a more adaptive ethical and legal framework in dealing with new forms of digital crime.

Conceptual Framework

The conceptual framework of this study is grounded in the integration of socio-economic, behavioural, and institutional factors that collectively explain the rise and persistence of cybercrime in Nigeria. Drawing from empirical findings and established criminological theories—such as Strain Theory, Routine Activity Theory, and Theory of Deterrence—the framework positions cybercrime not merely as a technological issue but as a multidimensional problem rooted in broader systemic conditions. At the core of the framework are three interrelated constructs: socio-economic pressure, institutional weakness, and individual behavioural orientation.

Socio-economic pressure encompasses factors such as high unemployment, poverty, and the pursuit of quick wealth. These conditions create psychological and economic strain, particularly among youth, which aligns with Merton's Strain Theory. Individuals facing limited legitimate means of success are more likely to turn to cybercrime as an alternative path (Okosun & Ilo, 2023).

Institutional weakness includes poor law enforcement capacity, lack of effective cybercrime regulation, and corruption. These gaps diminish deterrence, as outlined in the Theory of Deterrence, and increase the perceived impunity for cybercriminals (Abdulkadir & Abdulkadir, 2019).

Behavioural orientation captures the influence of negative role models, greed, gullibility, and what is locally referred to as "Abdulistic mentality" — a mindset favouring wealth acquisition without legitimate effort. This aligns with Routine Activity Theory, as unprotected digital environments and unaware victims offer ample opportunities for cybercrime (Nzeakor et al., 2020).

These constructs converge to shape the economic consequences of cybercrime, including operational disruptions, reputational damage, loss of revenue, and declining trust in the financial system. This framework offers a holistic lens through which policy responses can be designed, balancing economic empowerment, legal reform, digital literacy, and technological safeguards to combat cybercrime effectively in Nigeria's evolving digital landscape.

This research is of high urgency, considering that the ongoing digital transformation in Nigeria has not been accompanied by the readiness of communities and institutions to manage cybercrime risks. The impact is not only technical but also includes macroeconomic dimensions such as declining public trust in the banking system, disruption of digital business activities, and increasing operational costs due to the need for more sophisticated security systems. This research generally aims to explore the relationship between cybercrime and national economic conditions. This study will make a scientific and practical contribution to formulating public policy, the design of national digital security systems, and sustainable educational strategies. Specifically, this study explores (1) how socio-economic factors such as unemployment, poverty, and the desire to acquire instant wealth affect the increase in cybercrime rates in Nigeria. (2) To what extent do low cybersecurity literacy and weak law enforcement contribute to Nigerians' vulnerability to cyberattacks?

2. Methods

This study used a quantitative approach with a purposive research design. This approach was chosen to gain a systematic and measurable understanding of the impact of cybercrime on the Nigerian economy. A purposive design is used to ensure that the target population that has knowledge and experience relevant to the phenomenon being studied can be reached appropriately. The main focus of the research is on individuals who actively use computers, bank accounts, and the Internet in their daily lives, both for personal and professional interests.

The data in this study was collected through a survey method using a structured questionnaire designed by the researcher himself. The instrument is titled Cybercrime and the Nigeria Economy: Causes, Implications, and Path Forward (C.N.E.C.I.P.F.). The questionnaire was compiled to identify respondents' perceptions, experiences, and views regarding the causes, impacts, and solutions to cybercrime in Nigeria. The study population consisted of two main groups: (1) Customers and bank staff from five major banks in Nigeria, namely Access Bank, First Bank, GT Bank, UBA, and Zenith Bank; (2) Students and academic staff from the Bursary Department,

Computer Science Department, and Ignatius Ajuru University of Education, who are active users of information and communication technology. The random sampling technique is used to obtain a representative sample of the target population. A total of 300 copies of the questionnaire were distributed to the selected respondents, and 260 questionnaires were successfully returned and could be used for data analysis, which showed a response rate of 86.7%.

The data that had been collected from the questionnaire were analyzed using a quantitative descriptive analysis method through a basic percentage approach. Each response was compiled and calculated based on the frequency of occurrence to illustrate the patterns, tendencies, and distribution of respondents' answers related to the phenomenon of cybercrime. The results of this analysis are used to answer research questions and draw conclusions regarding the impact of cybercrime on the Nigerian economy, as well as provide strategic recommendations for countering it.

3. Results

Table 1 shows the causes of cybercrime in Nigeria. From the table above, it can be deduced that the majority of the respondents anonymously agreed to the causes of cybercrime in Nigeria, which constitutes an aggregate percentage of 76.5% to that of *Yes Respondents*, which is above the aggregate percentage criterion of 50% and also above the *No Respondents* of 23.5%.

Response of respondents of the causes of cybercrime in Nigeria.

Table 1. What are the causes of cybercrime in Nigeria?

S/N	Items	Option	Frequency	%	Decisions
1	Urbanization and civilization have led to an increase in cybercrime.	Yes No	175 85	67.3 32.7	Agreed
2	High rate of unemployment.	Yes No	257 3	98.8 1.2	Agreed
3	Quest for quick wealth at the expense of one's life.	Yes No	259 1	99.6 0.4	Agreed
4	Law enforcement organizations are not sufficiently equipped, and laws relating to cybercrime are not being appropriately enforced	Yes No	196 64	75.4 24.6	Agreed
5	Negative role model.	Yes No	177 83	68.1 31.9	Agreed
6	Corruption.	Yes No	239 21	91.9 8.1	Agreed
7	Gullibility/Greed.	Yes No	146 114	56.2 43.8	Agreed
8	Poverty.	Yes No	203 57	78.1 21.9	Agreed
9	Other concerns include the spread of cyber cafés and the open nature of the Internet**.**	Yes No	152 108	58.5 41.5	Agreed
10	Abdulistic mentality, i.e. the act of making money without working.	Yes No	186 74	71.5 28.5	Agreed
	Aggregate %			76.5/23.5	Agreed

Source: Authors Field Work, 2024.

Table 1 provides compelling evidence that cybercrime in Nigeria is driven by a multifaceted set of factors, as all ten listed items surpassed the 50% aggregate agreement threshold, with an overall agreement rate of 76.5%. This demonstrates a strong consensus among respondents that cybercrime is not the product of a singular cause but the outcome of a complex interplay between socio-economic pressures, institutional deficiencies, and individual behavioral tendencies.

From a socio-economic perspective, the most highly endorsed causes were the high rate of unemployment (98.8%) and the quest for quick wealth (99.6%). These results reflect widespread economic insecurity and a cultural shift toward materialism, particularly among youth who may view cybercrime as a pragmatic means of upward mobility. Additional factors such as poverty (78.1%) and the so-called "Abdulistic mentality" (71.5%)—a belief in acquiring wealth without legitimate labor—further illustrate how economic desperation and distorted social values fuel

engagement in digital crime. Institutional weaknesses also featured prominently, with inadequate enforcement of cybercrime laws and poorly equipped law enforcement agencies (75.4%) and rampant corruption (91.9%) identified as enabling factors. These findings indicate a systemic failure in governance and legal deterrence, creating an environment in which offenders perceive minimal risk of detection or punishment.

Behavioral and cultural dimensions were likewise significant. A notable proportion of respondents cited negative role models (68.1%) and gullibility and greed (56.2%) as drivers of cybercriminal behavior, suggesting that societal admiration of wealth—regardless of its origin—may be normalizing deviance. Furthermore, urbanization and modernization (67.3%), as well as the proliferation of cyber cafés and the open nature of the internet (58.5%), were viewed as technological enablers providing both opportunity and anonymity for offenders.

Table 1. above shows the causes of cybercrime in Nigeria. From Table 2. below it can be deduced that the majority of the respondents anonymously agreed to the causes of cybercrime in Nigeria, which constitutes an aggregate percentage of 84.8% to that of *Yes Respondents*, which is above the aggregate percentage criterion of 50% and also above the *No Respondents* of 15.2%.

Response of respondents to the implications of cybercrime in Nigeria.

Table 2. The implications of cybercrime in Nigeria's Economy

S/N	Items	Option	Frequency	%	Decisions
1	There has been an increase in the cost of operating a business as a result of the increase in the cost of protecting cybersecurity technology, insurance premiums and public relations support.	Yes No	242 18	93.1 6.9	Agreed
2	Disruption of business operation.	Yes No	226 34	86.9 13.1	Agreed
3	Altered business practices.	Yes No	209 51	80.4 19.6	Agreed
4	The reputational damage to the country's name.	Yes No	253 7	97.3 2.7	Agreed
5	Loss of revenue.	Yes No	248 12	95.4 4.6	Agreed
6	Loss of intellectual property.	Yes No	198 62	75.4 24.6	Agreed
7	Reduction in competitive edge.	Yes No	205 55	78.8 21.2	Agreed
8	Productivity losses and rising costs.	Yes No	191 69	73.5 26.5	Agreed
9	Retard financial inclusion.	Yes No	179 81	68.8 31.2	Agreed
10	Loss of confidence in the country's banking sector.	Yes No	243 17	93.5 6.5	Agreed
11	Monetary losses.	Yes No	234 26	90 10	Agreed
	Aggregate %			84.8/15.2	Agreed

Source: Authors Field Work, 2024.

4. Discussion

Causes of Cybercrime in Nigeria

The findings from this study confirm that a complex interplay of socio-economic pressures, institutional weaknesses, and individual behavioural tendencies fuels cybercrime in Nigeria. Cybercrime thrives in a landscape filled with socio-economic pressures, weak institutions, and individual mindsets distorted by the glorification of instant wealth.

First, socio-economic pressures such as high unemployment, poverty, and limited social mobility have been the main triggers for the emergence of digital deviant behaviour. In this context, many young generations see cybercrime as an alternative to achieving better economic status. As expressed by Nzeakor et al. (2022), The imbalance between economic expectations and the realities of life creates vulnerabilities that are exploited by cybercriminals, especially among students and young internet users whose digital literacy is still low. Second, institutional weakness is a significant aspect in explaining the weak deterrence of the State's against cybercrime. Inconsistent law enforcement, limited capacity of digital security agencies, and regulations that are not adaptive to cyber dynamics create a grey space that actually strengthens the cybercrime ecosystem (Opasina, 2016). Third, psychosocial aspects and individual behaviour play a major role in normalizing cybercrime in public spaces. The phenomenon of Yahoo Boys, as a representation of cybercriminals in Nigeria, is often seen not as a crime but as a symbol of resistance to structural injustice (Ojolo & Singh, 2023). A study by Lazarus, Button, & Adogame (2022) shows that public perception comparing Yahoo Boys to corrupt politicians ("Yahoo Men") on social media, actually creates a moral justification for these illegal actions.

Among the most prominent causes identified are unemployment (98.8%), poverty (78.1%), and the desire for quick wealth (99.6%). These results support the Strain Theory, which posits that individuals under socio-economic stress may resort to deviant behaviour to achieve culturally valued goals. In the Nigerian context, limited access to formal employment opportunities pushes many—particularly youth—to engage in illicit digital activities as a coping mechanism (Okosun & Ilo, 2023).

Another critical factor is the inadequacy of legal and institutional structures. Respondents indicated strong agreement (75.4%) that poor enforcement of cybercrime laws and insufficient capacity of law enforcement agencies significantly contribute to the rise in cybercrime. This aligns with the Theory of Deterrence, which asserts that crime thrives when sanctions are either weak, uncertain, or poorly executed (Abdulkadir & Abdulkadir, 2019). The perception that cybercriminals can act with impunity further emboldens their actions.

Behavioural and cultural factors also play a substantial role. The influence of negative role models, widespread greed, and what respondents termed the "Abdulistic mentality"—the desire to make money without working—represent a value shift toward materialism over legitimate labour. These findings are well-explained by the Routine Activity Theory, which emphasizes the convergence of motivated offenders, suitable targets, and the absence of capable guardians (Nzeakor et al., 2020). Cyber cafés and the open nature of the Internet, cited by 58.5% of respondents, serve as accessible platforms for committing cybercrime with little oversight.

Implications of Cybercrime

The implications of cybercrime in Nigeria are extensive and deeply damaging to both economic stability and national reputation. The most immediate consequence, cited by 93.1% of respondents, is the increase in operational costs for businesses, especially in terms of investments in cybersecurity infrastructure (Atkins & Lawson, 2021), insurance, and crisis management. The continuous escalation of cybersecurity expenses diverts resources from core business activities and undermines productivity (Chowdhury & Gkioulos, 2021).

Moreover, disruption of business operations (86.9%), loss of revenue (95.4%), and loss of intellectual property (75.4%) reflect the vulnerability of Nigerian firms to cyberattacks. These impacts are not limited to the private sector; they erode public trust in digital systems and challenge broader financial inclusion initiatives. Nearly 93.5% of respondents agreed that cybercrime significantly undermines confidence in the banking sector (Khan et al., 2023; Riaz et al., 2024), deterring citizens from participating fully in the formal economy and digital payment systems. 97.3% of respondents noted that reputational damage has international ramifications. Nigeria's global image as a hub for cybercrime, especially associated with scams such as the "Nigerian Prince" fraud, not only deters foreign investment but also complicates international partnerships in technology and finance (Okosun & Ilo, 2023). This reputational loss creates a cycle of mistrust (van

Kersbergen & Tinggaard Svendsen, 2024) that extends beyond borders and undermines digital diplomacy.

5. Conclusion

This study reveals that cybercrime in Nigeria is a complex phenomenon influenced by socio-economic pressures, institutional weaknesses, and the orientation of individual behaviour. Based on the findings of the study, the main causes of cybercrime include high levels of unemployment, poverty, the impulse to acquire instant wealth, and weak enforcement of cyber laws and regulations. In addition, cultural factors such as the influence of negative role models, greed, and an "Abdulistic" mentality are also drivers of deviant behaviour in the digital space. The implications of cybercrime are broad and include increased business operating costs, financial and reputational losses, as well as decreased trust in the national financial system, especially the banking sector. This research shows that cybercrime not only has a technical impact but also has strategic consequences on the development of the digital economy and financial inclusion in Nigeria. The main contribution of this research is to present empirically and understand the root causes and economic impacts of cybercrime more comprehensively. With this approach, the research not only sheds light on the individual behaviour of perpetrators but also highlights the role of the social and institutional environment in strengthening the cybercrime ecosystem. As for the next direction of research, longitudinal and comparative studies across regions are recommended to evaluate the effectiveness of cyber policy interventions at the local and national levels. In addition, further research can explore the role of digital literacy and community participation in building community-based cyber resilience. This quantitative research can also be extended with a qualitative approach to delve deeper into the personal motivations and social dynamics that drive criminal behaviour in the digital space.

6. References

Abdulkadir, A. B., & Abdulkadir, A. O. (2019). Cybercrimes Act in Nigeria: Experimenting Compliance with Internationally Recognized Human Rights Provisions. *Journal of International Studies(Malaysia)*, *15*, 117–132. https://doi.org/10.32890/jis2019.15.8

Adebayo, O. S., Micah, J. B., Olusegun, G. S., Alabi, I. O., & Abdulazeez, L. (2022). Development of Secure Electronic Cybercrime Cases Database System for the Judiciary. *International Journal of Information Engineering and Electronic Business*, *14*(1), 1–16. https://doi.org/10.5815/ijieeb.2022.01.01

Adeyemo, K. A., Isiavwe, D., Adetula, D., Olamide, O., & Folashade, O. (2020). Mandatory adoption of the Central Bank of Nigeria's cashless and e-payment policy: Implications for bank customers. *Banks and Bank Systems*, *15*(2), 243–253. https://doi.org/10.21511/bbs.15(2).2020.21

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science*, *13*(1), 29. https://doi.org/10.1186/s40163-024-00230-w

Akanle, O., & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, characterization and strategies. *International Journal of Cyber Criminology*, *13*(2), 343–357. https://doi.org/10.5281/zenodo.3706618

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1756–1765. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Aldridge, J. (2019). Does online anonymity boost illegal market trading? *Media, Culture & Society*, *41*(4), 578–583. https://doi.org/10.1177/0163443719842075

Atkins, S., & Lawson, C. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5), 847–861. https://doi.org/10.1111/puar.13322

Bello, M., & Griffiths, M. (2021). Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies? In *Rethinking Cybercrime* (pp. 213–235).

Springer International Publishing. https://doi.org/10.1007/978-3-030-55841-3_11

Brinck, J., Nodeland, B., & Belshaw, S. (2023). The "Yelp-Ification" of the Dark Web: An Exploration of the Use of Consumer Feedback in Dark Web Markets. *Journal of Contemporary Criminal Justice*, *39*(2), 185–200. https://doi.org/10.1177/10439862231157519

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information & Computer Security*, *29*(5), 697–723. https://doi.org/10.1108/ICS-07-2020-0121

Garba, J. (2023). An Approach To Cybercrime Issues In Dandume Local Government Area Of Katsina State, Nigeria. *Nigerian Journal of Technology*, *42*(2), 249–256. https://doi.org/10.4314/njt.v42i2.13

Garba, J., Kaur, J., & Ibrahim, E. N. M. (2023). Awareness Of Cybercrime Among Online Banking Users In Nigeria. *Nigerian Journal of Technology*, *42*(3), 406–413. https://doi.org/10.4314/njt.v42i3.14

Kanu, I. A., Adidi, D. T., & Kanu, C. C. (2024). Artificial Intelligence And Cybercrime In Nigeria: Towards An Ethical Framework. *Dialogue and Universalism*, *34*(1), 207–221. https://doi.org/10.5840/du202434115

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis. *IEEE Access*, *11*, 80181–80198. https://doi.org/10.1109/ACCESS.2023.3298824

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). https://doi.org/10.1016/j.heliyon.2022.e11142

Lee, C. S., & Chua, Y. T. (2024). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093

Lyon, G. (2024). Informational inequality: the role of resources and attributes in information security awareness. *Information & Computer Security*, *32*(2), 197–217. https://doi.org/10.1108/ICS-04-2023-0063

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. *American Journal of Criminal Justice*, *46*(6), 862–881. https://doi.org/10.1007/s12103-021-09665-2

Nte, N. D., Esq, U. K., Enokie, B. K., & Bienose, O. (2020). Cyber Crime Management Among Students; An Evaluation of Legal Correlates of Cyber Crime Management among Tertiary Institutions Students in Nigeria (A Case Study of Delta State). *Journal of Indonesian Legal Studies*, *5*(2), 295–334. https://doi.org/10.15294/jils.v5i2.34005

Nzeakor, O. F., Nwokeoma, B. N., & Ezeh, P.-J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology*, *14*(1), 283–299. https://doi.org/10.5281/zenodo.3753223

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(3), 41–67. https://doi.org/10.52306/2578-3289.1098

Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, *6*(1), 55–77. https://doi.org/10.31920/2516-2713/2023/6n1a4

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

Opasina, O. K. (2016). The interplay between fragility and crime in African states: a case study of Nigeria and Côte d'Ivoire. *International Social Science Journal*, *66*(221–222), 285–301. https://doi.org/10.1111/issj.12126

Orbaningsih, D., Gitaria, M., & Gendut Budi, W. (2022). Innovation of Electronic-Based Multipurpose Credit Services to Improve Customer Satisfaction Through Loan Fee : A Study on Bank Jatim - Malang. *Economics, Business, Accounting & Society Review*, *1*(1), 49–57.

https://doi.org/10.55980/ebasr.v1i1.6

Raza, A., Hussain, M., Tahir, H., Zeeshan, M., Raja, M. A., & Jung, K.-H. (2024). Forensic analysis of web browsers lifecycle: A case study. *Journal of Information Security and Applications*, *85*, 103839. https://doi.org/10.1016/j.jisa.2024.103839

Razaque, A., Al Ajlan, A., Melaoune, N., Alotaibi, M., Alotaibi, B., Dias, I., Oad, A., Hariri, S., & Zhao, C. (2021). Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System. *Applied Sciences*, *11*(17), 7880. https://doi.org/10.3390/app11177880

Riaz, A., Ramay, S. A., Abbas, F., Hussain, A., Naveed, N., & Abbas, T. (2024). Analyzing the Impact of Cybercrime and Its Security in Banking Sectors of Pakistan by Using Data Mining. *Journal of Computing & Biomedical Informatics*, *08*(01). https://doi.org/10.56979/801/2024

Soares, A. B., Lazarus, S., & Button, M. (2025). Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud. *Deviant Behavior*. https://doi.org/10.1080/01639625.2025.2482824

van Kersbergen, K., & Tinggaard Svendsen, G. (2024). Social trust and public digitalization. *AI & SOCIETY*, *39*(3), 1201–1212. https://doi.org/10.1007/s00146-022-01570-4