



## Examination of Cyber Fraud and Business Development in Abuja-Nigeria 2015-2024

BATURE Sunday Ali<sup>1</sup>, Prof. UMAR Shehu Usman<sup>2</sup> &, Mohammed Ayuba Oche<sup>3</sup>

*Institute of Governance and Development Studies, Nasarawa State University, Keffi<sup>1</sup>, Department of Political Science, Nasarawa State University, Keffi<sup>2</sup>, Department of Sociology, Federal University, Lafia, Nasarawa State<sup>3</sup>*

Date of Submission: 14-02-2026

Date of Acceptance: 27-02-2026

### Abstract

This paper examined the trend of cyber fraud in Abuja-Nigeria 2015-2024: challenges and security implications. The study adopted the survey research design, the study population was 1,699,701 people, a sample size of 378 respondents was adopted using the Krejcie Morgan's formula. Multi-stage sampling technique was used. Questionnaire the major instrument of data collection. The quantitative data collected using the questionnaire instrument was analysed using descriptive statistics. It also revealed that the study revealed that the majority of the respondents perceived cyber fraud have significantly disrupts business operations, undermines investor confidence, and increases operational costs in Abuja. This finding agrees with Mohammed, Ali, and Abiodun (2024), Okoli (2023) and Uzoamaka (2023) in their respective studies on internet fraud among secondary school students in Bayelsa State. The study revealed that cybercrime incidents are relatively frequent and have become a noticeable part of the digital experience for a significant portion of the population. It reflects a consistent exposure to cyber threats and may highlight inadequate preventive measures. This result clearly shows that most respondents perceive a rising trend in cyber fraud incidents, suggesting an escalation in cybercrime activities in Abuja over the last five years. Government and concerned stakeholders should build on existing efforts to address the sociological challenges like unemployment influencing youth into cyber fraud in Abuja-Nigeria. It also recommends that the banking sector should engage cyber experts in Abuja to train business owners and corporations on how to detect cyber fraud during business transactions and to empower them to be extra vigilant to the activities of fraudsters in and around their business facilities in Abuja.

**Keywords:** Cyber, fraud, Business, Development

### I. Introduction

Over the last decade, the global community has been rapidly transformed, largely due to advancements in technical infrastructure, particularly the Internet. This digital revolution has facilitated seamless communication, information sharing, and business transactions across borders, leading to high interconnectedness and interdependence among nations, individuals, and businesses (Alao, Osah, & Eteete, 2019). The electronic market is now open to everybody, including criminals. It was projected that by 2020, global Cyber security spending will reach \$170bn, a 126% increase from \$75bn in 2015. According to the World Economic Forum's report Globalization 4.0, "More organizations than ever are conducting business online" (Broeders, 2021). However, alongside these benefits, the rise of the Internet has also introduced significant security challenges, one of the most concerning being cyber fraud. Cyber fraud involves illegal activities such as identity theft, hacking, online scams, and financial fraud perpetrated digitally. It is a subset of cybercrime that specifically targets economic systems, causing substantial financial harm to individuals, organizations, and nations.

The growing prevalence of cyber fraud has far-reaching implications, particularly on the economic security of nations. In recent years, the sophistication of cybercriminals has escalated, with many perpetrators leveraging advanced digital technologies to commit fraud, bypass security measures, and exploit vulnerabilities without the need for physical presence. This has raised serious concerns about the safety of financial systems and the ability of governments and institutions to protect their citizens' economic interests (Yakubu, 2017). Globally, cyber fraud has resulted in billions of dollars in financial losses, severely impacting businesses and governments alike. In response, nations are making significant efforts to fortify their cybersecurity systems, recognizing that unchecked cyber fraud can destabilize economies, destroy



critical infrastructures, and lead to substantial losses in national revenue (Fischer, 2009; Babayo et al., 2021).

Nigeria, as the most populous country in Africa, is particularly vulnerable to cyber fraud. With over 200 million people and a rapidly growing digital economy, the country has witnessed a surge in cybercriminal activities that directly threaten its economic security. The proliferation of internet in Nigeria has indeed come with unintended consequence, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. Nigeria is ranked among the top countries in the world for internet fraud, which has contributed to massive financial losses and a significant loss of investor confidence (Federal Bureau of Investigation, 2022). While the above is true, literature on the trends and pattern of cyber fraud is still scanty in Abuja. It is against the background of the foregoing that this study has examined the pattern and trend of cyber fraud in Abuja.

### **1.1 Statement of the Problem**

Cyber fraud in Abuja and Nigeria presents a significant and persistent threat to national economic development drive, primarily due to its transnational implications on growth and development of the Nigeria economy. For several years now, scammers in Abuja have continued to skillfully operate across borders taking advantage of legal and jurisdictional gaps that complicate prosecution and enforcement laws prohibiting cyber fraud especially Urbanized areas like AMAC, Bwari and Gwagwalada. This creates a fertile ground for fraudsters to perpetuate their schemes with relative impunity. In spite of the implementation of various countermeasures, including international cooperation between law enforcement agencies, public awareness campaigns, and legislative initiatives aimed at enhancing cybersecurity and financial regulations in Nigeria and Abuja in particular, these efforts are often undermined by the scammers' continuous adaptation and sophistication in their modus operandi. The fraudsters operating syndicate cells around AMAC, Bwari and Gwagwalada constantly evolve in their methods to exploit new vulnerabilities and obscure their identities, making it challenging to track and apprehend them by the constituted authorities.

Conspicuously, government have tasked several federal and state security agencies like the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and other related Crime, the Nigerian Police, Nigerian

Immigration Service, and the other informal local security networks to be vigilant and crackdown on cells of cyber criminals operating within the FCT (Ajani, 2025).

In spite of the above actions, in 2014 business owners lost a staggering sum of N 6.1 billion naira to fraudsters with 1,461 reported cases, the Federal Bureau of Investigation (FBI) reported 14,607 victims of advanced fee scams in 2019 with losses exceeding \$3.5 Billion. The Nigerian Inter Bank Settlement System (NIBSS) reported a surge of 1,461 fraud cases from 2015 to 2017. However, reports indicate a significant increase of cyber fraud in 2024 with notable increase in the amount involved and lost. The FITC fraud and Forgery Report for Q3 2024 shows a 65% jump in fraud cases reported by Nigerian Banks in both Abuja and Lagos. Also, EFCC has a record breaking 4,111 convictions in 2024 and recovered over N365.4 billion. Banks lost N53.4 billion naira to fraud in the first nine months of 2024 compared to N9.4 billion naira in 2023. According to Arise News report (10th March, 2025), the EFCC has made a recovery of 364.6 billion naira, \$214.5 million dollars, £54,318.64 pounds, €31,265, CAD \$2,990 and AUD \$740 all in 2024 respectively.

Consequently, the economic impact of cyber fraud has continued to grow, causing substantial financial losses and undermining trust in digital and financial systems across Lagos State. For instance, many businesses outlets do not accept wired transfer of money when purchases are made, this is owing to the prevalence of fake credit alerts, misrepresentation of figures and arbitrary debiting of business fund from unsuspecting business owners. Thus, the banking industry has made the matter even worse, business funds are not safe in the banks, people's money are being wired to different accounts and the legal framework for investigating such actions are complicated in Nigeria leaving victims to suffer without proper investigations (Ajani, 2025). These actions have made business and economic activities complex in the Abuja because people cannot access cash and many business owners are reluctant to accept transfer consequently, this has continued to affect the economic growth and development in Abuja.

### **1.2 Objectives of the study**

The main objective of the study is to examine the cyber fraud and Business development in Abuja-Nigeria 2015-2024. The specific objectives are to:

- i. Ascertain the prevalence type of cyber fraud trending in Abuja
- ii. Examine the role of unemployment on cyber fraud in Abuja



iii. Determine the impact of cyber fraud on business environment in Abuja

## II. Methodology

This paper examined the trend of cyber fraud in Abuja-Nigeria 2015-2024: challenges and security implications. The study

adopted the survey research design, the study population was 1,699,701 people, a sample size of 378 respondents was adopted using the Krejcie Morgan's formula. Questionnaire the major instrument of data collection. The quantitative data collected using the questionnaire instrument was analysed using descriptive statistics.

## III. Data Presentation and Analysis

### Demographical Data of the Respondents

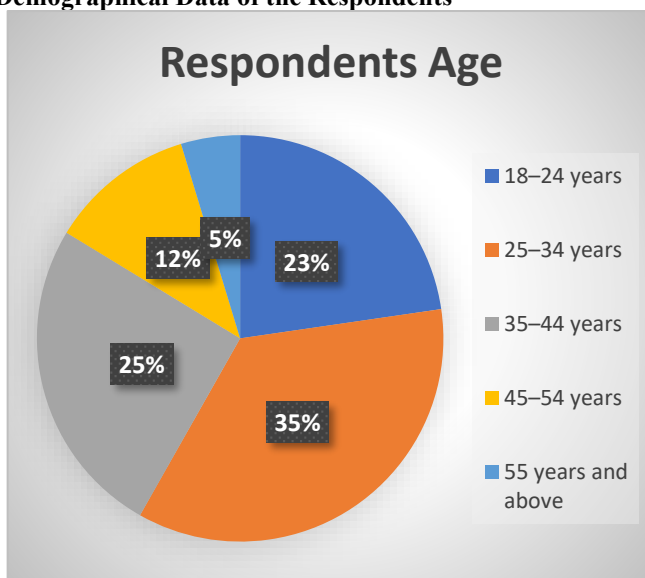


Figure 1

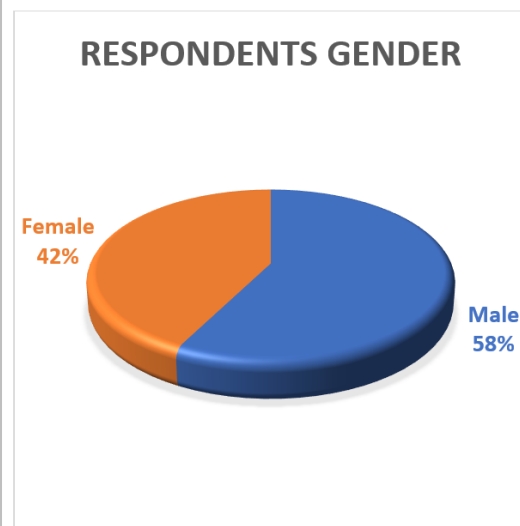


Figure: 2

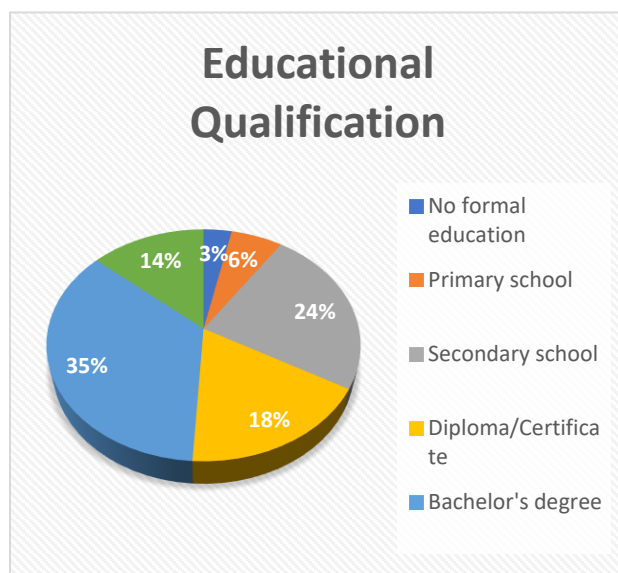


Figure: 3

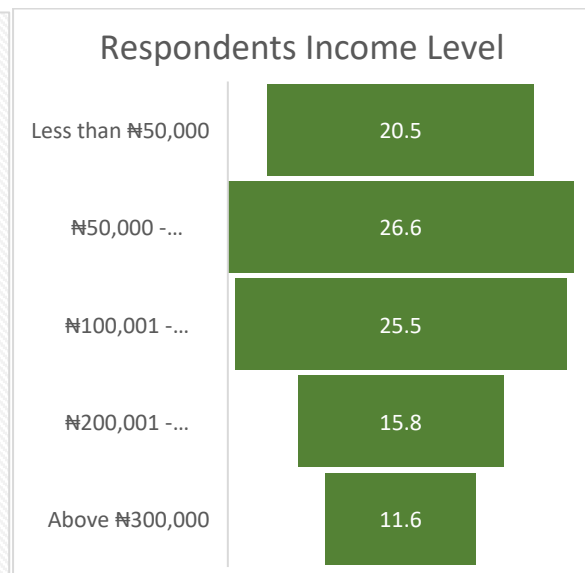


Figure: 4



Figure 1, indicated that majority of the respondents (35%) were within the age bracket of 25- 34 year of age, figure 2: shows that male (58%) respondents are the dominant gender in the study, the study further indicated that figure 3 indicated that majority of the respondents had diploma and other certificates basically. While figure: 4 revealed that majority of the respondents (26.6%)received #50,000 to #100, 000 as monthly income.

**Table 2: Responses on the frequency of cyber fraud incidence in Abuja**

Response	Frequency	Percentage (%)
Very often	98	27.1%
Often	112	31.0%
Occasionally	93	25.8%
Rarely	42	11.6%
Never	16	4.4%
Total	361	100

Source: Field Survey, 2025

Table 2: indicated that the highest percentage, 31.0% (112 respondents), indicates that many respondents believe cyber fraud occurs often in Abuja. This suggests that cybercrime incidents are relatively frequent and have become a noticeable part of the

digital experience for a significant portion of the population. It reflects a consistent exposure to cyber threats and may highlight inadequate preventive measures.

**Table 3: Responses on whether the rate of cyber fraud in Abuja increased in the past five years**

Response	Frequency	Percentage (%)
Strongly agree	134	37.1%
Agree	121	33.5%
Neutral	54	15.0%
Disagree	38	10.5%
Strongly disagree	14	3.9%
Total	361	100

Source: Field Survey, 2025

Table 4.4 presents respondents' perceptions of whether the rate of cyber fraud in Abuja has increased over the past five years. Out of the 361 respondents, the majority strongly agree (134 respondents; 37.1%) and agree (121 respondents; 33.5%), accounting for

a combined 70.6% who believe that cyber fraud has increased during this period This result clearly shows that most respondents perceive a rising trend in cyber fraud incidents, suggesting an escalation in cybercrime activities in Abuja over the last five years.

**Table 1: Respondents responses on whether they have ever been a victim of cyber fraud**

Response	Frequency	Percentage (%)
Yes	204	56.5%
No	157	43.5%
Total	361	100

Source: Field Survey, 2025

Table 1: indicated that the highest proportion of victims (56.5%) suggests that cyber fraud is a serious and growing concern, with significant implications for individuals' financial security, data safety, and overall trust in digital

transactions. On the other hand, the 43.5% who have not experienced cyber fraud may reflect differences in exposure levels, use of preventive measures, or varying awareness of cybersecurity practices.

**Table 4.5 Responses on type of cyber fraud ever encountered or heard of the most.**

Type of Cyber Fraud	Frequency	Percentage (%)
Phishing	104	28.8%
Identity theft	72	19.9%



Online scams (e.g., fake lotteries, job offers)	98	27.1%
Unauthorized access to financial accounts	57	15.8%
Others	30	8.3%
Total	361	100

Source: Field Survey, 2025

Table 4.5 shows the types of cyber fraud that respondents have either experienced or heard of the most in Abuja. Out of 361 respondents, the most reported types were phishing (104 respondents; 28.8%) and online scams such as fake lotteries and job offers (98 respondents; 27.1%), followed by

identity theft (72 respondents; 19.9%). Thus, the findings shows that phishing and online scams are the most prevalent forms of cyber fraud in Abuja, together accounting for 55.9% of reported cases. Identity theft also appears as a significant threat, affecting nearly one-fifth of the respondents.

Table 4.6 Respondents views whether unemployment contributes to the rise of cyber fraud in Abuja

Response	Frequency	Percentage (%)
Strongly agree	141	39.1%
Agree	128	35.5%
Neutral	42	11.6%
Disagree	33	9.1%
Strongly disagree	17	4.7%
Total	361	100%

Source: Field Survey, 2025

The analysis revealed that a significant proportion of respondents (33.8% strongly agree and 37.1% agree) believe that the level of internet literacy in Abuja contributes to the persistence of cyber fraud (Table 4.7). This represents a cumulative 70.9% of the respondents, indicating a strong perception that internet literacy plays a pivotal role. The reasoning

behind this could be twofold. On one hand, higher internet literacy may empower individuals to exploit digital systems maliciously, thereby fostering cyber fraud. On the other hand, low or insufficient literacy among some segments creates vulnerabilities that cybercriminals exploit, particularly through phishing, identity theft, and social engineering schemes.

Table 4.12 Respondents view on whether cyber fraud negatively impacts the business environment in Abuja.

Response	Frequency	Percentage (%)
Strongly agree	142	39.3%
Agree	131	36.3%
Neutral	54	15.0%
Disagree	23	6.4%
Strongly disagree	11	3.0%
Total	361	100%

Source: Field Survey, 2025

The findings in Table 4.12 reveal that a significant majority of respondents believe cyber fraud negatively impacts the business environment in Abuja. Specifically, 142 respondents (39.3%) strongly agreed, and 131 respondents (36.3%) agreed, representing a combined 75.6% who affirm this negative impact this distribution suggests a dominant perception among the respondents that cyber fraud significantly disrupts business operations, undermines investor confidence, and increases operational costs in Abuja.

#### IV. Discussion of Findings

The study revealed that cybercrime incidents are relatively frequent and have become a noticeable part of the digital experience for a significant portion of the population. It reflects a consistent exposure to cyber threats and may highlight inadequate preventive measures. This result clearly shows that most respondents perceive a rising trend in cyber fraud incidents, suggesting an escalation in cybercrime activities in Abuja over the last five years. This finding supports the findings of Ekpe (2023), Uji (2024) and Ajani (2025) in their



respective studies on cyber fraud in Lagos, Imo and Kwara State.

The study revealed that phishing and online scams are the most prevalent forms of cyber fraud in Abuja, together accounting for 55.9% of reported cases. Identity theft also appears as a significant threat, affecting nearly one-fifth of the respondents. This finding corroborates the studies conducted by Shawulu (2022), Anu-Okeke, (2024) and Ishaya (2024) on the prevalence of online fraud on unsuspecting residents in Karu area of Nasarawa State.

The study revealed that the majority of the respondents perceived cyber fraud have significantly disrupts business operations, undermines investor confidence, and increases operational costs in Abuja. This finding agrees with Mohammed, Ali, and Abiodun (2024), Okoli (2023) and Uzoamaka (2023) in their respective studies on internet fraud among secondary school students in Bayelsa State.

## V. Recommendations

The following recommendations was made to guide the findings:

- i. Government and concerned stakeholders should build on existing efforts to address the sociological challenges like unemployment influencing youth into cyber fraud in Abuja-Nigeria.
- ii. The punitive sanctions on identity theft particularly phishing should increase and youths involved should be forced to learn technical skills to enable them cope with the economic realities of Abuja.
- iii. The banking sector should engage cyber experts in Abuja to train business owners and corporations on how to detect cyber fraud during business transactions and to empower them to be extra vigilant to the activities of fraudsters in and around their business facilities in Abuja.

## References

- [1]. Abubakari, Y. (2021): The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: a review. *Social Space Journal* pp 137-176
- [2]. Adeniyi, I.A. (2021). Cyber Security in Nigeria: Appraising Cybercrime, the Existing Legal Framework, the Challenges and the Way Forward. *SSRN Electronic Journal*. doi:<https://doi.org/10.2139/ssrn.3991151>.
- [3]. Ajoke, O. Z. (2014): Impact of Economic and Financial Crime Commission on the Economic Development of Nigeria. Bachelor's Thesis (Turku University of Applied Science) Degree Program in International Business International Business Management 2014
- [4]. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, 27, 945-958.
- [5]. Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, 4(8), 1-19.
- [6]. Alao, D., Osah, G. and Eteete, A. (2019). Unabated Cyber Terrorism and Human Security in Nigeria. *Asian Social Science*, 15. doi:<https://doi.org/10.5539/ass.v15n11p105>.
- [7]. Amughoro, O. A. & Ijeoma, N. (2022): Advanced Fee Fraud, Money Laundering Controls and Economic Performance in Nigeria. *International Journal of Advances in Engineering and Management (IJAEM)* Volume 4, Issue 1 Jan 2022, pp: 719-728 www.ijaem.net ISSN: 2395-5252. DOI: 10.35629/5252-0401719728
- [8]. Babayo, S., Muhammad, Y., Usman, S. and Bakri, M. (2021). Cyber security and Cybercrime in Nigeria: the Implications on National Security and Digital Economy. 4(1), 27-61
- [9]. Bello, M. (2018). *Investigating Cybercriminals in Nigeria: a Comparative Study*. [online]
- [10]. 1library.net. Available at: <https://1library.net/document/y9mlr4jqinvestigating-cybercriminals-in-nigeria-a-comparative-study.html>.
- [11]. Bhasin, M. L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. *Ecoforum Journal*, 5(2). <http://www.ecoforumjournal.ro/index.php/eco/article/view/412>
- [12]. Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line?. *Journal of Cybersecurity*, 7(1), tyab010.



- [13]. Button, M. Tapley, J. and Lewis, C. (2012). The fraud justice network and the infra-Structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, 13 (1), 37-61.
- [14]. Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of Information Law and Technology*.  
[http://go.warwick.ac.uk./jilt/2009\\_/chawki](http://go.warwick.ac.uk./jilt/2009_/chawki)
- [15]. Chigozie-Okwum, C., Ugboaja, S., Micheal, D., & Osuo-Genseleke, M. (2017).
- [16]. Proliferation of cyber insecurity in Nigeria: a root cause analysis. *AFRREV STECH: An International Journal of Science and Technology*, 6(2), 53-60.  
<https://www.ajol.info/index.php/stech/article/view/161143>
- [17]. Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588 - 608.
- [18]. Drammeh, F. (2023): Trust and Fraud in Nigeria: A Comprehensive Analysis of Socioeconomic Factors and Regulatory Measures (June 10, 2023). Available at SSRN: <https://ssrn.com/abstract=4475135> or <http://dx.doi.org/10.2139/ssrn.4475135>
- [19]. Dzumira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16-26.
- [20]. Ebem, D.U., Onyeagba, J.C. & Ugwuonah, G.E. (2017). Internet Banking: Identity Theft and Solutions -The Nigerian Perspective. *Journal of Internet Banking and Commerce*, 2 2(2), 1-15.
- [21]. Efiog, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal*, 3(3).
- [22]. Glickman, H. (2005). The Nigerian "419" Advance Fee Scams: Prank or Peril? *Canadian Journal of African Studies / Revue Canadienne Des Études Africaines*, 39(3), 460-489.  
<https://doi.org/10.1080/00083968.2005.10751326>
- [23]. Grigoreva E., Fesina E., (2013). Economic Security as a Condition of Institutional Support of Economy Modernization. *World Applied Sciences Journal*, vol. 31, no. 5, pp. 940-948.
- [24]. Guariniello, C., and DeLaurentis, D., (2014). Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. *Procedia Computer Science*, 28, pp. 720-727.
- [25]. Hassan, A.B., Lass, F.D. and Makinde, J., (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, 2(7), pp.626- 631.
- [26]. Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, 1(1), 137-154.
- [27]. Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behaviour*, 35: 1, 20-40. DOI: 10.1080/01639625.2013.822209
- [28]. Hunton, P., (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), pp. 528-535.
- [29]. Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. In *2016 IEEE International Conference on cybercrime and computer forensic (ICCCF)* (pp. 1-9). IEEE. <https://ieeexplore.ieee.org/abstract/document/7740439/>
- [30]. Idowu, O.A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. 3(1), 1-12.
- [31]. Igwe, C. N. (2011) Socio-economic developments and the rise of 419 Advance-Fee Fraud in Nigeria. *European Journal of Social Sciences* March 2011 20(1):184-193.
- [32]. Ismagilov I.I., (2012). Strategic management of enterprise development in the conditions of formation of the network economy. *Kazan economic bulletin*, vol. 1, pp. 16-18.
- [33]. Lamensch, M. And Ceci, E. (2018): VAT fraud Economic impact, challenges and policy issues Policy Department for Economic, Scientific and Quality of Life Policies



- Directorate-General for Internal Policies: PE 626.076 – October 2018 EN STUDY R
- [34]. Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behaviour*, 126, 106979. doi:10.1016/j.chb.2021.106979
- [35]. Litvinenko A.N., (2013). Economic and national security: the problem of concepts correlating Scientific and technical statements, S.-Petersburg State Polytechnic University, *Economic sciences*, № 3 (173), pp. 9-15.
- [36]. Makeri, Y.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), pp.315–321. doi:https://doi.org/10.23956/ijarcsse/v6i12/01204.
- [37]. Molokwu , A. N. . (2022). Socioeconomic Predictors of Cybercrime among Nigerian Youths in Ibadan Metropolis. *Turkish International Journal of Special Education and Guidance & Counselling ISSN: 1300-7432*, 11(1), 61–68. Retrieved from https://www.tijseg.org/index.php/tijseg/article/view/167
- [38]. Nigeria Criminal Code, (2004), Federal Republic of Nigeria. Nissenbaum, H., (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, pp. 61-73.
- [39]. Ogham S. C. (2023): Scrutiny of the Legal and Regulatory Framework of e-commerce in Nigeria. *Nigerian Bar Journal*. Ajol-file-journals\_693\_articles\_254146\_64
- [40]. Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2020). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, 14(2), 460-478. https://search.proquest.com/openview/dc68d59c9f55b14f96e5d089123de874/1?pq-origsite=gscholar&cbl=55114
- [41]. Olowu, D. (2009). Cyber-Crimes and the boundaries of domestic legal responses: case for aAn inclusionary framework for Africa. *Journal of Information, Law & Technology*, 1.
- [42]. Oriola, T. A. (2005): Advance fee fraud on the Internet: Nigeria's regulatory response.
- [43]. *Computer Law & Security Review*, Volume 21, Issue 3, 2005, Pages 237-248, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2005.02.006. (https://www.sciencedirect.com/science/article/pii/S0267364905000701)
- [44]. Pal, A., Herath, T., De', R., & Rao, H. R. (2021). Is the convenience worth the risk? An investigation of mobile payment usage. *Information systems frontiers*, 23, 941-961. https://link.springer.com/article/10.1007/s10796-020-10070-z
- [45]. Potts, M., (2012). The state of information security. *Network Security*, 2012, pp. 9-11.
- [46]. Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. Trends and Issues in Crime and Criminal Justice [Electronic Resource], (420), [1]-6. https://search.informit.org/doi/10.3316/ielapa.655572069982261. Updated 2024 https://doi.org/10.52922/ti268334
- [47]. Seissa, I. G., Ibrahim, J., & Yahaya, N. (2017). Cyber terrorism definition patterns and mitigation strategies: A literature review. *International Journal of Science and Research (IJSR)*, 6(1), 180-186.
- [48]. Smith, R. G., Holmes, M. N., and Kauffman, P. (1999). Trends and issues in crime and criminal justice No. 121: Nigerian Advance Fee Fraud. *Australian Institute of Criminology*; Retrieved on 15.01.2005: http://www.aic.gov.au/publications/tandi/ti121.pdf
- [49]. Tendulkar, R. (2013). *Cyber-crime, securities markets and systemic risk*. CFA Digest, 43(4), 35- 43.UK: Oxford University Press.
- [50]. Udelue, M. C., Mathias, B. A., & Ezech, S. S. (2020). socioeconomic correlates of youths involvement in cybercrime: perceptions of residents in Onitsha south LGA, Anambra State, Nigeria. *International Journal of Social Sciences and Humanities Reviews*, 10(3), 66-79.



- <https://www.academia.edu/download/110084003/526.pdf>
- [51]. Unini, C. (2019). Cyber Defamation: Be Careful About What You Post Online. The Nigeria
- [52]. Lawyer.Availableat:  
<https://thenigerialawyer.com/cyber-defamation-be-careful-about-what-you-post-online/>
- [53]. Vito, G.F. & Maahs, J.R. (2012). *Criminology: Theory, research and policy*. Sudbury: Jones and Bartlett Learning.
- [54]. Von Solms, R., and Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, 38, pp. 97-102.
- [55]. Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.
- [56]. Wolfe, D. & Hermanson, D.R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 74 (12), 38 – 42.
- [57]. Xin, Q., Zhou, J., & Hu, F. (2018). The economic consequences of financial fraud: Evidence from the product market in China. *China Journal of Accounting Studies*, 6(1), 1–23.  
<https://doi.org/10.1080/21697213.2018.1480005>
- [58]. Yakubu, M.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(1), 315–321.  
[doi:https://doi.org/10.23956/ijarcsse/V6I12/01204](https://doi.org/10.23956/ijarcsse/V6I12/01204)