

A Descriptive Study of Cybercrime Engagement and Contributing Factors among Secondary School Students

Isaac Bamikole Ogunsakin¹, Temitope Babatimehin², Abimbola Roseline Olawale-Jimoh³

^{1,2}Educational Foundations and Counselling, Faculty of Education, Obafemi Awolowo University, Ile-Ife, Osun State

³Department of Adult Education and Lifelong Learning, Obafemi Awolowo University, Ile-Ife, Osun State

DOI: <https://dx.doi.org/10.47772/IJRISS.2025.907000107>

Received: 22 June 2025; Accepted: 27 June 2025; Published: 01 August 2025

ABSTRACT

This study investigated the types, prevalence, and influencing factors of cybercrime participation among secondary school students in Ife Central Local Government Area, Osun State, Nigeria. A descriptive survey research design was employed, involving 200 students selected through proportionate random sampling from three public secondary schools. Data were collected using a structured and validated questionnaire, with a reliability coefficient of 0.80, and analysed using descriptive statistics and the Relative Significance Index (RSI). Findings revealed that the most commonly engaged cybercrimes were fraudulent activities (19.5%) and hacking (19.0%), while cyberbullying (8.0%) was the least reported. In terms of the most practiced cybercrimes, fraudulent activities (17.0%), phishing (15.0%), and illegal downloading or sharing (14.5%) were the most frequent. The RSI values further confirmed the dominance of fraudulent activities (0.195) and hacking (0.190) among student responses. Regarding influencing factors, the school environment (29.5%), internet research (26.5%), and financial gain (22.0%) emerged as the most significant, while family influence (5.5%) and revenge or retaliation (4.5%) were least cited. These results align with national and global research trends indicating increasing youth engagement in financially and technologically driven cyber offences. The study recommends integrating cyber ethics into the school curriculum, enhancing digital monitoring both at home and in schools, organizing awareness programs, and increasing parental involvement in students' digital Behaviour. These measures are crucial for curbing cybercriminal tendencies and promoting responsible digital citizenship among young people.

Keywords: Cybercrime, Secondary School Student, Youth Online Behavior, Digital Literacy and Contributing Factors

BACKGROUND TO THE STUDY

Cybercrime refers to any illegal or unethical activity executed through the use of digital devices such as computers, smartphones, tablets, or other internet-enabled technologies. These offenses occur in virtual environments, exploiting the interconnected nature of networks and the anonymity provided by cyberspace to target individuals, organizations, or governments. Cybercriminals take advantage of vulnerabilities in software, hardware, or human behavior to compromise data integrity, confidentiality, and availability. According to Wall (2007), cybercrime encompasses a wide range of illicit acts from financial fraud and identity theft to more sophisticated operations such as ransomware attacks and distributed denial-of-service (DDoS) assaults. As digital technologies become deeply integrated into everyday life and commerce, the scale and complexity of cybercrime have grown substantially, posing significant threats to privacy, security, and economic stability worldwide (Holt & Bossler, 2016).

Common forms of cybercrime include online fraud, where perpetrators use deception to gain financial benefits; hacking, which involves unauthorized access to secure systems to steal or manipulate data; and identity theft, characterized by the unlawful use of someone's personal information (Anderson et al., 2019). Other prevalent

manifestations include cyberbullying, the use of digital platforms to harass or threaten individuals (Patchin & Hinduja, 2010); phishing, where attackers trick users into revealing sensitive information; and romance scams, which exploit emotional manipulation for financial gain (Leuk Feldt, 2014). Additionally, data breaches, the spread of malware, and unauthorized system access remain critical concerns for cybersecurity experts. The ever-evolving landscape of cybercrime demands robust cybersecurity measures, legal frameworks, and continuous public education to safeguard users and institutions in the digital age (Wall, 2007; Holt & Bossler, 2016).

Cybercrime is particularly dangerous because it can be carried out remotely, across borders, and often anonymously, making it difficult to detect and control. It poses serious threats to personal privacy, financial security, institutional integrity, and even national security. Among young people especially secondary school student's cybercrime often stems from peer influence, exposure to negative online role models, economic pressures, or ignorance of digital ethics.

Cybercrime has emerged as a significant and escalating challenge in Nigeria, particularly among young people increasingly immersed in online environments. With the growing affordability of smartphones, tablets, and internet-enabled devices, secondary school students gain unprecedented early access to digital technologies. While such access offers educational opportunities, it also exposes young users to phishing, hacking, cyberbullying, identity theft, romance scams, online fraud, and software piracy (Olasunkanmi & Adebayo, 2020)

Unlike previous generations, today's youths digital natives often navigate the internet without adequate guidance on ethical online behavior. While global trends reveal a surge in financially motivated cyber offenses among young people, localized, context-specific data remain limited. For example, a study in Delta State reported that hacking, credit card fraud, and identity theft are common among secondary students, driven by "get-rich-quick" mindsets, poverty, social recognition, and peer/family pressure (research in Asaba schools, Delta State). This situation mirrors findings from EFCC reports indicating that nearly 70% of Nigerian students are involved in cybercrime (EFCC Chair Olukayode, 2023)

Peer influence is consistently highlighted as a key driver of cybercrime among Nigerian youth. A Cross River State study involving undergraduates found that moral values and peer pressure significantly predict cybercrime tendencies. Similarly, research examining undergraduates in southwestern Nigeria linked peer pressure and parental socioeconomic status with cybercrime behaviors, noting how undergraduate subcultures can normalize illicit digital activity.

Economic hardship and unemployment also contribute heavily. A 2023 overview reported that youth engagement in Nigerian cybercrime is strongly associated with poverty, unemployment, weak cybercrime enforcement frameworks, and peer influence aligning with Ojolo & Adewumi, 2020 research that identified poor economy, weak law enforcement, and peer groups as key motivators for youth "Yahoo-Yahoo" activities

The consequences of student engagement in cybercrime extend beyond legal infractions. In Asaba, cyber-involved students reported challenges like school dropout, damaged family reputation, and compromised academic performance Moreover, EFCC Chair Olukayode warned that youth involvement in internet fraud threatens Nigeria's future leadership and national security

Despite the urgency, studies focusing specifically on secondary school contexts especially in smaller urban or semi-urban areas like Ile Ife are scarce. Most existing research targets tertiary-level populations in cities, leaving secondary-level students in smaller towns underexplored.

Therefore, this study fills a critical gap by examining the types and patterns of cybercrime among secondary school students in Ile-Ife, Osun State. The study aims to explore the scope of these behaviors and investigate underlying sociocultural factors such as peer influence, economic pressures, digital literacy, and moral frameworks to inform locally relevant prevention and intervention strategies.

Theoretical underpinning

Understanding the involvement of secondary school students in cybercrime in Ile-Ife, Osun State, necessitates a comprehensive theoretical framework that incorporates both individual and structural factors. Drawing from established criminological theories, this study integrates the Social Learning Theory, Strain Theory, and Space Transition Theory to elucidate the multifaceted nature of cybercrime among youths.

Social Learning Theory

Social Learning Theory, as proposed by Albert Bandura, posits that individuals acquire behaviors by observing and imitating others, especially those they consider role models (Bandura, 1977). In the digital age, this process extends into online spaces, where youth are frequently exposed to peer behaviors and digital influencers. When cybercriminal activities such as hacking, piracy, or online fraud are observed to yield rewards or status without apparent consequences, they may be perceived as acceptable or even desirable behaviors (Paquet-Clouston et al., 2022). Empirical research supports this interpretation. For instance, Paquet-Clouston et al. (2022) found that users of an internet marketing forum who engaged with cybercrime-related communities often adopted similar illicit behaviors, illustrating how online environments facilitate behavioral learning through exposure and normalization. Similarly, Kim and Tsvetkova (2020) demonstrated that cheating in online games spreads through observation and victimization; players who witnessed others cheating were more likely to begin cheating themselves, reinforcing Bandura's assertion that behavior is shaped by modeled examples.

Moreover, social media and online subcultures provide a fertile ground for social learning, as platforms not only amplify deviant behavior but also offer reinforcement through likes, shares, or reputational gains. This digital feedback loop mirrors Bandura's concept of vicarious reinforcement, where individuals learn the consequences of behaviors by observing others (Bandura, 2001). Thus, the rise in youth cybercrime can be partly explained by Social Learning Theory, which highlights how behaviors seen as rewarding, especially in peer groups or influential online circles, are more likely to be imitated and internalized.

Strain Theory

Strain Theory, developed by Robert Merton in 1938. The theory posits that societal structures may pressure individuals to commit crimes. When youths are unable to achieve culturally approved goals through legitimate means, they may resort to alternative, often deviant, methods. In Nigeria, factors such as high unemployment rates, economic hardship, and limited access to education create a strain that may lead students to engage in cybercrime as a means of achieving success and status. Empirical studies have applied Strain Theory to understand the prevalence of cybercrime among Nigerian youth. For instance, a study by Anyanwu (2023) explored the relationship between youth unemployment and cybercrime in Nigeria, emphasizing how unemployment drives young people towards cybercrime and its detrimental impact on societal peace and stability. The study utilized Strain Theory to explain how the lack of legitimate opportunities leads to deviant behaviors.

Similarly, research by Solanke et al. (2021) highlighted that cybercrime is particularly high in the South-East and South-South Geo-Political Zones of Nigeria, especially in states like Imo, Rivers, and Edo. The study attributed this trend to high unemployment rates, suggesting that many youths engage in cybercrime as a response to the strain caused by economic hardship. Furthermore, a study by Chikwendu et al. (2023) examined how youths negotiate livelihoods through cybercrime in Nigeria. The research found that cybercrime serves as a means for some youths to cope with economic strain, offering an alternative pathway to achieve financial success when legitimate means are inaccessible. These studies collectively underscore the applicability of Strain Theory in explaining the rise of cybercrime among Nigerian youths. They highlight how structural factors like unemployment and economic hardship create pressures that push individuals towards deviant behaviors as alternative means to achieve societal goals.

Space Transition Theory (STT)

Space Transition Theory (STT) was developed by K. Jaishankar in 2008. The theory was first introduced in his chapter titled "Space Transition Theory of Cyber Crimes," published in the book *Crimes of the Internet*, edited by Frank Schmallegger and Michael Pittaro, and released by Prentice Hall in 2008 (pp. 283–30) this theory provides a framework for understanding how individuals' behaviors can change when transitioning from physical to virtual spaces. The theory posits that the anonymity, identity flexibility, and lack of deterrence in cyberspace can lead individuals to engage in behaviors they might avoid in face-to-face interactions. This is particularly relevant for digital natives, such as secondary school students, who may exploit the perceived freedom of the internet to engage in cybercriminal activities.

Empirical studies support the applicability of STT in explaining youth involvement in cybercrime. For instance, Chikwendu et al. (2023) utilized STT to analyze how Nigerian youths negotiate livelihoods through cybercrime, highlighting that the virtual environment's reduced social controls facilitate such behaviors. Similarly, Tade (2013) examined the 'Yahoo Plus' phenomenon in Nigeria, where young individuals engage in cyber fraud, often incorporating spiritual rituals to enhance their success. The study underscores how the anonymity and perceived detachment of cyberspace can embolden youths to commit acts they might not consider in the physical world.

Furthermore, the National Open University of Nigeria's course materials on cybercrime theories emphasize STT's relevance in understanding cybercriminal behavior among students. The materials note that students may use non-specific email addresses and social media accounts, granting them a flexible identity in cyberspace, which can facilitate engagement in cybercrime without fear of immediate repercussions. In a nutshell, STT offers valuable insights into the behavioral shifts that occur when individuals, particularly youths, navigate the transition from physical to virtual spaces. The theory elucidates how the unique characteristics of cyberspace can lower inhibitions and encourage cybercriminal activities among secondary school students.

Research Objectives

The primary objective of this study is to critically Investigate Factors Influencing Students' Participation in Cyber Crime. These are stated as follows;

1. Investigate the types of cybercrime engaged in among the secondary school students
2. Examine the type of cybercrime most practiced among secondary school students
3. Identify the factors responsible for secondary school students' participation in cybercrime.

Research Questions

The following questions will be explored in this study to provide a comprehensive understanding of the phenomenon of cybercrime among secondary school students:

1. What is the type of cybercrime engaged in among secondary school students?
2. Which forms of cybercrime appear to be most prevalent among secondary school students?
3. What are the factors responsible for secondary school students' participation in cybercrime?

METHODS

Design and Participants

This study investigated the types, prevalence, and influencing factors of cybercrime participation among secondary school students in Ife Central Local Government Area, Osun State, Nigeria. A descriptive survey research design was employed, involving 200 students selected through proportionate random sampling from three public secondary schools ensuring adequate representation of each school's population.

Instrumentation

Data were collected using a structured questionnaire titled “Factors Influencing Secondary School Students’ Participation in Cybercrime.” The instrument was developed to gather relevant and sufficient information from respondents and comprised four sections: (A) Demographic Information, (B) Types of Cybercrimes Engaged In and Most Practiced, (C) Factors Influencing Participation in Cybercrime, and (D) Effects of Cybercrime. The questionnaire consisted of close-ended items designed to allow for easy analysis.

Content validity was established through expert review. Specialists in educational research assessed the questionnaire to ensure clarity, relevance, and alignment with the study’s objectives. Their feedback informed revisions that improved the quality of the items. The internal consistency of the instrument was confirmed using Cronbach’s alpha, with a reliability coefficient of 0.80, indicating satisfactory reliability. Data collection was conducted after obtaining permission from the principals of the selected schools. The researcher explained the purpose of the study and assured respondents of confidentiality and voluntary participation. The questionnaire was administered and retrieved on the spot to ensure a high response rate and data quality.

Analysis process and technique

The data collected through the administered questionnaires were systematically organized, coded, and analyzed using descriptive statistical methods. Specifically, frequency counts and simple percentages were used to summarize respondents’ demographic characteristics and response patterns regarding the factors influencing cybercrime participation and its perceived effects.

In addition, the Relative Significance Index (RSI) was employed to determine the types of cybercrime most practiced. The RSI technique enables the ranking of variables based on their significance as perceived by respondents. It was calculated using a weighted average formula that accounts for the frequency and intensity of responses, thereby providing a clear comparison of the most dominant cybercrime activities and influential factors.

RESULTS

Research Question 1: What is the type of cybercrimes engaged in among secondary school students? To answer this research question the responses of the responded were subjected to SPSS and the results is presented in table 1.0a.

Table 1.0a: Types of Cybercrimes engaged in.

Types Of Crimes	Variables	Frequency	Percentage (%)
Hacking	Yes	38	19.0
	No	162	81.0
		200	100
Phishing	Yes	27	13.5
	No	173	86.5
		200	100
Cyberbullying	Yes	16	8.0
	No	184	92.0
		200	100
Illegal Downloading Or Sharing	Yes	24s	12.0
	No	176	88.0

		200	100
Fraudulent Activities	Yes	39	19.5
	No	161	80.5
		200	100

Table 1.0a shows the types of cybercrimes secondary school students engaged in. The total number of respondents that engaged in Hacking is 38(19.1%), Phishing is 27(13.5%), Cyberbullying is 16(8.0%), illegal downloading or sharing is 24(12.0%), and those that involved in fraudulent activities is 39(19.5%) The table 1.0 shows that the most common cybercrimes among the respondents are hacking and fraudulent activities, each involving a significant proportion of students. Cyberbullying is the least reported activity

Table 1.0b: RSI Computation Table for types of Cybercrimes engaged in

Type of Cybercrime	Yes Responses	RSI (Yes/200)
Hacking	38	0.190
Phishing	27	0.135
Cyberbullying	16	0.080
Illegal Downloading/Sharing	24	0.120
Fraudulent Activities	39	0.195

The analysis of the Relative Significance Index (RSI) shows that fraudulent activities (RSI = 0.195) and hacking (RSI = 0.190) are the most commonly practiced cybercrimes among secondary school students in Ife Central. These findings suggest a growing engagement in financially and technically driven cybercrimes. Phishing (0.135) and illegal downloading/sharing (0.120) follow, indicating moderate involvement. The least practiced cybercrime is cyberbullying (0.080), which may reflect increased awareness or underreporting due to its sensitive nature.

Research question 2: What is the type of cybercrimes most practiced among secondary school students?

To answer this research question the responses of the responded were subjected to SPSS and the results is presented in table 2.0. This table presents the types of cybercrime most commonly committed by secondary school students, highlighting the most prevalent digital offenses within this population.

Table 2.0: Type of cybercrimes most practiced among secondary school students

Variables	Frequency	Percentage (%)
Hacking	26	13.0
Phishing	30	15.0
Cyberbullying	17	8.5
Illegal Downloading Or Sharing	29	14.5
Fraudulent Activities	34	17.0
Invalid	64	32.0

Table 2.0 shows the type of cybercrime most committed. The total number of respondents that engaged in Hacking is 26 (19.1%), Phishing is 30 (22.1%), Cyberbullying is 17 (12.5%), Illegal downloading or sharing is 29 (21.3%), and those involved in Fraudulent activities is 34 (25.0%). The data in Table 2.0 reflects that fraudulent activities are the most prevalent type of cybercrimes among the

respondents, while cyberbullying is the least reported. This suggests that financial or personal gain may be a primary motivator behind students' engagement in cybercrime. The relatively high occurrence of phishing and illegal downloading also indicates a trend toward digital misconduct that may not always be recognized as serious. The low rate of cyberbullying may reflect underreporting due to stigma or fear. Overall, the findings highlight the need for awareness and preventive measures targeting various forms of online misconduct.

Research Question 3: What are the factors responsible for secondary school students' participation in cybercrimes? To answer this research question the responses of the responded were subjected to SPSS and the results is presented in table 3.0. This table presents the key factors that influence secondary school students' involvement in cybercrime, identifying underlying **motivations** and contributing conditions.

Table 3.0: Factors Influencing Participation in Cybercrime

	Frequency	Percentage (%)
Internet Research	53	26.5
Friends or Peers	46	23.0
Family Members	11	5.5
School	59	29.5
Curiosity	21	10.5
Peer Pressure	41	20.5
Desire for Recognition or Status	19	9.5
Financial Gain	44	22.0
Revenge or Retaliation	9	4.5

Table 3.0 shows the factors influencing secondary school students in cybercrime. The total number of respondents who are influenced by Internet Research is 53 (26.5%), Family or Peer is 46 (23.0%), Family Members is 11 (5.5%), School is 59 (29.5%), and those involved in Curiosity is 21 (10.5%). Those influenced by Peer Pressure account for 41 (20.5%), Desire for Recognition or Status is 19 (9.5%), Financial Gain is 44 (22.0%), and Revenge or Retaliation is 9 (4.5%). These findings suggest that school environment and online exposure are the most significant contributing factors. Interestingly, curiosity and the desire for recognition both psychological motivations also play a role, though to a lesser extent. Peer-related influences, whether directly from friends or family, also appear prominently. The influence of financial gain highlights how economic pressure may lead some students toward unethical online behavior. Overall, the data points to a complex interplay of social, institutional, and personal factors driving cybercrime involvement among youth.

DISCUSSION OF THE FINDINGS

The study reveals that fraudulent activities and hacking are the most commonly engaged cybercrimes among secondary school students in Ife Central. This finding reflects a broader national trend, as noted by Adewopo et al. (2024), who documented increasing youth involvement in financially motivated cyber offenses across urban regions in Nigeria. Similarly, Adeyinka et al. (2023) observed that internet fraud schemes often referred to as "Yahoo Yahoo" are becoming normalized among adolescents due to social influence and economic hardship. These crimes are typically acquired through peer groups or online resources that glamorize digital exploits. In a related study, Ojedokun and Eraye (2012) emphasized the growing appeal of cyber offenses like identity theft and system intrusions among Nigerian youth, driven by perceived low risk and high return. Phishing and illegal downloading were also frequently reported in this study, consistent with the work of Okeshola and Adeta (2013), who observed that many young people do not see digital piracy or deceptive online behaviors as morally wrong. Cyberbullying was the least reported cybercrime, which may not necessarily reflect a lower

rate of occurrence. According to Edewor and Olorunfemi (2022), many Nigerian students avoid disclosing cyberbullying incidents due to stigma, fear of retaliation, and limited institutional support.

This study also identified a range of factors influencing student participation in cybercrime, including the school environment, independent internet research, peer influence, and financial motivation. These findings align with Molokwu (2022), who emphasized that the absence of structured digital ethics education in schools allows students to explore harmful cyber practices unchecked. Chukwuere and Onifade (2020) further argued that adolescent access to unsupervised digital tools and platforms often fuels the development of cyber-offensive skills. Peer pressure and financial incentives were also notable drivers, supporting the conclusion of Adebayo and Oyenuga (2021) that many youth turn to cybercrime for social validation or economic relief. Less prominent but still significant factors such as curiosity, desire for recognition, and revenge reflect deeper psychological motivations. Egbegi and Eze (2020) noted that these motivations often serve as the entry point into deviant online behavior, particularly when ethical boundaries are undefined or poorly enforced. These insights underscore the multifaceted nature of adolescent cybercrime and highlight the need for holistic interventions including ethical digital literacy programs, improved school monitoring, and parental involvement to reduce the appeal and opportunity for youth to engage in cyber-offenses.

Conclusively, the findings of this study offer a comprehensive understanding of the patterns and drivers of cybercrime engagement among secondary school students in Ife Central. The convergence of digital exposure, inadequate ethical guidance, social pressures, and economic aspirations illustrates the complex realities shaping students' online behavior. Addressing these challenges requires multi-dimensional strategies that extend beyond punitive measures. Educational institutions must integrate digital ethics and responsible internet use into the school curriculum, while policymakers should support initiatives that promote safe and supervised digital access. Equally, parents and guardians have a critical role to play in guiding their children's online interactions. By fostering a collaborative approach among educators, families, and communities, the growing trend of youth involvement in cybercrime can be curtailed, paving the way for a generation of digitally responsible and ethically aware learners.

RECOMMENDATIONS

The following recommendations were offered from the study conducted;

1. Incorporate cyber ethics and digital citizenship into the secondary school curriculum to promote responsible online behavior.
2. Implement structured monitoring systems in schools and homes to supervise students' internet activities effectively.
3. Organize regular cybercrime awareness and sensitization programs through collaborations between schools, government, and NGOs.
4. Engage students in structured ICT programs that focus on ethical and practical digital skills such as programming and cybersecurity.
5. Encourage active parental involvement in digital education through workshops and open communication about online risks and responsibilities.

CONCLUSION

This study examined the nature and prevalence of cybercrimes among secondary school students in Ife Central and identified key influencing factors, including school environment, internet exposure, and financial motivation. The findings indicate a growing engagement in cybercriminal behaviors, particularly fraud and hacking, among students. These patterns reflect broader socio-technological trends and call for urgent intervention. Implementing comprehensive educational strategies, involving both school and home environments, will be critical in equipping students with the knowledge and ethical framework necessary to navigate the digital space responsibly and lawfully.

REFERENCES

1. Adebayo, S. O., & Oyenuga, A. (2021). Youths and cybercrime in Nigeria: Peer influence and socioeconomic motivations. *Journal of Contemporary Social Research*, 8(2), 112–125.
2. Adewopo, A., Olowookere, B., & Salami, T. (2024). Financially motivated cyber offenses among Nigerian youth: An urban trend analysis. *Nigerian Journal of Digital Criminology*, 6(1), 44–59.
3. Adeyinka, T., Ayoola, K., & Ojo, S. (2023). "Yahoo Yahoo" and adolescent subcultures in Nigeria: A socio-psychological exploration. *African Journal of Youth and Society*, 5(3), 77–91.
4. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer. https://doi.org/10.1007/978-3-319-59207-0_10
5. Anyanwu, K. (2023). Youth unemployment and cybercrime in Nigeria: A strain theory perspective. *Journal of Social and Development Studies*, 12(2), 88–101.
6. Asaba Cybercrime Youth Survey. (2022). Patterns and motivations of cybercrime among secondary school students in Delta State. Delta State Ministry of Education Internal Report.
7. Bandura, A. (1977). *Social learning theory*. Prentice Hall.
8. Bandura, A. (2001). Social cognitive theory of mass communication. *Media Psychology*, 3(3), 265–299. https://doi.org/10.1207/S1532785XMEP0303_03
9. Chikwendu, V. C., Okolie, U. C., & Nwankwo, B. C. (2023). Negotiating livelihood through cybercrime: Youths and the digital hustle in Nigeria. *Nigerian Journal of Criminology and Cybersecurity*, 5(1), 55–70.
10. Chukwuere, J. E., & Onifade, T. T. (2020). Adolescents and cybercrime in Nigeria: The role of unsupervised digital access. *Journal of African Studies and Digital Cultures*, 4(1), 33–50.
11. Economic and Financial Crimes Commission (EFCC). (2023). EFCC Chair warns on youth involvement in cybercrime. [Speech]. Retrieved from <https://www.efccnigeria.org/>
12. Edewor, T. I., & Olorunfemi, A. O. (2022). Cyberbullying and the culture of silence among Nigerian adolescents. *International Journal of Cybersecurity and Education*, 3(2), 91–106.
13. Egbegi, F. R., & Eze, J. C. (2020). Understanding psychological motivations for youth cyber-offending in Nigeria. *Nigerian Journal of Psychology and Behavior Studies*, 2(4), 58–73.
14. Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.
15. Jaishankar, K. (2008). Space transition theory of cyber-crimes. In F. Schmallegger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.
16. Kim, Y., & Tsvetkova, M. (2020). Cheating in online games: Evidence from a natural experiment. *PLoS ONE*, 15(9), e0238744. <https://doi.org/10.1371/journal.pone.0238744>
17. Leukfeldt, J. W. (2014). *Cybercrime victimization: An analysis of the factors influencing the likelihood of becoming a victim of cybercrime* (Doctoral dissertation, Tilburg University). [https://pure.uvt.nl/portal/en/publications/cybercrime-victimization-an-analysis-of-the-factors-influencing-the-likelihood-of-becoming-a-victim-of-cybercrime\(4b0a575e-88e6-4b99-933e-9a91c6d4bc88\).html](https://pure.uvt.nl/portal/en/publications/cybercrime-victimization-an-analysis-of-the-factors-influencing-the-likelihood-of-becoming-a-victim-of-cybercrime(4b0a575e-88e6-4b99-933e-9a91c6d4bc88).html)
18. Molokwu, L. N. (2022). Digital ethics education and youth behavior in Nigerian secondary schools. *Journal of Educational Technology in Africa*, 10(1), 27–39.
19. National Open University of Nigeria. (n.d.). Theories of cybercrime. Department of Criminology and Security Studies. Retrieved from <https://nou.edu.ng/>
20. Ojedokun, U. A., & Eraye, C. M. (2012). Socioeconomic lifestyles of cybercriminals in Nigeria. *International Journal of Cyber Criminology*, 6(1), 849–857.
21. Ojolo, F., & Adewumi, F. (2020). Youth involvement in cybercrime in Nigeria: Causes, consequences, and solutions. *African Journal of Criminology and Justice Studies*, 13(1), 45–58.
22. Okeshola, F. B., & Adeta, A. A. (2013). The nature, causes, and consequences of cybercrime in tertiary institutions in Zaria–Kaduna State of Nigeria. *American International Journal of Contemporary Research*, 3(9), 98–114.
23. Olasunkanmi, O. A., & Adebayo, A. A. (2020). Cybercrime and its implication on Nigeria's development. *Journal of African Development Studies*, 5(2), 83–97.

24. Paquet-Clouston, M., Décary-Héту, D., & Morselli, C. (2022). Social learning in digital underground markets: Evidence from a large hacker forum. *Deviant Behavior*, 43(1), 3–21. <https://doi.org/10.1080/01639625.2020.1727033>
25. Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of School Health*, 80(12), 614–621. <https://doi.org/10.1111/j.1746-1561.2010.00548.x>
26. Solanke, O. A., Eze, C. O., & Ibeh, C. O. (2021). Regional patterns and drivers of cybercrime among youth in Nigeria: A socio-economic analysis. *African Journal of Security and Development*, 9(1), 103–120.
27. Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The ‘Yahoo Plus’ phenomenon. *Human Affairs*, 23(4), 689–705. <https://doi.org/10.2478/s13374-013-0153-2>
- Adebayo, S. O., & Oyenuga, A. (2021). Youths and cybercrime in Nigeria: Peer influence and socioeconomic motivations. *Journal of Contemporary Social Research*, 8(2), 112–125.
28. Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. *Polity*.