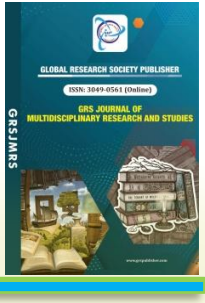
OPEN ACCESS

GRS Journal of Multidisciplinary Research and Studies
Abbreviate Tittle- GRS J Mul Res Stud
ISSN *(Online) - 3049-0561*
https://grspublisher.com/journal-details/GRSJMRS

Vol-3, Iss-6 (Jun)-2026)



Statistical Analysis of Cybercrime Participation among Undergraduate Students of Mass Communication in Federal University Lokoja (Ful)

[1]Israel Nandi Bigun, [2]Ajare Emmanuel Oloruntoba

[1, 2]Federal University Lokoja, Nigeria.

Article History
Received: 15.05.2026
Accepted: 10.06.2026
Published: 26.06.2026

Corresponding Author:
Israel Nandi Bigun

Abstract: This study seeks to examine the prevalence and determinants of cybercrime participation among undergraduate students of mass communication in federal university Lokoja. The ultimate goal is to foster a safer digital environment within the university community while promoting ethical digital practices among students. Using the Edwin Sutherland's *Differential Association Theory* and Albert *Bandura's Social Learning Theory* which provided a nexus between social/digital interaction and learning/adoption of deviant behavior, the study adopted descriptive survey. The finding shows that 100-level students recorded the highest cybercrime participation rate (72%), followed by 200-level (69%). Findings also revealed that peer influence significantly influences cybercrime participation among students and that the significant influence of peers' financial gains on students' interest in cybercrime, indicate that economic pressure is a key factor. The study therefore recommends among other things, the introduction of mandatory first-year cybersecurity education and increased structured academic engagement to reduce idle time and prevent early student involvement in cybercrime. The study also recommends the integration of compulsory cyber ethics and legal awareness courses across all levels while fostering collaboration among institutions, private sector, and government to provide scholarships that alleviate financial pressures and discourage student involvement in cybercrime.

***Keywords**: Cybercrime, digital environment, deviant behaviour, digital interaction, cybersecurity.*

Cite this Article

I. Nandi Bigun, A.Emmanuel. Oloruntoba (2026) Statistical Analysis of Cybercrime Participation among Undergraduate Students of Mass Communication in Federal University Lokoja (Ful) *GRS Journal of Multidisciplinary Research and Studies, Vol-3 (Iss-6). 38-44*

Introduction

It is manifestly evident that cybercrime is a pressing global issue especially in universities where the increasing reliance on digital technology exposes students to both risks and opportunities for unethical activities. Among undergraduate students, cybercrime participation has emerged as a significant concern, fueled by various socioeconomic, academic, and psychological factors. This phenomenon threatens not only the ethical fabric of academic institutions but also the broader societal effort to combat digital crimes (Adebayo & Yusuf 2019).

The prevalence of cybercrime has become a significant concern in Nigeria, particularly within university environments where young people are increasingly exposed to digital technologies. Among undergraduate students, cybercrime participation often manifests through activities such as internet fraud, hacking, and identity theft. This growing trend poses a challenge to academic institutions, as it not only disrupts the ethical foundation of education but also undermines societal values and economic stability. Universities as centers of knowledge and innovation are increasingly implicated in these issues, with some students leveraging their technological skills unethically to engage in cybercrimes (Aluko & Odusanya, 2022).

Federal University Lokoja, a leading academic institution in Kogi State, is no exception to these challenges. The university's vibrant student population and access to digital infrastructure create an environment where cybercrime participation could potentially thrive. Several factors may contribute to this issue, including financial pressures, peer influences, academic stress, and easy access to internet-enabled devices. While cybercrime participation may be driven by a combination of these socioeconomic, academic, and psychological factors, understanding the interplay between these determinants is crucial for addressing the problem effectively (Ibrahim & Bello, 2020).

This study focuses on examining the prevalence and determinants of cybercrime participation among undergraduate students at Federal University Lokoja. It seeks to determine how communication environments (digital/media) shape this behavior. By identifying the key drivers of the behavior, the research aims to provide a multifaceted, but contextual understanding of how cybercrime manifests within a university setting. Furthermore, the findings will offer valuable insights for policymakers, educators,

and university administrators to develop targeted strategies that address the root causes of cybercrime. The ultimate goal is to foster a safer digital environment within the university community while promoting ethical digital practices among students.

Literature Review

Cybercrime is a global phenomenon that has evolved with the rapid advancement of digital technologies, posing significant challenges to various sectors, including education. Among undergraduate students, cybercrime participation has emerged as a pressing issue, fueled by factors such as socioeconomic constraints, academic pressures, and peer influences (Olufemi & Adesola, 2020). This literature review explores the existing body of knowledge on the prevalence, determinants, and impact of cybercrime participation, focusing on the role of universities in addressing this growing concern.

Studies indicate that cybercrime participation among university students is on the rise, particularly in developing countries like Nigeria (Okonkwo & Adewale, 2021; Ibrahim & Aminu, 2022). Particularly, Okonkwo and Adewale (2021) registered that internet fraud, popularly known as "Yahoo Yahoo," is increasingly being normalized among young people in Nigeria, including university students. The advent of digital devices and high-speed internet has facilitated access to tools and platforms that enable cybercriminal activities (Williams & Yusuf, 2021). Similarly, Ibrahim and Bello (2020) assert that students view cybercrime as a means of economic survival amidst financial hardships, with a significant proportion of undergraduates engaging in online fraud, hacking, and identity theft. Despite this prevalence, universities often lack adequate mechanisms to track and address such behaviors (Adebayo & Yusuf, 2019).

It is pertinent to note that while cybercrime is often viewed as a male-dominated activity, gender dynamics also play a role. Studies suggest that while male students are more likely to engage in technical forms of cybercrime such as hacking, female students are more vulnerable to cybercrimes like “sextortion” and identity theft (Okeke & Durojaiye, 2021). Hence, this distinction underscores the need for a nuanced approach to addressing cybercrime within university settings, considering the different ways in which students experience and participate in such activities (Smith, & Adeyemi, 2020).

Eminently, the rise of cybercrime among undergraduate students in Nigerian universities presents a significant threat to the integrity of academic institutions and the broader societal effort to combat digital criminal activities. Federal University Lokoja, like many higher education institutions, is not immune to this growing concern. While technological advancements have created opportunities for academic growth and innovation, they have also provided avenues for students to engage in unethical practices such as internet fraud, hacking, and identity theft. This participation in cybercrime disrupts the ethical foundation of education, undermines public trust in academic institutions, and contributes to the broader proliferation of cybercriminal activities in society (Olanrewaju & Igbokwe 2021).

Despite the growing prevalence of cybercrime in Nigerian universities, limited research has been conducted to understand the underlying factors that drive this behavior among students. According to Davies and Dutton (2015) factors such as financial constraints, peer pressure, academic stress, and easy access to digital technologies are often cited as potential contributors. However, the lack of comprehensive, institution-specific research makes it challenging to address these issues effectively (Okonkwo, et al., 2020). As such, Federal University Lokoja as a microcosm of this broader trend, provides a unique setting to explore these dynamics.

The implications of cybercrime participation extend beyond individual students to affect the broader university environment (Jagboro, & Akinrinmade, 2021). Cybercrime undermines the integrity of academic institutions, tarnishing their reputation and diminishing public trust. According to Smith and Adeyemi (2020), universities associated with high levels of cybercrime face difficulties in attracting funding and partnerships, as they are perceived as breeding grounds for unethical behavior. Furthermore, cybercrime participation can negatively impact students’ academic performance. Studies have shown that students involved in cybercrime often prioritize their illicit activities over academic responsibilities, leading to poor grades and eventual dropout (Ibrahim & Aminu, 2022; Alabi & Oladipupo, 2020).

Theoretical Framework

This study is predicated upon the tenets and assumptions of the Differential Association Theory (DAT) as put forward by Edwin Sutherland (1947) and the Albert Bandura’s (1977) Social Learning Theory (SLT). First, scholars have opined that the DAT is one of the most important symbolic interactionist theories in the last 60 years that explain criminal behavior through the process of socialization and the contacts between members of social groups to which one belongs (Petrovic & Mesko, 2004; Maloku, 2020). The theory assumes that an individual learns delinquent behavior, accepts it from others, and learning flows through the communication process. This implies that the frequency of interaction with deviant peers leads individuals to accept such behavior through communication (Maloku, 2020). Within the context of this study, DAT is crucial in explaining how students may learn and adopt cybercrime behaviors through frequent interaction with peers or online networks that support or justify such activities. The theory suggests that the more students are exposed to pro-cybercrime attitudes within their communication environments, the higher their likelihood of participating in cybercrime.in a nutshell, the theory is suitable for this study because it provided a lens through which learned behavior through interaction with others and exposure to pro-cybercrime attitudes via digital communication can be measured.

On the other hand, the SLT postulates that people learn from their interactions with others in a social context. It contends that separately, by observing the behaviors of others, people develop similar behaviors, and that after observing the behavior of others, people assimilate and imitate that behavior, especially if their observational experiences are positive ones or include rewards related to the observed behavior (Navabi & Bijandi, 2012). According to Bandura, imitation involves the actual reproduction of observed motor activities (1977). This theory is relevant in this study in explaining how students may engage in cybercrime after observing and imitating behaviors modeled by peers or online influencers, especially when such actions appear rewarding or go unpunished. It suggests that exposure to cybercrime-related content and reinforcement within digital environments increases the likelihood of students participating in such activities.

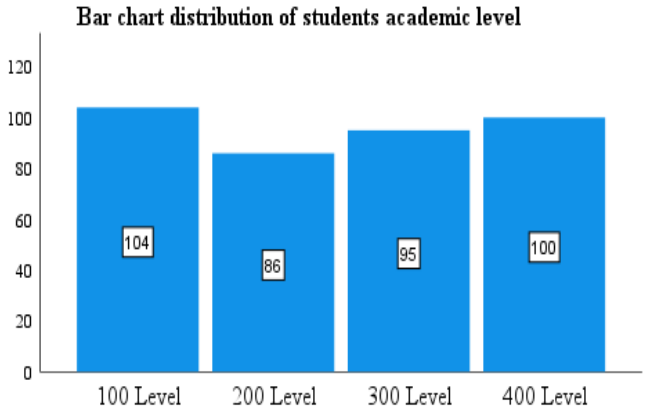
Methodology

The study was conducted at Department of Mass Communication Federal University Lokoja, located in Kogi State, Nigeria. Established in 2011, the university has a diverse undergraduate student population across various faculties. This setting is ideal for exploring the dynamics of cybercrime participation using survey method due to its vibrant academic environment and growing digital infrastructure. The study population consists of all undergraduate students enrolled in the Department during the 2023/2024 academic session. A sample size of 400 students was determined using Taro Yamane's formula for sample size calculation, ensuring adequate representation of the student population. Stratified random sampling was employed to ensure proportional representation from each academic level. This technique is crucial for capturing diverse perspectives across the university's faculties and departments.

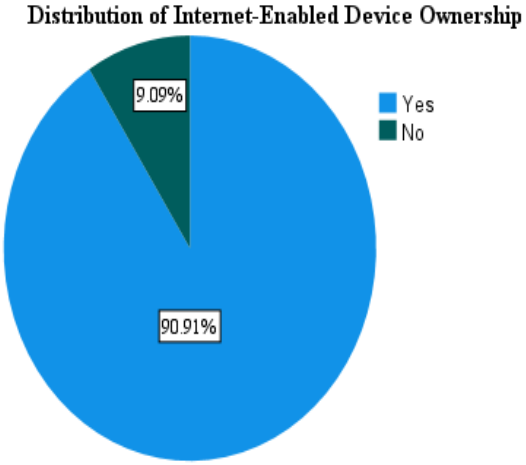
Data was collected using a structured questionnaire designed to capture information on cybercrime participation and its determinants. The questionnaire consist of three sections: demographic information (age, gender, and academic level), cybercrime participation (types of cybercrimes engaged in, frequency, and motivations), and determinants (factors such as financial pressures, peer influence, academic stress, and access to technology). The questionnaire was distributed in-person to ensure a high response rate. The questionnaire was distributed to target students of mass communication from 100level to 400level. Ethical considerations, including informed consent and confidentiality, were be strictly adhered to during data collection. The collected data was analyzed using both descriptive and inferential statistical methods. Descriptive statistics, including frequencies and percentages, will summarize demographic characteristics and the prevalence of cybercrime participation. Logistic regression and multivariate analysis, and chi-square tests were as well employed to assess the relationship between various determinants of cybercrime participation. Statistical software such as SPSS was used to conduct the analysis, and a result was presented using tables, charts, and graphs for clarity.

Results

Demographic Analysis



Out of 400 questionnaires distributed, 385 were returned and valid for analysis, representing a response rate of 96.3%. The bar chart indicates that 100 Level students had the highest representation with 104 respondents (27.0%), followed by 400 Level with 100 respondents (26.0%), 300 Level with 95 respondents (24.7%), while 200 Level recorded the least with 86 respondents (22.3%).



The pie chart shows that 90.91% of respondents own at least one internet-enabled device, while 9.09% reported not owning any. This indicates that the majority of the study population has access to internet-enabled devices, suggesting a high level of digital accessibility among the respondents.

Levels	YES			NO
	F	%	F	%
100 Level	75	72	29	28
200 Level	59	69	27	31
300 Level	51	54	44	46
400 Level	66	66	34	34

Objective 1

To determine the prevalence of cybercrime participation among undergraduate students of

Prevalence of Cybercrime Participation by Academic Level

The cross-tabulation shows that 100-level students recorded the highest participation rate (72%), followed by 200-level (69%), 400-level (66%), and 300-level students (54%), suggesting that participation cuts across all academic groups. However, 300-level students recorded the narrowest margin between affirmative and negative responses (54% vs. 46%), indicating a slight decline in participation at the mid-programme stage, possibly reflecting increased academic engagement or growing awareness of cyber ethics.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.211[a]	3	.042
Likelihood Ratio	8.080	3	.044
Linear-by-Linear Association	2.380	1	.123

Hypothesis Statement

H_0: There is no significant difference in the prevalence of cybercrime participation across academic levels among undergraduate Mass Communication students.

H_1: There is a significant difference.

Test Statistic

Chi-Square (χ^2) test $\chi^2(3) = 8.211$, $p = .042$

Level of Significance

$\alpha = 0.05$

Decision Rule

If the p-value is less than α value ($p < 0.05$), then the null hypothesis (H_0) will be rejected other-wise there is no significant reason to reject null hypothesis statistically.

Conclusion

Since the p-value ($p = .042$) is less than the significance level ($\alpha = 0.05$), the null hypothesis is rejected. The Pearson Chi-Square test result $\chi^2(3) = 8.211$, $p = .042$ reveals a statistically significant difference in cybercrime participation across academic levels among undergraduate. This confirms that cybercrime participation does not occur equally across all academic levels. 100-level students recorded the highest participation rate (72%), followed by 200-level (69%), 400-level (66%), and 300-level students (54%).

Objective 2

To analyze the relationship between peer influence and students' likelihood of engaging in cybercrime.

PEER INFLUENCE AND CYBERCRIME	Strongly Disagreed		Disagreed	Agreed	Strongly Agreed

	F	%	F	%	F	%	F	%
Peers influence students' involvement in cybercrime.	46	11.9	76	19.7	130	33.8	133	34.5
Students involved in cybercrime are respected among their peers.	58	15.1	91	23.6	121	31.4	115	29.9
Peer pressure can push students to engage in cybercrime.	41	10.6	70	18.2	119	30.9	115	40.3
Seeing peers make money from cybercrime increases interest in it.	43	11.2	75	19.5	89	23.1	178	46.2
Students involved in cybercrime often encourage others to join.	52	13.5	73	19.0	127	33	133	34.5

The table reveals a strong positive relationship between peer influence and students' likelihood of engaging in cybercrime, with most respondents agreeing that peer dynamics significantly drive participation. The statement "seeing peers make money from cybercrime increases interest in it" recorded the highest agreement (69.3%), indicating that financial modeling through peer observation strongly motivates involvement. Similarly, 68.3% agreed that peers influence students' involvement in cybercrime, while 71.2% confirmed that peer pressure can push students into such activities, collectively highlighting the role of peer networks in normalizing cybercriminal behavior among students.

PEER INFLUENCE AND CYBERCRIME	t		df	Sig 2 tailed
Influence of peers on students	-7.967		384	.001
Introduction to cybercrime	-44.78		384	.001
Respect given to students involved in cybercrime	-4.921		384	.001
Effect of peer pressure	-9.900		384	.001
Influence of peers' financial gains	-10.16		384	.001
Encouragement by peers	-7.334		384	.001

Hypothesis Statement

H_0: Peer influence has no significant effect on cybercrime participation among undergraduate students at Federal University Lokoja.

H_1: Peer influence has no significant effect on cybercrime participation among undergraduate Mass Communication students at Federal University Lokoja.

Test Statistic

One-Sample t-test (Test Value = 2.5)

Level of Significance

$\alpha = 0.05$

Decision Rule

If the p-value is less than the significance level ($p < 0.05$), the null hypothesis (H_0) is rejected. Otherwise, do not reject null hypothesis

Conclusion

Since all six items recorded p-values of less than .001, which is far below the significance level of $\alpha = 0.05$, the null hypothesis is rejected for all factors.

The One-Sample t-test results confirm that peer influence is a statistically significant factor of cybercrime participation among undergraduate students at Federal University Lokoja. All six factors influence were rated significantly below the neutral midpoint of 2.5, with negative mean differences.

Objective 3

To provide recommendations for mitigating cybercrime participation and promoting ethical digital practices among students.

1. The finding shows that 100-level students recorded the highest cybercrime participation rate (72%), followed by 200-level (69%), calls for the immediate introduction of

mandatory cybersecurity awareness programme targeting students from their first year of study.

2. From the second objective One-Sample t-test confirmed that peer influence significantly influences cybercrime participation (t = -44.778, p = .001). The university should therefore establish structured peer mentorship schemes that will affects the power of peer networks positively by pairing vulnerable students with responsible senior students who can model ethical digital behavior.

3. Since peer introduction to cybercrime was the strongest influence factor (t = -44.778, p = .001), students clearly lack adequate ethical digital education. Cyber ethics, digital responsibility, and cybercrime law awareness should be formally integrated as a compulsory course unit within all the levels.

4. The significant influence of peers' financial gains on students' interest in cybercrime (t = -10.158, p = .001) tells us that economic pressure is a key factor. The school, private organizations and public sector should organize a scholarship scheme to reduce the rate of students involving themselves in cybercrime.

Discussion

Out of 400 questionnaires distributed, 385 were returned and valid for analysis, representing a response rate of 96.3%. The bar chart indicates that 100 Level students had the highest representation with 104 respondents (27.0%), followed by 400 Level with 100 respondents (26.0%), 300 Level with 95 respondents (24.7%), while 200 Level recorded the least with 86 respondents (22.3%). The pie chart shows that 90.91% of respondents own at least one internet-enabled device, while 9.09% reported not owning any. This indicates that the majority of the study population has access to internet-enabled devices, suggesting a high level of digital accessibility among the respondents. This confirms that cybercrime participation does not occur equally across all academic levels. 100-level students recorded the highest participation rate (72%), followed by 200-level (69%), 400-level (66%), and 300-level students (54%). The statement “seeing peers make money from cybercrime increases interest in it” recorded the highest agreement (69.3%), indicating that financial modeling through peer observation strongly motivates involvement. Similarly, 68.3% agreed that peers influence students’ involvement in cybercrime, while 71.2% confirmed that peer pressure can push students into such activities, collectively highlighting the role of peer networks in normalizing cybercriminal behavior among students.

Note!! This section is supposed to present finding according to each of the objectives without percentages/statistics.

Conclusion

This study concludes that peer influence significantly influences cybercrime participation among students. It also concludes that since peer introduction to cybercrime was the strongest influence factor, students clearly lack adequate ethical digital education. Additionally, the significant influence of peers' financial gains on students' interest in cybercrime indicate that economic pressure is a key factor.

Recommendations

In light of the results discussed above, the study advances the following recommendations. These recommendations were derived from the key findings and are intended to address the gaps and issues and issues identified in the course of the analyses. They also aim to provide practical and scholarly guidance for stakeholders, policy makers, and future researchers seeking to build on the knowledge generated through this study.

1. Given that students at the 100-level exhibited the highest rate of involvement in cybercrime, followed by those at the 200-level, there is a compelling need for the early introduction of mandatory cybersecurity awareness programmes. Such interventions should be implemented from the first year of study to inculcate responsible digital behavior at the onset of students’ academic journey. Additionally, structured academic engagement through increased coursework and supervised activities may serve as a preventive mechanism by minimizing idle time that could otherwise be exploited for involvement in cybercrime or related deviant activities.

2. It is recommended that institutions establish structured peer mentorship programmes aimed at positively harnessing the influence of peer networks. By promoting pro-social values and academic responsibility through guided peer interactions, such initiatives can mitigate negative peer pressure and reduce students’ susceptibility to cybercrime.

3. Cyber ethics, digital responsibility, and awareness of cybercrime legislation should be systematically integrated into the academic curriculum as compulsory course units across all levels of study. This would ensure that students are consistently exposed to the legal, ethical, and social implications of their online behavior throughout their academic progression.

4. There is a need for collaborative efforts between academic institutions, private sector organizations, and government agencies to develop and implement scholarship schemes and financial support programmes. These initiatives would help alleviate economic pressures that may drive some students toward cybercrime, while simultaneously promoting academic excellence and ethical conduct.

Weakness and Future Research

This study provide valuable inferences into the effectiveness of digital technology on degree project output of students of biotechnology, it is important to note that certain limitations may arise. These include potential biases in self-reported data, as participants may overestimate or underestimate their library usage or research productivity. Additionally, the study will focus on a single department, single university, limiting the generalizability of the findings to other institutions. This study is restricted to federal university Lokoja. Increasing the scope and frame to extend to other institutions in Nigeria can be a full study.

Note: This is not for this study please. Recheck.

Authors Contributions

All authors contributed immensely in the aspect of technical writing.

Acknowledgment

The authors thank the Federal University Lokoja and tertiary education trust fund (Tetfund) that makes resource material available to perfect this article.

Ethics

This is the original manuscript; there will be no expectation of any ethical problems. Ethical approval for this study was sought from the relevant institutional review board at Federal University Lokoja. Participation was voluntary, and informed consent will be obtained from all participants. The study ensured confidentiality and anonymity of responses, with all data used strictly for research purposes. Participants had the right to withdraw from the study at any point without consequence.

References

1. Adebayo, T., & Yusuf, A. (2019). Cybersecurity awareness in Nigerian universities: The role of educational institutions in safeguarding students. Journal of Educational Technology and Security, 10(2), 45-60.
2. Adebayo, T., & Yusuf, H. (2019). Cybercrime and peer influence in Nigerian universities: An emerging concern. *Journal of Social Media and Technology, 14*(1), 23-35.
3. Alabi, A., & Oladipupo, D. (2020). Peer influence and its role in the propagation of cybercrime among Nigerian undergraduates. International Journal of Cyber Socialization, 5(1), 47-58.
4. Aluko, O., & Odusanya, S. (2022). The impact of internet-enabled platforms on online harassment in Nigerian universities. Journal of Digital Safety, 5(1), 87-102.
5. Bandura, A. (1977). *Social learning theory*. Prentice-Hall.
6. Davies, C., & Dutton, T. (2015). Online cheating and exam fraud prevention: A review of technology in higher education. Educational Technology Research and Development, 63(3), 451-473.
7. Ibrahim, S., & Bello, M. (2020). Gender-based cybercrimes in Nigerian universities: A study on the vulnerabilities of female students. *Journal of Cybercrime and Education, 7(*3), 115-130.
8. Ibrahim, T., & Aminu, K. (2022). The relationship between financial hardship and cybercrime participation among Nigerian undergraduates. *Journal of Digital Ethics, 9*(2), 67-82.
9. Jagboro, O., & Akinrinmade, A. (2021). Gender and cybercrime: Exploiting vulnerabilities in Nigerian higher education institutions. *International Journal of Gender Studies and Technology, 8(*4), 212-229.
10. Maloku, A. (2020). Theory of differential association. *Academic Journal of Interdisciplinary Studies, 9*(1), 170-178.
11. Mesko, G. & Petrovic, B. (2004). *Kriminologija [Crimonology]*. Pravni Fakultet.
12. Nabavi, R. T., & Bijandi, M. S. (2012). Bandura's social learning theory & social cognitive learning theory. *Theory of developmental psychology*, *1*(1), 1-24.
13. Okeke, C., & Durojaiye, A. (2021). Cybercrime and university students: A gendered analysis of online harassment and fraud. *International Journal of Cyber Studies*, *5*(2), 121-138.
14. Okonkwo, P., Okojie, S., & Nwachukwu, I. (2020). Social engineering techniques and their impact on university students in Nigeria: A gender-based analysis. Journal of Information Security, 12(1), 78-92.
15. Olanrewaju, M., & Igbokwe, A. (2021). Cybercrime and its effects on university students' academic performance in Nigeria. *Cybercrime Studies, 6*(4), 50-63.
16. Olufemi, O., & Adesola, J. (2020). The role of technology in cybercrime participation among Nigerian university students. *Journal of Educational and Social Research*, *10*(2), 101-114.
17. Onu, L., & Eze, E. (2023). Integrating cybersecurity awareness into the curriculum: An analysis of Nigerian universities' response to rising cybercrime. Education and Technology Review, 16(3), 102-120.
18. Smith, J., & Adeyemi, M. (2020). The rise of digital fraud and its impact on Nigerian university students. *Journal of Cyber Fraud and Crime*, *7*(2), 45-59.
19. Sutherland, E. H. (1949). *White collar crime*. Dryden Press.
20. Williams, R., & Yusuf, H. (2021). Enhancing gender-sensitive cybersecurity policies for Nigerian higher education institutions. *Gender and Technology Journal*, *3*(1), 14-29.