African Journal of Interdisciplinary Research and Policy Studies (AJIRPS)

Journal home page: https://ojs.universityedu.org/index.php/ajirps

Article

Knowledge and Adherence to Cyber Crime Act of Nigeria among Undergraduates of Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State

Chinonso Adikuru
Department of Mass Communication, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State. Nigeria.

Shadrach Idi
Department of Mass Communication, Taraba State University, Jalingo. Nigeria

Citation:

Adikuru C. and Idi S. (2026). Knowledge and Adherence to Cyber Crime Act of Nigeria among Undergraduates of Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State. *African Journal of Interdisciplinary Research and Policy Studies*. 1(1), 75-85.

Received: July 23, 2026
Accepted: September 29, 2026
Published: September 29, 2026

License: CC BY 4.0

Open Access article.

Abstract: This study examines the knowledge and adherence to the Cybercrime Act of Nigeria among undergraduate students at Chukwu Odumegwu Ojukwu University (COOU), Igbariam, Anambra State. The study employed a quantitative survey research design, with a sample size of 384 selected using Krejcie and Morgan's sampling table. Data were collected through an online questionnaire and analyzed using descriptive statistics, including frequency counts, percentages, mean scores, and standard deviation. The findings reveal a moderate awareness of cybercrimes among students, but a low understanding or knowledge of the specifics of the Cybercrime Act, including penalties and enforcement mechanisms. Additionally, the study found low adherence to the provisions of the Act, with most students unconcerned about engaging in activities that could potentially violate the law. The study recommends that universities integrate comprehensive education on the Cybercrime Act into their curriculum, collaborate with law enforcement agencies to raise awareness, and establish cyber safety clubs in universities to improve students' adherence to the law and their protection from cyber threats.

Keywords: Adherence, Awareness, Cyber Crime Act, Knowledge, Undergraduates.

Introduction

New media technologies, such as the internet, smartphones, and social media, have revolutionised communication globally. This advancement has transformed nearly every aspect of human life, including personal interactions, commerce, education, and healthcare. It has significantly contributed to socio-economic development by enabling organisations and governments to improve service delivery. This evolution also has served as a platform for youth mobilization and advocacy by making governments and its institutions accountable (Adikuru & Obiora, 2021). Moreover, new media technologies have created numerous job opportunities, particularly for youths. Across the globe, young innovators, including those in Nigeria, have leveraged these technologies to achieve financial independence and address societal challenges, thereby fostering societal growth (Ekwenchi & Shadrach, 2023, Obiora, Uche & Adikuru, 2025).

*Correspondence: cc.adikuru@coou.edu.ng

However, the rise of new media technologies has introduced unprecedented challenges, particularly in the form of cybercrime. As industries increasingly integrate these technologies, criminal elements have adapted, employing sophisticated strategies to exploit digital platforms (AllahRakha, 2024). Cybercrime has become one of the most pervasive global threats, manifesting in various forms such as internet fraud, cyberbullying, and data breaches. These crimes carry financial, social, and physical repercussions. For instance, the Centre for Strategic and International Studies (CSIS) estimates that cybercrime inflicts $600 billion in annual losses on the global economy (CSIS, 2018).

Nigeria is among the countries most severely affected by cybercrime. According to the Nigerian Communications Commission (NCC), the nation loses approximately $500 million annually to cybercrime, with individual victims suffering losses averaging ₦1.2 million per attack (Sibe, 2024). Beyond financial implications, cybercrime has tarnished Nigeria's global image (Mordi, 2019; Igba et al., 2018) and extended to life-threatening incidents such as rape and murder (Apantaku, 2021).

In response to this menace, various regional and national legislation has been established to combat cybercrime. Globally, frameworks such as the European Union's General Data Protection Regulation (GDPR) and Africa's African Union Convention on Cyber Security and Personal Data Protection aim to enhance digital security. Nationally, the United Nations Conference on Trade and Development (UNCTAD, 2016) reports that cyber laws have been enacted or are pending adoption in 194 member countries. In Nigeria, the Cybercrime (Prohibition, Prevention, etc.) Act was enacted in 2015 to address crimes such as identity theft, hacking, and financial fraud, aiming to protect individuals, organisations, and the government (Ibrahim et al., 2023). Despite the existence of this Act, cybercrime remains a growing concern in the country.

Research highlights that university students are among the major users of the internet. They utilise it for various purposes, including academic research, social interactions, and entertainment. Studies reveal that undergraduate students spend significant screen time engaging in online social interactions (Shadrach, 2020; Shadrach & Abugu, 2021). This extensive online presence makes undergraduates not only vulnerable to cybercrimes but also potential perpetrators of offences such as internet fraud, cyberbullying, and identity theft. Despite the enactment of the Cybercrime Act in 2015, reports of cybercrimes in Nigeria have continued to rise, with a significant proportion of culprits being young individuals, many of whom are university students.

This study aims to interrogate the knowledge, awareness, and behavioural adherence of undergraduates at Chukwuemeka Odumegwu Ojukwu University (COOU) to the Cybercrime Act, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State, represents a microcosm of the Nigerian youth population within the academic setting. Its student demographic reflects the broader societal trends in technology adoption and online behaviour.

Statement of the problem

Cybercrime Act is designed to mitigate the increasing menace of cybercrime that has bedeviled the Nigeria Internet space and undermining its effective utilization or meaning economic and personal goal among many people. However, whether, individuals especially undergraduate students of universities in Nigeria are aware of the Act remains under researched. Existing research has extensively explored the economic and social implications of cybercrime, but there is a dearth of studies focusing on the awareness, knowledge, and behavioural responses of university students to cybercrime legislation. Specifically, limited attention has been given to understanding how undergraduates at institutions like Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State, engage with the Cybercrime Act and its provisions. This lack of scholarly focus creates a critical gap in the literature, as understanding this population's interaction with cybercrime legislation is essential for designing effective awareness campaigns and enforcement strategies. This study seeks to address this gap by investigating the knowledge and behaviour of undergraduates at Chukwuemeka Odumegwu Ojukwu University regarding the Cybercrime Act. It aims to provide empirical evidence on their level of awareness, compliance, and attitudes toward the legislation, thereby contributing to broader efforts to mitigate cybercrime in Nigeria.

Objectives of the Study

The objective of this study is to investigate the knowledge of and adherence to the Cybercrime Act among undergraduate students of COOU, Igbariam, Anambra State. The specific objectives are as follows:

1. To determine the level of awareness of the Cybercrime Act among undergraduate students of COOU.
2. To ascertain the level of knowledge about the Cybercrime Act among undergraduate students of COOU.
3. To examine the level of adherence to the provisions of the Cybercrime Act among undergraduate students of COOU.

Research questions

The research questions for this study are as follows:

1. What is the level of awareness of the Cybercrime Act among undergraduate students of COOU?
2. What is the level of knowledge about the Cybercrime Act among undergraduate students of COOU?
3. To what extent do undergraduate students of COOU adhere to the provisions of the Cybercrime Act?

Theoretical Framework

The study is anchored on the Theory of Planned Behaviour (TPB) by Ajzen (1991), which posits that individuals' decisions to take specific actions are influenced by three key factors: attitude, subjective norms, and perceived behavioural control. Attitude refers to the degree to which an individual evaluates the outcome of an action as either positive or negative. Subjective norms involve the influence of social pressures and the expectations of significant others, such as peers, family, and society. Perceived behavioural control relates to an individual's belief in their capability to perform a particular behaviour (Ajzen, 2011).

The theory is particularly relevant to this study as it provides a framework for analysing students' attitudes towards the Cybercrime Act. For example, if students perceive adherence to the Cybercrime Act as beneficial—such as protecting their personal data and avoiding legal consequences—they are more likely to comply. Conversely, if they view the Act as irrelevant or overly restrictive, they may disregard its provisions. Additionally, undergraduate students' behaviours towards the Act can be influenced by subjective norms, such as their social circles, including friends, online communities, and societal expectations. If their peers value compliance with the Cybercrime Act, students may feel motivated to adhere to its regulations. On the other hand, a culture of disregard for such laws within their peer groups could encourage non-compliance.

Finally, perceived behavioural control plays a critical role in shaping students' adherence to any safety requirements. This involves their perception of their ability to understand and follow the provisions of the Cybercrime Act. Adequate knowledge and understanding of the Act can boost students' confidence in adhering to it, whereas a lack of understanding may lead to unintentional violations. By applying the TPB, the study seeks to explore these behavioural dynamics and their influence on students' knowledge and adherence to the Cybercrime Act.

Literature Review

Cybercrime Act of Nigeria

The Cybercrime Act**,** is a Nigerian law designed to address the growing concerns of cybercrimes and ensure cybersecurity within the country. It was signed into law in 2015 to provide a legal framework for the prevention, detection, investigation, and prosecution of cybercrimes, as well as to regulate electronic communications and transactions. Before the establishment of the Cybercrime (Prohibition, Prevention, etc.) Act, Nigeria had several legislations aimed at tackling crimes, including cybercrimes. These included the Nigeria Criminal Code Act of 1990, the Economic and Financial Crimes Commission Act of 2004, and the Advance Fee Fraud and Other Related Offences

Act of 2006. However, none of these laws were specifically designed to comprehensively address the challenges posed by cybercrimes. They were considered inadequate due to the evolving nature of technology and the increasing adoption of digital platforms by Nigerians (Maitanmi, Ogunlere, Ayinde, & Adekunle, 2013). This inadequacy created the need for a more robust framework, culminating in the enactment of the Cybercrimes Act of 2015.

The journey toward the Cybercrime Act began in September 2008, when the Nigerian government proposed a bill titled *"A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for Other Related Matters."* The bill aimed to revise and consolidate existing legislation to address electronic fraud effectively. It passed its second reading in November 2012, but the increasing prevalence of fraudulent activities, public outcry over cyber-related crimes, and the insufficiency of existing laws prompted further action. These factors led to the signing of the Cybercrime (Prohibition, Prevention, etc.) Act into law in May 2015 (Moga, Galle, & Rukayyat, 2021).

The Cybercrime Act of 2015 established a comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, investigation, and prosecution of cybercrimes. It aimed to ensure cybersecurity and the protection of computer systems, networks, and electronic communications. According to Obi and Uji (2023), the Act was a significant step in discouraging negative online behaviours such as cyberstalking, cybersquatting, computer-related fraud and forgery, and cyberterrorism. Additionally, the Act sought to protect Critical National Information Infrastructure and uphold privacy rights, intellectual property, and data security.

In 2025, the Act underwent significant revision with the passage of the Cybercrime (Prohibition, Prevention, etc.) (Amendment) Act of 2024. This amendment introduced key changes that enhanced Nigeria's cybersecurity framework, further strengthening its ability to address emerging challenges in the digital space (Ugwuoke, 2024). The Cybercrime Act represents a critical step in Nigeria's effort to align with global standards for combating cybercrime and safeguarding the digital ecosystem, providing a much-needed framework for addressing both current and future cyber threats.

Review of Empirical Studies

There are few studies that focus on the knowledge and attitudes toward cyber laws, which highlight varying levels of awareness and understanding across different populations. Scholars like Jordaan (2015) investigated South African adults' awareness of the Protection of Personal Information Act, 4 of 2013. The study, conducted in selected suburbs of Pretoria, revealed that 71% of South Africans were unaware of the Act. This lack of awareness is not unique to South Africa. O'Keefe and Connolly (2011) found similar gaps in knowledge regarding privacy regulations in the United States, while Dommeyer and Gross (2003) reported similar findings in Australia. These studies collectively point to a general lack of awareness regarding cyber laws in these regions.

In India, Parmar and Patel (2016) surveyed netizens and found that, regardless of their information technology (IT) background, most individuals were unable to stay updated with the latest developments in cyber law and computer security. This problem was even more pronounced among those not working in the IT sector. A related study by Mehta and Singh (2013) examined cyber law awareness in Indian society and uncovered significant gender disparities in knowledge, with male internet users showing greater awareness than their female counterparts.

Svensson (2022) conducted a study on millennial men in Sweden to assess their understanding of governmental data collection practices online. The qualitative study, which involved 16 semi-structured interviews, found that most participants lacked knowledge of how data collection is conducted and were unfamiliar with the relevant regulatory framework. Similarly, Tahir et al. (2024) explored the awareness and understanding of cybersecurity rules among Pakistan's general population. They gathered data from a diverse sample, including IT professionals, law enforcement officers, legal experts, and the general public. The results indicated varying levels of comprehension, with IT professionals and legal experts demonstrating a higher level of understanding. The study identified key barriers to awareness, such as rapid technological changes, insufficient public awareness, and limited resources for law enforcement.

In Nigeria, Shadrach and Ekwenchi (2023) investigated millennials at Federal Universities in the northeast region to assess their knowledge of cyber protection measures, including the Cybercrime Act. The study revealed a concerning lack of knowledge among participants about the Act and other legislative measures. Similarly, Mejabi, Awoniyi, Oyekunle, and Azeez (2018) examined the legal and technical knowledge of cybersecurity protection among students at the Federal University of Technology Minna. Their study, which involved 160 respondents, found a generally low level of knowledge about legal data privacy protection. Tiwalade, Dawson, and Batmaz (2015) conducted research on Nigerians' perceptions of personal data protection and privacy. Their findings indicated that while Nigerians were aware of cyber risks, particularly those involving financial data theft, they expressed a lack of trust in the government's ability to protect their data effectively through legislation or enforcement. These studies illustrate a widespread lack of knowledge about cyber laws, data protection, and privacy across different countries, highlighting the importance of increased awareness and education on these crucial issues.

Methodology

This study employed a quantitative survey research design to examine the knowledge and adherence to the Cybercrime Act among undergraduate students at Chukwuemeka Odumegwu Ojukwu University (COOU), Igbariam, Anambra State. The population of students from the office of the Registrar is 15,130. A sample size of 384 was selected using Krejcie and Morgan's sampling table. The multi-stage sampling technique was used to select the respondents. In the first stage, COOU was divided into its respective faculties. The second stage involved the random selection of one department from each faculty. The third stage focused on selecting the study unit, where random sampling through balloting was applied at each stage to ensure fairness and representativeness. Data for the study were collected via an online questionnaire. The collected data were then analyzed using descriptive statistics, particularly simple percentages frequency counts, mean score and standard deviation with tables used to present the findings. This approach allowed for a comprehensive understanding of the students' awareness and adherence to the Cybercrime Act.

Analysis and Presentation of Data

Table 1: Demographic Description of Respondents

Demographic Category	Frequency (f=384)	Percentage (%)
Gender		
Male	220	57.29%
Female	164	42.71%
Level in School		
Year 1	80	20.83%
Year 2	60	15.63%
Year 3	100	26.04%
Year 4	50	13.02%
Year 5	94	24.48%
Age Bracket		
18-20	150	39.06%
21-25	180	46.88%
26-30	38	9.90%
31-35	16	4.17%
Extent of Internet Use		
High	350	91.15%
Moderate	30	7.81%
Low	4	1.04%

Source: Online Survey, 2026

Table 1 above provide information regarding the characteristics of the respondents. The study showed a higher representation of male respondents, with 220 males (57.29%) compared to 164 females (42.71%). This indicates that the male undergraduates at Chukwuemeka Odumegu Ojukwu University, Igbariam, Anambra State, were more likely to participate in the study. This gender disparity could reflect the general gender composition of the student population at the university. The majority of respondents were from higher academic levels, particularly Year 3 (100 respondents, 26.04%) and Year 5 (94 respondents, 24.48%). These two groups together accounted for over half of the total sample. Year 1 students were the next largest group, with 80 respondents (20.83%), followed by Year 2 students at 60 (15.63%) and Year 4 students at 50 (13.02%). The larger representation of students in Year 3 and Year 5 suggests that these groups may have a more established understanding and experience with the university system, potentially influencing their awareness of the Cybercrime Act.

The respondents were predominantly between the ages of 18 and 25, which is typical for undergraduate students. A total of 150 respondents (39.06%) were in the 18-20 age bracket, while 180 respondents (46.88%) fell within the 21-25 range. Together, these two age groups made up 85.94% of the total sample, reflecting the age demographics of the university's student body. Smaller numbers of respondents were in the 26-30 (9.90%) and 31-35 (4.17%) age groups, indicating that older undergraduates were less represented in the study. Furthermore, the study participants showed a high level of internet engagement, with 350 respondents (91.15%) reporting high usage. A smaller proportion of respondents, 30 (7.81%), reported moderate internet usage, and only 4 respondents (1.04%) indicated low internet use. This suggests that most undergraduates at Chukwuemeka Odumegu Ojukwu University are highly familiar with the internet, which is particularly relevant when examining their knowledge and adherence to the Cyber Crime Act, as internet activity plays a central role in cybercrimes.

Table 2: Level of awareness of the Cybercrime Act among undergraduate students of COOU?

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean (X)	SD
I am aware of cybercrimes in Nigeria.	50 (13.02%)	60 (15.63%)	120 (31.25%)	100 (26.04%)	54 (14.06%)	3.13	1.22
I have read about the Cybercrime Act.	70 (18.23%)	90 (23.44%)	110 (28.65%)	80 (20.83%)	34 (8.85%)	2.79	1.22
I often hear discussions in the media about the Cybercrime Act.	60 (15.63%)	70 (18.23%)	140 (36.46%)	90 (23.44%)	24 (6.25%)	2.86	1.13
I am aware of the penalties outlined in the Cybercrime Act for cyber-related offences.	80 (20.83%)	100 (26.04%)	120 (31.25%)	70 (18.23%)	14 (3.65%)	2.58	1.12
I am aware of the key stakeholders responsible for implementing and enforcing the Cybercrime Act.	90 (23.44%)	80 (20.83%)	110 (28.65%)	70 (18.23%)	34 (8.85%)	2.68	1.26
Cumulative Score						**2.81**	**1.20**

N=384, *Criterion Mean:* 3.0*and above =High; 2.50-2.90=Moderate,* $\bar{x}$*≤=Low awareness*

Table 2 presents data regarding the level of awareness of the Cybercrime Act among undergraduate students of COOU. The mean scores (X) for individual items reveal a moderate level of awareness overall, with a cumulative mean of 2.81 and a standard deviation (SD) of 1.20. While the majority of respondents showed awareness of cybercrimes in Nigeria (mean = 3.13, SD = 1.22), awareness of specific aspects of the Cybercrime Act, such as reading about it (mean = 2.79, SD = 1.22) and hearing media discussions (mean = 2.86, SD = 1.13), was moderate. Awareness of the penalties outlined in the Act (mean = 2.58, SD = 1.12) and key stakeholders responsible for enforcement (mean = 2.68, SD = 1.26) was comparatively lower. These findings suggest that the undergraduate students of COOU have moderate exposure to the Cybercrime Act.

Table 3: Level of Knowledge about the Cybercrime Act among Undergraduate Students of COOU

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	(X)	(SD)
I know the purpose of the Cybercrime Act in Nigeria.	80 (20.83%)	100 (26.04%)	120 (31.25%)	50 (13.02%)	34 (8.85%)	2.58	1.15
I understand the types of cybercrimes addressed by the Cybercrime Act.	90 (23.44%)	110 (28.65%)	120 (31.25%)	40 (10.42%)	24 (6.25%)	2.50	1.17
I am know the penalties associated with specific cyber offences.	100 (26.04%)	110 (28.65%)	120 (31.25%)	30 (7.81%)	24 (6.25%)	2.44	1.18
I can identify examples of activities that are considered cybercrimes.	90 (23.44%)	100 (26.04%)	130 (33.85%)	40 (10.42%)	24 (6.25%)	2.50	1.14
I know the rights and responsibilities of individuals as stated in the Cybercrime Act.	110 (28.65%)	120 (31.25%)	100 (26.04%)	40 (10.42%)	14 (3.65%)	2.40	1.16
I can explain the role of law enforcement agencies in implementing the Cybercrime Act.	120 (31.25%)	110 (28.65%)	90 (23.44%)	50 (13.02%)	14 (3.65%)	2.39	1.19
I understand the legal implications of violating the provisions of the Cybercrime Act.	100 (26.04%)	110 (28.65%)	120 (31.25%)	40 (10.42%)	14 (3.65%)	2.46	1.17
Cumulative score						2.47	1.17

N=384, *Criterion Mean:* 3.0*and above =High; 2.50-2.90=Moderate,* $\bar{x}$*≤=Low*

The Table above presents data on the level of knowledge about the Cybercrime Act among undergraduate students of COOU. The outcome shows that the overall knowledge is poor, with a cumulative mean score of 2.47**,** which is within the "Low" knowledge range according to the criterion mean. The individual item mean scores range from 2.39 to 2.58**,** indicating that students generally lack in-depth knowledge about the Cybercrime Act. Most students either "Strongly Disagree" or "Disagree" with statements about their understanding of key provisions of the law, such as the purpose of the Act, types of cybercrimes, penalties for cyber offences, and the roles of law enforcement agencies.

Table 3: Adherence to the Provisions of the Cybercrime Act among Undergraduate Students of COOU

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	X	SD
I avoid engaging in online activities that violate the Cybercrime Act.	100 (26.04%)	110 (28.65%)	120 (31.25%)	40 (10.42%)	14 (3.65%)	2.38	1.19
I do not participate in online fraud or any activities related to cybercrime.	110 (28.65%)	120 (31.25%)	90 (23.44%)	40 (10.42%)	24 (6.25%)	2.41	1.21
I respect the intellectual property rights of others when using the internet.	90 (23.44%)	110 (28.65%)	130 (33.85%)	40 (10.42%)	14 (3.65%)	2.45	1.16
I refrain from spreading false information or cyberstalking others online.	110 (28.65%)	100 (26.04%)	120 (31.25%)	40 (10.42%)	14 (3.65%)	2.42	1.18
I report cybercrimes or violations of the Cybercrime Act to the authorities.	120 (31.25%)	110 (28.65%)	90 (23.44%)	50 (13.02%)	14 (3.65%)	2.38	1.19
I take personal responsibility for ensuring my online activities comply with the Cybercrime Act.	90 (23.44%)	110 (28.65%)	120 (31.25%)	50 (13.02%)	14 (3.65%)	2.41	1.17
I avoid sharing or using unauthorized copyrighted content on the internet.	100 (26.04%)	110 (28.65%)	120 (31.25%)	40 (10.42%)	14 (3.65%)	2.42	1.19
Cumulative score						2.40	1.18

N=384, *Criterion Mean:* 3.0*& above =High; 2.50-2.90=Moderate,* $\bar{x}$*≤=Low*

Table 4 above present data on adherence to the provisions of the Cybercrime Act among undergraduate students of COOU. The result shows that the overall adherence is low, as reflected by the cumulative mean score of 2.40, which falls below the "moderate" category threshold of 2.50. For each item, the mean scores range from 2.38 to 2.45, indicating that most students either engage in online activities that could violate the Cybercrime Act or do not fully comply with its provisions. The highest percentage of students selected responses indicating "Strongly Disagree" or "Disagree" for most items, suggesting a significant lack of adherence to ethical online behavior. The standard deviation for all items ranges from 1.16 to 1.21, showing a moderate level of variability in the responses, but the general trend points to poor adherence to the Cybercrime Act.

Discussion of findings

The findings from this study highlight a concerning trend regarding the awareness, knowledge, and adherence to the Cybercrime Act among undergraduate students at COOU. In terms of awareness, the students demonstrated a moderate understanding of cybercrimes in Nigeria, with some exposure to the Cybercrime Act through media discussions and readings. However, their awareness of specific details, such as the penalties outlined in the Act and the stakeholders responsible for its enforcement, was noticeably lower. This suggests that while students may have a general awareness of the issue of cybercrime, they are not sufficiently informed about the legal framework designed to combat it. These findings support prior research on the subject. Tahir et al. (2024) observed that the general public in Pakistan struggled with awareness. Similarly, in South Africa, Jordaan (2015) found that a significant portion of the population was unaware of the Protection of Personal Information Act, a legal framework similar to Nigeria's Cybercrime Act.

When it comes to knowledge, the findings reveal a gap in students' comprehension of the Cybercrime Act. Despite some level of awareness of cybercrimes, their understanding of the law's purpose, the types of cybercrimes it addresses, and the penalties for violating its provisions remains weak. This lack of knowledge suggests that although students may be exposed to the topic, there is insufficient emphasis on educating them about the specifics of the law, its implications, and their role in adhering to it. The findings of this study align with and support prior research regarding the general lack of awareness about cyber laws, particularly the Cybercrime Act. Svensson (2022) revealed that millennials in Sweden lacked understanding of governmental data collection and the regulatory framework, which resonates with the finding that students at COOU lack detailed knowledge of the Cybercrime Act's purpose, penalties, and enforcement mechanisms. Similarly, Shadrach and Ekwenchi's investigation into the knowledge of the Cybercrime Act among Nigerian university students showed a similar pattern of poor knowledge, mirroring the results of this study. Mejabi et al.'s (2018) study at the Federal University of Technology Minna also revealed low levels of knowledge regarding legal data protection, further reinforcing the finding that students at COOU have a limited understanding of cyber law.

The study also revealed the students' adherence to the provisions of the Cybercrime Act. The data show that most students are unconcerned about engaging in activities that could potentially violate the Act. As a result, their adherence to the provisions of the Act is low. These findings align with those of Ekwenchi and Shadrach (2024), who revealed a poor attitude toward cyber protection strategies among students, where they did not utilize the legal framework to regulate their cyber behavior or protect themselves from cyber-attacks.

In relation to the Theory of Planned Behaviour (TPB), the low adherence and knowledge levels observed in this study can be linked to the components of the theory. The students' attitudes towards the Cybercrime Act appear to be influenced by their lack of knowledge about the potential consequences of non-compliance, which could lead to negative outcomes. This lack of awareness may reduce their perceived behavioral control, leading them to underestimate the importance of adhering to the Cybercrime Act. Furthermore, social norms within the student population may also play a role, with students possibly not feeling societal pressure to comply with the Cybercrime Act, contributing to low levels of adherence.

Conclusion and Recommendations

The findings from this study highlight significant gaps in the awareness, knowledge, and adherence to the Cybercrime Act among undergraduate students at COOU. While the students demonstrated a moderate awareness of cybercrimes, their understanding of the specifics of the Cybercrime Act, including penalties and enforcement mechanisms, was notably lacking. Furthermore, the students' knowledge of the law's purpose, the types of cybercrimes it addresses, and the penalties for violations was insufficient, reflecting an overall lack of in-depth understanding. This knowledge gap, coupled with low adherence to the provisions of the Act, suggests that students are not fully equipped to comply with the law or protect themselves from potential cyber threats. Based on the findings, the study recommends that:

1. Institutions should collaborate with law enforcement agencies to raise awareness about the Cybercrime Act. Collaboration could also include hosting joint events where students can interact directly with law enforcement officers, gaining a better understanding of how the Act is enforced and the penalties for violations.
2. There is an urgent need for universities to integrate more comprehensive education on the Cybercrime Act into their curriculum. This education should focus on the specific provisions of the Act, including penalties, the roles of enforcement agencies, and the consequences of cybercrime. Such efforts could increase students' knowledge and foster a greater understanding of the importance of adhering to cyber laws.
3. Security agencies involve in the implementation of the Cybercrime Act should intensify surveillance to improve compliance among the populace especially among students. They should create cyber safety clubs in universities to encourage cyber safety practices among study.

References

Adikuru, C. C., & Obiora, A. V. (2021). Social media as an avenue for youth mobilization for national security: A study of the Endsars protest in Nigeria. *GVU Journal of Communication Studies,* 3, 15-23

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Albarracín, D., Johnson, B. T., Fishbein, M., & Muellerleile, P. A. (2001). Theories of reasoned action and planned behavior as models of condom use: a meta-analysis. *Psychological bulletin*, *127*(1), 142–161. https://doi.org/10.1037/0033-2909.127.1.142

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Apantaku, P. O. (2021). *Cybercrime: Motivations, modes, and emerging trends with Nigeria as a case study* (Doctoral thesis, University of Portsmouth). University of Portsmouth, Institute of Criminal Justice Studies.

AllahRakha, N. (2024). Transformation of crimes (Cybercrimes) in digital age. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.156 Center for Strategic and International Studies (CSIS)**.** (2018, February). *Economic impact of cybercrime—No slowing down.* https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Dommeyer, C.J. & Gross, B.L. 2003. What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing,* 17(2):34–51

Ekwenchi, O.C & Shadrach, I. (2023b.). Awareness, Concern, Knowledge, and Attitude to Online Data Privacy Risks and Protection Strategies among Millennials at Selected Federal Universities in North-East Nigeria. *Makurdi Journal of Communication Research*, 10 (2), 1-17.

Ibrahim, Y. A., Faki, S. A., Yusuf, M., Usman, A. S., Ishaya, A. O., Brijik, A. H., Aremu, J. O., & George, C. A. (2023, November 21–23). *Cybercrime and cyber law in Nigeria: An overview of challenges and way forward.* In *Proceedings of the International Conference on Computing and Advances in Information Technology (ICCAIT 2023)* (pp. xx–xx). Ahmadu Bello University.

Igba, D. I., Igba, E. C., Nwambam, A. S., Nnamani, S. C., Egbe, E. U., & Ogodo, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research,* 13(2), 1144–1154.

Imam, M. A. N. A., & Usman, G. I. (2024). Cyber crimes as emerging global threats: Nigerian context. *International Journal of Social Sciences and Management Research,* 10(5), 196. https://www.iiardjournals.org

Jang, Y., & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework-A Focus on Digital Policies in Australia, Canada, and the UK. *Children (Basel, Switzerland)*, *10*(8), 1415. https://doi.org/10.3390/children10081415

Jegede, A. E., Olowookere, E. I., & Elegbeleye, A. O. (2016). Youth identity, peer influence, and internet crime participation in Nigeria: A reflection. *Ife PsychologIA, 24*(1), 37–47. © 2016 Ife Centre for Psychological Studies/Services, Ile-Ife, Nigeria.

Jordaan, Y. (2015). Public awareness and concerns relating to the Protection of Personal Information Act. *African Journal of Public Affairs*, *8*(2), June.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Moga, E., Galle, S. A. (Ph.D.), & Rukayyat, A. (2021). A historical assessment of cybercrime in Nigeria: Implication for schools and national development. *Journal of Research in Humanities and Social Science, 9*(9), 84-94. https://www.questjournals.org

Mordi, M. (2019). "Is Nigeria Really the Headquarters of Cybercrime in the World?" Guardian. https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-inthe-world/. Accessed March 25, 2020.

Nwokoro, C. V., Chima, F. O., Ndom, D. A., & Iheonu, O. M. (2022). Youth's engagement in cybercrime (Yahoo-Yahoo) in Owerri Municipal of Imo State, Nigeria. *Journal ofEducation & Social Policy, 9*(4), 117. https://doi.org/10.30845/jesp.v9n4p13

Nzeakor, O. F. , Nwokeoma, B. N. , Hassan, I. , Ajah, B. O. & Okpa, J. T. (2022). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(3), 41-67. Available at: https://vc.bridgew.edu/ijcic/vol5/iss3/4

Obiora, A. V., Uche, O. A., & Adikuru, C. C. (2025). Encoding and decoding of emoji on social media for expression sharing among university students in Anambra State. DOI: 10.52589/AJSSHR-IWUY1DYS

O'Keefe, C.M. and Connolly, C. 2011. Regulation and perception concerning the use of healt data for research in Australia. Electronic Journal of Health Informatics, 6(2):1–13.Available from: http://www.ejhi.net/ojs/ index.php/ejhi/article/view/135 (Accessed: 2014 02-27).

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cyber crimes and cyber laws in Nigeria. *The International Journal of Engineering and Science (IJES), 2*(4), 19-25.

Shadrach, I. Anthony, G., & Mohammed, A. (2023). Making sense of Mobile Applications' Terms and conditions: Perspectives of Users in Taraba State, *IMSU Journal* of Communication Studies, 7 (1),1-12.

Sibe, R**.** (2024). Cybercrime and the challenge of static legislations in Nigeria. *Forbes Technology Council.*https://www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and the-challenge-of-static-legislations-in-nigeria/

Tahir, M. I., Sheraz, M. M., Asghar, M. S., Rafique, M. Z., Saqib, K. M., Ali, M. N., Shabbir, M., & Alam, B. (2024). Public awareness and understanding of cybersecurity legislation in Pakistan: A qualitative study on perceptions, knowledge, and compliance. *Remittances Review, 9*(3), 588-611. https://doi.org/10.33282/rr.vx9i2.33

Tiwalade, A., Dawson, R. & Batmaz, F. (2015). Nigerians' perceptions of personal data protection and privacy. https://www.researchgate.net/publication/275968129_Nigerians'_Perceptions_of_Personal_Data_Protection_and_Privacy

Udelue, M. C., & Mathias, B. (2019). Prevalence of cybercrimes among youths in Onitsha South Local Government Area of Anambra State, Nigeria. *International Journal of Health and Social Inquiry, 5*(1),

Ugwuoke, C. (2024). *Review of the 2024 amendment to the Cybercrimes Act*. Retrieved from https://kennapartners.com/review-of-the-2024-amendment-to-the-cybercrimes-act/

UNCTAD (2016, April 19). *Data protection frameworks must be compatible with international data flows for developing countries to benefit from the global digital economy*.https://unctad.org/news/data-protection-frameworks-must-be-compatible-international-data-flows-developing-countries