Investigating Undergraduate Students Levels of Cybercrime Awareness: A Study of Northwest University Sokoto, Sokoto State, Nigeria

Kamal Muhammad Sani [1], Mukhtar Abubakar Hassan [2], Mubarak Saidu [3], Sirajo Kabiru Umar [4], and Umar Dahiru Tata [5]

[1]Department of Sociology, Faculty of Management and Social Sciences, Rayhaan University Birnin Kebbi, Kebbi State, Nigeria

[2]Department of Psychology, Faculty of Management and Social Sciences, Northwest University Sokoto, Kalambaina Sokoto State, Nigeria

[3]Department of Sociology and Anthropology, Faculty of Social Sciences, University of Nigeria, Nsukka, Enugu State, Nigeria

[4]Department of Computer Science, Faculty of Computing and Sciences, Northwest University Sokoto, Kalambaina, Sokoto State, Nigeria

[5]Administrative Unit, Northwest University Sokoto, Kalambaina, Sokoto State, Nigeria

Correspondence: Kamal Muhammad Sani, Department of Sociology, Faculty of Management and Social Sciences, Rayhaan University Birnin Kebbi, Kebbi State, Nigeria

Email: kamalmsani92@gmail.com

Doi: 10.23918/ijsses.v12i1p19

Abstract: The purpose of this study was to examine the levels of cybercrime awareness among undergraduate students at Northwest University Sokoto (NWUS), a private university located in Kalambaina, Wammako Local Government Area, Sokoto State, Nigeria. We used a structured questionnaire to collect data from a sample of 125 undergraduate students (70 male and 55 female students). According to the study's results, the majority of the surveyed undergraduate students had a basic knowledge of prevalent cybercrimes such as identity theft, phishing attacks, revenge pornography, cyberbullying, and computer hacking, with males showing a higher awareness compared to their female pairs. However, the study discovered that the majority of the surveyed students showed a lack of awareness regarding cybercrime laws. These findings emphasized the need for educational institutions, including tertiary, secondary, and primary schools, to develop and integrate cybercrime education into the curriculum, which is crucial for equipping students, especially the vulnerable, with knowledge about cybercrime and cybersecurity to safeguard themselves. The study suggests that periodic seminars, workshops, and conferences should be organized for both students and staff to educate them about cybercrime and measures to prevent cybercrime victimization.

Keywords: Undergraduate Students, Cybercrime, Awareness, Cybercrime Victimization, Northwest University Sokoto, Nigeria

Received: 24.04.2024
Accepted: 13.11.2024
Sani, K. M., Hassan, M. A., Saidu, M., Kabiru, S., & Tata, U. D. (2024). Investigating Undergraduate Students Levels of Cybercrime Awareness: A Study of Northwest University Sokoto, Sokoto State, Nigeria. *International Journal of Social Sciences & Educational Studies*, 12(1), 19-39.

1. Introduction

The advent of the internet remains one of the best technological advancements in the world. Internet use has become a fundamental aspect of everyday life. According to Hassan (2013), in today's digital era, people depend on the internet for different activities such as social interaction, research, administration, and e-commerce. Despite the achievements that the internet has brought, it has also paved the way for new social issues, such as cybercrime. Scholars have identified cybercrime as a widespread form of criminal activity that has tormented human society. Okeshola and Adeta (2013) describe cybercrime as the online behaviors that are prohibited by law, including data breaches, online scams, cyberstalking, revenge porn, cyberbullying, cyberterrorism, phishing, and identity theft.

There has been a steady increase in the menace of cybercrime globally. It has negatively affected individuals, businesses, and public infrastructure. Over the last two decades, cybercrimes have claimed over 6.5 million victims, with an estimated loss of over $26 billion (Palatty, 2023). Statistics show that the menace of internet crime has increased. The Internet Crime Complaints Centre (IC3) received over 3.26 million cybercrime complaints, with adjusted losses estimated at $27 billion across the globe (Internet Crime Complaint Center, 2022). The global expansion of internet connectivity will widen the window of vulnerability for cybercrime. The next five years will experience a 15% increase in cybercrime, with a predicted cost reaching $10.5 trillion by the year 2025 (Palatty, 2023).

Nigeria is among the top nations with cybercrime attack vulnerabilities in Africa (Stephen, Caleb, & Inyang, 2017). The country is globally perceived as a breeding ground for cyber criminals and deviants (Okeshola & Adeta, 2013; Aliyu et al., 2021). Numerous forms of cyber threats, including identity theft, email scams, financial fraud, cyberpornography, cyberstalking, computer hacking, etc., are rampant in Nigeria. Ndubueze (2013) reminds us that the prevalence of criminal rudiments in the digital space made young people the most vulnerable group of online users. Radda and Ndubueze (2013) underscored the role played by the rapid increase in the use of computer-mediated communications, including social networking platforms, emails, and chatrooms. Research conducted by the Center for Strategic and International Studies (2014) pointed out that in Nigeria, an increase in cybercrime had cost businesses $400 billion annually. Similarly, the Nigerian Deposit Insurance Corporation's (NDIC) annual report indicated that over 15 billion Naira in financial losses were recorded as a result of financial fraud in the year 2018 (Kanu et al., 2023). This showed that the majority of the citizens are not conscious of the impacts posed by cyber threats and their consequences on the economy of a nation.

Research indicates that young people are more prone to engage in online criminal activities, and as such, the menace is more prevalent in developing countries like Nigeria. Ndubueze (2013) reported that cybercriminals are mostly young adults between the ages of twenty and thirty-five. Speaking in Abuja during a press briefing, Ola Olukoyede, the Executive Chairman of the Economic and Financial Crimes Commission (EFCC), expressed concern about the increasing rate of Nigerian youth engaging in cybercrime. According to him, a significant portion, 70 percent, of Nigerian university students are implicated in criminal activities, and seven out of ten youth participate in cybercrime (Adegbite, 2023).

Statistical reports show that cyberattacks on educational institutions have increased since the start of the novel COVID-19 pandemic (Philipose & Karthik, 2022). The survey done by Norton Life Lock, a

prominent cybersecurity firm in the United States, revealed that cybercrime victimization among US university students has increased by 24 percent during the pandemic. The study further revealed that students have been targeted with numerous kinds of cyber threats, such as phishing, identity theft, bullying, and revenge pornography, among others (Philipose & Karthik, 2022). In Nigeria, educational institutions, including NWUS, play an important role in addressing the menace of cybercrime. The university serves a diverse body of students that increasingly relies on information and communication technologies for academic and personal purposes. The rapid digital adoption coupled with limited cybercrime and cybersecurity awareness leaves students most vulnerable to cybercrime victimization, both as potential victims and perpetrators (Radda & Ndubueze, 2013). Inadequate awareness and education of cyber threats is a major concern in today's digital era. Nowadays, the majority of young adults, including undergraduates at NWUS, have fallen victim to numerous cyber threats. Unfortunately, many of the victims have limited awareness, leaving them susceptible, which ultimately contributed to their victimization.

Given this alarming increase in cybercrime victimization among students, it is crucial to understand their consciousness level towards these threats. Raising awareness in educational institutions such as NWUS is crucial to empowering students to safeguard themselves. This effort must extend beyond schools, involving homes, schools, markets, mosques, churches, and other places (Akogwu, 2012; Ndubueze & Abdullahi, 2019), to increase cybercrime awareness.

1.1 Problem statement

The cases of cybercrime victimization are increasing day by day in Nigeria, especially among students. Studies have shown that undergraduate students are the most vulnerable group. They largely constitute a category that is today referred to as "Generation Y" or "Generation Z." According to Ndubueze (2013), "Generation Y" spares a substantial amount of time navigating modern communication gadgets and the internet, especially social media platforms like Twitter (now X), Facebook, Instagram, and WhatsApp, among others. This behavior increases their chances of cybercrime victimization. A lack of awareness on cybercrime and cybersecurity includes: vulnerability to various cyber threats like identity theft, phishing attempts, computer hacking, cyber pornography, cyberstalking, cyberbullying, and virus attacks, among others; and ignorance about online safety measures such as the utilization of strong user IDs and passwords, utilizing firewalls, and the installation of antivirus software, among others.

1.2 Scope and Limitations of the Study

The study is limited to Northwest University Sokoto, and it focused on undergraduate students from the academic faculties of computing and sciences, management and social sciences, and education. The survey examines the awareness level of 125 undergraduate students regarding some common cyber threats, including identity theft, computer hacking, revenge pornography, phishing attacks, and cyberbullying, as well as cybersecurity measures like the use of complex passwords/user IDs.

Despite the importance of the results, the study acknowledges certain shortcomings. For instance, the limited size of the sampled respondents may undermine the reliability of the findings and their applicability to the entire undergraduate students' body at NWUS and other educational institutions. Again, the study

focused on selected prevalent cybercrimes, which may not cover the whole range of cyber threats that students face in today's digital world.

1.3 Objectives of the study

The objectives of this study are as follows:

- To find out the level of cybercrime awareness among undergraduate students at NWUS.
- To examine gender differences in the level of cybercrime awareness among undergraduate students at NWUS.
- To examine the level of cybercrime awareness across the academic faculties at NWUS.
- To make recommendations that will help enhance awareness of cybercrime and cybersecurity.

2. Literature Review

2.1 Crime

Paul Tappan (1947, as cited in Paranjape, 2019, p. 19) defines crime as "an intentional act or omission in violation of criminal law committed without defense or justification and penalized by the law as a felony or misdemeanour." Crime, according to Siegel (2012, p. 14), is "the violation of societal rules of behavior as interpreted and expressed by a criminal legal code created by people holding social and political power." Crime can be explained as all acts that are specifically outlawed in the legal course of a given jurisdiction (Marsh et al., 2006).

2.2 Cybercrime

The term "cyber" originated from the phrase "cybernetics," which refers to the study of communication and human and machine control (Maurya & Suryavanshi, 2023). Proscribed behavior committed or facilitated through the internet is cybercrime. It can range from security breaches to identity theft and include cyber stalking, child pornography, online identity theft, revenge porn, virus attacks, posting hate speech, advanced fee fraud, etc. According to Vajagathali, Navaneeth, & Balaji (2019), cybercrime is a type of criminality that utilizes technology, such as computers, smartphones, and other digital devices, to commit digital piracy, identity theft, financial theft, computer hacking, embezzlement, espionage, etc. The Nigerian Cybercrime Working Group (2005, p. 2) defines cybercrime as "the conduct prohibited by law with prescribed punishment carried out using computer electronic auxiliary devices, processes, or procedures." Pati (as cited in Paranjape, 2019) further explains that cybercrime is carried out on the internet using a computer as either a tool, target, or means of committing further crime. Individuals who use computers and other technology tools to commit crimes are referred to as cybercriminals (Singh, Gupta, & Kumar, 2016).

2.3 Cybercrime Awareness

According to Kokoszka (2007), awareness is a sense that comes with the experience of phenomena such as cybercrime. In other words, awareness is the ability to observe, feel, and be conscious of happenings, objects, or sensory patterns. Lee and Lim (2019, p. 1) posit that "awareness is a starting point to recognize,

understand, or know a situation or fact, and the perception makes a difference in how to deal with it." Similarly, "cybercrime awareness" refers to the level of understanding and knowledge that people and businesses possess regarding numerous cyber threats and online criminal activities (Lee & Lim, 2019). Jaishankar (2011) argues that the cyberspace has raised the chances for many threats and dangers, putting individuals and businesses at risk. Mupila Gupta, and Bhardwaj (2023) underscored the significance of enhancing cybercrime awareness among different demographics, including students and adults, to mitigate the threats and dangers associated with online criminal activities. Improving awareness levels can lead to a decrease in cybercrime victimization rates, underscoring the significance of educational programs, seminars, workshops, conferences, and training to enhance people and businesses understanding of cybersecurity measures (Ndubueze & Abdullahi, 2019).

2.4 Related Works

Jadhav and Makwana (2023) examined the consciousness level of cybercrime among college-going students in Vadadora, Gujarat, India. The scholars utilized a semi-structured questionnaire that included the demographics of seventy college students. The survey results show that the majority of the sampled respondents are aware of different types of cybercrime most prevalent in Indian society.

Parwani, Nikose, and Rathor (2022) conducted a survey to educate people about cybercrime and its consequences. The scholars examined the perceptions of fifty respondents to determine their level of awareness about cybercrime. The survey results revealed that adults are more aware of cybercrime than young individuals.

Ndubueze and Abdullahi (2019) conducted a survey on cyber victimization awareness among internet-active undergraduate students in Nigeria. A total of ninety-nine undergraduate students from two public universities participated in the study. As per the study findings, the majority of the surveyed students indicated their awareness and understood that unconsciousness of cyber threats can lead to victimization. The scholars suggested increasing cybercrime and cybersecurity awareness initiatives, especially among susceptible students in Nigeria.

Archana and Shah (2016) investigated the extent of cybercrime awareness among Indian citizens. The survey has a total of one hundred sampled respondents. The majority of the sampled respondents demonstrated moderate awareness, highlighting the need for increased awareness efforts.

Bala (2022) examined the cybercrime awareness among B.Ed. students. The sample of the survey was eighty students, 40 male and 40 females, from both city and countryside areas. The result of the study revealed no significant difference between cybercrime consciousness among genders, but there is a significant difference among locations. In another study, Spring (2018) surveyed two hundred B.Ed.'s from a college of education in Lucknow, Uttar Pradesh, India. The scholar examined the cybercrime consciousness of the sampled students with respect to gender and age. As per the survey findings, male B.Ed. students have a higher level of consciousness than their female B.Ed. counterparts.

Vajagathali et al. (2019) study focuses on cybercrime awareness among faculty students in Mangolere. Utilizing a well-structured questionnaire, the scholars examine the perception and consciousness of 150 students by focusing on numerous types of cyber threats, including computer viruses, identity theft, piracy,

and pornography. As per the survey results, the majority of the participants from technical-related fields (science, medicine, and engineering) have a higher level of cybercrime consciousness than students from non-technical-related disciplines (arts and law).

The study on cyber-security awareness in Saudi Arabia, Alotaibi, Furnell, Stengel, and Papadaki (2017) investigated the level of cybersecurity awareness among Saudi Arabian students. The survey findings show that the majority of the surveyed students demonstrated a lower level of cybersecurity awareness. In contrast, Senthilkumar and Easwaramoorthy (2017) examined cybersecurity awareness among selected students in India. They found that two-thirds of the sampled students have a moderate awareness of cybercrime and cybersecurity. They recommended more awareness and training programs, especially among the vulnerable groups.

Wambui, Nyambura, and Njeru (2022) conducted a study on cybercrime awareness among netizens of higher education institutions. The study results indicated that the majority of the sampled respondents (63.4 percent) lack awareness of cybersecurity. The researchers believed that increasing awareness among students and staff can enhance cybercrime and cybersecurity consciousness.

Mehta and Singh (2013) did a comparative to investigate awareness of cyber laws in India. They found a significant gender difference, with males being more informed of cyber laws than females.

2.5 Theoretical Framework

2.5.1 Space Transition Theory

The Space Transition Theory (STT) of cybercrime was developed by Professor Jaishankar Karupnnan in 2007 (Jaishankar, 2007). STT aims to explain the causes of illegal activities occurring in cyberspace. According to Jaishankar, a separate theory for cybercrime is necessary because general theoretical explanations are insufficient for a comprehensive explanation of online criminal activities (Ndubueze, Igbo, & Okoye, 2013).

Jaishankar explains space transition as the movement of people from one space to another (for example, from physical space to cyberspace and vice versa). He maintained that people behave differently when they move from one space to another, leading to changes in their behaviors.

The propositions of the STT include:

a. Persons with repressed criminal behavior in physical space have a propensity to commit crimes in cyberspace, which they otherwise would not commit in physical space due to their status and position.
b. Identity flexibility, dissociative anonymity, and a lack of deterrence factors in cyberspace provide the offender with the choice to engage in cybercrime.
c. The criminal behavior of offenders in cyberspace is likely to be imported into physical space, and vice versa.
d. Intermittent ventures of offenders in cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

(a) Strangers are likely to unite in cyberspace to commit crimes in physical space, while (b) Associates from physical space are likely to unite to commit crimes in cyberspace.

e. Persons from closed societies are more likely to commit crimes than people from open societies.
f. The conflicts between the norms and values of physical space and the norms and values of cyberspace lead to cybercrime.

In line with the above, Jaishankar contends that the nature of cyberspace allows criminals to victimize people without being identified or apprehended. Identity flexibility, dissociative anonymity, a lack of deterrents, the intermittent involvement of offenders in cyberspace, and the dynamic nature of cyberspace all contribute to the prevalence of cybercrime. As a result, individuals and businesses that lack the awareness or skills to protect themselves are susceptible to cybercrime victimization.

STT is the first attempt to use cybercrime-specific theory to explain crime and deviance in cyberspace (Danquah and Longe, 2011). Also, Ndubueze and Ismail (2021) posit that Jaishankar's STT has paved the way for new areas of investigation by focusing on the emerging trends of offenses involving computers and the internet. However, Muhammed and Ibrahim (as cited in Ndubueze & Abdullahi, 2019) criticized the theory, arguing that it does not incorporate demographic aspects that encourage cybercrime.

3. Methodology

3.1 Study setting

According to Ogunbameru and Ogunbameru, (2010), the setting of research refers to the particular place or location where a study was conducted. This present research was carried out at NWUS, a private university in KM 10 Kalambaina, Wammako Local Government Area, Sokoto State, Nigeria. The university was established in 2022 by the former governor of Sokoto State, Senator Aliyu Magatakarda Wamakko. The name "Northwest" implies the Northwest geopolitical zone of Nigeria, where the university is located. The name was chosen to reflect the significance of education to the overall development of the zone, as can be gleaned from the efforts of the Late Sir. Ahmadu Bello, the then Sardauna of Sokoto and premier of Northern Nigeria. The motto of NWUS is "knowledge, excellence, and success," which is a reflection of the university's goals and objectives to encourage the development of knowledge as a fundamental basis for excellence in the pursuit of success. From the onset, NWUS commenced academic activities with 15 courses housed in three academic faculties, namely: the Faculty of computing and sciences (which comprises the department of computer science, the department of biological sciences, the department of chemistry, the department of physics, and the department of mathematics), the Faculty of management and social sciences (which comprises the department of sociology, the department of psychology, the department of economics, the department of public administration, the department of accounting, and the department of business administration), and the Faculty of education (which comprise the department of educational foundation, the department of special education, and the department of library science).

3.2 Study Design

The study design is described as "the plan, structure, and strategy of investigation conceived so as to attain answers to research questions and to control variables" (Ogunbameru & Ogunbameru, 2010, p. 109).

Mangal and Mangal (2013) explained that the descriptive survey technique is widely used in educational, social, and management sciences to evaluate and present the status of a given situation or phenomenon, such as awareness of cybercrime. Hence, this present study adopted a descriptive survey research design to collect relevant first-hand information regarding the awareness of cybercrime among undergraduate students at NWUS.

3.3 Population

Mangal and Mangal (2013) describe the study population as the group of individuals who meet specific criteria and are accessible for a study. Defining the study population is crucial for the validity of study results (Ogunbameru & Ogunbameru, 2010). In this present study, the targeted population comprises all registered undergraduate students at NWUS.

3.4 Sample

A sample is a small subset of a larger population that is selected to stand for the entire population. Ogunbameru and Ogunbameru (2010) suggest that selecting a sample size is critical considering the impossibility of studying the entire population. To ensure that every undergraduate student at NWUS participates in this present study, the researcher utilized random sampling techniques to choose the sample from the targeted population because he believes that the selected respondents can represent the entire population. In this study, a total of 125 undergraduate students were selected randomly to represent the population. The chosen participants comprise 70 male and 55 female students from the faculty of computing and sciences, the faculty of management and social sciences, and faculty education.

3.5 Ethical Considerations

To guarantee voluntary participation in this study, the selected participants were provided with a consent form, which they had to sign before filling out the study questionnaire. Thus, informed consent was obtained from questionnaire respondents at the beginning of the process. Participants were informed that their participation was voluntary and that they had the right to opt-out at any stage of the study. Also, the study guaranteed absolute confidentiality and anonymity for the participants. The instruments used for data collection did not collect any personal information revealing the identity of the participants. To avoid exposure of study findings, the collected data is only available to the researchers of this study.

3.6 Data Collection

With regards to data collection, a semi-structured questionnaire was the tool used in collecting data from the sampled undergraduate students. The instrument aids in facilitating a complete understanding of respondents' awareness towards different forms of cyber threats. Permission to carry out the survey was sought from the vice chancellor through the Dean students' affairs of NWUS. An approval was granted to collect data from the enrolled undergraduate students. The data collection process utilized the self-administration method. The researcher identified three major places, including lecture rooms, the university cafeteria, and social centres within the university campus, to administer the questionnaire. At these places, the researcher randomly selected undergraduate students, administered and waited to clarify

any challenges about the instrument, and collected the questionnaire when it was filled out. The informed consent of the questionnaire respondents was obtained at the beginning of the process.

3.7 Data Analysis

According to Mangal and Mangal (2013), data analysis entails the modelling and conversion of survey findings to present information, make recommendations, and draw conclusions in a study. In this present study descriptive statistic were utilized for the analysis of the study's data. Statistical Packages for Social Sciences (SPSS) Version 26 was used to analyze the collected quantitative data. In the domain of arts, management, and social sciences, SPSS is a commonly recognized tool used for statistical analysis of quantitative data generated via the questionnaire (Mangal & Mangal, 2013). Thus, SPSS is suitable for this current study because it will help in the effective handling of the quantitative data collected from the sampled undergraduate students. Firstly, the collected data were sorted, coded, and entered into the computer for analysis. Secondly, the data were presented using a frequency distribution table and percentage. This approach enables the researcher to interpret the quantitative results and identify trends and patterns of cybercrime awareness among the sampled respondents. By utilizing descriptive statistics, the data analysis aligns with the objectives of the study.

4. Results

4.1 Socio-demographic characteristics

Table 1: Socio-demographic characteristics of the surveyed undergraduate students

Gender	Details	Frequency	Percent	Cumulative Percent
	Male	70	56	56
	Female	55	44	100
	Total	125	100	
Age	16-20	53	42.42	42.42
	21-25	47	37.6	80
	26-30	15	12	92
	30 above	10	8	100
	Total	125	100	
Academic Faculty	Computing and Sciences	79	63.2	63.2

	Management and Social Sciences	30	24	87.2
	Education	16	12.8	100
	Total	125	100	
Daily-used devices	Smartphone	100	80	80
	Laptop	18	14.4	94.4
	Desktop	2	1.6	96
	Tablet	5	4	100
	Total	125	100	
The most used social network	WhatsApp	44	35.2	35.2
	Snapchat	15	12	47.2
	Instagram	7	5.6	52.8
	Facebook	22	17.6	70.4
	TikTok	19	15.2	85.6
	Twitter	7	5.6	91.2
	YouTube	8	6.4	97.6
	Telegram	3	2.4	100
	Total	125	100	

Source: Field Survey, 2023

From Table 1, The majority (80%) of the surveyed undergraduate students were between 15 and 25 years of age. Male students constituted the majority (56%), and female students 44%. Furthermore, students were classified according to academic faculties; the majority (63%) were from the faculty of computing and sciences, followed by the faculty of management and social sciences (24%), and the faculty of education (12.8%). Regarding students' regular device usage, the majority (80%) of the students used smartphones, 14.4% of the students used laptops, 4% of the students used tablets, and only 1.6% of the students used desktops. Regarding the most-used social media, all the students reported regular use of various social media platforms.

4.2 Cybercrime Awareness

Table 2: Cybercrime Awareness

Response	Frequency	Percent	Cumulative percent
Yes	89	71.2	71.2
No	30	24	95.2
No Response	6	4.8	100
Total	125	100	

Source: Field Survey, 2023

In line with the data displayed in Table 2, more than three-quarters (71.2%) of the sampled undergraduate students indicate their awareness of cybercrime, while 24.8% were not aware. Very few 4.8 did not provide a response.

Table 3: Awareness of Computer Hacking

Response	Frequency	Percent	Cumulative percent
Yes	102	81.6	81.6
No	19	15.2	96.8
No Response	4	3.2	100
Total	125	100	

Source: Field Survey, 2023

Table 3 shows that the majority (81.6%) of the surveyed undergraduate students were aware of computer hacking, while 15.2% were unaware.

Table 4: Awareness of Revenge Pornography

Response	Frequency	Percent	Cumulative Percent
Yes	90	72	72
No	35	28	100
No Response	0	0	

Total	125	100	

Source: Field Survey, 2023

Table 4 indicates that the majority (72%) of the surveyed undergraduate students were aware of revenge pornography, while 28% were unaware.

Table 5: Awareness of Identity Theft

Response	Frequency	Percent	Cumulative Percent
Yes	120	96	96
No	4	3.2	96.2
No Response	1	0.8	100
Total	125	100	

Source: Field Survey, 2023

Table 5 depicts that nearly all (96%) of the surveyed undergraduate students were aware of identity theft. While very few (3.2%) expressed their unawareness.

Table 6: Awareness of Phishing

Response	Frequency	Percent	Cumulative Percent
Yes	79	63.2	63.2
No	40	32	95.2
No Response	6	4.8	100
Total	100	100	

Source: Field Survey, 2023

Table 6 clearly showed that more than half of the sampled undergraduate students (63.2%) were aware of phishing. However, a significant proportion (32%) said they were unaware of this type of cyber threat. Only a few (4.8%) of the students did not respond.

Table 7: Awareness of cyberbullying

Response	Frequency	Percent	Cumulative Percent
Yes	87	69.6	69.6
No	34	27.2	96.8
No Response	4	3.2	100
Total	125	100	

Source: Field Survey, 2023

As per the data presented in Table 7, a significant majority (69.6%) of the sampled undergraduate students at NWUS were aware of cyberbullying. Furthermore, 27.2% said they were not aware, and 3.2% did not respond.

4.3 Cybersecurity awareness

Table 8: Awareness of user ID and password

Response	Frequency	Percent	Cumulative Percent
Yes	90	72	72
No	31	24.8	96.8
No response	4	3.2	100
Total	125	100	

Source: Field Survey, 2023

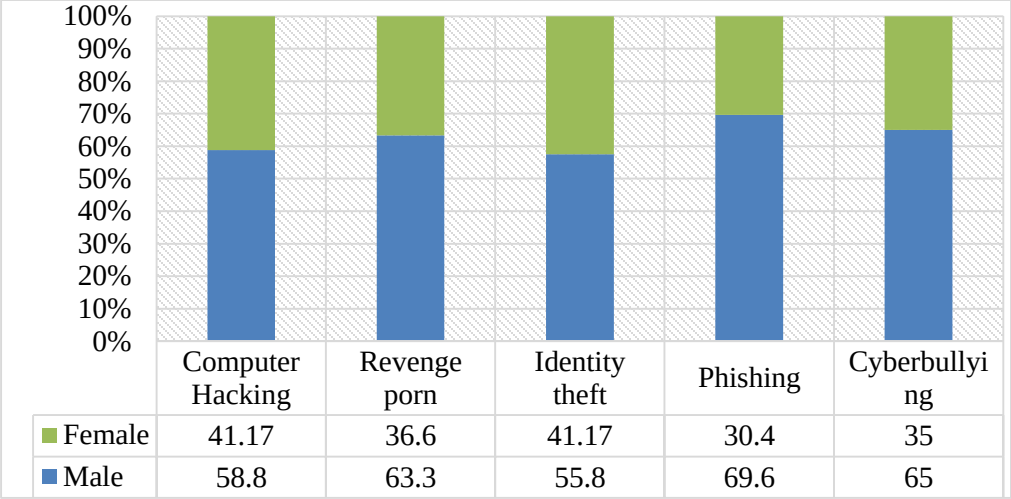
From Table 8, more than two-thirds (72%) of the sampled undergraduate students were aware of user IDs and passwords. 24.8% of the respondents were unaware, and only 3.2% did not respond.

Table 9: Awareness of Cybercrime Laws

Response	Frequency	Percent	Cumulative Percent
Yes	20	16	16
No	100	80	96
No Response	5	4	100
Total	125	100	

Source: Field Survey, 2023

Table 9 shows that a significant majority (84%) of the sampled undergraduate students were not aware of cybercrime laws in Nigeria, while a few (16%) said they knew them.

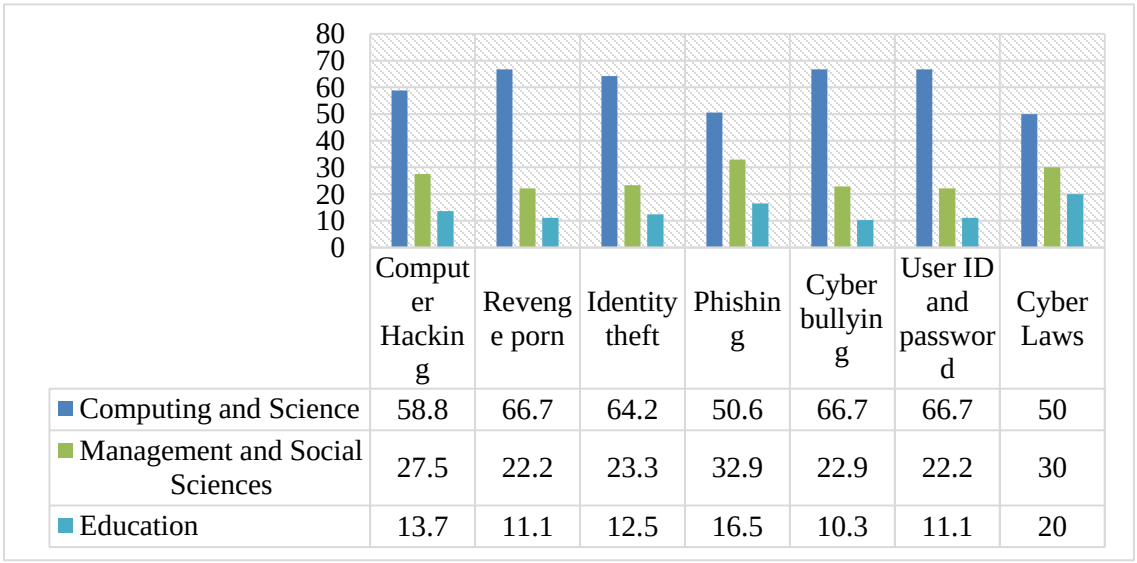


	Computer Hacking	Revenge porn	Identity theft	Phishing	Cyberbullying
Female	41.17	36.6	41.17	30.4	35
Male	58.8	63.3	55.8	69.6	65

Source: Field Survey, 2023

Figure 1: Bar graph comparing genders' awareness of cybercrime.

In order to find out which gender is more aware of cybercrime; we compared male and female undergraduate students. As can be seen in Figure 1, findings indicate that both genders expressed awareness of different types of cybercrime; however, it is notable that male students showed a higher level of awareness regarding different forms of cybercrime compared to their female counterparts.



	Computer Hacking	Revenge porn	Identity theft	Phishing	Cyber bullying	User ID and password	Cyber Laws
Computing and Science	58.8	66.7	64.2	50.6	66.7	66.7	50
Management and Social Sciences	27.5	22.2	23.3	32.9	22.9	22.2	30
Education	13.7	11.1	12.5	16.5	10.3	11.1	20

Source: Field Survey, 2023

Figure 2: Bar graph comparing awareness of cybercrime across academic faculties.

To determine the levels of awareness across the academic faculties, a contrast and comparison analysis was conducted. Figure 2 provides a graphic representation of the results. It was found that students in the faculty of computing and sciences have the highest level of awareness regarding different kinds of cybercrime and cybersecurity. Following behind were students in the faculty of management and social sciences. While students in the faculty of education have the lowest awareness.

5. Discussion

The main purpose of this study was to assess the level of cybercrime awareness among undergraduate students at NWUS. Based on the quantitative data, the majority of the surveyed students (71.2%) are conscious of various kinds of cybercrime. These findings are consistent with previous studies. Sreehari et al. (2018) reported an awareness level of 77 percent among college students in Koshi, Kerala, India. Similarly, Tafa, Alfa, and Suleiman (n.d.) examined cyber consciousness and involvement among students of tertiary institutions in Zamfara State, Nigeria. Findings of the study revealed that the majority (71.83%) of the participants in their study were aware of cybercrime. This connotes that the higher conscious level found in this and previous studies shows a significant increase in cybercrime awareness among students, which could be because of the increasing adoption of modern technologies for both academic and personal purposes (Aliyu et al., 2021; Mwiraria et al., 2022; Ayyoub et al., 2022). Further, it is imperative to highlight that a notable proportion (28.4%) of the surveyed students show their unawareness. Augustina (2015, cited in Ndubueze & Abdullahi, 2019) argues that ignorance of cyber threats is a major factor contributing to youth vulnerability to cybercrime victimization. Also, this finding agrees with Jaishankar (2007) SST, which argues that unawareness of cybercrime and victimization increases the likelihood of being victimized, especially among adolescents who spend a substantial amount of their time online. Thus, it is essential to raise more awareness, especially among the vulnerable group of youth (Akogwu, 2012; Ndubueze & Abdullahi, 2019).

The quantitative data indicate a difference in cybercrime awareness levels between genders. As per the study findings, 63% of the surveyed male undergraduate students demonstrated consciousness of different types of cybercrime, while 36.8% of female students indicated similar awareness. These findings are similar with previous studies that reported gender disparities in cybercrime awareness. Chaudhuri (2022) found a significant gender difference, with male students of B. Ed. showing more consciousness towards cybercrime than female students in the training college of Cooch Behar district, West Bengal, India. Similarly, Spring (2018) reported that male students are more conscious and positive than female students' counterparts. In contrast, in their study in Malaysia, Hasan et al. (2015) discovered that female students have more awareness of cybercrime and assess its consequences differently than their male counterparts. The current and past studies findings suggest that male students perceive cybercrime as a more significant threat, which could be due to the nature and types of online activities such as social media engagement, online trading, and online gaming they engage in. Thus, this exposure can create the need for awareness, as they may encounter cyber threats frequently. Nevertheless, as far as cybercrime is concerned, it knows no gender or sex. Thus, regardless, it is pertinent to raise more awareness among both male and female students.

The study's results show that there is a considerable difference in awareness levels among students across the academic faculties. The majority 61.4% of the surveyed undergraduate students from the faculty of

computing and sciences exhibited consciousness of various types of cybercrimes, compared to 25.7% from the faculty of management and social sciences and 12% from the faculty of education. These findings are consistent with earlier studies. For example, Vajagathali et al. (2019) investigated the awareness of cybercrime among faculty students in Mangolere by focusing on various kinds of cyber threats. They discovered that the majority 67 percent of students in technical fields such as physics, chemistry, engineering, and medicine were more aware of cybercrime than 33 percent of students in non-technical disciplines such as psychology, sociology, and law in Mangolere, India. Our findings (25.7%) for management and social sciences students and 12.8% for education students echo similar awareness levels to Vajagathali's survey, highlighting that efforts should be made to raise awareness among students in the faculty of management and social sciences and the faculty of education.

However, among the surveyed undergraduate students who demonstrated a higher level of awareness about numerous cybercrimes, there was a significant increase in the adoption of security practices such as using strong passwords and user IDs, as well as being cautious while navigating modern communication technologies and the internet. This shows that increasing awareness of cybercrime and cyber victimization not only raises awareness but also inspires students to use defensive measures.

The results of this present study underscored the need for increasing awareness of cybercrime and cybersecurity, especially among the vulnerable internet users, including the students. Thus, educational institutions, including NWUS, should make cybercrime an important component of their school curriculum to provide students with the needed education and skills to protect themselves from cybercriminals and deviants. The study results also indicate a connection between awareness and the adoption of cybersecurity practices; students who demonstrated a higher level of consciousness were more likely to utilize strong passwords/user IDs and be more careful while navigating modern communication technologies. This underscored the need for developing and implementing of educational programs that inform students about cybercrime and cybersecurity.

Further, the significant disparity in awareness among students in various academic faculties implies that targeted intervention initiatives are crucial. Precisely, the faculty of management and social science and the faculty of education should receive focused education programs to close the awareness gap. Thus, educational institutions, including NWUS, should develop and implement cybercrime and cybersecurity education programs, workshops, conferences, and seminars to personalize the peculiar needs of each faculty.

6. Conclusion and Recommendations

The study examined the level of cybercrime awareness among undergraduate students with reference to NWUS. The results of this present study demonstrate that two-thirds of the sampled undergraduate students at NWUS had a reasonable awareness of different forms of cybercrime. It is clear that the percentile of awareness among the students is high for identity theft (96%), followed by computer hacking (82%), revenge pornography (72%), cyberbullying (70%), and phishing (63.2%). However, most of the students are not sufficiently conscious of cybercrime laws in Nigeria. The study results also revealed a significant difference in terms of gender and academic faculties level of awareness. A significant proportion (63 percent) of male students are more aware than their female counterparts. On the other hand,

the study also found that students from the faculties of computing and sciences and management and social sciences demonstrated higher awareness than students from the faculty of education.

Overall, the study concluded that the majority of the sampled undergraduate students are aware of cybercrime, with male students showing a comparatively higher consciousness than their female counterparts, which implies that information about cybercrime has been reaching a substantial portion of the students. Also, the gender disparity signifies that male students have more experience regarding technology and cyber threats. In other words, it shows wider societal movements in how genders engage with modern technologies. Additionally, the significant disparity in awareness level in terms of gender and across the three academic faculties implies the need for increasing awareness among female students in both technical and non-technical fields.

Moreover, the study enables us to understand the awareness level among undergraduate students. After understanding their awareness level, we can enhance their cybercrime and cybersecurity consciousness. Ndubueze and Abdullahi (2019) believe that awareness about cyber threats and dangers not only helps in decreasing the possibility of victimization but also deters students from engaging in cybercrimes. Thus, the findings of the study will be beneficial for NWUS in particular and other educational institutions to understand the level of students' awareness and come up with mechanisms to increase their consciousness regarding cybercrime.

However, despite the significance of the study, it is pertinent to mention that the 125 sample respondents for this study represent the entire undergraduate students at NWUS, which undermines the reliability of the survey findings. Also, conducting a survey at NWUS only limits the generalizability of the findings to other tertiary institutions. Another limitation is that the study focused on selected most prevalent cybercrimes, which may not cover the entire range of cyber threats that students face in today's digital world. Future studies could expand the sample size and include other categories of cybercrime faced by students.

Based on the study results, the following few recommendations can be helpful:

1. There is a need for NWUS and other educational institutions to come up with mechanisms for raising cybercrime consciousness among both students and staff. This can be done by:

    - Establishing a unit dedicated to informing all students and staff about the nature, causes, and consequences of cybercrime.
    - Inviting cybersecurity experts to discuss the issues pertaining to cyber threats and dangers.
    - Inviting legal professionals to inform the students of issues regarding cybercrime laws and reporting of cybercrime victimization.
    - Organizing educational programs, conferences, seminars, and workshops related to cybercrime and cybersecurity.
2. There is a need for all internet users, including students and staff, to adopt numerous cybersecurity measures. Users are advised to:

    - Avoid accepting unnecessary offers that pop up while navigating the internet.

- Avoid informing anyone of your computer or mobile phone password.
- Avoid opening suspicious messages or links.
- Avoid revealing key personal details on social media platforms including Facebook, WhatsApp, Twitter (now X), TikTok, etc.
- Avoid writing down identification and financial details such as bank verification number (BVN), national identification number (NIN), etc. anywhere.
- Be cautious when accepting friend requests on social media platforms.
- Regularly change computer and mobile phone passwords.
- Use strong passwords that contain characters, upper and lowercase letters, symbols, and numbers.

3. The role of the law enforcement agencies, including the Nigerian Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), and other stakeholders in combating cybercrime in Nigeria, cannot be underestimated. As such, they are advised to:

- Bring out a mass awareness campaign across all the Nigerian educational institutions, including universities, secondary schools, and primary schools, informing students on the effects of cybercrime on individuals, businesses, and the economy.
- Employ sophisticated cybersecurity technologies to identify and apprehend cybercriminals.
- Encourage citizens to report any incidents to the appropriate authorities.
- Ensure strict compliance and application of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
- Establish synergy between the law enforcement agencies and other stakeholders to share data on cybersecurity efforts.

7. Conflict of Interests

There is no conflict of interest for this study.

8. Acknowledgment

We would like to acknowledge the undergraduate students who voluntarily participated in this study. Special thanks go to the pioneering vice chancellor of NWUS, Professor Ahmed Ibrahim Maigari, for his kind assistance and encouragement. We are also grateful to the Dean of the Faculty of Computing and Sciences, Dr. Muhammad Bashir Sulaiman, and the Dean of Student Affairs, Dr. Rabiu Muhammad.

References

Adegbite, A. (2023, December 7). Youth involvement in cybercrime threat to future leadership. The Punch. https://punchng.com/youth-involvement-in-cybercrime-threat-to-future-leadership-efcc/?amp

Akogwu, S. (2 012). *An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria* (unpublished B.Sc. project). Department of Sociology, Ahmadu Bello University, Zaria.

Aliyu, A., Aliyu, M., Ahmad, A., & Abdullahi, S. (2021). Investigating Cybersecurity Awareness among Tertiary Institutions Students in Nigeria. *International Journal of Advances in Engineering and Management (IJAEM), 3(2), 111-118.* https://doi.org/10.35629/5252-0310111118

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). "A survey of cyber-security awareness in Saudi Arabia," *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Barcelona, Spain, 5–7 December 2016, pp. 154- 158. https://doi.org/10.1109/ICITST.2016.7856687

Archana, C. N., & Shah, V. (2016). Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India). *International Journal of Advance Research and Innovative Ideas in Education*, 2 (6), 1164-1172. https://www.ijariie.com

Ayyoub, H. Y., AlAhmad, A. A., Serhan, A., Abdallat, M. F., Al-Muheisen, E., Boshmaf, H., … Alshamaileh, Y. (2022). Awareness of electronic crimes related E-learning among students at the University of Jordan. *Heliyon, 8.* https://doi.org/10.1016/j.heliyon.2022.e10897

Bala, R. (2022). A Study of Cyber Crime Awareness Among B.Ed. Students. *Paripex - Indian Journal of Research*, 11(4), 2250–1991. https://doi.org/10.36106/paripex

Center for Strategic and International Studies (2014). *Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II.* Washington, DC: Center for Strategic and International Studies (CSIS).

Chaudhuri, S. K. S. (2022) A Study on Awareness among the B. Ed. College Students Towards Cybercrime. *Journal of Humanities and Social Science (IOSR-JHSS)* 27(11), 2279-0837, www.iosrjournals.org

Danquah, P., & Longe, O. B. (2011). An empirical test of the space transition theory of cyber criminality: The case of Ghana and beyond. *African Journal of Computing & ICTs*; l4(2), 37-48. http/www./padanquah@ait.edu.gh

Hasan, M. S., Abdul Rahman, R., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences,* 11 (4), 395- 404. https://doi.org/10.3844/jssp.2015.395.404

Hassan, S. (2013). *Mass communication, Principles and Concepts* (2nd ed.). New Delhi: CBS Publishers and Distributors Pvt Ltd.

Internet Crime Complaint Center (2022). Internet Crime Report 2021. https://www.ic3.gov

Jadhav, N., & Makwana, V. (2023). A Study on Awareness of Cybercrimes Among Youth. *International Journal of Research Publication and Reviews*, 4(2), 1258-1260. www.ijrpr.com

Jaishankar, K. (2007). Establishing theory of cybercrimes, *International Journal of Cyber Criminology*, 1(2), 7-9. https://www.cybercrimejournal.com

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. USA: CRS Press.

Kanu, C., Nnam, M. C., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2023). Frauds and forgeries in banking industry in Africa: a content analyses of Nigeria Deposit Insurance Corporation annual crime report. *Security journal*, 36(4), 671-692. https://doi.org/10.1057/s41284-022-00358-x

Kokoszka, A. (2007). *States of Consciousness: Models for Psychology and Psychotherapy*. New York: Springer Business Media.

Lee, H., & Lim, H. (2019). Awareness and Perception of Cybercrimes and Cybercriminals. *International Journal of Cybersecurity Intelligence and Cybercrime*, 2 (1), 1-3. https://doi.org/10.52306/02010119UYIB64

Mangal, S. K., & Mangal, S. (2013). *Research methodology in behavioral sciences*. Delhi: PHI Learning Private.

Marsh, I., Mevil, G., Morgan, K., Norris, G., & Walkington Z. (2006). *Theories of crime*. Canada: Rutledge Taylor & Francis e-library.

Maurya, S., & Suryavanshi, P. (2023**).** Pilot Study: Cyber Crime Awareness in College-Going Students in KMCL University. *International Journal of Creative Research Thoughts (IJCRT),* 11(5), 2320-2882. https://www.ijcrt.org

Mehta, S., & Singh, V. (2013). A Study of Awareness about Cyber Laws in the Indian Society. *International Journal of Computing and Business Research*, January, 4(1), 2229-6166.

Mupila, F. K., Gupta, H., & Bhardwaj, A. (2023). An Empirical Study on Cyber Crimes and Cybersecurity Awareness. *Research Square*, 1- 24. https://doi.org/10.21203/rs.3.rs-3037289/v1

Mwiraria, D. R., Ngetich, K., & Mwaeke, P. (2022). Factors Associated with Cybercrime Awareness Among University Students in Egerton University, Njoro Campus, Nakuru County, Kenya. *European Journal of Humanities and Social Sciences*, 2(3), 63-68. http://dx.doi.org/10.24018/ejsocial.2022.2.3.256

Ndubueze, P. N. (2013). Generation Y and Online Victimization in Nigeria: How vulnerable are younger respondents? A paper delivered at the Second International Conference of the South Asian Society of Criminology and Victimology (SASCV), January 11-13, 2013 at Kanyakumari, Tamil Nadu, India.

Ndubueze, P. N., & Abdullahi, A. S. (2019). Awareness of Cyber Victimization among Internet-active Undergraduate Students in Selected Nigerian Universities. *Fulafia Journal of Sociological Studie*s, 3(1), 19-26

Ndubueze, P. N., & Ismail, U. (2021). Cybercrime Awareness among Police Personnel in Lagos, Nigeria Article · *NOUN Journal of Criminology and Security Studies*, 2(2), 165-173.

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cybercrime victimization among Internet active Nigerians: An analysis of the socio-demographic correlate. *International Journal of Criminal Justice Sciences*, 8(2), 225-234

Nigeria Cyber-crime Working Group (NCWG) (2005). *Nigerian National Cyber Security Policy.* A Draft Document by the Nigeria Cyber-crime Working Group, Abuja. Retrieved from www.eshekels.com/downloads/e-government%203.pdf

Ogunbameru, O. A., & Ogunbameru, B. O. (2010). *Contemporary Methods in Social Research.* Ile-Ife: Kuntel Publisher.

Okeshola, F.B., & Adeta, A. K. (2013). The Nature, Causes, and Consequences of Cybercrime in Tertiary Institutions in Zaria, Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 98-114

Palatty, N. J. (2023). 90+ Cyber Crime Statistics 2024: Cost, Industries & Trends. https://www.gestastra.com/blog/security-audit/cyber-crime-statistics/

Paranjape, V. N. (2019). *Criminology & Penology with Victimology*, *Eleventh Edition*. Allahabad: Central Law Publications.

Parwani, P., Nikose, P., & Rathor, J. (2022). Awareness Regarding Cyber Crime among People. *International Journal of Research Publication and Reviews*, 3(1), 944-947. www.ijrpr.com

Philipose, G., & Karthik, A. (2022). Assessing Cybercrime Awareness and Internet Usage among Students: Implications for Policy and Education. *European Chemical Bulletin*, 11(11), 1147–1153.

Radda, S. I., & Ndubueze, P. N. (2013). Fear of Online Victimization Among Undergraduate Students: A Comparative Study of Two Selected Urban Universities. *African Journal of Criminology and Justice Studies, 7(1), 35-46.* https://digitalscholarship.tsu.edu/ajcjs/vol7/iss1/4

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security Awareness among College Students in Tamil Nadu. In: Materials Science and Engineering Conference Series 263: 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Siegel, L. J. (2012). *Criminology*. USA: Wadsworth, Cengage Learning.

Singh, O., Gupta, P., & Kumar, R. (2016). A Review of Indian Approach towards Cybersecurity. *International Journal of Current Engineering and Technology*, 6(2), 644-648. https://inpressco.com/category/ijcetbit

Spring, N. (2018). A Survey of B.Ed. Students' Perception and Awareness towards Cybercrime. *Journal of Emerging Technologies and Innovative Research (JETIR*), 5(9), 406-417. www.jetir.org

Sreehari, A., Abinanth, K. J., Sujith B, Unnikuttan P. S., & Jayashree, M. (2018). A Study of Awareness of Cyber Crime Among College Students with Special Reference to Kochi. *International Journal of Pure and Applied Mathematics*, 119(16), 1353-1360. http://www.acadpubl.eu/hub/

Stephen, A. O., Caleb, E. B., & Inyang, O. I. (2017). Cyber Security in the Banking Sector: An Appraisal of Audit Committee Effectiveness; *International Reviews of Management and Marketing* 7(2), 340–346. https://www.econjournal.com

Tafa, T. O., Alfa, A. S., & Suleiman, A. J. (n.d.). A Study of Cybercrime Awareness and Involvement among Students of Tertiary Institutions in Zamfara State of Nigeria. *International Journal of Research in Education, Science and Technology*, 3(3), 36-44. https://www.globalacademicstar.com/download/article/a-study-of-cybercrime-awareness-and-involvement-among-students-of-tertiary-institution-in-zamfara-state-of-nigeria-90988.pdf

Vajagathali, M., Navaneeth, K. S., & Balaji, N. B. (2019). Cyber Crime Awareness among College Students in Mangalore. *Journal of Forensic Sciences and Criminal Investigation.* 12(1), 001-006. https://doi.org/10.19080/JFSCI.2019.12.555828

Wambui, B. M., Nyambura, H., & Njeru, D. (2022). A Survey of Cyber Crime Awareness among Netizens of Higher Education Institutions: A Case Study of Zetech University. *International Journal of Computer Applications Technology and Research*, 11(11), 359-370, https://doi.org/10.7753/IJCATR1111.1002