Examining Cybersecurity Conscience among Tertiary Institution Students in Nigeria

Aminu Aliyu[1;] Abdulmalik Ahmad[2]
[1&2]Umaru Ali Shinkafi Polytechnic, Sokoto,
Nigeria

Abstract
It is crucial to include cybersecurity in university curricula to assist students in accessing social media and the Internet safely. Understanding the principles of cybersecurity and the efforts undertaken by institutions and the government to establish cybersecurity as a stand-alone degree program, along with other relevant fields, has received a lot of attention lately. To raise awareness of cybersecurity, several organisations (including NITDA, NCC, NCS, and CPN) and academics organised conferences, workshops, seminars, and guidelines that were published. In this research, a survey of 9 tertiary schools from Kano, Kaduna, and Sokoto was carried out. Utilising a methodical, practical sampling methodology to target 100 respondents from each institution (Universities, Polytechnics, and Colleges of Education), SPSS v17 software was used to analyse the data gathered from the paper and pen cybersecurity awareness questionnaire. The important results showed that the majority of students are aware of the dangers and crimes posed by cyberspace. Additionally, the results showed that while the majority of students care about choosing strong passwords, they are careless about changing them regularly. Many students lock their computers with a password when they are away. Furthermore, the findings revealed that many students are less vigilant towards virus attacks. However, the majority are aware of the dangers of revealing personal information and location on social media. In the end, it is recommended that all stakeholders should take proactive steps to protect themselves, their data and information, as well as their network infrastructure against cybercrimes or threats. Today, there is increasing use of Internet technology in education, such as e-learning platforms, online databases, online course repositories, YouTube videos, social media platforms, etc. The need for data protection becomes a matter of concern.
Today, hundreds of cybercrimes involving data misuse, privacy invasion, students visiting dangerous websites, etc., are reported. Therefore, it is crucial to know how to use the Internet safely.

Keywords: Cybercrime; cybersecurity; tertiary institution; awareness, Nigeria

1. Introduction

E-learning platforms, online databases, online course repositories, YouTube videos, and social networking sites are just a few examples of the internet technology that is being utilised in education more and more. Concerns are raised by the necessity of data protection. The way that students and academics use the internet has changed significantly in the last few years. It is now commonplace to enter information online in order to enroll in an online course, tutorial, or

DOI: https://doi.org/10.5281/zenodo.17205448

earning site. In a similar vein, the amount of data students provides for online assignments or result calculation on online learning platforms has grown along with their overall practice.

Innumerable information penetrations and awareness have already been brought about

by this, and they will only increase and standardise.

Currently, institutions have implemented a number of online learning tools that require lecturers and students to submit personal information on online platforms that are vulnerable to hacking. Also students have expanded their use of the Internet, including online films, businesses and games. Internet-capable equipment, although providing resources for study, communication, and cooperation, also poses a risk of bodily and mental harm to its users and their data. Thus, it is critical to determine the level of cybersecurity knowledge among students at higher institutions. Understanding why people and organisations continue to offer free online knowledge-based courses, what they gain, and what they do with users' information are basic topics that everyone should be aware of.

There are thousands of cybercrimes reported today, including privacy invasion and data misuse, pupils visiting risky websites, and so on. As a consequence, knowing how to use the internet securely is critical. As a result, cybersecurity must be understood and practiced in order to protect the privacy of data held by both instructors and pupils in educational settings. Tirumala et al. (2016) examined students' knowledge and awareness of cybersecurity, as well as their internet usage. The study's findings revealed that cybersecurity knowledge among students was generally low, with the majority of students being unfamiliar with fundamental cybersecurity words and lacking familiarity with daily cyber dangers such as phishing. The findings also reveal that the majority of students were unaware of cybersecurity tools for tablets and cell phones, which were used to access e-learning materials. Due to the COVID-19 lockdown, universities and other higher education

institutions were forced to close and switch to remote online learning. Governments, private institutions, educators, organizations, parents, and carers around the world are facing serious, unheard-of difficulties as a result of the closure. As ICT has advanced in education, learning has become more accessible, interesting, and contextualised thanks to online YouTube and video-based courses, e-books, simulations, models, graphics, animations, quizzes, games, e-businesses, and e-notes. For educational institutions, teachers' use of cyber tools and awareness of cyber safety and security are essential in the information technology age in general and this lockdown context in particular. because students might be more tech-savvy than their teachers think. While students are computerised locally, many adults rely on the occasional instructional exercise to learn how to use another program or application. Because they've been using apps, smartphones, and internet platforms their entire lives, they naturally know how to use them. This suggests that if given the right motivation, students could probably figure out how to hack into other people's records, including those of their teachers. A student might be able to figure out the secret key and alter one or two assessments, for example, if they weren't satisfied with the results of the course assessments. Therefore, it is necessary to give lecturers the authority to protect themselves and their students from online attacks.

Students are sometimes the ones who cause cybersecurity problems in the classroom, but in other cases, they might be the ones at fault. At the same time, many children can easily learn computer programs and even hack data. They might not have the mental

DOI: https://doi.org/10.5281/zenodo.17205448

acuity to recognise every cybersecurity danger they encounter. In order to increase students' likelihood of defending themselves online, teachers can legitimately secure their students and educate them about cybersecurity. Whether they want to or not, students' computer-related tendencies could endanger other students, teachers, and the school. When it comes to using the internet, students are consistently becoming more knowledgeable than teachers

They probably have access to every component of the most popular internet projects and cutting-edge devices. If they needed to hack into the records, this could put them in a significant, advantageous position over the teacher. As a teacher, you probably have a lot of online forms. Grades, notes, progress reports, contacts, personal information, and other identifying information belonging to the student could be compromised today. Students who have sensitive and private information in their personal records are at serious risk from the unreliable and inadequate network security. Intervention or a solution to improve cybersecurity is necessary due to the real-world consequences of these attacks. Higher education institutions must be ready and take all necessary safety precautions by adhering to security protocols if they plan to access all of the data stored on those records. They must keep an eye out and stop students from abusing them. Therefore, it is crucial to research the degree of cybersecurity awareness among students in postsecondary institutions in a few states in Northwestern Nigeria.

2. Literature Review

The Internet is now a commonplace part of daily life and has drastically altered how people communicate and process data and information. In certain developing nations, such as Nigeria, technological advancement has the potential to accelerate social, political, and economic transformations. They can also promote illegal activity in any nation. Nigeria as a whole has not fallen behind in terms of internet usage and penetration, mostly through mobile devices. It is both a potential source of cybercrime activity and a nation vulnerable to cybercriminals' attacks (Makare, 2024).

Even though banks and other financial institutions may be the target of the majority of cybercrime attacks, internet users in the general public are also susceptible to similar criminal activity (Kshetri, 2019).

In order to address the risks of cybercrime, it is crucial to evaluate the awareness and readiness of local internet providers and users. Any criminal activity carried out via the Internet is referred to as cybercrime (Osho & Adepoju, 2016; Aneke, et al., 2020). In addition to denial of service, downloading illicit files, failing to deliver goods or services, and hacking, this includes violations of intellectual property rights, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other crimes made possible by the Internet (Ajeet, 2014). The hardest part of cybercrime is figuring out exactly where and when the users committed the crime, as well as identifying the method they used to do it. Because of its anonymity, the Internet is a perfect medium and tool for a lot of organised crime (Ajeet, 2014; Omodunbi et al., 2023). Security agencies struggle to determine the source of cybercrimes because the speed at which cyber technology is evolving always outpaces their efforts (Majesty, 2010; Roshan, 2008). Accordingly, before the intrusion, cybercafé operators and system developers should think about creating an integrated tracking system that can identify and stop any questionable activity on their servers (Aliyu et al., 2020).

Cybercrime has become a sophisticated and extraordinary phenomenon in developing nations like Nigeria, according to Frank and Odunayo (2023). As Ezeanokwasa (2019) points out, this

DOI: https://doi.org/10.5281/zenodo.17205448

calls for a swift response in the form of laws that would protect cyberspace and its users.

It is challenging for police to investigate cybercrime because it is typically committed from remote locations. Policing becomes even more challenging when enabling regulations are lacking. According to statistics, Nigeria came in at number 43 in EMEA and third out of the ten countries that perpetrate cybercrime worldwide (Frank & Odunayo, 2023). However, despite the assistance of the Nigerian Cybercrime Working Group (NCWG), the National Cybersecurity Initiatives (NCI), established in 2003, have not yet achieved the suggested desired objectives (Awhefeada & Bernice, 2020).

Therefore, in order to safeguard the private sector, IT infrastructures, and facilities for information security and economic development, the government must intervene through the ministry of communication and digital economy. Cybercafés currently offer a variety of services, including academic research, online video games, entertainment, filling out application forms (for jobs, admissions, exams, visas, licenses, etc.), personal browsing, emails, and online tests (CBT). Cybercafés are the main location for students to access the Internet for homework and senior projects at higher education institutions. Regrettably, Internet cafes have contributed to the country's increased adoption of IT, but they have also made it possible for its misuse to spread. To access pornographic content, some young people go to cybercafés. Despite the nation's persistent efforts to combat Internet pornography, there are very few cybercafés with content filters.

Installed and downloaded to filter unwanted content on the Internet (Kshetri, 2019; Geoff et al., 2024; Longe et al., 2024). Although the majority of cybercafés posted warnings about using pornographic websites and engaging in spam, many users frequently disregarded the warnings and continued sending unsolicited emails, visiting sex websites, and downloading and viewing illegal content (including music, video, and other multimedia). According to Longe et al. (2024), the installation of fixed wireless facilities in Nigerian networks has added another dimension to the problem of cybercrimes, in addition to the readiness and use of Internet facilities in cybercafés for pornography and other cybercrimes. Similarly, the Yahoo Boys exploited cybercafés all over the nation as a safe haven for illegal activity directed at weaker users. They are involved in unlawful activities like hacking exam systems, travel websites, bank accounts, ATM cards, email accounts, and e-commerce websites. Consequently, phishing has gained a lot of popularity as criminals impersonate product websites to trick unsuspecting Internet users into providing their financial information while placing orders for phoney goods (Longe et al., 2024). Due to the occurrence of cybercrimes such as spamming, credit card fraud, ATM fraud, phishing, and identity theft through that café network, security agencies have shut down numerous cybercafés (Olumide and Victor, 2021; Augustine, 2022).

At the moment, there aren't any standardised, current cybersecurity guidelines for starting and running a cybercafé. A number of cybercafés were forced to close because their patrons were afraid of being hacked, scammed, or infected by viruses. The primary goal of this study was to find out how much knowledge students at universities, polytechnics, and educational colleges in Sokoto, Kaduna, and Kano had about cybersecurity threats and practices.

DOI: https://doi.org/10.5281/zenodo.17205448

3. Research Methodology

Three universities, polytechnics, and colleges of education in Sokoto, Kano, and Kaduna were chosen for this study, and their students' awareness of cybersecurity was investigated using a descriptive research methodology. Students at each school were given a questionnaire directly. The study only included students from computer science departments. The survey includes demographic information and multiple-choice questions about password strength, internet safety and computer protection, viruses and cyberattacks, and social media use and privacy threats for
Nigerian university students. The frequency of Internet use, safety procedures, and cybersecurity risk management in schools were also questioned. The three chosen universities, polytechnics, and colleges of education in Sokoto, Kaduna, and Kano comprised the sample of 100 students.
At the conclusion of the survey, 900 responses in all were returned. Software called SPSS v17 was used to analyse the data that was gathered.

4.1. Results

Eight of the nine institutions chosen for this study received 110 questionnaires during the data collection process. Due to the students' vacation at the time of data collection, no data was gathered at Sokoto State University. This study focusses on eight tertiary institutions: ABU, BUK, KDPOLY, KNPOLY, SOPOLY, KDCOE, KNCOE, and SSCOE. Only 20 of the 882 surveys that were sent were not returned, representing a 2.5% failure rate. Following data screening, 66 questionnaires were rejected because they were incomplete, poorly completed, or lacked Internet experience.
800 responses in total were deemed usable and utilised for the analysis of the study's data. Consequently, 800 responses were deemed adequate to fulfil the minimal sample size needed for basic statistical analyses (Gefen et al., 2000; Kim, Oh, Shin, and Chae, 2009).

4.1. Demographic Data

The Table 1 presents the results of the respondents' demographic factors which indicates that there were more male (55.3%) respondents than female (44.7%) from the 8 institutions surveyed. Out of the 800 respondents, 244 are between the ages of 16-25, 393 are aged 26-35, 130 are aged 36-45, whereas only 33 are aged 46 and above. Moreover, the number of respondents' types of institutions is proportionately equal. The majority of the respondents (53.5%) say they have been using the Internet for five years or above. The time spent by the majority of the respondents (59.3%) using the Internet is from 30 minutes or above. Most of the respondents are regular users (449/56.1%) of the Internet in addition to 207 (25.9%) that always online. About 642 (80.8%) of the respondents use smartphones to browse, and only 44 (5.5%) use a Desktop computer to browse the Internet. This is a clear indication of Desktop computers' lack of popularity and about to being replaced by Laptops and Smartphones. In terms of the activities performed online majority go online for academic purposes 65.0%, followed by social media 61.5%, email 54.5%, online games/audio/video 29.9% and finally online shopping with only 18.5%.

DOI: https://doi.org/10.5281/zenodo.17205448

Table 1: Respondents' demographic profile

Demographic		N	%
Gender	Male	445	55.3
	Female	355	44.7
Age	16 – 25	244	30.4
	26 – 35	393	49.3
	36 – 45	130	16.3
	46 above	33	4.1
Type of Institution	University	201	25.1
	Polytechnic	299	37.4
	College of Education	300	37.5
What is the duration of your Internet usage	one – four years	184	23.0
	five– seven years	188	23.5
	eight + years	428	53.5
How many minutes do you spend online browsing	one to two hours	74	9.3
	three to four hours	114	14.3
	five to six hours	138	17.3
	Seven + hours	474	59.3
How often do you stay online	Always	207	25.9
	Regularly	449	56.1
	Rarely	128	16.0
	Never	15	1.9
Please select the device you use for Internet browsing	Desktop	44	5.5
	Laptop	108	13.5
	Smartphone	642	80.3
	Others	6	0.8
Which activities do you frequently perform on the Internet (online):	Email	364	54.5
	Shopping	148	18.5
	Games/music/video	239	29.9
	Social Media	492	61.5
	Education	520	65.0
	Others	13	1.6

4.2. Factor 1: Password Strength

The length of the password, alphanumeric and special characters, and frequent password changes all contribute to its strength. (Senthilkumar and Sathishkumar, 2017). The students' responses, as indicated in Table 2, show that the majority of them do not periodically change their passwords and use the same password for different accounts. However, the overwhelming majority (518) says they never share their password with someone and therefore indicates a high level of security awareness regarding safeguarding their password. Though a high percentage (55%) says they used a password found in the dictionary, the majority reported that they take quick measures to recover their password when compromised. Also, they create a lengthy and strong password with a minimum of 8 characters including alphanumeric, special, numbers, upper-, and lower-case letters.

DOI: https://doi.org/10.5281/zenodo.17205448

Table 2: Password Strength

Please indicate the extent to which you do the following	Never	Once	Rarely	Regularly	Always
• Regularly changing the password	246	161	179	152	62
• Using old passwords again	248	181	114	135	122
• Making use of the same password across all of your accounts	295	129	99	119	158
• Giving Someone Your Passwords	518	81	92	55	54
• Maintaining your password in your web browser	326	107	98	109	160
• Utilising a dictionary-based password	476	107	74	55	88
• Do you take additional measures to recover your password if you believe it has been compromised?	172	167	117	126	218
• Creating a strong and long password that contains at least 8 characters, including special characters, numbers, capital and lowercase letters, etc.	126	120	94	174	286

4.3. Factor 2: Computer Protection

In terms of computer protection majority of the students indicated a high level of awareness, especially by shutdown their computers when they are away. Password protection of a computer is the easiest and cheapest method. Only 210 out of 800 students reported not allowing their hotspot to connect automatically, but the rest allow it once, rarely, and regularly. 285 says they always delete all personal information before giving their computers out for repairs, which shows a considerable amount of security and privacy consciousness.

Table 3: Computer Protection

Please indicate the extent to which you do the following:	Never	Once	Rarely	Regularly	Always
• When you are not using your computer, do you shut it down, log off, or password-protect it?	192	89	79	128	312
• Do you make sure your hotspot or modem doesn't connect on its own?	205	148	128	109	210
• Before having your computer fixed or replaced, do you delete any sensitive, private, or private information?	180	109	120	106	285

4.4. Factor 3: Virus Attacks

According to the responses received in Table 4, many students are not conscious of virus attacks, as 352 say they do open and reply to emails from unknown sources. About 166 say they never reinstall the OS despite experiencing virus attacks through content filtering software. However, many students indicated that they regularly and always update their antivirus software automatically every week. This shows a high degree of awareness about virus attacks, especially when downloading online content.

DOI: https://doi.org/10.5281/zenodo.17205448

Table 4: Virus Attacks

Please indicate the extent to which you do the following:	Never	Once	Rarely	Regularly	Always
• Do you run a weekly or more frequent check on your antivirus program?	156	112	137	198	197
• Since new viruses and worms that spread quickly are released every day, do you have your antivirus program set to update automatically?	128	148	116	195	213
• Do you use an up-to-date virus scanner to check for viruses before installing or using any software from anywhere?	149	129	155	160	207
• Avoid installing applications or free software from unreliable sources on your computer.	267	152	141	118	122
• When using content filtering software, you do see extensions like. bat,.cmd,.exe,.pif,.scr, or .zip.	198	130	199	119	154
• Reinstalling the operating system may or may not be necessary, depending on the level of virus infection on your computer.	166	159	181	140	154
• How often do you receive unwanted emails (phishing) from unknown persons	252	169	171	106	102
• How often do you open or reply to unwanted emails (phishing) received from unknown persons	352	119	126	99	104

4.5. Factor 4: Social media use

Social media has become a major source for revealing personal information and resulting in identity theft. It has become part of every student's life. This study intends to determine the amount of private information students reveal on their respective social media accounts. Table 5 shows that on average majority of students the never published their career achievements, identity such as name, home address, phone number, etc. 147 students say they always accept friend requests from unknown persons. 231 out of 800 say they never reveal their location on social media as an indication of security consciousness. According to Senthilkumar and Sathishkumar (2017), when compared to other identity outsourcing, accepting strangers into a social network is thought to pose the biggest threat. The second most significant piece of personal information that is shared on social media is a person's location, which is updated whenever they travel. Career details and having an original display picture have very little bearing on publishing when compared to these two.

Table 5: Social media use

Please indicate the extent to which you do the following:	Never	Once	Rarely	Regularly	Always
• How often do you upload/post your picture, audio, or video on social media (e.g., WhatsApp, Facebook, TikTok, etc)	154	101	192	165	188
• How often do you accept friend requests from unknown persons on social media	166	142	198	147	147
• How often do you update your locations on social media	231	162	186	114	107
• How often do you reveal your career/personal achievements	244	137	168	150	101
• How frequently do you share your name, address, phone number, and other personal details on social media	268	160	142	131	99

DOI: https://doi.org/10.5281/zenodo.17205448

1. Conclusion

Cybercrimes are now a global epidemic that threatens national security in many countries. Internet users are prone to stealing the personal information of ordinary people by visiting websites that are already infected with viruses, responding to phishing emails, storing logging information in a third-party location, or even sharing private information over the phone or posting personal information on social networking sites. According to the survey's findings, Nigerian university students are quite aware of cybersecurity threats. That is sufficient to help them defend themselves and their computers against hackers; therefore, a higher level of awareness needs to be raised. Due to the potential impact on students' and the public's privacy, cybercrime activities must be investigated and promptly addressed. Numerous stakeholders, including users, operators, internet service providers ISP, cybersecurity organisations, and the government agencies, must be involved in fighting cybercrime attacks. To improve the general public's readiness to handle the risks of computer crimes, more measures will be implemented. Antivirus software and other programs designed to improve readiness levels should be made available, as well as their costs. The public will be better equipped to handle the dangers of cybercrime in this way. It should also be a regular practice to educate the public on how to protect their information when using the internet. Rather than depending solely on the self-administered survey to measure the degree of understanding and readiness, it would be crucial to conduct group discussions with internet managers and end users to ascertain the degree of awareness and readiness regarding cybercrimes. In this manner, data collection problems that are likely to be unclear are resolved and made clear.

References

Adebusuyi, A. (2022): The Internet and Emergence of Yahoo Boys Sub-Culture in Nigeria, *International Journal of Cybersecurity*

Ajeet, S. P. (2014). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3 (6)*. Available: www.ijettcs.org.

Aliyu, M., Tambuwal, A. B., Namahe, Y. U. (2020). Investigating Factors and Extenuation Strategies for Mobile Phone Use While Driving in Nigeria. *Caliphate Journal of Science & Technology (CaJoST), Vol. 2(2).*

Aneke, S. O., Nweke, E. O., Udanor, C. N., Ogbodo, I. A., Ezugwu, A. O., Uguwishiwu, C. H., & Ezema, M. E. (2020). Towards Determining Cybercrime Technology Evolution in Nigeria. International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS) Vol. IX, Issue IV, April 2020 | ISSN 2278-2540

Augustine C. Odinma, MIEEE (2022): Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, Nov 1-2.

Awhefeada, U. V., & Bernice, O. O. (2020). Appraising the Laws Governing the Control of Cybercrime in Nigeria. *Journal of Law and Criminal Justice*, *8*(1), 30-49.

Ezeanokwasa, J. O. (2019). Child Pornography under the Cybercrimes Act 2015 of Nigeria: The Law its challenges. *African Journal of Criminal Law and Jurisprudence, 4.*

Frank, I. and Odunayo, E. (2023). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International *Journal of Cognitive Research in science, engineering, & education (IJCRSEE), 1* (1).

Geoff, H., Anthony, P., Gopalakrishnan, S. and Manav, M. (2024). Trends in Spam

DOI: https://doi.org/10.5281/zenodo.17205448

Products and Methods. Conference on e-mail and Antispam.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Managament, 22:2, 77-81, https://doi.org/10.1080/1097198X.2019.1603527

Longe O. B & Longe F. A (2024): The Nigerian Web Content: Combating the Pornographic Malaise Using Content Filters. *Journal of Information Technology Impact*, Vol. 5, No. 2, pp. 5964.

Longe, O, Omoruyi, I & Longe, F (2024): Implications of the Nigeria Copyright Law for Software Protection. *The Nigerian Academic Forum Multidisciplinary Journal.* Vol. 5, No. 1. pp 7-10.

Majesty, H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.

Makeri, Y. A. (2024). Cyber Security Issues in Nigeria and Challenges. *International Journal Advanced Research in Computer Science and Software Engineering*, *7*(4).

Olumide, O. O. and Victor, F. B. (2021): E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology*, Vol. 11 (1), May 2021 (spring).

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *Journal of Engineering and Technology*, *1*(1), 37-42. http://engineering.fuoye.edu.ng/journal/index.php/engineer/article/

Osho, O., & Adepoju, S. A. (2016). Cybercafés in Nigeria: Curse to the Internet. International Conference on Information and Communication Technology and Its Applications *ICTA 2016*, 117-123.

Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at - http://www.http://www.asclonline.com/index.php?titl e=Rohas_Nagpal,

Sodiq, K. A. (2012). Assessment of the Management of ICT Infrastructure of Selected Cybercafes in Lagos State. *Journal of Educational and Social Research*, *2*(9), 181-181.

DOI: https://doi.org/10.5281/zenodo.17205448