JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(2), JUNE, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

An Assessment of Cybersecurity Awareness among Students of Tertiary Institutions in Zaria

Agballa U. B., Umar Kabir., Abdullahi O. A., Hassan M. G., Bello Musbahudeen, Bashir Abdulrahman, , Karagama I. M.
Department of Computer Science
Nigeria Institute of Leather and Science Technology Zaria, Nigeria.

ABSTRACT
The rapid growth of internet usage and digital technologies has increased students' exposure to cyber threats, particularly within tertiary institutions. Cybersecurity awareness is essential for protecting personal data, institutional systems, and national digital infrastructure. This study conducted a survey across eight tertiary institutions in Zaria, selecting 100 respondents from each institution, this includes Ahmadu Bello University (ABU), Nuhu Bamalli Polytechnic, the Nigerian Institute of Leather and Science Technology (NILEST), Federal University of Education (FUE) Zaria, ABU College of Health Sciences, ABU Division of Agricultural Colleges, the Nigerian College of Aviation Technology (NCAT), and St. Luke's College of Nursing, using a systematic convenience sampling method. Data on students' cybersecurity awareness were collected through a paper-based questionnaire and analyzed using SPSS version 17. The findings reveal moderate awareness levels, with significant gaps in practical cybersecurity behaviors such as password management, phishing detection, and data protection. The study recommends the integration of cybersecurity education into academic curricula, increased institutional awareness programs, and policy-driven interventions to enhance students' cybersecurity preparedness.

ARTICLE INFO
Article History
Received: February, 2026
Received in revised form: April, 2026
Accepted: April, 2026
Published online: June, 2026

KEYWORDS
Cybersecurity Awareness, Tertiary Institutions, Students, Zaria, Information Security

1. INTRODUCTION

The increasing reliance on digital technologies for academic, social, and financial activities has exposed students in tertiary institutions to a wide range of cyber threats. Cyberattacks such as phishing, identity theft, malware infections, and social engineering attacks are becoming more prevalent, particularly among young internet users. In Nigeria, the rapid adoption of mobile devices and online platforms has further amplified these risks.

Tertiary institution students represent a highly active digital population, frequently engaging in online learning platforms, social media, electronic payments, and cloud-based services. Despite this high level of engagement, many students lack adequate knowledge and skills to protect themselves against cyber threats. In Zaria, a major educational hub in Northern Nigeria, the presence of multiple tertiary institutions makes cybersecurity awareness among students an issue of growing importance.

Currently, educational institutions have adopted numerous e-learning platforms that require both students and instructors to provide personal information online, making these systems potential targets for cyberattacks. Students' engagement with internet-enabled activities such as online videos, gaming, and social media has increased significantly. Although internet-based technologies offer valuable opportunities for learning, communication, and collaboration, they also expose users and their personal data to risks of

Corresponding author: Aqballa, U. B.
agballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(2), JUNE, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

physical, emotional, and cyber-related harm (National Cyber Security Alliance & Norton by Symantec, 2010).

In recent times, numerous cybercrime incidents related to privacy breaches, data misuse, and students' exposure to unsafe websites have been reported. Consequently, understanding safe internet usage has become increasingly important. Cybersecurity awareness and practices are therefore essential for protecting the personal data of both students and educators within academic environments. Tirumala *et al*. (2016) conducted a survey examining students' levels of cybersecurity knowledge and awareness in relation to their internet usage. The findings revealed that overall cybersecurity awareness among students was generally low, with a significant proportion lacking familiarity with basic cybersecurity concepts and exhibiting limited understanding of common cyber threats.

This study seeks to assess the level of cybersecurity awareness among students of tertiary institutions in Zaria, focusing on their understanding of cyber threats, security practices, and attitudes toward online safety.

2. LITERATURE REVIEW

Cybersecurity awareness refers to an individual's understanding of cyber risks and the adoption of safe behaviors to mitigate such threats. Studies have shown that low awareness levels significantly increase vulnerability to cybercrime, particularly among students and young adults. Previous research indicates that students often possess basic knowledge of cybersecurity concepts but fail to apply safe practices consistently.

Nigeria has increasingly become vulnerable to cybercriminal attacks and is often identified as a potential hub for cybercrime activities (Makare, 2017). Although many cyberattacks are directed at financial institutions such as banks, students, members of the general public who use the Internet are equally susceptible to becoming victims of these crimes (Kshetri, 2019). Consequently, it is crucial to evaluate the level of awareness and readiness of local Internet service operators and users in responding to cyber-related threats.

Cybercrime encompasses all forms of illegal activities conducted through the Internet (Osho & Adepoju, 2016; Aneke et al., 2020). These activities range from denial-of-service attacks, illegal file downloads, and failure to deliver goods or services, to hacking, intellectual property violations, economic espionage, online extortion, identity theft, international money laundering, and numerous other Internet-enabled offenses.

Detecting cybercrime is particularly challenging due to the difficulty in identifying the exact techniques used, as well as determining the precise location and timing of such crimes. The anonymity provided by the Internet makes it a preferred medium for organized criminal operations (Omodunbi et al., 2016). As a result, cybercafé operators and system developers are encouraged to implement embedded monitoring and tracking mechanisms capable of detecting and preventing suspicious activities before system breaches occur (Aliyu et al., 2020).

In developing nations such as Nigeria, cybercrime has grown rapidly in both scale and sophistication, necessitating urgent legislative and regulatory interventions to safeguard cyberspace and its users (Ezeanokwasa, 2019). The remote nature of cybercrime further complicates law enforcement efforts, and the lack of comprehensive regulatory frameworks exacerbates these challenges.

Although the National Cybersecurity Initiatives (NCI), established in 2003, were designed to address these issues, they have yet to fully achieve their intended goals, even with support from the Nigerian Cybercrime Working Group (NCWG) (Awhefeada & Bernice, 2020). Therefore, stronger involvement from the government, particularly through the Ministry of Communications and Digital Economy, is required to protect IT infrastructure, the private sector, and national information systems critical to economic growth.

Currently, cybercafés offer a wide range of services, including Internet browsing, email communication, online applications for

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(2), JUNE, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

employment, education, examinations, visas, licensing, computer-based tests (CBT), academic research, online gaming, and entertainment. In tertiary institutions, cybercafés serve as central access points for completing assignments and final-year research projects. However, despite their role in promoting information technology adoption in Nigeria, cybercafés have also contributed to the proliferation of cyber-related abuses.

In Nigeria, limited formal cybersecurity education and inadequate institutional policies have contributed to poor cybersecurity hygiene among students. Research has highlighted common issues such as weak password usage, lack of awareness of phishing attacks, and negligence toward data privacy. However, there is limited empirical research focusing specifically on cybersecurity awareness among students in Zaria, creating a gap that this study aims to address.

METHODOLOGY

This study employed a descriptive **survey** design to examine the level of cybersecurity awareness among students from selected tertiary institutions in Zaria, including Ahmadu Bello University (ABU), Nuhu Bamalli Polytechnic, the Nigerian Institute of Leather and Science Technology (NILEST), Federal University of Education (FUE) Zaria, ABU College of Health Sciences, ABU Division of Agricultural Colleges, the Nigerian College of Aviation Technology (NCAT), and St. Luke's College of Nursing. Data were collected through questionnaires administered directly to students within their respective institutions.

The questionnaire consisted of demographic information and multiple-choice items addressing key cybersecurity issues such as password strength, computer protection and Internet safety, virus and cyber-attack awareness, social media usage, and privacy threats affecting students in higher institutions in Zaria. Additional questions assessed the frequency of Internet usage, cybersecurity practices, and strategies for managing cyber risks within the schools.

A sample of 100 students was selected from each of the eight institutions, resulting in a total of 800 valid responses at the conclusion of the survey. The collected data were analyzed using SPSS version 17 software.

3.1 Data Collection

A structured questionnaire was used to collect data. The instrument consisted of three sections:

- Demographic information
- Knowledge of cybersecurity threats
- Attitudes toward cybersecurity awareness

The questionnaire was administered physically and electronically to ensure wider participation.

3.2 Sample Size and Sampling Technique

A random sampling technique was employed to select respondents from different academic levels and disciplines. A total of **1008** questionnaires were distributed, out of which **800** were validly returned and analyzed.

RESULTS AND DISCUSSION

During the data collection phase, 110 questionnaires were administered to each of the eight tertiary institutions included in the study. The institutions surveyed comprised Ahmadu Bello University (ABU), Nuhu Bamalli Polytechnic, the Nigerian Institute of Leather and Science Technology (NILEST), the Federal University of Education (FUE) Zaria, ABU College of Health Sciences, ABU Division of Agricultural Colleges, the Nigerian College of Aviation Technology (NCAT), and St. Luke's College of Nursing. Out of the 880 questionnaires distributed, 27 were not retrieved, representing a non-response rate of 3.0%. Following data screening, 53 questionnaires were excluded due to incomplete responses, improper completion, or insufficient Internet usage experience. Consequently, 800 questionnaires were deemed valid and used for the final data analysis. This sample size was considered adequate to satisfy the minimum requirement for conducting basic statistical

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

analyses, as supported by Shin and Chae (2009).

4.1 Demographic Data

Table 1 presents the demographic characteristics of the respondents. The data show a slightly higher proportion of male respondents (54.1%) compared to female respondents (45.9%) across the eight surveyed institutions. Of the 800 participants, 245 were aged 15–20, 400 were 21–25, 125 were 26–30, and only 30 were 31 years and above. The distribution of respondents by type of institution was fairly even.

Regarding Internet usage, a majority of respondents (53.5%) reported having used the Internet for five years or more. Most respondents (59.5%) spend 30 minutes or more online during a typical session. Regular Internet users accounted for 439 respondents (54.8%), with an additional 202 respondents (25.2%) indicating they are always online. Smartphones were the primary device for Internet access, used by 642 respondents (80.3%), while only 44 respondents (5.5%) used desktop computers, highlighting the declining popularity of desktops in favor of laptops and smartphones.

In terms of online activities, the majority of respondents use the Internet for academic purposes (65.0%), followed by social media engagement (61.5%), email communication (54.5%), online gaming or audio/video.

Table 1: Respondents' demographic profile

Demographic		N	%
Gender	Male	432	54.1
	Female	368	45.9
Age	15 – 20	245	30.6
	21 – 25	400	50
	26 – 30	125	15.6
	31 above	30	3.7
How long have you been using Internet?	1 – 2 years	180	22.5
	3 – 4 years	192	24
	5 + years	428	53.5
How many minutes do you spend online browsing?	1–10 minute	74	9.3
	11–20 minute	120	15
	21–30 minute	130	16.2
	31+ minutes	476	59.5
How often do you stay online?	Always	202	25.2
	Regularly	439	54.8
	Rarely	136	17.0
	Never	23	2.9
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 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

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 14(2), JUNE, 2026
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbufstejoste.com

4.2 Factor 1: Password Strength

Password strength is determined by factors such as the use of alphanumeric and special characters, password length, and regular password updates (Senthilkumar & Sathishkumar, 2017). As shown in Table 2, most students reported that they do not change their passwords regularly and often use the same password across multiple accounts. However, a large majority (N = 518) indicated that they never share their passwords with others, reflecting a strong awareness of password security. Although 55% admitted to using passwords that can be found in dictionaries, most respondents stated that they take prompt action to recover their accounts if their passwords are compromised. Additionally, students reported creating long and robust passwords of at least eight characters, incorporating a mix of alphanumeric characters, special symbols, and both uppercase and lowercase letters.

Table 2: Password Strength

Please indicate the extent to which you do the following	Never	Once	Rarely	Regularly	Always
• Periodical change of password	240	167	180	151	62
• Reusing previous passwords	250	183	119	135	113
• Using the same password for each of your accounts	285	129	89	129	168
• Sharing password with Someone	518	81	92	55	54
• Saving your password on your browser	316	127	98	89	170
• Using a password that is found in a dictionary	476	107	74	55	88
• If you think your password has been compromised then do you take further step to recover it	170	160	117	129	224
• Making the password as lengthy as possible and strong like minimum 8 and above characters using special characters, numbers, upper/lower case letters etc.	126	120	94	174	286

4.3 Factor 2: Computer Protection

Regarding computer protection, most students demonstrated a high level of awareness, particularly by locking their computers when unattended. Using passwords to secure computers remains one of the simplest and most cost-effective security measures. Only 220 out of the 800 students reported that they prevent their devices from automatically connecting to hotspots, while the remaining students allow automatic connections either occasionally or regularly. Additionally, 275 students stated that they always erase personal information before sending their computers for repair, indicating a significant degree of privacy and security consciousness.

Table 3: Computer Protection

Please indicate the extent to which you do the following:	Never	Once	Rarely	Regularly	Always
• Do you shutdown, logoff or lock your computer with password, when you are away.	192	89	79	128	312
• If you have a modem/hotspot, do you make sure it does not connect automatically?	205	145	128	104	220
• Do you remove personal, confidential or sensitive data before giving your computer to be repaired or replaced?	185	109	125	106	275

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

4.4 Factor 3: Virus Attacks

Based on the responses presented in Table 4, a considerable number of students showed limited awareness of virus-related threats, as 347 respondents indicated that they open and respond to emails from unknown senders. Additionally, about 171 students reported that they do not reinstall their operating systems even after encountering virus infections, despite using content-filtering software. Nevertheless, many respondents stated that they regularly or consistently update their antivirus software on a weekly automatic basis. This reflects a relatively high level of awareness regarding protection against malware, particularly when downloading content from the internet.

Table 4: Virus Attacks

Please indicate the extent to whichyou do the following:	Never	Once	Rarely	Regularly	Always
• Do you check the antivirus software at least every week	156	112	137	198	197
• Do you set antivirus software for automatic updates (because new, fast spreading worms and viruses are released every day)	128	148	116	195	213
• Before implementing or using any software from any source, do you check for viruses with a current virus scanner	149	129	155	160	207
• Do not install free software/application on your computer from an untrusted source.	267	152	141	118	122
• You do notice the extensions such as: .bat, .cmd, .exe, .pif, .scr, or.zip through content filtering software.	198	130	199	119	154
• Depending on the extent of virus infection on your computer, do you re-install the operating system?	171	159	186	140	154
• How often do you do 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	347	119	126	99	109

4.5 Factor 4: Social media use

Social media has emerged as a significant channel through which personal information is disclosed, often increasing the risk of identity theft. It has become an integral part of students' daily lives, and this study examines the extent to which students share private information on their respective social media platforms. As shown in Table 5, the majority of respondents reported that they rarely publish personal details such as career achievements or identifying information, including names, home addresses, and phone numbers. However, 140 students indicated that they consistently accept friend requests from unknown individuals. Additionally, 236 out of the 800 respondents stated that they never share their location on social media, reflecting a level of security awareness. According to Senthilkumar and Sathishkumar (2017), accepting friend requests from unfamiliar users represents one of the most significant threats within social networks, surpassing other forms of identity exposure. This is followed by the frequent sharing of location information, which constitutes another major privacy risk. In comparison, disclosing career-related information or using real profile pictures poses relatively less risk in terms of personal data exposure.

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

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 request from unknown persons on social media	166	149	198	147	140
• How often do you update your locations on social media	236	162	186	119	107
• How often do you reveal your career/personal achievement	244	137	168	150	101
• How often do you post your personal information such as name, address, phone number etc. on social media	268	160	142	131	99

5. CONCLUSION

Globally, cybercrime has evolved into a serious threat to national security across many countries. Internet users frequently engage in unsafe online behaviors such as visiting malware-infected websites, responding to phishing emails, storing login credentials on third-party platforms, sharing sensitive information over the phone, and disclosing personal data on social media, all of which expose individuals to identity theft and other cyber threats. The findings of this study indicate that students in Nigerian tertiary institutions possess a relatively moderate level of awareness regarding cybersecurity and cyber threats. This level of awareness is beneficial in helping them protect both themselves and their computing devices from cyber attackers; however, there remains a need to further strengthen awareness at more advanced levels.

Cybercrime activities must be promptly monitored and addressed, as they pose significant risks to the privacy and security of students and the wider public. Effectively combating cyber threats requires the collaborative efforts of multiple stakeholders, including end users, service providers, internet operators, cybersecurity agencies, and government authorities. Additional measures should be implemented to improve public readiness in managing computer-related crimes. In particular, security tools such as antivirus software and other protective applications should be made more affordable and accessible to users. This would enhance the ability of the general public to adequately defend against cyber threats. Furthermore, continuous public education on safe online practices and data protection is essential. Beyond the use of self-administered questionnaires, conducting group discussions with internet service managers and end users is recommended to better assess levels of awareness and preparedness. Such interactive approaches allow for clarification of misunderstandings and improve the quality and reliability of data collected.

6. RECOMMENDATIONS

Based on the findings, the study recommends:

1. Integration of cybersecurity education into tertiary institution curricula.
2. Regular cybersecurity awareness workshops and seminars for students.
3. Development of institutional cybersecurity policies and guidelines.
4. Collaboration with cybersecurity professionals to provide practical training.
5. Encouragement of safe online practices through continuous awareness campaigns.

Corresponding author: Aqballa, U. B.
aqballaubi@gmail.com
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.

REFERENCE

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), 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

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*.

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

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81, https://doi.org/10.1080/1097198X.2019.160 3527

Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. International *Journal Advanced Research in Computer Science and Software Engineering, 7*(4).

Senthilkumar, K.; Easwaramoorthy, S. A Survey on Cyber Security Awareness among College Students in Tamil Nadu. IOP Conf. Ser. Mater. Sci. Eng. **2017**, 263, 042043

Tirumala S. S., A. Sarrafzadeh and P. Pang, "A survey on internet usage and cybersecurity awareness in students," *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 2016, pp. 223-228, doi: 10.1109/PST.2016.7906931.

Corresponding author: Aqballa, U. B.
✉ *aqballaubi@gmail.com*
Department of Computer Science, Nigeria Institute of Leather and Science Technology, Zaria.