International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 111-118 www.ijaem.net ISSN: 2395-5252

Investigating Cybersecurity Awareness among Tertiary Institutions Students in Nigeria

Aminu Aliyu[a], Mansur Aliyu[b], Abdulmalik Ahmad[c] and Shitu Abdullahi[d]

[a]*Umaru Ali Shinkafi Polytechnic, Sokoto, Nigeria*
[b]*Sokoto State University, Sokoto, Nigeria*
[c and d]*Umaru Ali Shinkafi Polytechnic, Sokoto, Nigeria*

Submitted: 25-09-2021 Revised: 01-10-2021 Accepted: 05-10-2021

ABSTRACT

Incorporating cybersecurity into the university curriculum is very important to help students stay safe using the Internet and social media. Today, much attention has been given to understanding cybersecurity concepts and the effort made by government and institutions to help introduce cybersecurity as an independent degree programme and other related disciplines. Several bodies (such as NITDA, NCC, NCS, and CPN) and scholars developed workshops, seminars, conferences were conducted, and guidelines were developed and disseminated for creating awareness on cybersecurity. In this research, a survey of nine tertiary institutions from Kaduna, Kano and Sokoto was carried out. Targeting 100 respondents from each institution (Universities, Polytechnics and Colleges of Education) using a systematic convenient sampling technique. The data collected on the student's cybersecurity awareness with paper and pen questionnaire was analyzed using SPSS v17 software. The significant findings revealed that majority of the students are conscious of cybercrime and threats. Also, the findings revealed that most students are negligent in changing their password periodically, but are concerned in creating strong password. Many students locked off their computers with password when they are away. Furthermore, the findings revealed that many students are less vigilant towards virus attacks. However, 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 protecting themselves, their data and information, as well as their network infrastructure against cybercrimes or threats.

Keywords: Cybersecurity; cybercrime; awareness, tertiary institution; Nigeria

I. INTRODUCTION

Today, there is increasing use of Internet technology in education such as e-learning platforms, online databases, online courses repositories, YouTube videos, social media platforms etc. The need for data protection becomes a matter of concern. How academics and students utilizes the web has changed a lot in recent times. Entering information online to join a learning site, tutorials or online classes has become the daily standard. Similarly, students' data to calculate results or assign tasks online on e-learning platforms has grown, and the students' usage in general. This has prompted numerous information penetrations and awareness as of now, and will continue to increase and standardize.

Presently, Institutions have introduced multiple e-learning resources that require teachers and students to enter their personal information on online platforms, which are prone to be hacked. Students have increased their usage of the Internet, online videos and games, etc. The Internet-capable technology, with its gift of resources for learning, communication, and collaboration, comes with dangers of physical and emotional harm to its users and their data (National Cyber Security Alliance & Norton by Symantec, 2010). Thus, it is essential to understand the level of awareness of tertiary institutions' students on cybersecurity. To understanding why people and organizations continue to create online knowledge based courses free, what they do they gain, and what they do with the users information are basic questions everybody needs to know.

Nowadays, there are hundreds of cybercrimes reported on privacy invasion and data misuse, students getting onto unsafe sites, etc. As a result, the role of understanding how to use the Internet safely is essential. Thus cybersecurity needs to be understood and practiced to secure the privacy of data of both the teachers and the students in an educational setting. Tirumala et al. (2016), surveyed students' understanding and awareness of cybersecurity with information on their internet usage. The study's outcome indicated that cybersecurity awareness among the students was commonly low, most significant number of the students was inexperienced with basic cybersecurity terms and did not exhibit enough familiarity with everyday cyber threats, for example, phishing. The outcome further shows that most of the students didn't know about cybersecurity apparatuses for tablets and cell phones, which utilized gadgets for e-learning resources.

The COVID-19 lockdown has forced the universities and other higher institutions to close and had to go for remote online learning. The closure has placed unprecedented challenges on governments, institutions, teachers, parents, and caregivers worldwide. With the development of ICT in education, online video-based courses, e-books, simulations, models, graphics, animations, quizzes, games, and e-notes make learning more accessible, engaging, and contextualized. In the information technology era in general and in this lockdown context in specific, teachers' use of cyber tools and need to be aware of cyber safety and security is necessary for educational institutions. Since students may be more tech-savvy than their teachers envision. While numerous grown-ups depend on the periodic instructional exercise to figure out how to utilize another program or application, students are computerized locals. They naturally realize how to use applications, cell phones, and online stages since they've been used them their entire lives. This implies, with the correct inspiration, the students could most likely make sense of how to hack into other records, which may include teachers also. For instance, if a student wasn't happy with the course assessment scores, he/she may have the option to make sense of the secret key and change an evaluation or two. Thus, the lecturers need to be empowered to shield both themselves and their understudies from digital assaults. Sometimes, students may be the offenders of cybersecurity issues in the classroom; however, they may be the people in question in others. At the same time, numerous youngsters can learn computerized programs without much of a stretch and may even hack data. They may not be sufficiently sharp to detect each cybersecurity chance that they experience. As a teacher, it is possible to legitimately secure students and encourages them about cybersecurity to get all the more likely to defend themselves on the web.

Regardless of whether the students intend to or not, the students could put teachers, the school, and other students in danger with their computerized propensities. The students are regularly getting more educated than teachers when it comes to internet usage. They likely can utilize each element of the most mainstream online projects and advanced gadgets. This could give them a substantial favorable position over the teacher if they needed to hack into the records. As an instructor, one most likely has various online forms. Today, the student's marks, memos, progress reports, contacts, personal details, and other identifying information are at risk of being exposed. The poor and disruptive network security poses a significant threat to students whose personal records contain personal and sensitive information. The practical effects of these attacks require intervention or remedy to increase cybersecurity. The higher institutions have to be prepared and instead take all precautions by following security measures if they approach all the data put away on those records. They need to be alert and prevent misuse by students. Thus it is essential to study the students' level of awareness of cybersecurity in tertiary institutions in selected states in Northwestern Nigeria

II. LITERATURE REVIEW

Today, Internet has become part of everyday life and has fundamentally changed people’s habits regarding data and information communication and processing. Nowadays, technological advancement in some developing countries like Nigeria have the potential to grow their economic, social, and political changes. They can also advance criminal activities in any given country. As a nation, Nigeria has not been left behind in internet penetration and usage, primarily via mobile phones. It is a country prone to attacks by cybercriminals and a possible source of cybercrime activities (Makare, 2017). While most cybercrime attacks might target financial institutions like banks, internet users within the general public are also likely to become victims of similar criminal activities (Kshetri, 2019). Therefore, it is essential to assess both the awareness and preparedness level of local internet operators and users to deal with the threats of cyber-criminal activities.

Cybercrime refers to any criminal activity executed through the Internet (Osho & Adepoju, 2016; Aneke, et al. 2020). This involves many things from denial of service, downloading illegal files, non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other Internet-facilitated offenses (Ajeet, 2014). Cybercrime is most difficult to immediately detect the method used to carry out the Crime, to know precisely where and when the users carried out the Crime. The anonymity of the Internet makes it an ideal channel and instrument for many organized criminal activities (Ajeet, 2014; Omodunbi et al. 2016). The speed of cyber technology changes always beats security agencies' efforts, making it difficult for them to identify the origin of cybercrimes (Majesty, 2010; Roshan, 2008). As such, cybercafé operators and system developers need to consider developing an in-built tracking system that can detect and block all suspicious activities on their servers before the intrusion (Aliyu et al., 2020).

In developing countries like Nigeria, according to Frank and Odunayo (2013), the cybercrime phenomenon has become a sophisticated and extraordinary increase recently and therefore called for a quick response in providing laws as highlighted by Ezeanokwasa (2019) that would protect cyberspace and its users. Cybercrime is involved and committed mostly from remote locations, making it difficult for police. The absence of enabling regulation makes policing even more difficult. Statistically, Nigeria ranked 43 in EMEA and ranked third among the ten nations that commit cybercrime in the world (Frank & Odunayo, 2013). Even though, the National Cybersecurity Initiatives (NCI) that was created in 2003 are yet to meet the proposed desired objectives, despite the help from the Nigerian cybercrime working group (NCWG) (Awhefeada & Bernice, 2020). Therefore, the government through the ministry of communication and digital economy must come in to protect the private sector, IT infrastructures, and facilities for information security and economic development.

Presently, cybercafés provide services such as personal browsing, emails, filling application forms (i.e., for jobs, admissions, exams, visas, licensing, etc.), online exams (CBT), academic research, online video games, and entertainment, etc. In higher institutions, cybercafés are the hub of accessing the Internet for assignments and final year projects. Unfortunately, while Internet cafes helped enhance IT adoption in the country, they have also allowed multiplying its abuses. Some youth visits cybercafés to access pornographic materials. Despite the consistent fight against Internet pornography in the country, only a few cybercafés where content filters are downloaded and installed to filter unwanted Internet content (Kshetri, 2019; Geoff et al. 2005; Longe et al., 2005). Despite majority of the cybercafés placed warning notices against surfing pornographic sites and spamming activities, still many users often ignored the notice, and keep sending spam mails, browse sex sites, surf and download unauthorized contents (such as video films, musical audios and other multimedia contents). Apart from the readiness and usage of Internet facilities in cybercafés for pornography and other cybercrimes, the installation of fixed wireless facilities in the Nigerian network landscape has added another dimension to the cybercrimes problem (Longe et al., 2005).

Similarly, the yahoo boys used cybercafés across the country as a medium for safe criminal activities against vulnerable users. They are engaged in illegal activities such as hacking e-commerce sites, bank accounts, ATM cards, email accounts, examination systems, travel sites, etc. As a result, phishing has become very popular as criminals simulate product websites to deceive innocent Internet users into submitting their financial credentials while ordering fake products (Longe et al., 2005). Thus, many cybercafés have been sealed off by security agencies due to the perpetration of cybercrimes, e.g., spamming, credit card fraud, ATM frauds, phishing, and identity theft using that café network (Olumide and Victor, 2010; Augustine, 2010). Currently, there is a lack of standardized up-to-date cybersecurity guidelines on the establishment and operations of cybercafé. Some cybercafés were shut down due to a lack of patronage by people scared of scammed, hacking, or virus attacks.

The main purpose of this study was to investigate and assess the level of cybersecurity threats and practices awareness among students of universities, polytechnics, and colleges of education in Sokoto, Kaduna and Kano.

III. RESEARCH METHODOLOGY

In this paper a descriptive research method was adopted to explore students' awareness of cybersecurity from three selected universities, polytechnics, and colleges of education in Sokoto, Kano, and Kaduna. A questionnaire was administered directly to the students at their respective schools. Only students of computer science departments were studied. The questionnaire comprises of demographics data, multiple-choice questions focussing on passwords strength, computer protection/ internet safety, virus/cyber-attacks, social media use/threats to privacy of students in higher institutions in Nigeria. Questions about frequency of Internet use, safety practices, and management of the risks to cybersecurity at schools were asked as well. The sample of 100 students was drawn from the three selected universities, polytechnics, and colleges of education in Sokoto, Kano, and Kaduna. A total of 900 responses were returned at the end of the survey. The data collected was analyzed using SPSS v17 software.

IV. RESULTS

During the data collection 110 questionnaire were distributed to 8 out of nine institutions selected to this study. Data was not collected at Sokoto state university because the students were on vacation at the time of data collection. The 8 tertiary institutions covered in this study are ABU, BUK, KDPOLY, KNPOLY, SOPOLY, KDCOE, KNCOE, and SSCOE. Out of the 880 questionnaires distributed only 22 were not returned which is 2.5% failure rate. After the data screening, 58 questionnaires were dropped due to lack of completeness, improper filling, and lack of Internet experience. A total of 800 responses were found usable and therefore used for the study data analysis. Thus, 800 responses was considered sufficient to meet the minimum sample size requirement for conducting simple statistical analyses (Gefen et al., 2000; Kim, Oh, Shin and Chae, 2009).

4.1 Demographic Data

The Table 1 presents the results of the respondent's demographic factors which indicates that there were more male (54.1%) respondents than female (45.9%) from the eight institutions surveyed. Out of the 800 respondents 243 are between the age of 15-20, 394 are aged 21-25, 130 are aged 26-30, whereas only 33 are aged 31 and above. Moreover, the number of the respondent’s type of institution is proportionately equal. Majority of the respondents (53.5%) says they have been using Internet for five years and above. The time spent by majority of the respondents (59.3%) using Internet is from 30 minutes and above. Most of the respondents are regular users (449/56.1%) of Internet in addition to 207 (25.9%) that always online. About 642 (80.8%) of the respondents uses smartphones to browse, only 44 (5.5%) uses Desktop computer to browse the Internet. This is clear indication of Desktop computers lack of popularity and about to be faced out 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%.

Table 1: Respondents’ demographic profile

Demographic		N	%
Gender	Male Female	433 367	54.1 45.9
Age	15 – 20 21 – 25 26 – 30 31 above	243 394 130 33	30.4 49.3 16.3 4.1
Type of Institution	University Polytechnic College of Education	201 299 300	25.1 37.4 37.5
How long have you been using Internet?	1 – 2 years 3 – 4 years 5 + years	184 188 428	23.0 23.5 53.5
How many minutes do you spend online browsing?	1–10 minute 11–20 minute 21–30 minute	74 114 138	9.3 14.3 17.3

	31+ minutes	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 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

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

Table 2: Password Strength

Please indicate the extent to which you do the following	Never	Once	Rarely	Regularly	Always
• Periodical change of password	246	161	179	152	62
• Reusing previous passwords	248	181	114	135	122
• Using the same password for each of your accounts	295	129	99	119	158
• Sharing password with Someone	518	81	92	55	54
• Saving your password on your browser	326	107	98	109	160
• 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	172	167	117	126	218
• 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

In terms of computer protection majority of the students indicated high level of awareness especially by locking their computers when they are away. Password protection of 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 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
• 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	148	128	109	210
• Do you remove personal, confidential or sensitive data before giving your computer to be repaired or replaced?	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 says they do open and reply to emails from unknown sources. About 166 says they never re-install 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 high degree of awareness about virus attacks especially when downloading online contents.

Table 4: Virus Attacks

Please indicate the extent to which you 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?	166	159	181	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	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 to identity theft. It has become part of every student's life. This study intend to know the amount of private information students revealed on their respective social media accounts. Table 5 shows that on average majority of the never published their career achievements, identity such as name, home address, phone number etc. 147 students says they always accept friend request from unknown persons. 231 out of 800 says they never reveal their location on social media as indication of security consciousness. According to Senthilkumar and Sathishkumar (2017) accepting unknown persons in social network is considered to be the major threat in social network compared to any other identity outsourcing. Followed by updating locations every time where ever they go is second major personal data of a person published in social networks. Compared to these two, career details and having original display picture has very less impact on publishing.

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	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 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

V. CONCLUSION

Globally, cybercrimes has become a pandemic to national security in many nations. Internet users continuously to visit the websites which is already infected with viruses, replying phishing e-mails, storing logging information in an third party location, or even sharing confidential information over the phone, exposing personal information to social networking are tend to steal personal information of common people. This survey result shows that the tertiary institution students in Nigeria are having considerable level of cybersecurity awareness and threat issues. That is good enough to assist them in protecting themselves and their computers from hackers and hence the awareness has to be created in higher level.

Cybercrime activities need to be checked and quickly addressed as they can affect the privacy of students and the general public. Addressing cybercrime attacks requires involvement of many stakeholders – the users, operators, internet service providers, cybersecurity agencies, and the government. Further measures shall be put in place to enhance preparedness for handling risks of computer crimes among the general public. The availability and price of antivirus and other software meant to enhance the preparedness levels should be made accessible. This way, it will be easier for the general public members to prepare adequately to deal with threats of computer crimes. Educating the general public on how they should safeguard their information when going online should also be undertaken regularly. It would be essential to carry out group discussions with the internet managers and end-users to determine the extent of awareness and preparedness about computer crimes; this is rather than relying only on the self-administered questionnaire to assess the level of understanding and preparedness. This way, issues that are likely to be confusing are sorted out and clarified in data collection.

REFERENCES

[1]. Adebusuyi, A. (2008): The Internet and Emergence of Yahoo boys sub-Culture in Nigeria, International Journal of Cyber Criminology

[2]. 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.

[3]. 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).

[4]. 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

[5]. Augustine C. Odinma, MIEEE (2010): Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, Nov 1-2.

[6]. 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.

[7]. 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.

[8]. Frank, I. and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in science, engineering, & education (IJCRSEE), 1 (1).

[9]. Geoff, H., Anthony, P., Gopalakrishnan, S. and Manav, M. (2005). Trends in Spam Products and Methods. Conference on e-mail and Antispam. Available online at www.ceas.org

[10]. 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

[11]. Longe O. B & Longe F. A (2005): The Nigerian Web Content: Combating the Pornographic Malaise Using Content Filters. Journal of Information Technology Impact, Vol. 5, No. 2, pp. 5964.

[12]. Longe, O, Omoruyi, I & Longe, F (2005): Implications of the Nigeria Copyright Law for Software Protection. The Nigerian Academic Forum Multidisciplinary Journal. Vol. 5, No. 1. pp 7-10.

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

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

[15]. Olumide, O. O. and Victor, F. B. (2010): E-Crime in Nigeria: Trends, Tricks, and Treatment. The Pacific Journal of Science and Technology, Vol. 11 (1), May 2010 (spring).

[16]. 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/

[17]. 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.

[18]. 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,

[19]. 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.