Cyberspace Activities Awareness and Security Strategies in Tertiary Institutions in Nigeria

NJOKU D. O.[1], NWOKORIE. E. C.[2], OKOLIE. S. A.[3], ODII. J. N.[4]
[1, 2, 3, 4]*Department of Computer Science, Federal University of Technology, Owerri*

Abstract- This study attempts to examine the activity, awareness and measures being adopted by staff and students in tertiary institutions to overcome the cyber security challenges. A total of one hundred and twenty (120) staff and students were sampled from three different tertiary institutions in Owerri-Imo State, Nigeria using random sampling technique. A structured questionnaire was used as data collecting instrument. The views representing the opinions of the respondents were sought on issues on cyber space activity, security awareness and strategy adopted by staff and students. With respect to activity on cyberspace, there is a variation of engagement by respondents. On the cyberspace activities engaged, majority of the respondents, 82% of the population claimed that they involve in Google search. When asked about their awareness to certain educational cybercrimes, majority, 89%, claimed to be aware of spamming. Most of the staff and students sampled on security awareness responded that they are familiar with some threats used to steal and leak their information and identity. However, all of the biggest cybercrimes the education sector are battling recently like phishing, ransomware and DDoS which have been used to attack schools on a regular basis are not that popular among the staff and students. A very important revelation from this study was that issues related to cybercrime are not being reported to law enforcement agents by staff and students of tertiary institutions. This poses great danger to the fight against cybercrime. All the users of Information Technology (IT) facilities in tertiary institutions should be educated on the risk of cyber-attacks and how to manage it. This includes reporting to law enforcement agency. It is recommended that the government and the authorities of tertiary institutions in Nigeria introduced cyber security law as part of the courses to be taken. The network users should be made to know their roles and responsibilities in ensuring a safe and efficient cyber pace.

Indexed Terms- Cybercrime, Cyber Security, Cyber Space, Information Technology, Tertiary Institution

I. INTRODUCTION

Over the past decades, innovations in mobile phones and computers technology have changed the concept of cyberspace activities. This has also brought about the emergence of different cybercrimes due to lack of security. In order to keep personal and professional information safe from attacks, various means have been devised by stakeholders in Information Technology (IT) to provide security for themselves and their private documents. Cyber security plays a substantial role in the current growth of IT services. Cyber security has been described in [1] as an attempt by users to keep personal and professional information unharmed from the attacks on the internet. Protecting networks, computers, programmes from unauthorized access and loss is the foremost function of cyber security application.

Information Technology (IT) has made education more innovative. In this modern age, technology and education are interconnected. Modern technology is being deployed in educational institutions across the globe to provide effective teaching and learning and facilitate innovative research and collaboration among institutions. It is even common these days to see advanced technology being used at primary education level for academic purpose. Upgrade in technology, no doubt, will offer limitless benefits and boost and upgrades the procedures of education [2].

The use of IT facilities increases efficiency and productivity, and makes educational tasks easier. Nevertheless, it suffers from a number of threats to its reliability and integrity. This is mostly viewed from the threats to the privacy of individuals or corporate institutions regarding the security of their information, which has been on increase over the years. The threat of cyber security is increasing daily basis and it is adversely impacting on user of IT facilities in the society. Concerning research, educational institutions are increasingly being targeted by cybercriminals. A cybercriminal, internal or external, to an institution, can gain unauthorized access (hack) into the cyber system or database of an institution to obtain sensitive, confidential information or private through social engineering tactics [2]. An unsuspecting user within an institution can as well be hacked by cybercrime actor and leak private information.

In Nigeria, a good number of users are unaware of the risks posed by using unprotected or unsecured cyberspace. This is also true of educational institutions in Nigeria whose websites and database are often attacked by cybercriminals to alter the results of students, change admission status, leak private information and carry out other mischievous actions. Hence, educational institutions in Nigeria should take the actions that will help to protect themselves from any form of cyber threats from within or outside.

It has been reported that educational institutions are now regularly being targeted by cybercriminals. In respect to this, Biddle [3] reported that data breaches amounting to 13% in the first half of 2017 were accounted for by the education sector. This the report stated resulted to the compromise of about 32 million records. In fact, it can be said that one of the main reason for the increasing cyber-attacks on tertiary institutions is because of the varied data on their database. The diverse data stored by the tertiary educational institutions in Nigeria include: information of staff and students, information on healthcare, and information on finance. These stolen records could be sold on the dark web were it would be used for identity theft and fraud [3].

The increasing demands for increased IT capabilities from students and staff as well as contending with frequent attacks by cybercriminals, calls for educational institutions to be more proactive and prepared to balance the provision of access points to staff and students while defending against influx of endpoints from cybercrime on their networks. Hence, there is growing number of devices and applications linking to educational institution’s network per user. This situation has given rise to increasing attack surface.

In this paper, the issue of cyber space and security awareness in tertiary institutions in Nigeria is examined. The objective is to examine the activities, awareness and measures being adopted by stakeholders in tertiary institutions to overcome the cyber security challenges. The remaining part of this paper is divided into four (4), which include review of issues of cyber security, methodology, findings and discussion, and conclusion and recommendations.

II. REVIEW OF PREVIOUS LITERATURE

In this section, the works done by previous authors with respect to issues bordering on cybercrime and cyber security are examined.

In the study of Das and Patel [1], the issues, challenges and solutions to cyber security for social networking sites (SNS) were highlighted. While stressing the initiatives of government to eradicate serious issues on cyber security, it recommended appropriate ways individuals and government could adopt in collaboration with private sector to achieve a safe cyber-space.

Makeri [4] studied cyber security issues in Nigeria and challenges. The author makes effort to provide an overview of cybercrime and cyber security. The definition of the concept of cybercrime, identification of motives behind cybercrime and ways to get rid of it were established. The author further looked at the action of cyber criminals and the motive for their involvement. Methods to protect users from the activities of cybercriminals and to checkmate them were emphasized.

Omodunbi et al [5] examined the most common cybercrimes in the various sectors of the Nigerian economy. An analysis of cybercrimes in tertiary institutions in Ekiti State indicated majority of the crimes were carried out by the youth. The authors then highlighted certain measures to detect and prevent the cybercrimes in Nigeria.

Ibikunle and Eweniyi [6] presented approach to cyber security in Nigeria with the attendant challenges and the way forward. The concept of cybercrime and cyber security was highlighted. The motive behind cybercrime and involvement was looked. The authors then provided practical and logical techniques for overcoming cyber threats were established.

Kshetri [7] looked at cybercrime and cyber security in Africa. The author stated that cybercrimes within and outside Africa economies are on the increase, but there has been progress recorded in the continent to check the activities of cyber attackers especially the use of cyber security legislation and enforcement measures. The author then recommended that since cyber-attacks in developing economies such as the ones in Africa are geared towards targeting specific industry sectors, research should focus on various economic sectors so as to compare and contrast the sector facing high profile of cybercrimes.

Oforji et al [8] examined cyber security and its associated challenges in Nigeria with recommendations on the way to tackle the menace of cybercrime. In a similar work by Uwadia and Eti [9], the authors maintained that increasing unemployment has resulted proliferating cases of cybercrime in Nigeria. Nevertheless, a bill has been passed by the legislative organ of government to address issues of cybercrime.

Osho et al [10] presented a qualitative analysis of cyber security policy and strategy in Nigeria. The authors analyzed the documents of Nigerian National Cyber Security Policy and Strategy in terms of selected harmonized strategy developmental frameworks and also carried out comparative evaluation of related documents from other selected nations. The authors stated that the finding from the analysis revealed that the document met majority of the expectations in terms of content, however, it did not mention some of the items of concern that affects cyber security in various sectors of Nigerian economy.

Dambo et al [11] in their study on cyber space technology stated that due to the serious threat posed by cybercrime activities, cyber security has become an issue of national concern in Nigeria. The authors argued that despite the fact modern computers and mobile phones technology come with built-in firewall security software, the computers are still not hundred percent accurate and reliable to secure users information.

Ibrahim [12] maintained that three possible factors are responsible for cybercrimes in Nigeria. The author highlighted socioeconomic, psychosocial and geopolitical as the three factors. These factors, the author stated, challenged the statistical data used to making submission regarding cybercrime actions throughout Nigeria. The study provided new approach to establishing the reason for the large variances of cybercrime so as to provide a more obvious definition of cybercrime in Nigeria and other countries. This, the author, argued that the culture of domain and nuances has the same effect for online as they do offline.

In a research designed and administered with the aim of testing the impact of cybercrime on users in Palestine, Amro [13] stated that the study revealed that majority of the cybercrimes were largely based on hacking of victims on social networks.

Odo and Odo [14] investigated the extent of involvement in cybercrimes among students of tertiary institutions in Enugu state of Nigeria employing cross sectional survey design. The findings revealed that the involvement of students in cybercrime depends on gender and type of institution. The authors maintained that from the finding that the involvement of students in cybercrime would adversely affect educational value as well as setback in the economy of the state.

Hassan et al [15] identified urbanization, unemployment and poor enactment of cybercrime legislation as some of the causes of cybercrimes in Nigeria. The authors suggested that individuals or corporate institutions should take appropriate steps to protect their IT infrastructure; while the government should ensure strict enforcement of cybercrime laws.

Okeshola and Adeta [16] examined the nature, causes and implication of cybercrime in Nigerian tertiary institution considering Zaria in Kaduna state. In the study, the authors argued that due to harsh economic condition and the fact that people who are without economic success are not valued, the pressure to become financially successful has compelled individuals to involve in various forms of cybercrimes in Nigeria.

The literature reviewed so far indicated that there is still a gap to be covered in cybercrime issues in Nigeria, notwithstanding the appreciable work done already. Majority of the literature have concentrated on general issues of cyber security in various sectors. This study however, seeks to examine the knowledge (in terms of cyberspace engagement and awareness) of stakeholders in tertiary institutions in Nigeria.

III. METHODOLOGY

This study uses structured questionnaire as data collection instrument. In order to narrow down the investigation, three prominent tertiary institutions in Owerri were considered for drawing respondents.

A. Survey Location

Owerri is the capital of Imo state in Nigeria. Owerri is well known for having high level of literate inhabitants. Majority of the people living in Owerri are civil servants, though mixed up with reasonable number of business men/women and sizeable number of farmers. Owerri is located at latitude 5.4836302 and longitude 7.0332499, in the northern hemisphere [17]. It has an elevation of 71 m (LatLong.net) There are five (5) five famous tertiary institutions in Owerri. However, three (3) institutions have been randomly selected to carry out this study. The selected tertiary institutions are: Imo State University (IMSU), Federal Polytechnic, Nekede (FEDPONEK) and Federal University of Technology Owerri (FUTO). The purpose of selecting these institutions was based on their popularity as institutions of first choice for students who seek admission within and outside the Owerri city.

B. Research Population and Sampling

The population of the study was divided into three (3) groups. These groups were drawn from:

a) Students within the selected tertiary education institutions.
b) Non-academic staff
c) Lecturers of the selected tertiary institutions, who either in computer science department or computer/electrical and electronic engineering Department.

A total of 120 people were sampled using random sampling technique, administered questionnaires and then grouped into three (3). The age of each respondent is either 18 or above. The probability sampling technique used was simple random sampling (SRS).The data obtained was evaluated and analyzed using descriptive statistical approach (using frequency tables and charts). Table 1 shows the way the questionnaires were distributed to the participants from the selected tertiary institutions.

Table 1 Order of distributing questionnaires

Institution	Students	Non-Academic staff	Lecturers
IMSU	25	10	5
FEDPONEK	20	10	10
FUTO	25	10	5
Total	70	30	20

Most of the distributed questionnaires were given to the students because from the literature survey carried out, it was observed that majority of the people who engage in cybercrimes are youths which match with the category of students. The respondents were further divided into

IV. FINDINGS AND DISCUSSION

A. Findings

Demographics of Respondents: This is analyzed using two separate pie charts in Fig.1 and 2 to represent the responses of the various respondents in terms of their demography.

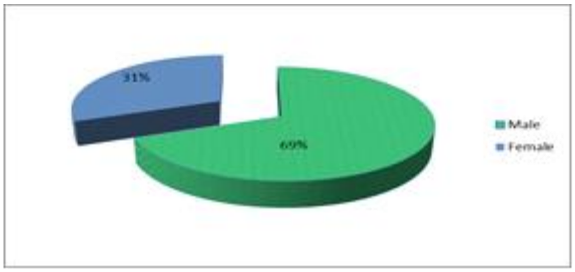

Fig. 1 Gender distribution

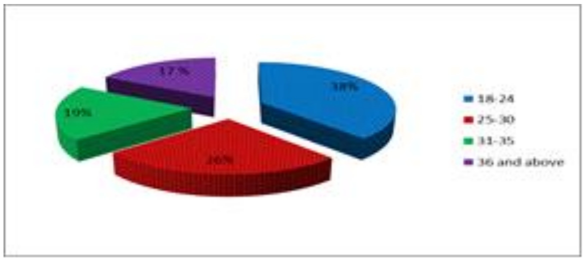

Fig. 2 Age distribution

Activity engaged-in on the Internet: In this case, the study attempts to examine and identify the nature of things the respondents access while on cyberspace. Their views were sought on what they do online by responding Yes or No as shown in Fig. 3

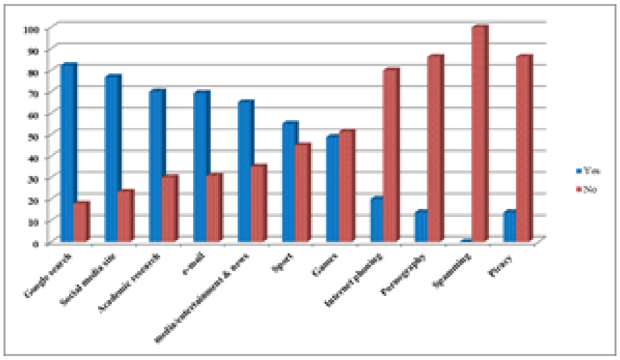

Fig. 3 Activity engagement on the internet

Cybercrime awareness: The response representing the opinions of the participants is shown in Fig.4

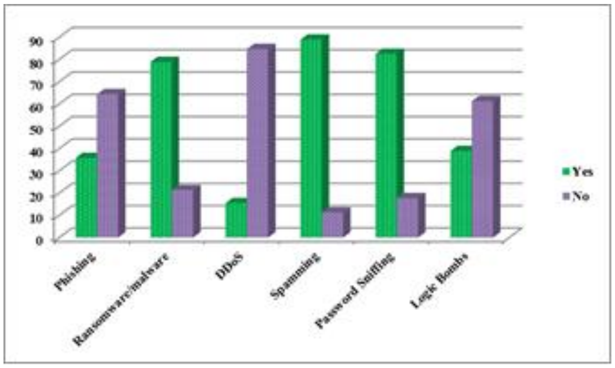

Fig. 4 Cybercrime awareness among staff and students

Security measures: The response of the of the participants on the measures they take in ensuring that they are protected from cyber-attacks on their mobile phones or computers is presented in Fig. 5.

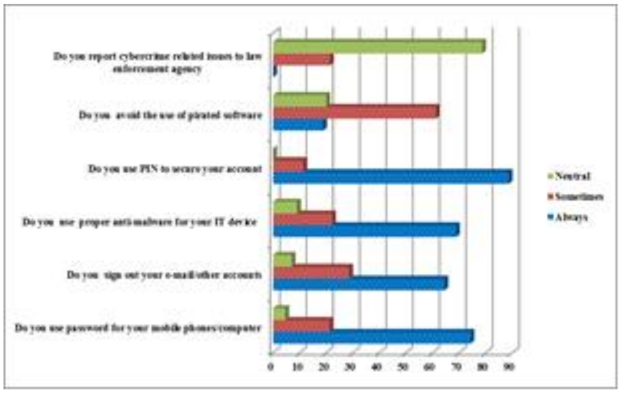

Fig. 5 Response on the extend of protection used

B. Discussion

The two Figures (Fig. 1 and 2) represent the respondents' gender and age. The responses on gender reveal that male respondents represent 69% (83) of the population while the females account for 31% (37). The male respondents outnumbered the females because of the females where met to participate showed indifferent about the issue. On the other hand, the age distribution shows that the respondents (38%) are between 18 to 24 years, this is followed by those between 25 to 30 years (26%) and 31 to 35 years (19%), while those between 36 years and above (17%) represents the least set of respondents.

In Fig. 3, the responses to the cyberspace activities the respondents engage in are presented. From the findings, it is seen that majority of the respondents engage in Google search activity (82%), social media site (77%), academic research (70%), e-mail (69%), media/entertainment and news (65%) and sport (55%). Alternatively, only a small number of the respondents engage pornography (14%) and piracy (14%). However, none of the respondents admitted of being involved in spamming. The low affirmation to pornography and piracy engagements as well as the nil acceptance of spamming can be attributed to the sensitivity of such activities on the internet.

Fig. 4 shows the findings on the views of the respondents in terms of their awareness to certain educational cybercrimes. The Figure shows that majority of the respondents are only aware of spamming (89%), password sniffing (82%) and ransomware/malware (79%). While less than average number of the population admitted to be conversant with plagiarism (45%), logic bombs (39%), and phishing (36%), only few are familiar with distributed denial of service (DDoS) attacks (15%). The fact that most of the respondents are not conversant with cybercrimes like plagiarism, phishing and DDoS is not impressive. For instance, it is reported in (business and technology) that among the biggest cybercrimes the education sector are battling are phishing, ransomware and DDoS which have been used to attack schools on a regular basis in recent times. These cyber-attack strategies pose serious cyber security issues to tertiary institutions because they are used to leak personal information, to carry out data extortion for money, or render institutions incapacitated. However, the fact that less than average number of the respondents are aware of plagiarism can be attributed to the fact that majority of the participants are people between 18 to 24 years who are probably undergraduates.

The responses of the security strategy the respondents adopt or are familiar with are presented in Fig.5. Majority of the respondents said they always use Personal Identification Number (PIN) to protect their account (89%), password for their mobile phones/computers (74%), proper anti-malware for their computer (69%), and sign out their e-mail/other accounts. However few population of the respondents said they always avoid the use of pirated software (19%) while none of the respondents affirmed to have always reported issues of cybercrime to law enforcement agency. The finding shows that more than average number of the population said they sometimes avoid the use of pirated software (61%), while on reporting related cybercrime related issues to law enforcement agency 21.4 % said they sometimes do that with majority (79%) being neutral. This can be attributed to the lack of trust on the law enforcement agency or lack of awareness/knowledge on the parts of the respondents on the extant law on cybercrimes and the role of law enforcement agency.

V. CONCLUSION AND RECOMMENDATIONS

This study reveals that most of the respondents actually engage themselves with certain activities on cyber space. The study also shows that most of the staff and students are conversant with some of the malicious attack targeted on educational institutions' cyber network. On the security strategy use to protect themselves from cybercriminals, most of them admitted to have always used a certain technique to overcome cyber threat. However, most of the respondents still use pirated software without their knowing that this can expose them and their IT devices to potential cybercriminals. The reporting of cyber security issues was not a common practice among respondents in tertiary institutions. Only few said they sometimes report cybercrime related issues to appropriate authority, while most of them were neutral. The study has attempted to examine the cyber space engagement and security awareness in tertiary institutions in Nigeria. The proper knowledge of the appropriate security measures around cyber space will help users of IT facilities in tertiary institutions in Nigeria to make inform decisions on how to keep themselves safe from cyber-attacks. A very important revelation from this study is that issues related to cybercrime are not being reported to law enforcement agents by staff and students of tertiary institutions. This poses great danger to the fight against cybercrime. All the users of IT facilities in tertiary institutions should be educated on the risk of cyber-attacks and how to manage it. This includes reporting to law enforcement agency. It is recommended that the government and the authorities of tertiary institutions in Nigeria introduced cyber security law as part of the courses to be taken. The network users should be made to know their roles and responsibilities in ensuring a safe and efficient cyber pace. Tertiary institutions in Nigeria should also endeavour to organize departmental or faculty workshops and seminars as often as possible to enlighten stakeholders on most recent tactics used by cybercriminals to steal information from unsuspecting user and other cyber malicious attacks on IT networks.

REFERENCES

[1] R. Das, and M. Patel (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 5, No. 4,833-838.

[2] Admin (2018). Education and Cyber Security: Challenges and Opportunities. The KnowledgeReview.http://theknowledgereview.com/education-cyber-security-challenges-opportunities/# (Sourced: 1/7/2019)

[3] S. Biddle (2017). Three of the Biggest Cyber Security Challenges Facing the Education Sector. Business and Technology.https:///www.fortinet.com/blog/business-and-technology (Sourced: 1/7/2019)

[4] Y. A. Makeri (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 7, No.4, 315-321.

[5] B. A. Omodunbi, P. O. Odiase, O. M Olaniyan and A. O. Esan (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, Vol. 1, No. 1, 37-42.

[6] F. Ibikunle, and O. Eweniyi (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in science, engineering and education, Vol.1, No.1.

[7] N. Kshetri (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, Vol. 22, No. 2, 77–81.

[8] J. C. Oforji, E. J. Udensi, and K. C. Ibegbu (2017). Cybersecurity Challenges in Nigeria: The Way Forward. SosPoly Journal of Science and Agriculture, Vol. 2, 1-5.

[9] F. Uwadia and F. I. Eti (2018). Cyber Security in Nigeria: Issues, Challenges and Way Forward. International Research Journal of Advanced Engineering and Science, Volume 3, Issue 2, pp. 351-354.

[10] O. Osho, and A. D. Onoja (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, Vol. 9, No. 1, 120–143

[11] I. Dambo, O. A. Ezimora and M. Nwanyanwu (2017). Cyber Space Technology: Cyber Crime,Cyber Security and Models of Cyber Solution, A Case Study of Nigeria. International Journal of Computer Science and Mobile Computing, Vol. 6, No. 11, 94-113

[12] S. Ibrahim (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44-57.

[13] B. Amro (2018). Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals. I.J. Wireless and Microwave Technologies, 5, 19-26

[14] C. R. Odo , and A. I. Odo (2015). The Extent of Involvement in Cybercrime Activities among Students' in Tertiary Institutions in Enugu State of Nigeria. Global Journal of Computer Science and Technology: H Information & Technology, Vol. 15, No. 3, 1-6.

[15] A. B. Hassan, F. D. Lass, J. Makinde (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology, Vol. 2, No. 7, 626-631

[16] F. B. Okeshola, and A. K. Adeta (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, Vol. 3 No. 9, 98-114.

[17] Geographic Coordinate of Owerri, Imo, Nigeria. https://www.geodatos.net/en/coordinates/nigeria/imo/owerri, (Sourced: 1/7/2019).