SMCC Business Administration Journal
ISSN Print: 2508-0512 · ISSN Online: 2508-0520
Volume 1 · June 2019
DOI:

Awareness and Impact of Cybercrime Among Selected University Undergraduates in Nigeria

MUTAHIR OLUWAFEMI ABANIKANNDA
http://orcid.org/0000-0001-5599-9577
mo.abanikannda@uniosun.edu.ng
Osun State University, Osun State, Nigeria.

Gunning Fog Index: 13.59 • Originality: 99% • Grammar Check 99%
Flesch Reading Ease: 38.71 • Plagiarism: 1%

ABSTRACT

This study examined the awareness and impact of cybercrime among selected university undergraduates in Osun state, Nigeria. A descriptive research of the survey type was adopted, 250 undergraduates who were randomly selected across five universities across the state. A validated and reliable questionnaire was used as an instrument. Data collected were analysed using frequency count of responses, simple percentages and relative importance index. Findings indicated that undergraduates are aware of the identities of cyber criminals based on the activities they engage in and a large percentage of the population of university undergraduates in Osun state are involved in cybercrime. The findings further revealed some well-known cybercrimes as well as the negative impacts of cybercrime on university undergraduates. The study concluded Undergraduates across universities have turned cybercrime into a way of living. Resulting from this study, it is clear that undergraduates in Nigeria's universities are becoming deeply involved in acts of cybercrime and some of them don't even know the gravity of the offenses they are committing even though some do. It was recommended that Students in tertiary institutions should also abstain from any illegal or criminal acts while using the internet not to become criminals without even knowing

KEYWORDS

Cybercrime, cyber insecurity, descriptive statistics, frequency count, Undergraduates, Nigeria

INTRODUCTION

Crime and criminality have been associated with man since his fall (Kamini, 2011). Crime remains elusive, ever striving to hide in the face of the development. Different nations have adopted different strategies to contend with a crime depending on their nature and extent. Certainly, a nation with a high incidence of crime cannot grow or develop as crime is conversely associated with development.

Singh, Gupta & Kumar† (2016) gave a generalized definition of cybercrime as comprising of unlawful acts wherein the computer is either a tool or target or both. Cybercrime has been used to describe a wide range of offenses, including offenses against computer data and systems such as hacking, computer-related forgery and fraud such as phishing, content offenses such as disseminating child pornography and copyright offenses such as the disseminating of pirated content (Okanlawon, Yusuf, & Abanikannda, 2015).

Cybercrime is any activity involving computers and networks. A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. This ranges from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime is not only limited to, anything from downloading illegal music files to stealing millions of dollars from online bank accounts, but also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the internet (Boniface & Michael, 2014).

The world of the internet today has become a parallel form of life living. The public are now capable of doing things which were not imaginable for years ago. The internet is fast becoming a way of life for millions of people and a way of living because of growing dependence and reliance of mankind on these machines. Internet has enabled the use of website communication, email and a lot of anything anywhere, it offers solutions for the betterment of humankind (Kamini, 2011). The internet creates unlimited opportunities for commercial, social and educational activities. Jide (2007) has however cautioned on the peculiar risks introduced by the net such as cybercrime. From business, industry, government to non-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, credit card frauds, spamming, phishing, ATM

frauds, identity theft and a blossoming haven for cybercriminal miscreants to perpetuate their insidious acts (Frank & Odunayo, 2013).

A cybercriminal is a person who commits a crime using the computer as a tool. A cybercriminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cybercrime (Singh, Gupta, & Kumarǂ, 2016). The population of online users makes it easy to target their victims without being physically present. This makes it quite difficult for law enforcement agents to trail cybercriminals online.

The first recorded cybercrime took place in the year 1820. It is noteworthy that the abacus, which is thought to be the earliest form of a computer has been around since 3500 BC, in India, Japan, and China. The era of modern computer, however, began with the analytical engine of Charles Babbage. In the year 1820, the loom was produced by Joseph Marie Jacquard, a textile manufacturer in France. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened.

Consequently, they committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cybercrime. The cyber criminals in this context were Jacquard's employees. Jackson & Robert (2016) noted that the prevalence of cybercrime in Nigeria is worrisome not only for the citizens of the country but the government as the image of the country is tarnished as a result of this menace. It is also part of the reasons, for the avoidance of Nigeria and Nigerians by foreign investors. Sesan, Soremi, & Bankole (2013) stated very clearly that, the Nigerian cyberspace has become an open arena for thieves and likes to display their various abilities by playing tricks using the computer system and network. Due to lack of adequate security on the internet, thieves and fraudsters have made Nigeria cyberspace their area of operation. Sesan (2010) in a crime report listed Nigeria third in terms of online crime activity and the prevalence of cybercrime among a sizeable number of young Nigerians.

Global tracking of cyber-attacks indicates that Nigeria is among countries with high cases of software piracy, intellectual property theft and malware attacks. This situation is a serious challenge to our resolve to take advantage of the enormous opportunities that the internet brings while balancing and managing its associated risks (Ewepu, 2016).

Owing to all aforementioned reasons, Nigeria's image has sunk so much over the years and this has adversely affected the integrity and good name of Nigerians all over the world. Even though a global phenomenon, Nigeria's situation regarding cybercrime has been one of the worst in the world. Nowadays in Nigeria, the menace of the so-called 'yahooboyism' as titled by (Adeniran, 2011), in which a category of young individuals referred to as 'yahooboys' commit an overwhelming majority of the cybercrimes in Nigeria. These yahooboys so called, live large without any hint of how tough it is to be successful or rich in a country like Nigeria. Some of them even spend money lavishly, in a way rich people don't normally do. The common source of this kind of undeserved wealth is through various illegal means which includes cybercrime mainly.

OBJECTIVES OF THE STUDY

The purposes of this research are to:

1. Examine the various activities of cybercriminals;
2. Determine the popularity of cybercrime among university undergraduates in Osun state; and
3. Access the impact of cybercrime on university undergraduates in Osun state.

METHODOLOGY

Research Design

This is investigative research which adopted a descriptive survey method. The researcher made use of questionnaires as the research instrument. The researcher made use of research questionnaires to find answers to the research questions of this study. Due to the large population involved, the researcher picked samples from the total population. The researcher distributed the questionnaires containing the research questions to the sample which have been used to represent the population.

Sample and Sampling Techniques

The sample size of this study comprised of 250 undergraduates. The sample respondents were selected using simple random sampling method. This method is one in which the respondents were selected randomly.

Research Instrument

The researcher made use of primary sources to collect data in this study. This study adopted a survey research method. Copies of questionnaires were used to collect primary data which formed the major instrument for the study. The questionnaire was designed with multiple options with some items drawn based on the 4-point Likert scale of Strong Agree, Agree, Disagree and Strongly Disagree. A questionnaire designed for the respondents in the selected institution consist of three sections namely Sections A, B, and C.

Validation Research Instrument.

The draft copy of the questionnaire has been shown to experts in measurement and evaluation in two universities, as well as a specialist in cyber technology all of whom pointed out necessary corrections which were effected to correlate with the purpose of the study before distribution to respondents. Both the face and content validity of the research instrument were thus assured.

Reliability of Research Instrument

A pilot study was conducted on a population that was not part of this study to test the reliability of the instrument. To determine whether the instruments were reliable or

not, the result of data collected from the pilot study was subjected to Cronbach's Alpha reliability test. The Cronbach reliability index of the instrument was found to be 0.78. Since this reliability coefficient was high and above 0.5, the instrument was adjudged good for the purpose for which it was constructed.

Method of Data Analysis

The data collected, through the questionnaires distributed were analysed using a statistical method of frequency count of responses, simple percentages and relative importance index.

RESULTS AND DISCUSSION

Table 1: Cyber Criminals Engaged Activities

S/N	Items	SA	A	D	SD	NR	RII	P (%)	Ranking
1.	A cybercriminal is someone who commits cybercrime.	190	48	4	3	5	0.92	92	1st
2.	A cybercriminal can be a teenager or an adult.	82	155	9	4	0	0.82	82	6th
3.	A cybercriminal can be a student, a lecturer, a civil servant, a military man or self-employed.	155	73	19	1	2	0.88	88	2nd
4.	A cybercriminal is anyone who damages any part of a computer with bad intention.	78	83	64	25	0	0.71	71	10th
5.	A cybercriminal is someone who steals any part of a computer.	109	72	50	19	0	0.77	77	9th
6.	A cybercriminal is anyone who commits forgery using the computer as a tool.	114	107	26	3	0	0.83	83	4th
7.	A cybercriminal is anyone who hacks into other people's computer.	118	104	25	2	1	0.84	84	3rd
8.	A cybercriminal is anyone who commits fraud using the computer as a tool.	118	96	35	1	0	0.83	83	4th
9.	A cybercriminal is anyone who uses the computer to commit piracy.	84	121	38	6	1	0.78	78	8th
10.	A cybercriminal is anyone who uses the computer to bully people.	89	112	47	1	1	0.79	79	7th

Table 1 shows the activities engaged by cybercriminals. The activities are as follow: committing cybercrime by 92%, can be a student, a lecturer, a civil servant, a military man or self employed by 88% followed by hacking other people's computer by 84%, committing fraud using the computer as a tool by 83% and committing forgery using the computer as a tool by 83%, can be a teenager or an adult by 82%, usage of computer to bully people by 79%, usage of the computer to commit piracy by 78%, stealing of any part of a computer by 77% and damaging of any part of computer with bad intention by 71%.

Table 2: How popular Cybercrime among undergraduates of universities in Osun state

S/N	Items	SA	A	D	SD	NR	RII	P (%)	Ranking
1.	Undergraduates are aware that some activities they carry out on the internet or with the computer are crimes.	143	76	19	10	2	0.85	85	2nd
2.	Some undergraduates use the computer to commit cybercrime knowingly.	85	147	17	0	1	0.82	82	3rd
3.	Some undergraduates are involved in online fraud.	145	80	22	1	2	0.87	87	1st
4.	Some undergraduates are involved in online gambling.	97	100	47	3	3	0.79	79	5th
5.	Many undergraduates are involved in yahooboyism.	109	100	33	2	6	0.80	80	4th
6.	Many undergraduates commit plagiarism of online articles.	94	107	45	2	2	0.79	79	5th
7.	Many undergraduates forge documents and certificates using the computer as a tool.	102	108	30	1	9	0.79	79	5th

Table 2 shows how popular cybercrime was among undergraduates of universities in Osun state undergraduates. These are well known cybercrime among undergraduates of universities in Osun state undergraduates: online fraud 87%, awareness of internet crime by 85%, committing cybercrime knowingly by 82%, yahooboyism by 80%, online gambling, plagiarism of online articles and the use of computer in forging of documents and certificates by 79%.

Table 3: Impacts of Cybercrime on undergraduates of universities in Osun state

S/N	Items	SA	A	D	SD	NR	RII	P (%)	Ranking
1.	Undergraduates who are involved in cybercrime become criminally oriented.	118	82	35	14	1	0.80	80	1st
2.	Some undergraduates become victims of cyber bullying by other undergraduates.	50	151	40	8	1	0.74	74	4th
3.	Undergraduates who are caught in the act of cybercrime are punished according to the law.	87	92	57	13	1	0.75	75	3rd
4.	Some undergraduates abandon their studies to get fully involved in cybercrime.	100	91	42	15	1	0.77	77	2nd

The Table 3 above shows the impacts of cybercrime on undergraduates of universities in Osun state. The impacts are as follow: undergraduates who are involved in cybercrime become criminally oriented by 85% followed by some undergraduates abandon their studies to get fully involved in cybercrime by 77%, undergraduates who are caught in the act of cybercrime are punished according to the law by 75% and some undergraduates becomes victims of cyber bullying by other undergraduates 74%.

Responses from respondents make it obvious that undergraduates in Nigerian universities are aware of the concept of cybercrime, and the existence of cybercriminals. The study revealed that phishing, hacking, cyberbullying, cyberstalking, blackmailing on the internet, fraud and forgery, are things that cybercriminals do, and also that undergraduates of universities in Osun state are aware of this fact.

A lot of undergraduates in the university are involved in cybercrime knowingly, while only a few are found in the act due to ignorance. The study also revealed that undergraduates are aware of the various activities engaged in on the internet or with the computer by them and their colleagues which make them potential criminals. This means that the involvement of undergraduates in cybercrime is not an act of ignorance but with guilty intentions. The aforementioned findings establishing the awareness and popularity of cybercrime among Nigerian undergraduates corroborate the positions of Sesan, Soremi, & Bankole (2013) who stated that the Nigerian cyberspace has become an open arena for thieves and likes to display their various abilities by playing tricks using the computer system and network. The findings are also buttressed by Sesan (2010) who reported that Nigeria is among the topmost in terms of online crime activity and that cybercrime is prevalent among a sizeable number of young Nigerians. Singh, Gupta, &

Kumar† (2016) also falls in line with these findings by stating that cybercrimes are often committed illegally and with guilty intention.

Moreover, the researcher discovered the various impacts of cybercrime on undergraduates of universities in Osun state. It was discovered that a lot of undergraduates become criminally oriented when they get involved in cybercrimes. Some undergraduates also become victims of cyberbullying, while some even abandon their studies to get fully involved in cybercrime. This finding agrees with the study of Adeniran (2011), in which he averred that young individuals including undergraduates commit an overwhelming majority of the cybercrimes in Nigeria by engaging in the so-called yahooboyism. Another researcher who agrees that the prevalence of cybercrime in Nigeria has produced a worrisome impact is Jackson & Robert (2016). Furthermore, findings on impact are in consonance with the position of Frank & Odunayo (2013), that the advent of internet has brought unintended consequences such as cybercrime amidst other criminal activities. Studies available were not contrary to the findings of this study.

CONCLUSIONS

In conclusion, one of the developing problems of the Nigerian economy is cybercrime, and undergraduates constitute a large percentage of the population of people perpetrating this crime. Undergraduates across universities have turned cybercrime into a way of living. Resulting from this study, it is clear that undergraduates in Nigeria's universities are becoming deeply involved in acts of cybercrime and some of them don't even know the gravity of the offenses they are committing even though some do. The bitter truth is that if urgent actions are not taken towards curbing cybercrime in Nigeria's universities, many undergraduates will turn cybercrime into a basic mode of living.

RECOMMENDATIONS

Based on the findings of this study, the following recommendations were made:

1) Students in tertiary institutions should also abstain from any illegal or criminal acts while using the internet not to become criminals without even knowing.
2) University authorities should ensure that students are allowed to use the I.C.T facilities, with guidance from the I.C.T officials.
3) Management of universities should orientate students on safe and careful use of their phones, computers and the internet in general.
4) Authorities of Nigerian universities should encourage and impact entrepreneurial skills on their undergraduate students, whereby they can make money without getting involved in criminal activities.
5) The government should improve on measures of monitoring activities on the internet to reduce the way people engage in internet frauds and scam.

6) Nigerian government should put in additional efforts in publicising the prosecution of cybercriminals as this will create awareness and deter potential cybercriminals.
7) Nigerian government should compel concerned agencies to improve on measures of monitoring activities on the internet to reduce the way people engage in internet scam and fraud.

LITERATURE CITED

Adeniran, A. I. (2011). Café culture and heresy of yahooboyism in Nigeria. *Cyber criminology: Exploring Internet crimes and criminal behavior*, 3-12. Retrieved on March 19, 2019 from https://bit.ly/2KWwdJh

Boniface, K. A., & Michael, K. A. (2014). Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *8*(9), 1582-1585. Retrieved on March 8, 2019 from https://bit.ly/2vfWfwp

Ewepu, G. (2016). Nigeria loses N127bn annually to cyber-crime. Retrieved Jun. 9, 2016 from https://bit.ly/2VaZns8

Sesan, G., Soremi, B., & Bankole, O. (2013). Economic cost of cybercrime in Nigeria. *Cyber Stewards Network Project, Munk School of global affairs, University of Toronto*. Retrieved on March 28, 2019 from https://bit.ly/2KVHYjl

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of cognitive research in science, engineering and education*, *1*(1). Retrieved on April 22, 2019 from https://bit.ly/2IKnB5T

Jackson, T.C. & Robert, W. E. (2016). Cybercrime and the challenges of socio-economic development In Nigeria. Journal of Research in National Development, 14(2).

Jide, A. (2007). Fighting cybercrime in Nigeria. Retrieved on March 9, 2019 from https://bit.ly/2IKjgzz

Kamini, D. (2011). Cybercrime in the society: problems and preventions. Journal of Alternative Perspectives in the Social Sciences (2011) 3 (1) 240-259

Okanlawon, A. E., Abanikannda, M. O., & Yusuf, F. A. (2015). University students' knowledge and attitude towards internet safety: a preliminary study. *Journal of Emerging Trends in Educational Research and Policy Studies*, *6*(3), 279-286. Retrieved on April 15, 2019 from https://bit.ly/2ve5QDY

Sesan, G. (2010).The New Security War (online). Retrieved on April 9, 2019 from https://bit.ly/2VZX4Fh

Singh, O., Gupta, P., & Kumar†, R. (2016). A Review of Indian Approach towards Cybersecurity. Retrieved on April 14, 2019 from https://bit.ly/2INZeEy