A Study of Cybercrimes Awareness and Involvement among Students of Tertiary Institutions in Zamfara State of Nigeria

BY

Tafa Taofik O.
Department of Computer Science,
Federal College of Education (Tech.) Gusau Nigeria,

Alfa Ahmad SHUAIB
Department of Liberal Studies
Abdu Gusau Polytechnic Talata Mafara Nigeria

&

A. J. SULEIMAN
Department of Public Law,
Ahmadu Bello University Zaria Nigeria

ABSTRACT

People's perception and attitude towards computer ethics and security significantly affect the way they use computers and computer related devices. This is especially the case among students of tertiary institutions who are generally regarded as major violators of computer ethics and security. This paper examines the level of cybercrime awareness and involvement among students of tertiary institutions in Zamfara state. A questionnaire-based survey method was adopted using questionnaire tagged "cybercrimes awareness among students of tertiary institutions (CASTI)". The findings of this study reveal that there are satisfactory levels of awareness among the students surveyed. However, only small percent of the students were able to exhibit a firm theoretical knowledge of the nature and common types of cybercrimes enlisted in Nigeria's Cybercrime Act 2015. The paper is of opinion that every internet user has a right to be aware of the consequences of its threats and misuses and as such recommends that adequate education on the issue should be on high priority.

KEYWORD: Cybercrime, fraud, awareness, cyber café

Introduction

As internet technology continues to expand and individuals continue to "log-on" at an ever-increasing rate, business transaction via computers have quickly expanded. Many transactions, more businesses and other forms of trade are now conducted online, often with the parties never physically meeting each other. Cyber-crimes are international in nature and do not respect political or geographical boundaries. Therefore, several countries tried to come up with coordinated efforts in combating these crimes. Nigeria on the other hand have been at the spot high from the international community for its citizen involvement in cyber-crime. It is ranked as the third in the world behind the United States and Britain, and the first within the Africa continent in the rate of cyber-crime prevalence (Malhotra and Malhotra, 2017). This conspicuous position has been a catalyst in the way the nation has handled issue concerning cyber-crime.

The limitation experienced in combating cyber-crime is related to the fact that these crimes have only been in existence for only as long as internet exist. This explain why it seems criminologists and other user protection agencies are ill-prepared towards fighting cyber-crime. With the increase in use of internet facilities and automated teller machine (ATM) for banking and other financial transactions in Nigeria, phishing attacks are also on the increase. Though Nigeria government, in an effort to curb the menace of cyber-crime enacted a law in 2015 that provide for the prohibition, prevention, detection, response, investigation and prosecution of cyber-crimes (FGN, 2015). In addition to this law, Nigeria government and other stake-holders in Nigeria need to create awareness about these cyber-crimes and subsequently combating them. This paper therefore finds out the level of cyber-crime awareness and involvement among tertiary institution students in Zamfara state.

Research problem

When the internet first went commercial and become affordable and easy enough to access for ordinary people it was a new frontier. Like the Wild West of old, it was mostly unregulated; legislators had not anticipated the rapid growth or the types of online behaviors that would require new laws and awareness to protect innocent users. Research conducted by Okeshola and Adeta (2013) indicated that majority of those involves in cybercrime are youths. The youths in every society is of great importance and concern to that society because they are looked upon as the leaders of tomorrow. Olaide and Adewole (2019), observed that a sizeable number of criminals in Nigeria fall within the youthful age. The youths at present have discovered different ways of using the internet in doing different types of criminal activities and these age brackets are usually found in tertiary institutions in Nigeria. Large numbers of these youths are found at our tertiary educational institutions.

The popular crimes in most Nigerian tertiary institutions include examination malpractices, cultism, falsification of results, rapes, robbery, sexual abuse, etc, but that does not mean that students of tertiary institutions are not engaging in cyber-crimes. Most students and institutional authorities are either less aware of this form of crime or has no mechanism in place to checkmate it. Many countries have passed laws to this effect but enforcing these is another problem. It can be frustrating for the victims of such crimes, when the perpetrators are never brought to book. Some countries also shy from investigating and enforcing these types of crime, because for a number of reasons. Enforcing laws governing online behaviours are institutionally more difficult than the enforcement of "traditional "law, most especially when people are less aware of such crime and law.

Purpose of the study

The purpose of the study is to evaluate the level of awareness of cyber crime among students of tertiary institutions in Zamfara state. Specifically, the study will:

- Determine the level of awareness of cyber-crime among students of tertiary institutions in Zamfara state of Nigeria
- Investigate whether students of tertiary institutions in Zamfara state of Nigeria are involved in cyber-crime.
- Identify places where cyber-crimes are perpetrated in Zamfara state of Nigeria.
- Identify the causes and consequences of cyber-crime among tertiary institution students.

Scope of the Study

The study was conducted in three tertiary institutions in Zamfara state. These institutions are Federal University Gusau, Federal Polytechnic Kaura Namoda and Zamfara State College of Education Maru. These three tertiary institutions were selected because they represent all the major types of tertiary education that an individual may attend to acquire knowledge in Zamfara state of Nigeria.

Research Questions

1. What kinds of activities do students of tertiary institutions in Zamfara state access on the internet?
2. What is the level of awareness of cyber-crime by students of tertiary institutions in Zamfara state?
3. What are the places where cyber-crime is committed in Zamfara state of Nigeria?
4. What are the causes and consequences of cyber-crime?

Literature Review

Internet is a global network that combines millions of computers spread accross countries and opens broad opportunities to obtain and exchange information (Vladimir, 2005 in Okeshola and Adeta, 2013). Internet has now been used for criminal purposes due to the economic factors. This criminal activity referred to as cyber-crime include hackers vandalizing web site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include denial of services and viruses attacks preventing regular traffic from reaching web site among others Narahari and Shah (2016).

Nigeria as a developing country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby, making different types of crime, including cyber-crime to strive. However, cause of cyber-crime in Nigeria cannot only be based only on economic challenge. As cited by Omodunbi et al (2016), some of the identified causes of cyber-crime are unemployment, quest for wealth, lack of strong cyber-crime laws and incompetent security on personal computers.

Over the years, the internet has witnessed an explosives growth with the number of hosts connected to the internet increasing daily at an exponential rate. As the internet grows to become more accessible and more useful in daily operation, so does the threat to its usage. In Nigeria, cybercrime has become one of the main avenues for stealing money and business espionage. Check Point, a global network cyber security vendor, in 2016, ranked Nigeria the 16th highest country in cyber-attacks vulnerabilities in Africa (Olaide and Adewole, 2019). Nigerians are known both home and abroad to be involve in perpetrating cybercrimes. The contribution of the internet to the development of Nigeria has had a positive impact also on various sectors of the country. However, sectors such as the banking and e-commerce sectors battle with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor (Omodunbi et al 2016).

McConnel (2000) in Okeshola and Adeta (2013) opined that cyber-crimes differ from most common crimes in four ways; easy to learn, require few resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present and often not clearly illegal. As such, cyber-crime has become one of the major security issues for law enforcement agencies and the world in general. Publication released by Economic and Other Financial Crime Commission (EFCC) of Nigeria in 2006, showed how a retired civil servant with two (2) other accomplices defrauded a German citizen name Klaus Wagner a sum of

$1,714,080 through the internet. According to Sesan (2010) in Okeshola and Adeta (2013), a 2007 internet crime report listed Nigeria third in terms of online crime activity and the prevalence of cyber-crime among a sizeable number of young Nigerians. Ribadu (2007), stated that the prominent forms of cyber-crime in Nigeria are cloning of websites, false representations, internet purchase and other e-commerce kinds of fraud. Olugbodi (2010) study shows that the most prevalent forms of cyber-crime are website cloning, financial fraud, identity theft, credit card theft, cyber harassment, fraudulent electronic mails, and cyber laundering and virus/worms circulation.

Research methodology

The study adapted the survey research design method, using a sample of Three hundred (300) respondents drawn from the three schools. A total of one hundred students were selected from each of the three schools using purposive sampling technique. The instrument used for the data collection in this study is questionnaire which contained close ended items. The questionnaire was self-constructed after extensive reading of related literature in order to ensure that relevant items were included. The closed ended questions were intended to collect data that would facilitate easy analysis. Copies of the questionnaire were administered by the researchers with the assistance of colleagues in the study schools to students and retrieved immediately from them in order to ensure high response rate. The returned questionnaires are two hundred and eighty-four (284) which was used for the study. The score of the questionnaire marked were collated, computed and analyzed using frequency count and percentages. This is because of the descriptive nature of the study.

Presentation of findings

Socio-demographic Attributes of Respondents

This section presents the socio- demographic attributes of the respondents. These attributes are sex, age, and marital status of respondents.

Table 1: Socio-demographic attributes of respondents

Sex	**Frequency**	**Percentage**
Male	180	63.38%
Female	104	36.62%
Total	284	100
Age	**Frequency**	**Percentage**
16-24	151	53.17
25-30	84	29.58
30-35	39	13.73
36 and above	10	03.52
Total	284	100
Marital status	**Frequency**	**Percentage**
Single	182	64.08
Married	88	30.99
Divorced	14	04.93
Total	284	100

From table 1, it was found that more than 63% of the respondents are males. The number of male respondents who participated in the study outweighs the female respondents because most of the females felt it was a male issue. Most of the respondents are young and majority of the respondents are single. This is not surprising bearing in mind that the study was conducted in three tertiary institutions in Zamfara state of which majority of the students are youths and single.

Activities respondents' access on the internet

This section identifies the kind of activities respondents' access on the internet

Table 2: Views of respondents on the activity they access while on the internet

Activity individual access	**Yes**	**Percentage**	**No**	**Percentage**	**Total**	**Percentage**
Google search	284	100	0	0	284	100
E-mail	245	86.27	39	13.73	284	100
Social media, such as Facebook, WhatsApp, etc	268	94.37	16	05.63	284	100
News/entertainment	152	53.52	132	46.48	284	100
Sports	131	46.13	153	53.87	284	100
Games	167	58.80	117	41.20	284	100
Internet phoning	25	08.80	259	91.20	284	100
Pornographic	26	09.15	258	90.85	284	100
Spamming	02	0.70	282	99.30	284	100

From table 2, it shows that majority of the respondents access Google search (100%), email (86.27%), social media (74.37%) and games (58.80%). This is unconnected to the fact that respondents are students. Only few respondents use the internet for phoning (8.80%) and pornography (9.15%). The low response of the respondents was as a result of the sensitivity of the topic and the study area.

Respondents' awareness of cyber crime

This section presents respondents' awareness of cyber crime

Table 3: Views of respondents as to whether they have heard of cyber-crime

Aware of cyber crime	Frequency	Percentage
Yes	204	71.83
No	80	28.17
Total	284	100

The above table indicates that majority of the respondents (71.83%) have heard of cyber-crime. This means that a very high percentage of the respondents are aware of the crime and are capable of filling, providing adequate and useful information to the questions in the questionnaire.

Respondents' knowledge of various types of cyber crime

This section presents respondents awareness of various types of cyber-crime.

Table 4: Views of respondents on the common types of cyber-crime

Types of cyber crime	Yes	Percentage	No	Percentage	Total	Percentage
Hacking	189	66.55	95	33.45	284	100
ATM card fraud	271	95.42	13	04.58	284	100
Pornography	140	49.30	144	50.70	284	100
Software piracy	169	59.51	115	40.49	284	100
Identity theft	152	53.52	132	46.48	284	100
Website cloning/ phishing	132	46.48	152	53.52	284	100
Cyber defamation	130	45.78	154	54.22	284	100
Virus/malware dissemination	121	42.61	163	57.39	284	100

Respondents are of the view that hacking (66.55%) and credit card frauds (95.42%) are the common type of cyber-crime in Zamfara state. However, virus dissemination (42.61%) and cyber defamation (45.78%) which are other types of cyber-crime got low response from the respondents.

Places where cyber-crime is perpetrated

This section identifies respondents' opinions on places where cyber-crime is committed.

Table 5: Views of respondents on places where cyber-crime is perpetrated

Types of cyber crime	Yes	Percentage	No	Percentage	Total	Percentage
Homes	235	82.75	49	17.25	284	100
Cyber cafes	204	71.83	80	28.17	284	100
Tertiary institutions	125	44.01	159	55.99	284	100
Private organisations	67	23.59	217	76.41	284	100
Government offices	25	08.80	259	91.20	284	100

Table 5 shows the perpetration places of cyber-crime. Findings reveal that 82.75% of the respondents agreed that cyber-crime is usually perpetrated at home and 71.83% are of the opinion that the crime is carried out at cyber cafes. This is to confirm the earlier statement made by operators of cyber cafe that with the introduction of internet modems, blackberry and smart phones cyber-crime could be committed at homes. This is also in line with findings

of Okeshola and Adeta (2013) which revealed that most cybercrimes are perpetrated either at a cyber café or at home.

Causes of cyber-crime

This section presents respondents views on the causes of cyber-crime

Table 6: Views of Respondents on the causes of cyber-crime

Causes of cyber crime	Agree	%	Undecided	%	Disagree	%	Total	%
Unemployment	214	75.35	24	08.45	46	16.20	284	100
Poverty	198	69.72	26	09.15	60	21.12	284	100
Peer group influence	225	79.22	18	06.34	41	14.44	284	100
Bad socialization	236	83.10	08	02.82	40	14.08	284	100
Easy access to internet	201	70.77	30	10.57	53	18.66	284	100
Corruption	189	66.55	43	15.14	52	18.31	284	100
Week law	199	70.07	36	12.68	49	17.25	284	100

Table 6 shows that virtually all respondents agreed that bad socialization (83.10%) and peer group influence (79.22%) are major causes of cyber-crime. Majority of the respondents also agreed that unemployment (75.35%), poverty (69.72%), easy access to internet (70.77%), corruption (66.55%) and week law (70.07%) are also other causes of cyber-crime in Zamfara state.

Consequences of cyber crime

Table 7: Views of Respondents on the consequences of cyber crime

Consequences of cyber crime	Agree	%	Undecided	%	Disagree	%	Total	%
Tarnishing the image of the country	230	80.99	14	04.93	40	14.08	284	100
Lack of trust and confidence on online transaction	269	94.72	05	01.76	10	03.52	284	100
Denial of innocent Nigerians opportunity abroad	185	65.14	14	04.93	85	29.93	284	100
Loss of employment	155	54.58	22	07.74	107	37.68	284	100
Loss of revenue	254	89.44	10	03.52	20	07.04	284	100
Loss of life	201	70.77	21	07.40	62	21.83	284	100

The above table shows the negative consequences of cyber-crime to the society. It was found that 94.72% of the respondents are of the view that cyber-crime leads to loss of trust and confidence on online transaction, and this according to Okeshola and Adeta (2013) is currently hindering profitable online transactions. Majority of the respondents (89.44%) were also of the view that cyber-crime leads to loss of revenue.

Conclusion

The study proves that majority of students of tertiary institutions in Zamfara state of Nigeria are aware of cybercrimes and its nature. The convergence of smart phones and internet are on stride and quite popular among the students of tertiary institutions and as such facilitate access to internet. This means, there is more scope for cybercrimes. Though many internet users claim to be aware of such crimes, still majority consider the cyber-crime as ATM fraud. Other than hacking, ATM fraud and software piracy, a quiet majority of users are not aware of crimes like website cloning, cyber defamation and virus dissemination, sharing disturbing content of pornography etc.

A high level awareness about information security and cybercrime issues amongst users at home, in government and educational institutions, especially young people, would decrease the occurrence of cybercrime (Sembok, 2003). More so, since youths are the most involved in this crime, there is need for them to be orientated, educated and empowered for Nigeria to have a greater future. There is need for security and regulating agencies to collaborate to fight the menace of cybercrime collectively this could be in the area of information sharing, infrastructure and personnel.

Recommendations

Based on the overall conclusions of the study, the following recommendations were made;

1. Government should bring out more awareness campaigns in various places, especially tertiary institutions where the potential internet users are high.
2. Rules and regulations that deal with cybercrimes should be implemented strictly to make sure that no one is taking the security issues for granted. Strict governance is required so that no one is inculcating the habit of indulging in illegal download and data theft.
3. Tertiary institutions should take special initiative to incorporate as part of general computer studies, cyber-crimes and security.
4. Cyber awareness or sensitization of the populace will go a long way in educating the masses on how to prevent common forms of cyber-crimes like email and ATM fraud, malware attacks, and limitation in the access of sexually explicit content from children and young people.

REFERENCES

FGN, (2015). *Cybercrimes* (prohibition, prevention, etc) act, 2015 Retrieved from https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

Malhotra, T. and Malhotra, M. (2017). Cyber-crime awareness among teacher trainees. *Scholarly research journal for multidisciplinary studies*, 4(31), 5249-5259.

McConnell International (2000). *Cyber crime and punishment?* Archaic law threaten global information. McConnell International LLC. Retrieved from www.mcconnellinternational.com

Narahari, A. C. and Shah, V. (2016). Cyber-crime and security – a study of awareness among young Netizens of Anand (Gujarat state, India). *IJARIIE.* 2(6), 2395-4396

Okeshola F.B. and Adeta A.K, (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 98-114.

Olaide S. and Adewole O. (2019). *Cyber Crime Embarrassing for Victims in Nigeria*. Unpublished research project. Retrieved from: https://projectchampionz.com.ng/2019/02/11/cyber-crime-embarrassing-victims-nigeria/

Olugbodi, K. (2010). *Fighting Cyber Crime in Nigeria.* Retrieved from http//www.guide2nigeria,com/news_articles_About_ Nigeria

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M. and Esan, A. O. (2016). Cybercrimes in Nigeria: analysis, detection and prevention. *FUOYE journal of engineering and technology*. 1(1), 37-42.

Ribadu, E. (2007). *Cyber Crime and Commercial Fraud*; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Sembok, T.M., (2003). *Ethics of information technology*. Proceedings of the Regional Meeting on Ethics of Science and Technology, RUSHAP, UNESCO, Nov. 5-7, Bangkok.

Sesan, O. M. (2010). Emotional intelligence and self-regulation among school – group adolescent: self efficacy as a mediator. *Contemporary Humanities.* 4(2), 209-222.

Vladimir, G. (2005). *International Cooperation in Fighting Cyber Crime*. Retrieved from www.crimeresearch.org