MPRI-JAEE | INTERNATIONAL JOURNAL OF ASSESSMENT & EVALUATION IN EDU.
VOL. 05 NO. 8 – JULY, 2024

CYBERCRIME AWARENESS AMONG UNDERGRADUATES OF AMBROSE ALLI UNIVERSITY EKPOMA, EDO STATE: THE EFFICACY OF VALUE EDUCATION

EMOSOGA, AFOKE JOSEPH; & DR. MRS. BLESSING IWUAGWU

Department of Educational Foundation and Management, Faculty of Education, Ambrose Alli University, Ekpoma-Edo State
Corresponding Author: *wilfok1989@gmail.com*

Keywords:
Cybercrime, Technology, Value, Education.

Abstract

This paper examined the awareness of cybercrime among undergraduates of Ambrose Alli University Ekpoma, Edo State. The descriptive research design was adopted in the study. The population covered all the 27,388 regular undergraduate students in Ambrose Alli University, Ekpoma in the 2018/2019 session. A sample size of 5478 students were drawn using purposive sampling technique. This represents about 20percent of the population. The instrument that was used for collection of data was a questionnaire titled: "Undergraduates Cybercrime Awareness Survey Checklist (UCASQ)". Research questions was analyzed using frequency count and percentages (%). The response option with the highest percentage was used to make decision on every item statement and response. Based on findings, it was concluded that undergraduates are aware of the types of cybercrime, the modes of cybercrime perpetration. It was recommended that there is need for the government to train special cyber security experts while aiding the existing law enforcement agencies, intelligence agencies and security agencies to understand both the nature of technology and the individuals involved in cybercrime.

Introduction

Cybercrime is a type of crime committed by individuals who make use of the computer as a tool and the internet as a means of connection to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cybercrime evolves from increase in digitalization, technology integration

EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

and the wrong application or abuse of internet services to perpetrate various atrocities such as fraud, theft, blackmail, forgery and embezzlement.

The convergence of computing and communications, and the rapid growth of digital technology have brought immense benefits to society, but these benefits also come with greater risks both nationally and internationally. Today, many traditional crimes are now being aided or abetted through the use of computers and networks, and wrongdoing previously never imagined has surfaced because of the incredible capacities of digital gadgets like Smartphone and computers.

Boateng, Longe, Mbarika, Avevor and Isabalija (2017) argued that the information technology revolution associated with the internet has brought about two edge functions: that is on one hand, it has contributed positive values to the world; while on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world. Cybercrime has no borders or physical boundaries, and also not subject to any form of importation, customs or forex constraints and due to lack of rules and codes of a central authority governing it, cybercrime can be perpetrated by any one from anywhere in the world. Hence, the nature of cybercrime in Nigeria is continually evolving with the emergence of new technologies. In Nigeria, cyber criminals in Nigeria make use of personal computers and internet as a tool to defraud and harm others. Relatedly, generally cybercrimes in Nigeria are targeted at individuals and not directly to computer systems hence requiring less technical expertise on the part of the criminals. These kinds of tool cybercrimes prevalent in Nigeria are perpetrated using different kinds of computer and telecommunication tools operational in the country. The prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other e–commerce kinds of fraud. Similarly, Olugbodi (2018), identified website cloning, financial fraud also popularly known as Yahoo-Yahoo, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus/ worms/ Trojans.

As early as 1986, the National Policy on Education (Federal Republic of Nigeria, revised 2004 and 2013) strongly recommended the need for value education due to the following reasons:

a) tremendous advance in Science and Technology has resulted in a complete change in the lifestyle of the people;
b) science and technology is being used to produce weapons of mass destruction endangering the very existence of the human race instead of using it for the betterment of human life;
c) erosion of traditional values;
d) life is becoming more complex as students of today have to face such moral situations in future, in which, instead of depending on others, they may be required to take their own decision; and

e) The youth are beginning to question the conduct of elders – especially political leaders as they do not see the relevance of the values preached (FRN, 2004, 2013).

From the foregoing, it is evident that value education is recognized by the federal government as an aspect of education that borders on inculcating moral and sound decision making principle into members of the society for right living. Hence, value education may have some implications on managing cybercrime in Nigeria. Previous studies on cybercrime has been carried out in Nigeria. Jackson and Robert (2016) examined the nature and dynamics of cybercrime in Nigeria and its contribution to the socio-economic development challenges in the country. The paper concludes that widespread cybercrime has negative impact on the socio-economic development of Nigeria as it tarnishes the image of the country at the global scale, deters foreign investments, and reduces confidence in the digital economy; with huge financial loses to individuals, business organizations and the government.

Maitanmi, Ogunlere, Ayinde and Adekunle (2013) examined the impact of Cyber Crimes on Nigerian Economy. The method we employed in this research was the survey method while the research design used was the purposive research design technique so as to meet up with the targeted presentation date. The responses from the respondents were collated and analysed using the simple percentage procedure and bar chart. The results show that cracking, software piracy, and pornography among others are prevalent crimes in Nigeria.

Duah and Kwabena (2015) examined the impacts on the socio-economic and educational developments in Ghana. Results indicated that cyber fraud is fast gaining grounds in Ghana and it cause direct financial losses to consumers and businesses. Tade and Aliyu (2011) investigated social organization of internet fraud among university undergraduates in Nigeria. The information obtained from the interview was analyzed using manual content analysis. Findings indicated that internet fraud in tertiary institutions are socially organized and highly networked. Boateng, Longe, Mbarika, Avevor and Isabalija (2010) investigated the prevalence of cybercrimes in Ghana and its impact on ICT adoption in Ghana. Findings from our research showed that although awareness of cybercrimes is on the increase, the crimes mostly go unreported.

Studies that focus on cybercrime largely concentrates on situations in the western world forgetting that the nature of cybercrime is such that geographical and political boundaries are being rendered irrelevant. A person who has access to computer and connected to the internet might be participating, attempting or planning a criminal act anywhere in the world (Kumar, 2013). Awe (2009), confirmed that computer attacks can be generated by criminals from anywhere in the world, and executed in other areas, irrespective of geographical location. And often these criminal activities can be faster, easier and more damaging with the use of the internet.

The above statement shows that it is a global issue and as such, has become an image nightmare for the Nigeria government to identify the remote causes and proffer solution. In Nigeria, perpetrators of this crime who are usually referred to as "yahoo yahoo boys" are taking advantage of ecommerce system available on the internet to defraud victims who are mostly foreigners in thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. They may pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have been duped or fallen victims. But this could not only be the techniques used by these cyber criminals. Attempt to address cybercrime by various governments and international organizations have not been successful owing to the fact that the identities remain inadequate. A study by Zero Tolerance (2016) indicates that cyber criminals are usually within the age of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life. Noting these observations, there is need to identify more attributes these cyber criminals posses as factors since it have been acknowledged that a good taste of life is a major factor.

Although, recent studies have been conducted on cybercrime in Nigeria (Akogwu, 2012; Okeshola, 2013;Folashade & Abimbola, 2013; Saulawa & Abubakar, 2014), all the studies examined the proliferation, causes and effect of the practice on youths in Nigeria as a whole. Also, many of the studies were mere theoretical discussion papers which did not collect data from any specific local government or state to determine the awareness of the types, causes, effects and implications of the cybercrime among undergraduates. Hence, a knowledge gap exists on cybercrime awareness among university undergraduates in Edo State. Consequently, this study will be undertaken to fill this gap by investigating the awareness of cybercrime among undergraduates of Ambrose Alli University Ekpoma.

Research Questions

The following research questions were answered in the study:

1) What is the awareness of undergraduates of Ambrose Alli University Ekpoma on the types of cybercrime perpetrated by fraudsters?
2) What is the awareness of undergraduates of Ambrose Alli University Ekpoma on the mode of cybercrime?

Methods

The descriptive research design was adopted in the study. The population of the covered all the 27,388 regular undergraduate students in Ambrose Alli University, Ekpoma in the 2018/2019 session. A sample size of 5478 representing 20% of students were drawn using purposive sampling technique. This represents about 20percent of the population. The

instrument that was used for collection of data was a questionnaire titled: "Undergraduates Cybercrime Awareness Survey Checklist (UCASQ)".

The face and content validity of this instrument (UCASQ) was carried out by the researcher and two experts in Educational Foundations in Ambrose Alli University, Ekpoma. The instrument was personally administered by the researcher and two other research assistants who were trained by the researcher. Research questions was analysed using frequency count and percentages (%). The response option with the highest percentage was used to make decision on every item statement and response.

Results

The result on the test of analysis is given as follows:

Research Question 1: What is the awareness of undergraduates of Ambrose Alli University Ekpoma on the types of cybercrime perpetrated by fraudsters?

Table 1: Responses on Students' Awareness on the types of Cybercrimes perpetrated among Undergraduates of Ambrose Alli University Ekpoma

s/n	Items	Aware	Not aware	
1.	Cyber Terrorism	3670(67%)	1808	(33%)
2.	Fraud - Identity Theft	4547(83%)	931	(17%)
3.	Drug Trafficking Deals	4163(76%)	1315	(24%)
4.	Malware	712(13%)	4766	(87%)
5.	Cyber Stalking	3670(67%)	1808	(33%)
6.	Spam	1534(28%)	3944	(72%)
7.	Logic Bombs	931(17%)	4547	(83%)
8.	Password Sniffing	4054(74%)	1424	(26%)
9.	Others	986(18%)	4492	(82%)

Result in Table 1 showed that majority of the respondent (N=3670) representing 67% agreed that youth are aware of cyber terrorism in Ambrose Alli University Ekpoma, 4547(83%) agreed that fraud - identity theft, 4163 (76%) agreed on drug trafficking deals, 712 (13%) disagreed on malware, 3670(67%) agreed that cyber stalking, 1534(28%) disagreed on spam, 931(17%) disagreed on logic boms, 4054(74%) agreed on password sniffing while 986(18%) disagreed on others. This indicates that majority of the respondents agreed that the types of cybeorcrime perpetrated among youths in Edo State include: cyber terrorism, fraud - identity theft, drug trafficking deals, cyber stalking and password sniffing

However, majority of the respondents are aware of the types of Cybercrimes perpetrated among Undergraduates of Ambrose Alli University Ekpoma.

Question 2: What is the awareness of undergraduates of Ambrose Alli University Ekpoma on the mode of cybercrime?

Table 2: Responses on Students' Awareness on the Modes of cybercrime operations among Undergraduates of Ambrose Alli University Ekpoma

s/n	Items	Fully aware	Not Aware
1	Unauthorized access to computer systems or networks/hacking	4328 (79%)	21 (21%)
2	Theft of information contained in electronic form	4930 (90%)	548(10%)
3	Email bombing	3999(73%)	1479(27%)
4	Data diddling	2903 (53%)	2575(47%)
5	Salami attacks	1753 (32%)	3725 (68%)
6	Denial of service attack	1917(35%)	3561(65%)
7	Web jacking	4602 (84%)	876(16%)
8	Internet time thefts	4930 (90%)	548(10%)
9	Others	2246(41%)	3232 (59%)

Result in Table 2 shows that 4328 of the respondent representing 79% stated that they are fully aware of unauthorized access to computer systems or networks/hacking, 4930(90%) are fully aware of theft of information contained in electronic form, 3999(73%) are aware of email bombing, 2903(53%) are not aware of data diddling, 1753(32%) are not aware of salami attacks, 1917(35%) are not aware of denial of service attack, 4602(84%) are fully aware of web jacking, 4930(90%) are fully aware of internet time thefts while 2246(41%) are not aware of others. This showed that majority of the respondents in this study indicates that they are fully aware of unauthorized access to computer systems or networks/hacking, theft of information contained in electronic form, web jacking and internet time thefts are the modes of cybercrime operations among youths in Edo State.

Implications and Discussion of Results

Following the tremendous advances in Science and Technology which is resulting in the gradual change in the lifestyle of the youths; and also bringing about the use of technology to perpetrate crimes; it is pertinent to inculcate some moral values in youths to discourage the perpetration of cybercrimes among youths who are seemingly becoming 'yahoo-boys', 'yahoo-girls', or 'gee-boys' or 'gee-girls'. Most of these lads (yahoo boys and girls) are undergraduates of Nigerian universities and young graduates involved in hacking, cloning and defrauding unsuspecting victims using tools such as password cracker, key loggers, network sniffers, port scanners, vulnerability scanners, exploits and so on (Duah & Kwabena, 2015). As an underworld criminal activity, cyber

criminals in Nigeria plan their executions in some details, as their perpetrations are deliberate with their victim-system or network pre-chosen and identified deliberately and not randomly. Their targets are usually the gullible, greedy, and inexperienced and those desperate for quick money, love and relationships.

In this regard, the outcome of this study shows that the respondents perceived that value education could: inculcate good manners in the Nigerian youth; develop in youths the value to work with dignity as opposed to indulging in cybercrime; help youths to live with a sense of integrity on financial matters with others; create in youths, the value to live in honesty when doing business with anyone; and expose youths to make business decisions based on sound moral principles. Hence, cybercrime could be managed by introducing value education to youths who are the major perpetrators of this dreadful act.

The result showed that that the types of cybercrime perpetrated among youths in Edo State include: cyber terrorism, fraud - identity theft, drug trafficking deals, cyber stalking and password sniffing. The result agrees with that of Jackson and Robert (2016) who noted that widespread cybercrime has negative impact on the socio-economic development of Nigeria as it tarnishes the image of the country at the global scale, deters foreign investments, and reduces confidence in the digital economy; with huge financial loses to individuals, business organizations and the government.

The result showed that youths are fully aware of unauthorized access to computer systems or networks / hacking, theft of information contained in electronic form, web jacking and internet time thefts are the modes of cybercrime operations among youths in Edo State. The result agrees with that of Duah and Kwabena (2015) who stated that cyber fraud is fast gaining grounds in Ghana and it cause direct financial losses to consumers and businesses. The result corroborates that of Tade and Aliyu (2011) who sobered that Internet fraud in tertiary institutions are socially organized and highly networked.

The result showed that causes of cybercrimes among youths in Edo State include: unemployment, quest for wealth, negative role models, and weak implementation of cybercrime laws. The result agrees with that of Boateng, Longe, Mbarika, Avevor and Isabalija (2010) who found out that although awareness of cybercrimes is on the increase, the crimes mostly go unreported

The result showed that tarnishing of the country reputation, lack of trust and confidence in transacting business with others, denial of innocent Nigerians opportunity abroad, it mimic the progress and development in the country are the implications of cybercrimes on social-economic development of youths in Edo State. The result is in with that of Maitanmi, Ogunlere, Ayinde and Adekunle (2013) who found out that cracking, software piracy, and pornography among others are prevalent crimes in Nigeria.

Conclusion

Cybercrime is one of the forms of abusing technological advancement and digitalization in this computer age. Based on findings, it was concluded that undergraduates are aware of the types, the modes of cybercrime perpetration and causes of cybercrime. Unauthorized access to computer systems or networks/hacking, theft of information contained in electronic form, web jacking and internet time thefts are the modes of cybercrime operations among youths in Edo State

Cyber terrorism, fraud - identity theft, drug trafficking deals, cyber stalking and password sniffing are the types of cybercrime perpetrated among youths in Edo State. Tarnishing of the country reputation, lack of trust and confidence in transacting business with others, denial of innocent Nigerians opportunity abroad, are some of the implications of cybercrimes on social-economic development of youths in Edo State. The result shows that some of the implications of cybercrime include the tarnishing of the country's reputation, lack of trust and confidence in transacting business with others, denial of innocent Nigerians opportunity abroad.

Recommendations

The following recommendations are made on the study:

1) There is need for the government to train special cyber security experts while aiding the existing law enforcement agencies, intelligence agencies and security agencies to understand both the nature of technology and the individuals involved in cybercrime.
2) University administrators should endeavour to inform or give orientation to students about the evils of indulging in cybercrime.

REFERENCES

Boateng, R., Longe, O., Mbarika, V., Avevor, I. & Isabalija, S. R. (2010). Cyber Crime and Criminality in Ghana: Its Forms and Implications. Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru, Pp. 1-10

CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.

DSL Reports (2011), Network Sabotage, Available at http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.

Duah, F. A. & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences,* 4(1), 22 – 34

Federal Republic of Nigeria (1986). *National Policy on Education (2nd Edition).* Yaba: Lagos

Federal Republic of Nigeria (2004). *National Policy on Education (4th Edition).* Yaba: Lagos Federal Republic of Nigeria (2013). *National Policy on Education (6th Edition).* Abuja: Lagos

IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/201.

Jackson T. C. B. J. & Robert, W. E. (2016).Cybercrime and the challenges of socio-economic development in Nigeria. JORIND 14(2), 42-49.

Jackson T. C. B. J. & Robert, W. E. (2016).Cybercrime and the challenges of socio-economic development in Nigeria. JORIND 14(2), 42-49.

Longe, O., Omoruyi, I., & Longe, F. (2016). Implications of the Nigeria Copyright Law for Software Protection. *The Nigerian Academic Forum Multidisciplinary Journal.* 5(1), 7-10.

Longe, O., Omoruyi, I., & Longe, F. (2005). Implications of the Nigeria Copyright Law for Software Protection. *The Nigerian Academic Forum Multidisciplinary Journal.* 5(1), 7-10.

Maitanmi, O., Ogunlere, S., Ayinde, S, & Adekunle, Y, (2013).Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering And Science (IJES)* 2(4), 45-51.

Maitanmi, O., Ogunlere, S., Ayinde, S. & Adekunle, Y. (2013).Impact of cybercrimes on Nigerian Economy. *The International Journal Of Engineering And Science (IJES)* 2(4), 45-51.

Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

Ribadu, N. (2007). Cybercrime and Commercial Fraud: A Nigerian PerspectiveModern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRAL Vienna, 9-12.

Tade, O. & Aliyu, I (2016). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology,* 5(2), 860-875.

Virus Glossary (2006). Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.html. Visited: 28/01/2012