Cybercrime and Computer Science Undergraduate Students in Private Universities in Nigeria: An Empirical Investigation

[1]Nwosu, Jonathan. C. PhD; [2]Adebawojo Bolanle PhD; & [3]Ifeoma Helen Ayeni M.Sc.

[1&3] *Babcock University, Ogun State. Nigeria*
[3]*Babcock University High School, Ogun State. Nigeria*

ABSTRACT
The increasing rate of cybercrimes in Nigeria and other countries of the world has given scholars a great concern. Cybercrime which is a criminal act perpetuated by individuals who have gained expertise in information and communication technology is a major threat to development. With the successful reduction of the world to a global village via information technology, computer science and its related discipline have continued to attract more students. A number of these students use their acquired knowledge to perpetuate crimes. And Crimes committed through cyber space has far reaching effects as its impacts are detrimental to the countries cohesion and development.
The purpose of this study was to explore cybercrime and computer science undergraduate students in private universities in Nigeria. The study adopted cross sectional survey design with a sample size of 1200 students cutting across six (6) private universities in Ogun State. Upon consent, participants were asked to complete the "Intent Towards Internet Fraud Scale (ITIFS). Data was analyzed using simple percentage, t-test and multiple regression. The participants demonstrated a high intent of involving in cybercrime. The results indicated a meaningful difference between male and female undergraduates' computer student. Also, age and students' level was found to be a significant factor predicting intent to involve in cybercrime among the participants.
Thus the study recommends that the educational system should place great emphasis on moral development as it has done in intellectual and social developments because this will help shape the minds of students towards productive ventures other than using their intellectual knowledge for criminal activities.
Keywords *Cybercrime, Computer Science, Undergraduate students, Private Universities.*

I. INTRODUCTION

Nigeria as a nation has moved from agranian society to a more technological advanced community characterized with an increased invention of electronic devices such as modern communication hard-wares, internet service and computer systems. This technological advancement has become an everyday thing in almost every home, while the menace of internet fraud is on the increase.

Though, the importance of advancement in technology is not far-fetched as it is now used in our everyday activities. The usage of computers, and most importantly, the internet is now so common that in homes where computers cannot be afforded, youths desperately resort to using cyber cafés just to have a feel of the internet. Recently, the use of the internet has also been extended to use on the mobile phone i.e. global system of mobile communication. Surfing the web can be done almost anywhere that mobile phones can reach (Egbe, Ojewunmi, & Olasupo, 2013).

Cybercrime as an epidemic is a borderless menace. It cuts across faiths, religious denominations and political systems and affects both young and old, male and female alike. As noted by Odo and Odo (2015) technological advancement in cyber space has made computer an integral component in national development. Criminal activities within the cyberspace are now on a global scale. Mattew (2010) sees cybercrime as any form of crime propagated by any individual through the use of a computer and internet. Debarati and Jaishankar (2011) view cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups), and mobile phones (SMS/MMS).

All over the world today, so many people have embraced cyber-crime as a means of livelihood at the expense of others physical and mental wellbeing. Tade and Aliyu (2011) affirmed that many have become rich through cybercrime while some others have been caught by the law. Folorunso, Vincent, Adekoyo and Ogunde, (2010) conducted a study at university of Agriculture Abeokuta, Ogun State, Nigeria on the 'Diffusion of Innovation in

social Networking sites among university students.' One of the major findings of the study shows that the respondents had attempted to try social networking sites before adopting its uses. Thus, the users of the sites often examine it and probably know the gratifications they could derive from the media before accepting to use any of them Folorunso, et al, (2010).

Chawki (2005) states that educating young people would help decrease the risk of students in cyberspace. Asokhia (2010) finds that the level of education contributes significant differences to the students' perceptions of cybercrime. Knowledge helps people to be more aware on cybercrime (Levin *et al*., 2008). The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies & regulations and sufficient protection of personal information (Choi, 2008; Levin *et al*., 2008; Chawki, 2005; Bougaardt and Kyobe, 2011).

Odo & Odo (2015) investigated the extent of involvement in Cybercrime activities among students' in tertiary institutions in Enugu state of Nigeria. Their findings showed that students of higher institutions in Enugu state are involved in cybercrime. It also showed that students' involvement in cybercrime is dependent on gender and Institution type.

Bamatraf and Al Anouti (2014) investigated the level of knowledge about cybercrimes among young adults within the United Arab Emirates, and found a statistical significant difference in the level of knowledge in terms of student major but not gender. Students specializing in Computer Information Technology (accounting for 21.5% of the participants) had the highest levels of knowledge as compared to all other students from other majors. This was in concordance with another finding in the study which revealed a strong correlation between the level of knowledge and the use of the internet/digital technology. Participants with heavy use of internet technology had a high level of knowledge about cybercrimes.

In Nigeria today, most of the criminal activities being experienced are perpetuated by the youths especially the educated ones (Olaide & Adewole, 2004, Ayodele & Wilson, 2014). Thus, it has become very important to empirically assess the extent of computer science undergraduates' involvement in cybercrime.

.

II PURPOSE OF THE STUDY

The purpose of this study was to explore cybercrime and computer science undergraduate students in private universities in Nigeria with a major focus on Ogun State. This will help the Governments of Nigeria who have displayed a burning desire to curb cybercrime as it poses great danger to its citizens by drastically reducing the nation's capacity for rapid development. Therefore, this study is crucial to the understanding of the factors predicting the intent to involve in cybercrime among Nigerian Undergraduates.

II. HYPOTHESIS

In order to achieve the purpose of this study, three hypotheses were formulated and tested at 95% confidence level.

1. *There is no significant difference between male and female undergraduate computer science students' intent to engage in cybercrime.*
2. *Participants' age will have no significant influence on intent to engage in cybercrime.*
3. *Participants' level of study will have no significant influence on intent to engage in cybercrime.*

III. METHODOLOGY

A. **Research Design:** This study adopted a cross-sectional research design where questionnaire was used to collect data from the respondents on the studied variables.

B. **Participants:** A total of one thousand two hundred (1200) computer undergraduate students from four private universities in Ogun State who had spent at least one full academic year with the institution were selected purposively for this study. The simple random sampling technique was used to select respondents across all the levels, which include 200 through 500 levels. The respondents' age range between 16- 25 years with mean age of 19.36 and standard deviation of 9.10.

C. **Instrumentation:**

The biographical data information sheet was used to collect information on the participants' gender (male or female), age in years, and field of study. Researcher developed questionnaire tagged "Intent Towards Internet Fraud Scale (ITIFS) was used to assess undergraduate computer science students' intent to engaged in cybercrime. The scale consists of 24 statements the use of internet sources for scam activities. The items were answered on a 5-point likert scale ranging from "very likely of me" to "Not very likely of me". The reliability of the ITIFS was ascertained with the use of Guttman split-half coefficient of internal consistency. The result of the analysis yielded a coefficient reliability.79.

D. **Procedure:** A set of questionnaires for assessing biographical data information, technology use, self-efficacy and students' academic standing questionnaire were administered on the sample

through the assistance of two (2) research assistants.

IV RESULTS AND DISCUSSIONS

TABLE I

Table 1: T-test analysis showing difference between male and female undergraduate computer science students' intent to engage in cybercrime

Gender	N	X	SD	Mean diff.	Df	t-cal.	t-crit.	P
Male	671	71.811	15.405	28.318	1198	3.543	1.960	
Female	529	43.493	13.807					Signif icant

Significant at 0.05 alpha level.

The results presented in Table 1 revealed that the obtained value of t is 3.543 for the gender difference in undergraduate computer science students' intent to engage in cybercrime which is higher than the t- critical value of 1.960 at .05 level of significance. This implies that there is a significant gender difference in undergraduate computer science students' intent to engage in cybercrime. Further analysis of the result based on the respondents' mean scores reveal that male undergraduate computer science students had an average mean score of 71.811 higher than their female counterparts with a mean score of 43.493. The implication of this is that male students have higher intention of involving cybercrime compared to their female counterpart.

The outcome of this findings contradicts the findings of Bamatraf and Al Anouti (2014) in their investigation of the level of knowledge about cybercrimes among young adults within the United Arab Emirates, and found no statistical significant gender difference. However, the study lend credence to the findings of Odo & Odo (2015) who investigated the extent of involvement in Cybercrime activities among students' in tertiary institutions in Enugu state of Nigeria and showed that students of higher institutions in Enugu state are involved in cybercrime. It also showed that students' involvement in cybercrime is dependent on gender.

TABLE III

Model summary of the multiple regression analysis between age and intent to engage in cybercrime

Variable	Source of variation	Sum of Square	Df	Means of Square	f-value	Sig.
Age	Regression	63.906	3	21.302		
	Residual	6623.885	1195	5.543	3.843	.003[a]
	Total	6687.791	1198			
	Adjusted R Square = .114, Std. Error of the Estimate = .510					

The research hypothesis which stated that "Participants age will have no significant influence on intent to engage in cybercrime" showed that age ($F_{(3,1198)} = 3.843$; $P < .05$) has a significant influence on intent to engaged in cybercrime among undergraduate computer science in private university in Ogun State. The results further revealed that 11.4% of the variance in the intent to engage in cybercrime among undergraduate computer science was accounted for by age. The implication of this result revealed that intent to engage in cybercrime among undergraduate computer science has something to do with age. This is in tandem with the previous findings that most of the criminal activities being experienced are perpetuated by the youths especially the educated ones (Olaide & Adewole, 2004, Ayodele & Wilson, 2014).

TABLE IIIII

Model summary of the multiple regression analysis between participants' level of study and intent to engage in cybercrime

Variable	Source of variation	Sum of Square	Df	Means of Square	f-value	Sig.
Level of Study	Regression	86.931	3	28.977		
	Residual	4227.860	1196	3.535	8.197	.000[a]
	Total	4314.791	1199			
	Adjusted R Square = .233, Std. Error of the Estimate = 11.203					

The research hypothesis which stated that "Participants' level of study will have no significant influence on intent to engage in cybercrime" showed that level of study ($F_{(3,264)} = 32.455$; $P < .05$) to a great extent will significantly influence undergraduate computer students intent to engaged in cybercrime. The results further revealed that 23.3% of the variance in the intent to engage in cybercrime among the undergraduates was accounted for by level of study. The implication of this result revealed that as students gained more knowledge on computer applications and logics propels their intent to engage in cybercrime or reduced it. This is supported by the findings of Asokhia (2010) that the level of education contributes significant differences to the students' perceptions of cybercrime. Knowledge helps people to be more aware on cybercrime (Levin et al., 2008). Thus, Bougaardt and Kyobe, (2011) noted that the number of cybercrime crimes and victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies & regulations and sufficient protection of personal information.

V CONCLUSION AND RECOMMENDATIONS

Nations all over the world including under-developed ones are becoming global village through technologies (ICTs) into all aspects of daily living not just as a means of economic survival and be more competitive in the global market but to improve daily living of the citizenry.

This study concludes that gender, age and level of study have significant influences on the level at which students will get involved in cybercrime. This study finds that female students are less prone to the involvement of cybercrime compared to their male counterparts. Also, the age of the students and level of study to an extent will influence the willingness and propensity to involve in cybercrime. It should be noted, however, that youths are the leaders of tomorrow and should be given proper education to be able to channel the energy towards more profitable ventures.

As a matter of urgency, government and other related stakeholders and other key player of the Nigerian Economy should try and create more job opportunities for our young graduates in order to alleviate their involvement in negative societal behavior. A better economic system, creation of opportunities for the young Nigerian, would also make a lot differences. Since it was observed that majority of the respondents perceived the involvement of young people in cybercrime as a result of economic condition.

REFERENCES

1) Asokhia, M., 2010. Enhancing national development and growth through combating cybercrime internet fraud: A comparative approach. *Journal of Social Sciences*., 23: 13-19.

2) Ayodele, K. O. & Uzuegbu-Wilson, E. (2012). Corruption in Nigeria: an empirical assessment of public institutions. *Babcock University Socio-legal Journal, 1(2), 218-228.*

3) Bamatraf, S, & Al Anouti, F. (2014). *Assessing the level of knowledge about cybercrimes among young adults within the United Arab Emirates.* Proceedings of The National Conference On Undergraduate Research (NCUR), University of Kentucky, Lexington, KY April 3-5, 2014

4) Bougaardt, G. and M. Kyobe, 2011. Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *Electr. J. Inform. Syst. Evaluat.*, 14: 167-178

5) Chawki, M., 2005. A critical look at the regulation of cybercrime. ICFAI J. Cyberlaw, 3: 1-55.

6) Chen, C.C., B.D. Medlin and R.S. Shaw, 2008. A cross-cultural investigation of situational information security awareness programs. *Inform. Manage. Comput. Security*, 16: 360-376.

7) Choi, K., 2008. *Structural equation modeling assessment of key causal factors in computer crime victimization*. Ph.D Dissertation, Indiana University of Pennsylvania, USA.

8) Folorunso, O. Vineent, R.O., Adekoya, A.F. & Adewal, O.O. (N.d). diffusion of Innovation in Social Networking Sites among University students. *In International Journal of Computer Science and Security* (JCSS), (4) 3, Pp. 361-372.

9) Levin, A., M. Foster, B. West, M.J. Nicholson and T. Hermandez *et al*., 2008. The next digital divide: Online social network privacy. Privacy and Cybercrime Institute, Ryerson University, Canada

10) Matthews, B. (2010) Computer Crimes: Cybercrime Information, Facts and Resources. Retrieved March 3, 2017 from http://www.thefreeresource. com/computer-crimes-cybercrime information-facts and-resources

11) Odo, C. R. & Odo, A. I. (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: Information & Technology*, 15(3), 1-6

12) Olaide, M. and Adewole, R. (2004). *Cyber Crime Embarrassing for Victims.* Retrieved September 2011 from http//www.heraldsun.com.au

13) Shariff, S. and S. Deni, 2005. *An exploratory study of level of awareness and perception towards computer ethics among it educators of institutes of higher learning* in Lembah Klang. Technical Report, Universiti Teknologi MARA, Malaysia

14) Tade, O. and aliyu, I. (2011), Social Organization of Internet fraud among University Undergraduates in Nigeria. *International Journal of cyber Criminology*. 5(2). pp 860-875