

---

## PERCEPTION OF INCIDENCES OF INTERNET CRIMES AMONG TERTIARY INSTITUTION STUDENTS' IN SOUTH-WEST, NIGERIA

*P. A. Amosun, O. A. Ige, and O. M. Adepoju*  
*Department of Teacher Education*  
*University of Ibadan, Ibadan, Nigeria*  
*E-mail: amosuns2002@yahoo.com, olugbengaige@gmail.com*

### **ABSTRACT**

This study investigated the perceptions of incidences of internet crimes among tertiary institution students' in South-West, Nigeria. The study was the descriptive type while a survey method was applied. Five hundred and thirty-five (535) male and female students were involved in the study. The instrument used for data collection is Tertiary Students' Questionnaire on Internet Crime' (TSQIC). Three research questions were answered in the course of the study. Percentage, Mean, and Standard Deviation were used for data analysis. Results indicated that students are not only aware of, but perpetrate all the twenty-two tested internet crimes. The results also show that tertiary students' majorly learn internet crimes through dismissed Information Technology experts in other companies or organizations. The study therefore recommended that further studies be conducted in other states in Nigeria to determine the realistic state of university students' involvement in internet crimes in order to fashion an organized attempt at stemming the tide of internet crime among tertiary institution students' in Nigeria.

**Keywords:** Perception; Internet Crime; Tertiary Institution Students'

### **INTRODUCTION**

The enormous growth in internet connectivity in association with the development of other electronic communication technologies has resulted in changes in many spheres of the society. The internet has become a key element in what is seen as globalization of society, providing technology that recognizes no national boundaries, that has no single owner and that is not regulated or controlled by any single national or international legal framework. Yet, the internet is found in every nation providing information and contact instantaneously to anybody at any point on the globe. Connectivity to the internet with the advantages it provides has ensured that every country is now connected. Some users of the internet have grown up to have an understanding of this super highway of information unlike the old generation of users, and take many faces to commit acts of crime and wrongdoing on the World Wide Web.

This account for the growing problems of internet crime in countries likes United States, Nigeria, Canada, Italy to mention a few. Some crimes committed on the internet have been exposed to the world and some remain a mystery until they are perpetrated against individuals or some companies<sup>[1]</sup>. Internet has changed much in the two decades since it came into existence, it was conceived in the era of time sharing, but has survived into the era of personal computers client server, peer to peer computing and the network computer. The internet was designed before the Local Area Networks (LANs) existed but has

accommodated the new network technology as well as the more recent Automated Teller Machine (ATM) and frame switched services. It was envisioned as supporting a range of functions from file sharing and remote log in to resource sharing, collaboration, spawned e-mail and more recently the World Wide Web. Most importantly, the internet started as the creation of a small band of dedicated researchers and has grown to be a commercial success with billions of dollars of annual investments<sup>[2]</sup>.

Internet crime is the unlawful conduct carried out with the use of computers, electronic and ancillary devices. It is unauthorized access, system interference, data inception, intellectual property theft, fraud and using computers to abuse data and sabotage networks. It also include disruption of network traffic, denial of service attacks or e-mail bombing, creation on distribution of viruses, identity theft, cyber stalking, cyber pornography and cyber squatting etc. Computer crime is a general term that embraces such crime as: phishing, credit card fraud, internet bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, creation and distribution of viruses and spam<sup>[3]</sup>. All these crimes are computer related and facilitated crimes. The Department of Justice in the United States categorizes computer crime in three ways: the computer as a target - attacking the computers of others (spreading viruses is an example); the computer as a weapon - using a computer to commit "traditional crime" that we see in the physical world (such as fraud or illegal gambling); the computer as an accessory - using a computer as a "fancy filing cabinet" to store illegal or stolen information<sup>[4]</sup>. Our view is that the growth of the threat of cyber crime has outpaced that of other cyber security threats consequent on the revelations from the annual internet crime reports.

### **STATEMENT OF THE PROBLEM**

The Internet Crime reports of years 2001 to 2009 put together by the National White Collar Crime Center and the Federal Bureau of Investigation rated Nigeria as one of the top ten countries perpetrator of internet crimes (see <http://www.ic3.state.gov>)<sup>[5]</sup>. The rating of Nigeria in the annual internet crime reports is usually second or third among the top ten countries perpetrators. Also, the age group of the perpetrators is similar to the age group of the secondary to post-secondary students in Nigeria, thus, necessitating the conduct of the study among tertiary students in Nigeria. The contact methods being employed by the scammers reflect the means in-use for communication on the internet by tertiary students in Nigeria. The contact methods comprise the following: Electronic mail (Email), webpage, instant messenger, Physical Mail, Wire, Bulletin Board, Fax, Chartrooms, In Person and Newsgroup<sup>[6]</sup>. Only Bulletin Board and Wire seems to be a rare means of communication among university students in Nigeria. This study, therefore, investigated perception of incidences of internet crimes among tertiary institution students in Southwestern, Nigeria. In addressing the problem of the study and to achieve the purpose of the study, the following research questions were answered:

1. Which of the internet crimes is commonly known to tertiary institution students' in Nigeria?
2. To what extent do tertiary institution students engage in internet crimes in Nigeria?

3. What are the sources of information about internet crimes to tertiary institution students' in Nigeria?

## **MATERIALS AND METHODS**

### **Research Design**

The design employed in the study was the descriptive type while a survey method was applied. The data were collected, analyzed and discussed without any manipulation of the variables involved in the study.

### **Population and Sample**

The population consisted of all the tertiary institutions (universities and polytechnics) in the South West region of Nigeria. Five hundred and Thirty-Five (535) male and female students were chosen at random from the three states (Lagos, Ogun and Oyo) for the study. The tertiary institutions selected for the study were: University of Lagos; Lagos State Polytechnic; University of Ibadan; The Polytechnic Ibadan; OlabisiOnabanjo University, Ago Iwoye; MoshoodAbiola Polytechnic, Abeokuta.

These tertiary institutions were selected due to presence of large internet cafes that were accessible to the students. The questionnaires were handed over to the café attendant who distributed to the first one hundred students that patronized the cafes. The questionnaires were administered in the following internet cafes: PMG Café, New Hall – University of Lagos; Quick Net Café – Lagos State Polytechnic; University ICT Centre – University of Ibadan; Access Point Café – The Polytechnic, Ibadan; TBO Café – OlabisiOnabanjo University, Ago – Iwoye; TMN Café – MoshoodAbiola Polytechnic, Abeokuta.

### **Research Instrument**

The research instrument used is a self-constructed questionnaire tagged 'Tertiary Students' Questionnaire on Internet Crime' (TSQIC). The instrument was used to collect information on students' background, knowledge of internet crimes, extent of students' involvement in internet crimes, sources of information on internet crimes. Section B of the instrument also elicited responses on students' awareness of internet crimes. A four point Likert scale with the following response options were used to gather relevant data for section A: Strongly Agree (4), Agree (3), Disagree (2), and strongly Disagree (1). Two option scales of 'Aware' and 'Not Aware' are used to elicit responses on students' awareness of internet crimes.

### **Validity and Reliability of the Instrument**

The instrument was given to experts in social science education for evaluation who examined the instrument for face and content validity in terms of the phrase used coverage of the seven selected sub-headings and structuring of the questionnaire upon which corrections were done. Of the seven selected sub-headings and structuring of the questionnaire upon which corrections were done, the final form of the items was then validated in terms of administering it on thirty students and a cronbach alpha of 0.70 was obtained.

### **Procedure for Data Collection**

In each of the internet café used in the six (6) selected schools, the instrument was administered to the first one hundred (100) students that patronized the internet café on the day of administration. 526 were gotten from the six selected schools and all the questionnaire were found suitable for analysis. It lasted for about four weeks.

### **Data Analysis and Results**

The data collected were analyzed using Mean (X), Standard Deviation (S.D), and Percentages (%).

### **Results**

R.Q.1: Which of the internet crimes is commonly known to tertiary institution students' in Nigeria?

**Table 1: Students' awareness to common internet crimes**

S/ NO	Statement <b>Types of Internet Crimes</b>	Aware		Not Aware	
		F	%	F	%
1	Nigerian letter fraud ( <b>on – line 419</b> ).	254	47.5	281	52.5
2	Spam (unsolicited electronic mail (e mail).	322	60.2	213	39.8
3	Virus	262	49.0	273	51.0
4	Hacking	298	55.7	237	44.3
5	Piracy	247	46.2	288	53.8
6	The use of another person's name and social security number to obtain goods and services ( <b>identity theft</b> ).	267	49.9	268	50.1
7	A confidence trick in which the target (person) is persuaded to advance a relatively small sums of money in the hope of realizing a much larger gain ( <b>Nigerian letter or 419 frauds</b> ).	242	45.2	293	54.8
8	The non-delivery of an item purchased through the internet auction site on non-payment for goods purchased through an internet auction site ( <b>Auction Fraud</b> ).	278	52.0	257	48.0
9	Using special hacking software that could record the sequence of key strokes those computer users made on their key boards or infiltrate internet banking ( <b>financial institutions fraud</b> ).	281	52.5	254	47.5

10	Kidnapping children via internet chat rooms.	323	60.4	212	39.6
11	Creation and distribution of computer viruses.	213	39.8	322	60.2
12	Asking people to invest in a non-existent business on-line ( <b>Business Fraud</b> ).	295	55.1	240	44.9
13	Illegal Trading	257	48.0	278	52.0
14	Fraud	157	29.3	378	70.7
15	The act of sending an e mail to internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users in to surrendering private information that will be used for identity theft ( <b>Phishing</b> ).	286	53.5	249	46.5
16	Defamatory Libel	260	48.6	275	51.4
17	Cyber Stalking	261	48.8	274	51.2
18	Counterfeit Cashier's Check	242	45.2	293	54.8
19	Obtaining goods without paying or to obtain unauthorized fund from an account ( <b>Credit card fraud</b> ).	326	60.9	209	39.1
20.	Debt Elimination	345	64.5	190	35.5
21.	Employment/Business Opportunities	201	37.6	334	62.4
22.	Investment Fraud	249	46.5	286	53.5

R.Q.2: To what extent do tertiary institution students' engage in internet crimes in Nigeria?

**Table 2: Students' responses on students' involvement in internet crimes**

S/ N O	Statement  <b>Students' involvement in 'Yahoo Yahoo'</b>	Strongly Agree		Agree		Disagree		Strongly Disagree		Mean	Standard Deviation
		F	%	F	%	F	%	F	%		
1.	Students use the credit card of other people to buy goods and services on the internet.	49	9.2	43	8.0	25	47.5	18	35.8	1.9	0.89
2.	Students placed adverts on websites to dispose and defraud users of the internet	13	2.4	61	11.4	28	52.2	17	33.9	1.8	0.72
3.	Students use computer program virus to crash the server of other users	39	7.3	37	6.9	24	45.4	20	38.6	1.8	0.88
4.	Students send electronic mails soliciting for foreign currency in Dollars (\$), Pounds (£), Euro (€) using other peoples identity.	31	5.8	50	9.3	23	43.4	22	41.0	1.8	0.83
5	Students watch sex films showing immoral sexual conducts on the internet.	45	8.4	48	9.0	24	45.5	19	36.7	1.9	0.89
6	Students use another person's name and social security number to obtain goods and services on the internet.	40	7.5	13	24.1	21	39.0	15	28.4	2.1	0.90
7	Students introduce internet users to non existing investment in order to defraud them.	67	12.5	92	17.2	22	41.0	15	29.6	2.1	1.10
8	Students help terrorist groups (Osama's group) to use internet in furthering their agenda.	12	23.7	12	23.7	13	24.2	14	27.9	2.4	1.13
9	Students use special software to hack financial institution websites in order to get bank codes and secret information.	21	3.9	57	10.7	27	51.3	18	34.4	1.8	0.80
10	Students buy goods and services on the internet without paying.	19	37.9	19	37.9	63	11.8	74	13.8	3.0	1.02
11	Students engage in kidnapping children via internet chat rooms.	19	35.0	15	28.2	10	20.8	75	14.0	2.8	1.12
12	Students use bogus and fake company names to defraud other	19	36.5	14	27.6	81	15.1	10	19.3	2.8	1.20

	internet users.										
13	Students use international money transfer agencies (i.e. western union) to carry out a scheme to defraud people.	15 4	28. 8	12 5	23. 4	14 1	26. 4	93	17. 4	2.5 5	1.20
14	Students randomly select email addresses and contacting them they have been selected as the winners of an international lottery.	93	17. 4	15 3	28. 6	20 4	38. 1	85	15. 9	2.5 0	1.00
15	Students illegally go into industry databases, promising to release control back to the company if funds are released.	81	15. 1	16 5	30. 8	17 8	33. 3	11 1	20. 7	2.4 0	1.00
16	Students disguise as Nigerian or foreign Government officials in order to defraud targeted internet users.	11 4	21. 3	11 1	20. 7	25 2	47. 1	58	10. 8	2.5 2	1.00
17	Students disseminate emails which are forged to appear as though it was sent by someone other than the actual source.	63	11. 8	19 3	36. 1	15 9	29. 7	10 7	20. 0	2.3 4	1.00
18	Students manipulate investors resulting in theft of capital	14 6	27. 3	16 2	30. 3	12 2	22. 8	10 5	19. 6	2.6 5	1.10
19	Students steal trade secret, suppliers' agreement, and personal records, research documents or prototype plans for a new product or service.	11 8	22. 1	14 7	27. 5	12 9	24. 1	13 2	24. 7	2.9 0	2.73
20	Students persuade people to invest a relatively small amount of money	10 3	19. 3	13 6	25. 4	19 4	36. 3	10 2	19. 1	2.4 4	1.00

R.Q.3: What are the sources of information about internet crimes to tertiary institution students' in Nigeria?

**Table 3: Students' responses on sources of information about internet crimes**

S/ N O	Statement Sources of Information	Strongly agree		Agree		Disagree		Strongly disagree		Me an  X	Standar d Deviatio n  S.D
		F	%	F	%	F	%	F	%		
1.	Students learn yahoo yahoo from their friends in Universities, Polytechnics, and colleges of Education.	141	26. 4	146	27. 3	112	20. 9	136	25. 4	2.5 0	1.15

2.	Students learn Yahoo Yahoo from IT experts in companies or organizations.	136	25.4	111	20.7	168	31.4	120	22.4	2.51	1.12
3.	Some Newspapers and Magazines do teach students how to do yahoo yahoo	51	9.5	177	33.1	160	29.9	147	27.5	2.24	1.10
4.	There are websites that teach students how to do yahoo yahoo.	83	15.5	171	32.0	152	28.4	129	24.1	2.40	1.02
5	Students recruit other students into 'Yahoo Boys' club.	72	13.5	137	25.6	172	32.1	154	28.8	2.23	1.01
6	Students who engage in yahoo yahoo are often initiated by their friends.	24	4.5	45	8.4	224	41.9	242	45.2	2.10	1.00
7	Students get the gist on Yahoo Yahoo from foreign yahoo yahoo professionals.	57	10.7	39	7.3	219	40.9	220	41.1	1.81	0.93

### **Discussion**

The study answered three research questions related to commonly known internet crimes among tertiary institution students, extent of tertiary institution involvement in internet crimes and students' sources of information about internet crimes. The results from table 1 show that tertiary institution students are aware of all the various internet crimes being perpetrated in Nigeria. The analysis shows that the most common internet crimes they are aware of: Spam (60.2%), Hacking (55.7%) Auction (52.0%), Financial Institution Fraud (52.5%), Kidnapping via chat rooms (60.4%), Business Fraud (55.1%), Phishing (53.5%), Credit Card Fraud (60.9%) and Debt elimination (64.5%). Credit Card Fraud has the highest frequency of 60.9%; the use of credit card is a relatively new feature of the economy in Nigeria. It may not be out of place to infer that those being defrauded on the internet are citizens of the developed nations of the world.

Table 2 shows that students use the credit card of other people to buy goods and services on the internet ( $\bar{x} = 1.91$ , S.D = 0.89); placed adverts on websites to defraud users of the internet ( $\bar{x} = 1.83$ , S.D = 0.72); use computer virus to crash the internet server of other users ( $\bar{x} = 1.80$ , S.D = 0.88); use electronic mails to solicit for foreign currency in Dollars (\$), Pounds (£), using other peoples identity ( $\bar{x} = 1.80$ , S.D = 0.83); watch immoral sexual conducts on the internet ( $\bar{x} = 1.80$ , S.D = 0.83); used another person's name and social security number to obtain goods and services on the internet ( $\bar{x} = 2.10$ , S.D = 0.90); introduces internet users to non existing investment opportunities with the intent of defrauding them ( $\bar{x} = 2.13$ , S.D. = 1.10); helps terrorist groups (Osama group) to use



internet in furthering their agenda ( $\bar{x} = 2.43$ , S.D. = 1.13), use special software to hack financial institution websites in order to get bank codes and secret information ( $\bar{x} = 1.84$ , S.D = 0.80); buy goods and services on the internet without paying ( $\bar{x} = 3.0$ , S.D = 1.02) engage in kidnapping children via internet chat rooms ( $\bar{x} = 2.82$ , S.D = 1.12); use bogus and fake company names to defraud other internet users ( $\bar{x} = 2.80$ , S.D = 1.20); use international money transfer agencies to carry out a scheme to defraud people (Western Union) ( $\bar{x} = 2.55$ , S.D = 1.20); randomly select email addresses contacting them they have been selected as the winners of an international lottery ( $\bar{x} = 2.50$  S.D = 1.0); illegally hack into industries databases promising to release control back to the companies on release of demanded funds ( $\bar{x} = 2.40$ , S.D = 1.0); disguise as Nigerian or foreign government officials in order to defraud targeted internet users ( $\bar{x} = 2.52$  S.D = 1.0); disseminate emails which are forged to appear as though it was sent by someone other than the actual source ( $\bar{x} = 2.34$ , S.D = 1.0); deceive and manipulate investors resulting in theft of capital ( $\bar{x} = 2.65$ , S.D = 1.10); steal trade secret, suppliers' agreement, personal records, research documents or prototype plans for a new product or service ( $\bar{x} = 2.90$ , S.D = 2.73); persuade people to invest a relatively small amount of money with the promise of giving a larger amount of money at a later date on the internet ( $\bar{x} = 2.44$ , S.D = 1.00). The buying of goods and services on the internet has the highest mean score ( $\bar{x} = 3.0$ , S.D = 1.02), this reveals that tertiary institutions 'shop lift' on the internet from companies in the developed nations and not Nigeria.

Table 3 shows that tertiary institution students learn internet crimes otherwise known as 'Yahoo Yahoo' from these sources: Friends in universities, polytechnics and Colleges of Education ( $\bar{x} = 2.50$ , S.D = 1.15); dismissed Information Technology experts in other companies or organizations ( $\bar{x} = 2.51$  S.D. = 1.12); Newspaper and Magazine ( $\bar{x} = 2.24$ , S.D = 1.10); Websites ( $\bar{x} = 2.40$ , S.D = 1.02); Yahoo Boyz' Clubs ( $\bar{x} = 2.23$ , S.D = 1.01); friends ( $\bar{x} = 2.10$ , S.D = 1.0); Self learning ( $\bar{x} = 2.23$ , S.D = 1.02); top government officials ( $\bar{x} = 2.81$ , S.D = 1.01) and foreign 'Yahoo Yahoo' professionals ( $\bar{x} = 1.81$ ; S.D. = 0.93). Learning internet crime through dismissed Information Technology experts in other companies or organizations ( $\bar{x} = 2.51$  S.D. = 1.12) has the highest mean score. This may account for the relatively ease of navigation on the World Wide Web by the internet scammers in Nigeria. It takes an information technology professional wield the dexterity that internet scammers in Nigeria used to scam their victims.

## CONCLUSION

This study investigated the perceptions of incidences of internet crimes among tertiary institution students' in southwestern, Nigeria. The results of the study have highlighted the commonly known internet crimes to tertiary institution students, extent of tertiary institution students' involvement in internet crimes, sources of information to tertiary institution students on internet crimes. It is suggested that further studies be conducted in other states in Nigeria to determine the realistic state of university students' involvement in internet

crimes. This will aid the government to fashion an organized attempt at stemming the tide of internet crimes in Nigeria. In addition to efforts being put in place to arrest the incidence of internet crimes by Economic and Financial Crimes Commission (EFCC), internet crime prevention education should be incorporated into the curriculum of civic and social studies education in Nigeria. This, it is believed will help students to learn the ideals of good citizenship and shun acts that can negatively impair on the integrity of Nigeria. The views represented in this paper, and any errors that accompany them, are, of course, ours.

### **ACKNOWLEDGEMENT**

We humbly express our appreciation to The National White Collar Crime Center and The Federal Bureau of Investigation in United States of America for providing The Internet Crime Reports on their website at no cost.

### **REFERENCES**

1. Kahn, R.E and Cerf, V.G. 1999. What is the Internet [And what makes it work]. Retrieved Nov. 5, 2006 from <http://www.isoc.org/internet/history/brief.shtm>  
Ige, O.A. 2010. Secondary School students' perceptions of incidences of internet crimes among school age children in Oyo and Ondo states. Retrieved May 24, 2010 from [http://www.kaspersky.com/it\\_conference](http://www.kaspersky.com/it_conference).
2. Leiner, B.M. Cerf, V.G; Clark, D.D. Kahn, R.E. Klenrock, L. Lynch, D.C. Postel, J. Roberts, L.G. and Wolff, S. 2003. A brief history of the internet. Retrieved Nov. 5, 2006 from <http://www.isoc.org/internet/history/brief.shtm>.
3. Amosun, P.A. and Ige, O.A. 2009. Internet Crime: A new breed of crime among in-school aged children in Nigeria. *The African symposium*. 9 (20): 90-98. ISSN Tx 6-342-323.
4. The United States Mission to European Union. 2004. Justice Department targets online fraud, Attorney General says. Retrieved Apr. 4, 2007 from <http://useu.usmission.gov/Brussels/Belgium>
5. The National White Collar Crime Centre. 2010. IC<sub>3</sub> 2009 Internet crime report (January 1, 2009 to December 31, 2009). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
6. The National White Collar Crime Centre. 2002. IC<sub>3</sub> 2001 Internet crime report (January 1, 2001 to December 31, 2001). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
7. The National White Collar Crime Centre. 2003. IC<sub>3</sub> 2002 Internet crime report (January 1, 2002 to December 31, 2002). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.

8. The National White Collar Crime Centre. 2004. IC<sub>3</sub> 2003 Internet crime report (January 1, 2003 to December 31, 2003). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
9. The National White Collar Crime Centre. 2005. IC<sub>3</sub> 2004 Internet crime report (January 1, 2004 to December 31, 2004). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
10. The National White Collar Crime Centre. 2006. IC<sub>3</sub> 2005 Internet crime report (January 1, 2005 to December 31, 2005). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
11. The National White Collar Crime Centre. 2007. IC<sub>3</sub> 2006 Internet crime report (January 1, 2006 to December 31, 2006). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.
12. The National White Collar Crime Centre. 2008. IC<sub>3</sub> 2007 Internet crime report (January 1, 2007 to December 31, 2007). Retrieved May 24, 2010 from <http://www.IC3.state.gov.Pg.1-29>.