

## Awareness and Involvement in Cybercrime among Undergraduate Students in Universities In Rivers State, Nigeria

Chinyere. Amini-Philips

Department of Educational Management University of Port Harcourt

Corresponding Author: Chinyere. Amini-Philips

---

**ABSTRACT:** *This study examined the level of awareness and involvement in cybercrime among undergraduate students in universities in Rivers State. Two research questions and two corresponding null hypotheses guided the study. A sample of 2600 undergraduate students was used with the help of stratified random sampling technique. A Questionnaire titled “Undergraduate Students Awareness and Involvement in Cybercrime Questionnaire (USAICQ) with a reliability coefficient of 0.81, was used for data collection. The descriptive statistics of mean and standard deviation were used to answer the research questions while the z-test statistics was used to test the null hypotheses at 0.05 alpha level of significance. It was found out among others that the aggregate mean set value of 3.37 is greater than the criterion mean value of 2.50 which implies that undergraduate students are very much aware of the cybercrimes. It was recommended among others that government and the university community should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with attendant adverse consequence of jeopardizing their educational accomplishment when convicted.*

**KEYWORDS:** *Awareness, Involvement and Cybercrime*

---

Date of Submission: 03-12-2017

Date of acceptance: 03-01-2018

---

### I. Introduction

Cybercrime in our contemporary society is one of the words frequently used by individuals. To understand the true meaning of cybercrime, there is the need to understand the slit meaning of cyber and crime. The term “cyber” is a prefix used to describe an idea as part of the computer and information age and “crime” can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. Cybercrime is defined as offence that is committed against individual or group 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 and mobile phones (Haider & Jaishankar, 2011). The reason for increase in cybercrime is not farfetched owing to the fact that they gain easy access to android phones, tablets, computers, internet and network facilities. Such crimes may threaten a nation’s security and financial health (Saul, 2007). Cybercrime can simply be explained as crimes carried out with the aid of a computer system.

The internet has offered a lot of platforms for useful research purposes; however, cybercrime is a worldwide problem that is costing countries billions of dollars. In Nigeria, cybercrimes seem to be perpetrated by people of all ages ranging from young to old, but in most recent instances the young appear to be the worst offenders. Akpan (2016) reported that cybercrime has put the Nigerian students in a serious quest for money other than the real deal of getting university education. Several youth engage in cybercrime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many. Ngozi (2016) submitted that the rate at which Nigerian youths are involving in one form of cybercrime or the other calls for urgent concern. Going by the nature that cybercrime can tarnish the image and reputation of organizations, institutions and individuals, it becomes very imperative; however, to investigate the level of awareness and involvement of university students in Rivers State in Cybercrime.

### II. Statement Of The Problem

The fundamental purpose of university education is the preparation of students for the future. Graduates of today and tomorrow are to flourish in the modern, fast-paced, high-tech world and as such, must have information seeking capacity and technology skills. These students must be information and technology

literate. The means of acquiring this literacy must be embedded in learning programmes and be part of students educational experience.

However, few undergraduates in universities and other higher institutions of learning in Nigeria may be aware of the cybercrimes carried out with the aid of a computer system otherwise called cybercrime, while very many may be unaware. Some of them may have been involved and even master-mind such a crime. Cybercrime appears to be a common practice among some Nigerians especially undergraduates including those who live in Rivers state. Such practice is associated with some obvious problems. The victims of cybercrime usually the gullible, go through serious pains (emotional/psychological) as they are duped of their hard earned money by fraudsters, who may even be their own children/relatives. There are cases of death by suicide arising from cybercrime. This is especially when victims think that all their lives have been taken away as a result of colossal lost in their money and investment. Sometimes perpetrators are caught and arrested, tried in courts and jailed for life. Sometimes parents of the victims caught die because they are not able to withstand the shame and trauma arising from their children/wards involvement in cybercrime. Moreover, the prevalence of cybercrime gives a country a bad image in the comity of nations. It also may threaten a nation's security and financial health. Students are now taking pleasure in defrauding public and private organizations as well as their fellow students at the expense of their academic pursuit. If this anomaly is not given urgent attention and remediation, our higher institution will become a place where criminals are groomed in order to defraud the school management and the society at large. This study is therefore set out to find out the level of awareness and involvement of undergraduate students in Rivers state in cybercrime.

### **III. Aim And Objectives**

The aim of this study is to determine the level of awareness and involvement of undergraduate students in cybercrime in Universities in Rivers State. Specifically, the objectives are to:

1. find out the level of awareness of undergraduate students on cybercrime in public universities in Rivers State.
2. determine the involvement level on cybercrime of undergraduate students in public universities in Rivers State.

### **IV. Research Questions**

1. What is the level of awareness of undergraduate students on cybercrime in public universities in Rivers State?
2. What is the involvement level on cybercrime of undergraduate students in public universities in Rivers State?

### **V. Hypotheses**

1. There is no significant difference between the mean scores of male and female undergraduate students on the level of awareness in cybercrime in public universities in Rivers State, Nigeria.
2. There is no significant difference between the mean scores of male and female undergraduate students on the level of involvement in cybercrime in public universities in Rivers State, Nigeria.

### **VI. Methodology**

The study adopted a descriptive research design. The population of the study consisted of all 44,500 students from University of Port-Harcourt (Uniport), 22,400 from Rivers State University and 15,000 students from Ignatius Ajuru University. A sample size of 4095 (1375 female and 2720 male students) was drawn from the population. The Taro Yamene's formula gave the minimum sample size of 396 that justifies the use of 5% of the population. Proportionate stratified random sampling technique was used in order to capture the subgroups which are male and female students. The instrument titled Undergraduate Students Awareness and Involvement in Cybercrime Questionnaire (USAICQ) was used for data collection. The USAICQ has two parts of 1 and 2. Part 1 contains the demographic information of the respondents while part 2 contains 11 items on Awareness and 11 items on involvement respectively. Part 2 on awareness was structured thus: Very Much Aware, Much Aware, Less Aware and Not Aware while Involvement was structured Very Much Involved, Much Involved, Less Involved and Not Involved. Face and content validities were ensured. The Cronbach Alpha internal consistency method was used to establish the reliability coefficient of USAICQ to be 0.81. The descriptive statistics of mean and standard deviation were used to answer the research questions while z-test statistics was used to test the null hypotheses at 0.05 alpha level.

### **VII. Results**

The results of this study are presented as shown below

#### **Research Question One**

What is the level of awareness of undergraduate students on cybercrime in public universities in Rivers State?

**Table 1:** Mean and standard deviation scores on the level of awareness of undergraduate students on cybercrime

| s/n | Items   | Male students |      | Female students |       | Mean set | Rank             | Remarks |
|-----|---|---------------|------|-----------------|-------|----------|------------------|---------|
|     |   | x             | Sd   | x               | Sd    |          |                  |         |
| 1   | Online drug trafficking   | 3.27          | 1.09 | 3.42            | 1.08  | 3.35     | 4 <sup>th</sup>  | VMA     |
| 2   | Cyber stalking  | 3.23          | 0.96 | 3.22            | 1.15  | 3.25     | 9 <sup>th</sup>  | MA      |
| 3   | Email hack  | 3.37          | 0.99 | 3.06            | 0.79  | 3.22     | 10 <sup>th</sup> | MA      |
| 4   | Hacking of organizational account                                 | 3.33          | 0.73 | 3.22            | 0.96  | 3.28     | 8 <sup>th</sup>  | MA      |
| 5   | identity theft (this is the impersonation of somebody)            | 3.32          | 0.91 | 3.28            | 1.08  | 3.30     | 6 <sup>th</sup>  | VMA     |
| 6   | Encrypting of files using public-key                              | 3.73          | 0.58 | 3.42            | 0.72  | 3.80     | 1 <sup>st</sup>  | VMA     |
| 7   | Online spam sending   | 3.47          | 0.83 | 3.17            | 0.92  | 3.32     | 5 <sup>th</sup>  | VMA     |
| 8   | Floation of illegal business proposal (phishing)                  | 3.37          | 0.96 | 3.22            | 0.93  | 3.29     | 7 <sup>th</sup>  | MA      |
| 9   | Cybercrime with direct contact through phone (social engineering) | 3.05          | 1.24 | 3.39            | 1.05  | 3.21     | 11 <sup>th</sup> | MA      |
| 10  | The use of remote administrative tools                            | 3.73          | 0.55 | 3.75            | 0.55  | 3.74     | 2 <sup>nd</sup>  | VMA     |
| 11  | Online child sexual abuse material                                | 3.08          | 0.96 | 3.69            | 0.82  | 3.39     | 3 <sup>rd</sup>  | VMA     |
|     |   | 36.95         | 9.80 | 36.84           | 10.05 | 37.03    |                  |         |
|     |   | 3.36          | 0.89 | 3.35            | 0.91  | 3.37     |                  |         |

**Legend: Very Much Aware (VMA), Much Aware (MA), Low Aware (LA) and Not Aware (NA)**

Table 1 shows that the items with serial numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 & 11 have their various mean values greater than the criterion mean value of 2.50 and therefore implies that undergraduate students are aware of the cybercrimes. The aggregate mean set value of 3.37 is also greater than the criterion men value of 2.50 showing that undergraduate students are very much aware of the cybercrimes.

**Research Question Two**

What is the involvement level in cybercrime of undergraduate students in public universities in Rivers State?

**Table 1:** Mean and standard deviation scores on the level of involvement of undergraduate students on cybercrime

| s/n | Items   | Male students |      | Female students |       | Mean set | Rank             | Remarks |
|-----|---|---------------|------|-----------------|-------|----------|------------------|---------|
|     |   | x             | Sd   | x               | Sd    |          |                  |         |
| 11  | Online drug trafficking   | 3.56          | 0.88 | 2.95            | 1.05  | 3.26     | 8 <sup>th</sup>  | MI      |
| 12  | Cyber stalking  | 3.39          | 0.87 | 3.53            | 0.72  | 3.46     | 2 <sup>nd</sup>  | VMI     |
| 13  | Email hack  | 3.31          | 1.12 | 3.17            | 1.03  | 3.32     | 5 <sup>th</sup>  | VMI     |
| 14  | Hacking of organizational account                                 | 3.06          | 0.04 | 3.58            | 0.67  | 3.39     | 4 <sup>th</sup>  | VMI     |
| 15  | identity theft (this is the impersonation of somebody)            | 3.31          | 0.89 | 3.27            | 1.13  | 3.29     | 7 <sup>th</sup>  | MI      |
| 16  | Encrypting of files using public-key                              | 3.31          | 0.79 | 3.56            | 0.88  | 3.44     | 3 <sup>rd</sup>  | VMI     |
| 17  | Online spam sending   | 3.06          | 0.71 | 3.39            | 0.73  | 3.23     | 9 <sup>th</sup>  | MI      |
| 18  | Floation of illegal business proposal (phishing)                  | 3.31          | 0.74 | 3.31            | 0.77  | 3.31     | 6 <sup>th</sup>  | VMI     |
| 19  | Cybercrime with direct contact through phone (social engineering) | 3.70          | 0.35 | 3.35            | 0.74  | 3.53     | 1 <sup>st</sup>  | VMI     |
| 20  | The use of remote administrative tools                            | 2.10          | 1.10 | 2.34            | 1.21  | 2.22     | 11 <sup>th</sup> | NI      |
| 21  | Online child sexual abuse material                                | 2.90          | 1.24 | 2.66            | 1.20  | 2.78     | 10 <sup>th</sup> | LI      |
|     |   | 35.01         | 8.73 | 35.11           | 10.13 | 35.23    |                  |         |
|     |   | 3.18          | 0.79 | 3.19            | 0.92  | 3.20     |                  |         |

**Legend: Very Much Involved (VMI), Much Involved (MI), Less Involved (LI) and Not Involved (NI)**

Table 2 revealed that items with serial numbers 11, 12, 13, 14, 15, 16, 17, 18, 19 & 20 have their various mean value above the criterion mean value of 2.50, therefore, undergraduate students are involved in these cybercrimes. The aggregate mean set value of 3.20 shows that undergraduate students are very much involved in cybercrimes.

**Hypothesis One**

There is no significant difference between the mean scores of male and female undergraduate students on the level of awareness in cybercrime in public universities in Rivers State, Nigeria.

**Table 3:** z-test calculation of the mean differences between male and female undergraduate students on their level of awareness of cybercrime

| Category        | N    | x    | Sd   | Df   | z-cal. | z-crit. | Remark                                   |
|-----------------|------|------|------|------|--------|---------|--|
| Female students | 1375 | 3.36 | 0.89 | 4093 | 0.33   | 1.96    | Hypothesis not statistically significant |
| Male students   | 2720 | 3.35 | 0.91 |      |        |         |  |

Table 3 showed that female students have mean and standard deviation scores of 3.36 and 0.89, while the male students have mean and standard deviation scores of 3.35 and 0.91 respectively. With a degree of freedom of 4093, it is shown that the calculated z-test value of 0.33 is less than the critical z-test value of 1.96, therefore, the null hypothesis is accepted.

### **Hypothesis Two**

There is no significant difference between the mean scores of male and female undergraduate students on the level of involvement in cybercrime in public universities in Rivers State, Nigeria.

**Table 4:** z-test calculation of the mean differences between male and female undergraduate students on their level of involvement in cybercrime

| Category        | N    | x    | Sd   | df   | z-cal. | z-crit. | Remark                                   |
|-----------------|------|------|------|------|--------|---------|--|
| Female students | 1375 | 3.18 | 0.79 | 2580 | 0.50   | 1.96    | Hypothesis not statistically significant |
| Male students   | 2720 | 3.19 | 0.92 |      |        |         |  |

Table 4 showed that female students have mean and standard deviation scores of 3.18 and 0.79, while the male students have mean and standard deviation scores of 3.19 and 0.9 respectively. With a degree of freedom of 4093, it is shown that the calculated z-test value of 0.50 is less than the critical z-test value of 1.96, therefore, the null hypothesis is accepted.

## **VIII. Discussion Of Findings**

The findings of the study are discussed as shown below

### **Students' Awareness of Cybercrimes**

The study revealed that students are aware of these cybercrimes: online drug trafficking; cyber stalking; email hacking; hacking of organizational account; identity theft; encrypting of files using public-key; online spam sending; floatation of illegal business proposal; cybercrime with direct contact through phone; the use of remote administrative tools and online child sexual abuse material. Their level of awareness is very high as buttressed by the aggregate mean set value of 3.20 which is greater than the criterion mean value of 2.50. The finding is in line with the finding of Ben (2017) when he found out that up to 90% of undergraduate students are very much aware of cybercrime and its activities. The finding does not also agree with the finding of Adanma (2017) when she found out that the awareness level of undergraduate student in cybercrime is still not fully ascertained.

### **Students' Involvement in Cybercrime**

The findings showed that students are involved in cybercrime in the areas of: online drug trafficking; cyber stalking; email hacking; hacking of organizational account; identity theft; encrypting of files using public-key; online spam sending; floatation of illegal business proposal; cybercrime with direct contact through phone; the use of remote administrative tools and online child sexual abuse material. The students in their various responses have shown that they have been involved in one form of cybercrime or the other in their various institutions. This finding is in line with the finding of Ngozi (2016) when she reported that the quest for money has made Nigerian youths to deeply involve themselves in cybercrime. She further found out that most of these students are deeply involved in cybercrime alongside their counterparts in the school. Denga (2011) disagreed vehemently with the finding of this study when he found out that undergraduates are fully occupied with academic and vocational activities that can make them associate with cyber theft.

## **IX. Conclusion**

Based on the findings, it is concluded that undergraduate students are very much aware of cybercrime and are very much involved in cybercrime activities.

## **X. Recommendations**

Based on the conclusion, the following recommendations were made:

1. It is recommended that government and the university community should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with attendant adverse consequence of jeopardizing their educational accomplishment when convicted.

2. Students should not be allowed by the school security network and administration to have account breaker devices and encryption keys installed in their electronic gadgets.

#### **References**

- [1]. Adanma, J. (2017). Awareness level of undergraduate students and cybercrime among undergraduate students in South-East zone of Nigeria. *Journal of Social Media Review*, 5(3), 20-29.
- [2]. Akpan, C. (2016). University students and cybercrime: An indispensable critical review. *Journal of Sociology*, 2(2), 181-186.
- [3]. Ben, F. (2017). Cybercrime awareness level of students: The media role. *Journal of Social Development*, 4(2), 92-101.
- [4]. Denga, A. (2011). Youths and cyber theft. Lagos: Ademola Publishers
- [5]. Halder, D., & Jaishankar, K. (2011). *Cybercrime and the victimization of women: Laws, rights and regulations*. Hershey, PA, USA: IGI Global.
- [6]. Ngozi, S. (2016). Students' perception of cybercrime and its implications. *Journal of Social Development*, 4(2), 50-57.
- [7]. Saul, H. (2007). *Social network launches worldwide spam campaign*. New York Times.

Chinyere. Amini-Philips "Awareness And Involvement In Cybercrime Among Undergraduate Students In Universities In Rivers State, Nigeria". *International Journal of Humanities and Social Science Invention(IJHSSI)*, vol. 7, no. 3, 2018, pp. 39-43.