2018

The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region

Kwaku Anhwere Barfi Mr.
University of Cape Coast, kwaku.barfi@ucc.edu.gh

Paul Nyagorme Dr.
University of Cape Coast, pnyagorme@ucc.edu.gh

Nash Yeboah Mr.
Sunyani Senior High School, yeboahnash@gmail.com

Introduction

The use of internet has facilitated business communication tremendously. However, Magele (2005) observed that the internet usage has become a double-edged sword providing opportunities for individuals and organisations and also bringing with it an increased information security risk. The desktop computers, as well as mobile devices such as laptops, smart phones and tablets that are connected wirelessly, have easy access to corporate networks and information. All these connectivity have made business and learning incredibly complicated.

There is no doubt that internet has changed the way business is conducted. The rapid changes in computer connectivity and innovation in digital technology provide numerous benefits to human life but it is not out of side effect such as cybercrime. Cybercrime is a new wave of crimes using internet facilities, which needs to be addressed urgently and earnestly by policy planners to protect the young generation as there is a high risk of becoming a victim of this crime (Mensch & Wilkie, 2011).

However, this change has come with associated risks, commonly referred to as cybercrime. Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission (Halder & Aishankar, 2011). Also, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking, stealing identities or violating privacy. Cybercrime is any illegal act committed using a computer network. Cybercrime is a subset of computer crime. Cybercriminals is not about hackers. They use the net as a tool of the crime for white collar crime, computer con artists, hackers, crackers and network attackers. In their study, Longe, Ngwa, Wada, Mbarika and Kvasny

(2010), long viewed Africa as flawless gem. They further reported that, Ghana has gained the unsavory distinction along with Anglophone African neighbors Nigeria and Cameroon as one of the top ten cybercrime generating states worldwide.

One of the notable reported case that occurred in Ghana was when Robert Wexler, a U.S. Congressman in Florida was communicated by a Ghanaian young man of age 27 in an attempt to blackmail Robert with information that was pilfered from Robert's rejected internal hard drive that had had its way to Ghana through importation of used computer market (Abugri, 2011, as cited in Warner, 2011). This case is not unique and will never be until appropriate measures have been adopted to clean up Ghana internet space. The study is part of this effort.

Statement of the Problem

Cybercrime has become a cankerworm eating very deep into social fiber of Ghanaian youth. Research findings on the profile of cybercrime in Ghana paint a very worrying picture which calls for concern (Warner, 2011). This concern even gets more disturbing when available literature indicates that, Ghana is named among the top ten countries in the world with high cybercrime prevalence. This revelation raises doubts about the role all have in providing information that will educates the public and for the government to take measures to minimise the growing cybercrime menace in the country.

Unfortunately, there is little research that has been conducted in cybercrime issues in Ghana. Moreover, there is little research that has been conducted in Ghana on how students perceive cybercrime issues, thereby leaving

the issue to perceptions and speculations. These are significant deficiencies in existing knowledge on cybercrime, because citizens and policy makers are denied vital information on the subject. This gap in research necessitated this study. To help contribute to the global war against cybercrime, an empirical investigation into students' awareness of Internet users towards cybercrime: evidence from Sunyani High School.

Research Objectives

More specifically, the main research questions are:

1. Assess the awareness level of students towards cybercrime issues?
2. Identify the forms of cybercrime in Ghana?
3. Identify the consequences involved in engaging in cybercrime?
4. What are the Challenges in Addressing Reported Cases of Cybercrime?

The following hypotheses were formulated to be tested:

H_o 1: There is no statistically significant difference between the knowledge of male and female students towards cybercrime.

H_o 2: There is an association between students' awareness of cybercrime and age group.

H_o 3: There is an association between awareness of cybercrime and programme level.

Review of Related Literature

Cybercrime has been a global phenomenon over the years. Inappropriate policies and procedures in handling cybercrime issues are of great concern to many researchers. Guillaume and Fortinet (2009) revealed that lack of procedures for digital evidence and knowledge of the law also pose legal threats to cyber

security checks. However, handling digital evidence is accompanied with unique challenges and requires specific procedures in gathering evidence.

Awareness of cyber issues is very necessary. Curtis and Colwell (2000) indicated that knowledge is very important for young people to prevent cybercrime (Chawki, 2005). Educating young people would decrease the risk of students in cyberspace. Asokhia (2010) found that the level of education contributes significantly to students' perception of cybercrime. Knowledge helps people to be more aware of cybercrime (Levin et al., 2008).

Theoretical framework

The study employs social strain theory to explain how existing societal structures could lead people into social vices like crime. Social strain theory appears to suggest that certain strains increase the likelihood of crime. Individuals who experience these strains become upset, and therefore tend to undertake crime as a coping mechanism (Yeboah, 2015). The theory emphasizes that social structures may pressure citizens to commit crimes.

Cybercrime in Ghana

Cybercrime in Ghana takes various forms. Burrell (2008) indicated that internet scamming/cybercrime in Ghana was an extension of a more benign practice: writing to foreign pen pals (boyfriends, girlfriends or relationships). Some of the young people who were involved in this practice valued these relationships primarily as strategic affiliations for realising material gain.

Warner (2011) noted that cybercrime is a relatively new phenomenon in Ghana that gained prominence in the country between 1999 to 2000. Warner

identified three main forms of cybercrimes prevailing in the country, namely: identity fraud, fake gold dealers and estate fraud. However, Warner (2011) concedes that the list is not exhaustive given the fact that technology keeps evolving by the day.

Research Methodology

Considering the nature of the research problem, the most appropriate research methodology that was used is the descriptive survey design. Descriptive survey design according to Amedahe and Gyimah (2003) makes use of various data collection techniques involving questionnaire. Descriptive design makes it possible for researchers to collect information about target audience without having to deal with the entire population.

For the purpose of this study, the entire population of students in Sunyani Senior High School was used. The population of students in Sunyani Senior High School is 1,505. Students in first to third years were randomly selected using purposive sampling. In all, 200 students were selected from the various programmes. The simple random sampling technique adopted gave every student an equal, calculable and non-zero probability of being selected for the study.

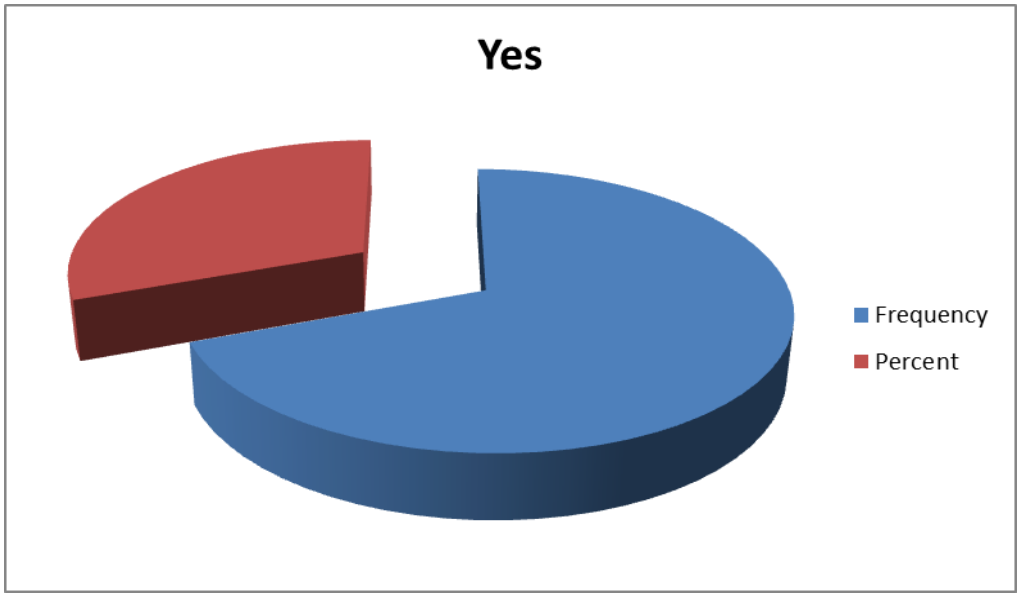
Questionnaire was administered by the researchers themselves and was completed on the spot by most respondents. Thus, the return rate was 100%. Statistical Product and Service Solutions (SPSS) was used for the analysis.

Result and Discussion

The analysis of demographic data was that 60.0% of the respondents are male and 40.0% are female. 25.4% (majority) of the respondent are in the age group of 15-17; 42.73% (majority) of the respondents are science students; 31.6% (majority) of the respondents are in the second year; 71.3% (majority) of the respondents' use internet for 2-4 hours; 32.2% (majority) of the respondents have knowledge of worst known threats hackers and 56% (majority) have knowledge of cyber fraud.

Research Question 1: What is students' awareness level of cybercrime in Ghana?

This question sought to establish students' awareness about cybercrime issues. Some indicators of awareness on cybercrime were used to collect data. There were mixed responses to this question. Respondents were asked if they have heard about cybercrime and the details are presented in figure 1.



Source: Field survey, 2017.

Figure 1: Respondents Awareness on Cybercrime

Figure 1 shows that as many as 160 (80.0%) of the respondents responded in the affirmative that they have heard about cybercrime. The remaining 40 (20.0%) responded in the negative. A deduction from the above is that, majority of the respondents have heard about cybercrime. The finding supports the work of Bakhoum et al., (2014) who concluded that majority of the student have heard about cybercrime.

Students were further asked to indicate their knowledge level on cybercrime issues and the details of are provided in Table 1.

Table 1: Distribution of Respondents Knowledge on Cybercrime

Knowledge on Cybercrime	Frequency	Percent
Crimes committed using computer or its system as tool (Cyber-enabled)	30	15.0
Crimes committed using computer as the target (Cyber-dependent)	60	30.0
All the above	110	55.0

Source: Field survey, 2017.

Table 1 reveals that few of the respondents believe cybercrime was either cyber-enabled 30 (15.0%) or cyber-dependent 60 (30.0%). However, an majority of students 110 (55.0%), believed that cybercrime was both cyber-enabled and cyber-dependent. In other words, majority of the respondents had what we can call a comprehensive knowledge of cybercrime. The finding supports the work of McGuire and Dowling, (2013), who concluded that most students have

knowledge on cybercrime. The study also agrees with the study done by Abdulai (2016), who concluded that most students have knowledge about cybercrime. However, the finding contradicts the work of Mesko and Bernik (2011). They concluded that majority of the student have poor knowledge about cybercrime.

Research Question 2: **What are the Forms of Cybercrime in Sunyani Municipality?**

In trying to answer this, students were asked to state the forms of cybercrime activities they know that exist in their locality. The details of their responses are represented in Table 2.

Table 2: Distribution of Forms of Cybercrime

Forms of Cybercrime	Frequency	Percent
Hacking	40	20.0
Credit card fraud	36	18.0
Software piracy	30	15.0
Cyber identity theft	22	11.0
Cloning of website/Phishing	11	5.5
Pornography	20	10.0
Sweet heart swindle (Social network)	15	7.5
Cyber defamation	10	5.0
Malicious program/ Virus dissemination	9	4.5
Cyber stalking	7	3.5
Total	**200**	**100**

Source: Field survey, 2017.

Findings in Table 2 reveals that 40 (20.0%) of the respondents indicated that hacking is a form of hacking, 36 (18.0%) associated theirs to credit card fraud, 30 (15.0%) also associated theirs to software piracy, 22 (11.0%) related their reason to cyber identity theft, 11 (5.5%) also related their forms to cloning of website or phishing. Again, 20 (10.0%) indicated pornography as a form of cybercrime, 15 (7.5%) associated theirs to sweet heart swindle (social network), 10 (5.0%) stated cyber defamation as a form and 9 (4.5%) also associated their reason to the malicious program or virus dissemination. The remaining 7 (3.5%) indicated cyber stalking as a form of cybercrime.

A deduction from the above is that the four major forms of cybercrime are hacking, credit card fraud, software piracy and cyber identity theft. These forms of cybercrime are quite similar to the forms given Ribadu (2007). He stated that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other electronic commerce kinds of fraud. Research by Olugbodi (2010), states that the most prevalent forms of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, fraudulent electronic mails, cyber laundering and virus or worms.

Research Question 3: **Research Question 3: What are the Consequences Involved in Engaging in Cybercrime?**

This question sought to establish if students know the consequences involved in engaging in cybercrime activities. Some indicators of consequences involved in engaging in cybercrime were used to collect the data**.** This includes

loss of life, tarnishing the country's image internationally, loss of revenue etc. The details are represented in Table 3.

Table 3: Consequences Involved in Engaging in Cybercrime

Consequences	Frequency	Percent
Tarnishing the country reputation	52	26.0
Denial of innocent Ghanaians opportunity abroad	42	21.0
Inimical to the progress and development in the country	55	27.5
Loss of employment	35	17.5
Loss of life	10	5.0
Loss of revenue	6	3.0
Total	**200**	**100**

Source: Field survey, 2017.

The findings in Table 3 reveals that 52 (26.0%) of the respondents indicated that one of the consequences involved in engaging in cybercrime is tarnishing the country reputation, 42 (21.0%) associated their consequence to denial of innocent Ghanaians opportunity abroad, 55 (27.5%) also associated theirs to inimical to the progress and development in the country, 35 (17.5%) related their consequence to loss of employment. Again, 10 (5.0%) indicated their consequence to loss of life and 6 (3.0%) also associated their reason to loss of revenue. A deduction from the above is that the three major consequences involved in engaging in cybercrime are this is inimical to the progress and development in the country, tarnishing the country reputation and denial of innocent Ghanaians opportunity abroad. This finding is consistent with the work

of Clarke and Knake (2010), who gave similar major consequences in cybercrime activities. The study supports the findings of Abem (2013), who also indicated similar consequences involved in engaging in cybercrime.

Research Question 4: What are the Challenges in Addressing Reported Cases of Cybercrime?

In trying to answer this, respondents were asked what was preventing authorities in addressing reported cases of cybercrime. Their responses are presented in Table 4.

Table 4: Challenges in Addressing Reported Cases of Cybercrime

Challenges	Frequency	Percent
There is no complete law in the statute books of the Republic of Ghana that addresses cyber or internet crime	26	13.0
Charges against cybercriminals, under the existing laws and regulations were inadequate	48	24.0
The charges carried lesser sanctions and also allowed suspects to be bailed	46	23.0
Lack of consensus on global cybercrime legislation	30	15.0
Lack of frequent training on ICT, updating and amendment of cyber laws to cater for new offenses under cybercrime	50	25.0
Total	**200**	**100**

Source: Field survey, 2017.

The data in Table 4 indicates that, out of the Two hundred students sampled, 26 (13.0%) admitted that there is no law in the statute books of the Republic of Ghana that addresses cyber or internet crime, 48 (24.0%) agreed that charges against cybercriminals under the existing laws and regulations were inadequate and 46 (23.0%) also admitted that cybercrime charges carried lesser sanctions and also allowed suspects to be bailed. Therefore, it cannot effectively, be used as a tool to prevent people from committing cyber offences. Consequently, most legal practitioners exploit these gaps in the legal system to their advantage, and have their clients escape adequate sentencing or punishment.

Furthermore, 30 (15.0%) of the respondents agreed that lack of consensus on global cybercrime legislation pose as a challenge in addressing cybercrime cases. This allows cybercriminals to migrate from countries where cybercrime laws and regulations are strict to cybercrime-friendly countries, thereby making it difficult to track them. Finally, 50 (25.0%) also admitted that lack of frequent training on ICT, updating and amendment of cyber laws to cater for new offenses under cybercrime is a challenge.The respondents indicated that without such technical skills, new forms of crime such as cybercrime were more likely to go unnoticed and unpunished. The challenges given by students were similar to the reasons given by Goodman and Brenner (2002), they indicated that cybercrime laws were lacking in Africa, the Middle East, Asia and Oceania.

Testing of Hypotheses

H_o 1: There is no statistically significant difference between the knowledge of male and female students towards cybercrime.

Table 5: The Independent T-Test of Gender on Students Knowledge on Cybercrime

Gender	M	SD	t	df	p
Male	17.80	3.44	-6.89	198	.793
Female	15.30	2.64			

Significant level 0.05

Source: Field survey, 2017.

Table 5 indicates that the difference between male and female students knowledge towards cybercrime was not statistically significant (t value = -6.89, P = .793). By the results, the study accepts the null hypothesis that there is no statistically significant difference between the knowledge of students towards cybercrime. This could be attributed to the fact that students' knowledge towards cybercrime cut across all the selected students for the study not on gender base. This may be the reason why there is no significant difference between them. This result supports the findings of Ngo and Paternoster (2011), who concluded that there is no significant difference knowledge of students towards cybercrime on gender.

H_o 2: There is an association between students' awareness of cybercrime and age group.

H_o 3: There is an association between awareness of cybercrime and knowledge level.

Table 6: Level of Awareness Between Age and Programme of Students

Level	Variables	F	p-value	Remarks
Awareness	Age	6.450	0.000	Significant
Awareness	Programme	5.230	0.001	Significant

Significant level 0.01

Source: Field survey, 2017.

Table 6 reveals that the p-values of both level i.e., level of awareness for age and programme are significant differences among students in different age groups and programme relating to their awareness of cybercrime at 1% level of significance. It indicates that there are significant difference between students' awareness of cybercrime between their age and programme of study. Therefore, H_2 and H_3 are accepted. This could be attributed to fact that the selected students ages and programme of study exposes them differently to issues of cybercrime activities. This result supports the findings of Bougaardt and Kyobe (2011), who concluded that there is significant difference between age and programme of study of students on awareness of cybercrime.

Recommendations

1. It is recommended that curriculum in the Senior High Schools should include courses on cybercrime, cyber management and its prevention in both tertiary and secondary schools to take care of social changes.
2. The Government of Ghana in conjunction with the security services should develop a national cyber security technology framework that specifies cyber security requirement controls for individual network user.

3. The Ghana Police service should develop and maintain a national culture of security standardise to coordinate cyber security awareness and education programme for all levels of students.
4. It is therefore incumbent on Parliament to enact cyber laws to churn out policies geared at equipping judges and lawyers with the requisite knowledge to understand the intricacies of cybercrime and to facilitate effective prosecution of cybercrime cases in Ghana.
5. A cybercrime court could also be established in Ghana to speed up prosecution of cybercriminals and encourage more judges and lawyers to specialize in cyber law.
6. However, relevant Ghanaian authorities must therefore institute appropriate measures to check the influx of e-waste into Ghana to mitigate the incidence of cybercrime in the country.

Conclusions

The results showed that majority of the students have knowledge about cybercrime. Specifically, the study revealed that the major forms of cybercrime were hacking, credit card fraud, software piracy and cyber identity theft. Again, the study indicated that the major consequences involved in engaging in cybercrime are inimical to the progress and development in the country, tarnishing the country reputation and denial of innocent Ghanaians opportunity abroad. Gender had no significant influence on the knowledge of students towards cybercrime. However, there are significant difference between students' awareness of cybercrime between their age and programme of study.