Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?

Longe, O.B
Dept of Computer Science, University of Ibadan, Ibadan, Nigeria
E-mail: longeolumide@yahoo.com

Chiemeke, S. C
Dept. of Computer Science,University of Benin, Benin City, Nigeria
E-mail: schiemeke@yahoo.com

Abstract

The identification of Information and Communication Technology (ICT) as an essential tool for sustainable development has proved to be worth every investment. As a result of this, Internet usage in Nigeria has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet access points. This has had several positive impacts on the socio-economic and educational developments in the country. Unfortunately, the country's image has also suffered as a result of the nefarious activities of some Nigerians, that has now turn the Internet into a cheap channel for the perpetration of criminal spamming activities known as the 'Advanced Fee Fraud (AFF)'. This paper investigated the level of involvement and the roles of Internet access points in the facilitation of fraudulent cyberspace activities in Nigerian. A self-designed questionnaire titled "The Role of Internet Access Points in the Facilitation of Cyber crimes in Nigeria" was administered in selected locations in South Western Nigeria. Statistical analysis of data using the Smith Statistical Package (SSP) showed that spamming activities remain prevalent among Nigerian Internet users. Our findings also revealed that Cyber cafés, more than any other Internet access points, have facilitated most cyber crimes. Recommendations were made based on our findings.

Keywords: Spam, Nigeria, Cybercrime, 419, Fraud, Cyber cafes, "Yahoo Boys".

Introduction

Advancements in Information and Communication Technology (ICT) has led to the representation of different types of information in electronic formats. The consequent today is that text, pictures and voice can all be digitised. Along with these geometric changes in information presentation and distribution are tandem demands in user expectations for more rapid, open, and global access to information than has been available in the past. However, this migration from traditional communication medium to the new mediat seem to constitute a threat to the existence of a number of traditional print institutions and has provided a platform for fraudulent internet activities. Computers are increasingly more affordable and Internet connectivity is also becoming commonplace. The introduction and embracement of the Global System for Mobile Communication (GSM) in Nigeria and the influx of digital and online services such as the MP3 players, Ipod, cell phones with internet access and blogs (instant news reporting on personal and corporate web pages).

Apart from the issue of piracy, other worrisome dimensions in cyberspace are pornography and SPAM mails. The Internet, aided by technology-induced anonymity has popularized the sex business more than any other means of advertisement. With unlimited access to a variety of websites, and the impediment of needing to enter a brothel physically removed, immoral gratification is just the click of a mouse away from any intending customer (Sackson, 1996). Anonymity has been an aid to most crimes perpetuated on the Internet and other IT applications. For instance, immoral contents can be viewed in the closet, on a laptop, on a palmtop etc without the reservation that any other person will know about the content being consumed. In the same vein, piracy of digital contents and spamming activities (Spamming is the act of sending unsolicited messages to many users at a time) can be carried out in the comfort of ones home.

While technological advancements have produced radical shifts in the ability to reproduce, distribute, control, and publish information, the Internet in particular has radically changed the economics and ease of reproduction. Reproduction costs are much lower for both rights holders (content owners) and infringers alike. One consequence is an erosion of what were once the natural barriers to infringement, such as the expense of reproduction and the decreasing quality of successive generations of copies in analogue media. Acquiring equipments for analogue reproduction are quite expensive, for example the printing press. Also digital copies produced using computers and Internet facilities are perfect replicas, each a seed for further perfect copies. The average computer owner today can easily do the kind and the extent of copying that would have required a significant investment and perhaps criminal intent only a few years ago. Computer networks have also radically changed the economics of distribution. With transmission speeds approaching a billion characters per second, networks enable sending information products worldwide, cheaply and almost instantaneously. As a consequence, it is easier and less expensive both for a rights holder to distribute a work and for individuals or pirates to make and distribute unauthorized copies.

Cyber Crime & Criminality In Nigeria

Crime remains elusive and ever strives to hide itself in the face of development. As measures and techniques for detecting crimes and criminals advance, criminals also look for means of hiding from these measures – the Internet currently serve as a hiding place for fraudsters who has simply migrated from the streets to an electronic platform offered by the world wide web. Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence (Sylvester, 2001). For Nigeria, a nation in the process of saving her face regarding cyber crimes, efforts are now being directed at the sources and channels through which cybercrimes are being perpetuated – the most popular one being Internet access points.

Majority of the cybercrimes perpetrated in Nigeria generally are targeted at individuals and not necessarily computer systems, hence they require less technical expertise. The damage done manifests itself in the real world. Human weaknesses such as greed and gullibility are generally exploited. The damage dealt is largely psychological and financial. These crimes are similar to theft, and the likes that have existed for centuries offline even before the development of high-tech equipment. Through the internet, the same criminals or persons with criminal intents have simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend (Aghatise, 2006).

The challenge in fighting cybercrimes today relates to the fact that cybercrimes have been in existence for only as long as the cyber space exists. This explains the unprepared ness of society and the world in general towards combating them. Numerous crimes are committed daily on the Internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world. Criminals involved in the advance fee fraud schemes (419) are now popularly referred to as “yahoo

boys' in Nigeria. The nation has therefore carved a niche for herself as the source of what is now generally referred to as '419' mails named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

Among categories of fraud identified by Peter & Grace (2001) are fraud committed against a number of individuals through print or electronic media, or by other indirect means. This would include Nigerian advance fee frauds (Smith, Holmes & Kaufmann 1999), share market manipulation, and deceptive advertising or investment solicitations pitched at a relatively large number of prospective victims. The following categories of crime are the most common ones in the Nigerian Internet landscape.

(a) Hucksters: The hucksters are characterized by a slow turnaround from harvest to first message (typically at least 1 month), a large number of messages being sent to each harvested spam-trapped addresses, and typical product based Spam (i.e. Spam selling an actual product to be shipped or downloaded even if the product itself is fraudulent). [4] Email addresses are obtained from Internet access points using e-mail address harvesting software (web spiders) such as E-Mail Extractor Lite1.4. These tools can automatically retrieve e-mail addresses from web pages. They are therefore referred to as harvesters.

(b) Fraudsters: The fraudsters are characterized by an almost immediate turnaround from harvest to first message (typically less than 12 hours), only a small number of messages are sent to each harvested addresses (e.g. phishing, "advanced fee fraud"-419 from the Nigerian perspective). Fraudsters often harvest addresses and send only a message to them all at a particular time. The tool for getting addresses are mailing address extractors (Longe & Chiemeke, 2006).

(c) Piracy : Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs. (Longe, 2004). This can be done in a number of ways. Usually pirates buy or copy from the Internet an original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as Internet piracy or warez. Modern day piracy may be less dramatic or exciting but is far subtler and more extensive in terms of the monetary losses the victim faces. This particular form of Cyber crime may be the hardest of all to curb as the common man also seems to be benefiting from it.

(d) Hacking: Young Nigerians can be observed on daily basis engaging in brainstorming sessions at Cybercafés trying to crack security codes for e-commerce, ATM cards and e-marketing product sites. The surprising thing is that even with their low level of education or understanding of the intricacies of computing techniques, they get results! Phishing is also becoming popular as criminals simulate product websites to deceive innocent Internet users into ordering products that are actually non-existent. Phising refer to imitating product and e-commerce web pages in order to defraud unsuspecting users. This method is used mostly to obtain credit card numbers.

Mediums For Perpetrating Cybercrimes In Nigeria

The Cyber criminals apart from the mentality and the strength of their motivations, needs to see the path of crime ahead of him clear of obstacles. If every single individual were to put up obstacles of their own, no matter how small, the crime path will seem to be far less lucrative in the eyes of even the most desperate criminal (Aghatise, 2006). Progress is observable in the fight against Internet pornography (except in few cyber cafes) content filters are downloaded and installed to filter unwanted Internet content (Longe & Longe, 2005). On the other hand, even in Cybercafés with notices warning

against spamming activities, bulk tickets are sold, obviously meant for the purpose of sending Spam mails.

Apart from the availability and usage of Internet facilities in cyber cafes for scam mails and other cybercrimes, the evolution of fixed wireless facilities in the Nigerian network landscape has added another dimension to the cybercrimes problem. Fraudsters who can afford to pay for Internet connection via fixed wireless lines can now perpetrate their evil acts within the comfort of their homes. In some cyber cafes, a number of systems are dedicated to fraudsters (popularly referred to as "yahoo boys") for the sole purpose of hacking and sending fraudulent mails. Other cyber cafes share their bandwidth (popularly referred to as home use) to some categories of customers who acquire systems for home use in order to perpetuate cybercrimes from their homes.

Efforts at preventing financial Cyber crime in Nigeria are on both at entrepreneurial, private and public pedestal. For café owners, notices are pasted on walls warning of possible arrests of scammers who send fraudulent mails. Individuals can only take precautions within the limit of the knowledge of the dynamics of the Internet and the e-mail system. Generally, users are learning not to respond to scam mails or mails presenting financial bogus proposals. For the government, the Economic and Financial Crimes Commission (EFCC) has been given powers to arrest and prosecute individuals and organisations suspected to be involved in the promotion of cybercrimes. The bill on cyber crime has also been passed by the National Assembly and it is not unusual to see bill boards donning Nigerian roads warning cyber criminals that the "hands of the law will soon get to them". As at the period of writing, there are virtually no known technical measures implemented for combating cyber crime in Nigerian cafes. Hopefully, the EFCC is working on something along this line.

Methodology

The intention of the research is two-fold. One is to study the usage profile of online facilities while the other is to determine the contributions of various Internet access points, within the research area, to the perpetration of Cyber crime in Nigeria.

Research Questions

Based on the foregoing, we intend to address the following questions that have emanated.

(1) What are the main preoccupations of Internet users in Nigeria?
(2) What are the perception of Internet users regarding the role of Internet access points in the facilitation of fraudulent cyberspace activities in Nigerian.

Study Population and Sampling Technique

A total of 50 Cybercafés satisfied the stratification for availability of computer facilities, speed, patronage and consistency for the first objective. For each of the café, 10 systems were selected randomly for observing user activities. The survey method employed for the second objective is the use of questionnaire, which solicits information from respondents selected for the research. The questionnaire titled *"The Role of Internet Access Points in the Facilitation of Cyber crimes" was administered to respondents in ten locations in South Western Nigeria.* Confidentiality of personal information was guaranteed as respondents were asked to specify their age, gender and occupation. The respondents were encouraged to provide honest answers and items in the questionnaire involving some Internet technicalities were explained to assist the respondents in understanding each question.

A total of 270 questionnaire were administered over a 3 months period cutting across four locations in Southwestern Nigeria. 241 questionnaires were returned out of which 232 satisfied the statistical stratification for age, gender and occupation.. The sampling technique used is the stratified sampling method in combination with simple random sampling. The simple random sampling

technique is a method employed in selecting a sample of considerate size from a given population of data used in the survey.

Research Instruments

The research instrument titled The questionnaire titled *"The Role of Internet Access Points in the Facilitation of Cyber crimes" was administered to respondents* to evaluate their views regarding the role of internet access points regarding the research question. The research instrument was administered by trained research students under the researchers and the researchers. Responses were on a five point Lickert Scale.

Validation and Reliability of the Instrument

The face-validity and content-validity of the instrument were verified by experts in the subject area. The various suggestions made were used to modify the instrument. The Alpha reliability measure for research data was 0.84. for the first questionnaire.

Data Presentation

Table 1 reports users activities as observed in the selected cyber café. Tables 2 and 3 gives a summary of the responses and analysis obtained from 324 respondents on Internet Access Points at which cybercrimes are perpetrated.

Table 1: Internet Activity Profile

INTERNET USAGE	TOTAL OBSERVATION	% of Total Response
News	25	5.0%
Entertainment (audio music & video)	15	3.0%
Sports	32	6.4%
Pornography	13	2.6%
Spamming	195	39%
Academic research	67	13.4%
Electronic Mailing	94	18.8%
Internet Phoning	21	4.2%
Travel Information	36	7.2%
Piracy	2	0.4%
TOTAL	500	100%

Table 2: Cyber Crime Perpetration Points

S/No	ITEMS	STRONGLY AGREE	AGREE	INDIFFERENT	DISAGREE	STRONGLY DISAGREE
1	Government Offices	44	33	28	50	45
2	Homes & Home Use	53	76	12	31	28
3	Private Organization Networks	43	34	26	52	45
4	Cyber cafes	71	68	6	32	23
5	Others	41	51	20	56	32
6	Tertiary institutions Networks	67	62	7	22	10
TOTAL		319	324	99	253	183
MEAN		53.16	54	16.5	42.16	30.5

Table 3: Chi-Square Analysis

x	f	f'	(f – f')	$(f - f')^2$	$x^2 = \frac{(f - f')}{f'}$
STRONGLY AGREED	319	235.6	83.4	6955.56	29.52
AGREED	324	235.6	88.4	7814.56	33.16
INDIFFERENT	99	235.6	-136.6	18659.56	79.20
DISAGREE	253	235.6	17.4	302.76	1.28
STRONGLY DISAGREED	183	235.6	-52.6	2766.76	11.74
TOTAL	1178	1178			154.90

X^2 value = 154.90; Degree of freedom = 5 - 1 = 4
X^2 at .99 at 4 d.f = 13.277 X^2 at .95 at 4 d.f = 9.488
X^2 value = 240.6
Degree of freedom = 5 - 1 = 4
X^2 at .99 at 4 d.f = 13.277 X^2 at .95 at 4 d.f = 9.488
240.6 > 13.277 > 9.488

From the analysis above, the difference between the actual and the theoretical distribution is significant and not due to chance.

Discussion of Findings

Table 1 revealed a number of interesting findings regarding the usage of Internet facilities in Nigeria:

(a) The fact that piracy activities come last agrees with the fact that piracy is not something that takes place in open Cybercafés. CDs, VCDs and DVDs etc are copied and pirated in the confines of offices and homes of the criminals, at times in commercial quantities. Arrests have been made in places such as Lagos and Onitsha in Markets where electronic products such as tape recorders, CD and DVD players are sold.

(b) There is a steady increase in the usage of the Internet for news, travel information and sports. This is not unconnected with the migration of most Nigerian newspapers online. Readers prefer to pay for Internet time (N60-N100 for one hour) as compared to buying newspapers for as much as N150 or N200 (Longe, 2006)

(c) Pornography has been combated to a large extent. Content filters are obviously working for most Cybercafés.

(d) Electronic mailing and academic research also occupy a pride of place, as they constitute appreciable percentage of Internet usage activities within the research area.

(e) However Internet phoning is on the decrease (Longe, 2006). This may not be unconnected with the fact that there are many alternatives such as fixed wireless and GSM systems.

(f) The dark side of this data depicted below is that spamming activities take the larger share of usage profile in the investigated terrain. A casual visit to cyber cafes in Cities such as Lagos, Benin City and Ibadan, Nigeria, from which data are gathered will confirm this positions.

From Table 2 the following can be inferred:

(a) Respondents conceded to the fact that most cybercrimes are perpetrated in cybercafe
(b) This is followed by networks within academic institutions.
(c) Users on the home front comes next.
(d) Cybercrimes are however less prevalent in private organizations and government offices.

The Chi square analysis (Table 3) showed that the differences in perception are not due to chance.

Conclusion

The embracement of the Internet culture in Nigeria has come with a lot of mixed feelings. Apart from the quest among users asking for local service providers to improve their quality of service, Internet etiquette regarding positive and constructive usage of electronic mail system remains a challenge as far as the issue of fraudulent Spam messages are concerned. The incredible volume of Spam emanating from Nigeria continues to be an issue of great concern to the nation and the world at large. These activities tax the bandwidth of the Internet resulting into slower speed of operation. It all bounces back on the service providers in terms of operating costs and more access cost for consumers of services.

Unfortunately, Cyber crime seems to be yielding much to criminals in the developing nations, so it is not going to be curbed that easily. Offline crime rates have reduced because the offline criminals have gone high-tech and are making “huge money” from the business. In fact, it is highly likely that Cyber crime and its perpetrators will continue developing and upgrading to stay ahead of the law. he Internet community must therefore engage in a collective effort to curb the Internet of the demeaning crimes it is helping to fuel. For Nigeria, the EFCC and of course ICT professionals will have to take decisive steps and formulate policies that will help in drastically reducing (if not eliminate) this menace at Internet access points. A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents as currently being pursued by the EFCC will be a potent remedy.

References

[1] Aghatise, E.J (2006): Cyber crime Definition. Computer Crime Research Center. June 28, 2006. Available online at www.crime-research.org

[2] Longe, O.B.& Chiemeke, S.C. (2006): The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences. Pp 1 – 7. Covenant University, Ota, Nigeria. June, 2006

[3] Longe O.B & Longe F.A (2005): The Nigerian Web Content: Combating the Pornographic Malaise Using Content Filters. Journal of Information Technology Impact, *Vol. 5, No. 2, pp. 59-64, 2005*

[4] Longe, O.B (2006): Web Journalism In Nigeria: New Paradigms, New Challenges. Journal of Society and Social Policy. Calabar, Nigeria (In Print)

[5] Peter, G & Grace, D. (2001): Red Flags of Fraud. Trends and Issues in Crime and Criminal Justice, no. 200, Australian Institute of Criminology, Canberra. Available online at http://www.aic.gov.au

[6] Sackson, M. (1996): Computer Ethics: Are Students Concerned. First Annual Ethics Conference. Available online at http://www.maths.luc.edu/ethics96/papers/sackson.doc

[7] Smith, R.G., Holmes, M.N. & Kaufmann, P. (1999): Nigerian advance fee fraud. Trends and Issues in Crime and Criminal Justice, No. 121. Australian Institute of Criminology, Canberra. Available online t http://www.aic.gov.au

[8] Sylvester, L. (2001): The Importance of Victimology in Criminal Profiling. Available online at: http://isuisse.ifrance.com/emmaf/base/impvic.html