INTRODUCTION

Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crime depending on their nature and extent. One thing is certain, it is that 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.

CYBERCRIME

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target.

Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

• Computer as a tool

When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

• Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using he computer as a tool, these crimes requires the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. But it is worth knowing that Africans and indeed Nigerians are yet to develop their technical knowledge to accommodate and perpetrate this kind of crime.

OBVIOUS CYBERCRIMES CATEGORIES AS OBSERVED IN SOME CYBER CAFES IN NIGERIA.

There are so many varieties of crimes that are committed on the internet daily, some are directed to the computer while others are directed to the computer users. In this study, I have identified some common crimes committed daily in Nigerian networks.

1. SPAMMING

Spamming is the act of sending unsolicited messages to many users at a time, possibly up to thousands, with the usual intention of advertising products to potential customers. Spamming can also be used as a form of irritation by singling out an email address and sending the owner of that address hundreds of emails per second. Spamming is usually random and untargeted but it can be targeted to either a group of people, for example, advertisements that cater for a particular group of

people, or certain persons, like in the case of spamming for the purpose of irritating the public. Contrary to popular belief, spamming has existed in Nigeria even before the advent of the Internet. During the period I spent working as a casual security staff with the Nigeria Postal Service (NIPOST), we (mail security staff) were asked to make sure that letters sent by some individuals be destroyed upon investigation. I was curios and decided to open one of the letters one day and see what the content really was; you can guess what the content of the letter was! Junk mail to postal addresses and annoying door-to-door salesmen are some examples of the more traditional form of spam. However, the Internet has given spam a much uglier face. Now, what used to be a minor irritation has become a veritable menace. The internet has enabled young Nigerians to become active cyber criminals. They queue up in cyber cafes to send "419 mails." (Nigerian word for fraudulent businesses online).

CATEGORIES OF SPAMMERS

Spammers are classified into two major faces;

a. Hucksters

The hucksters are characterized by a slow turnaround from harvest to first message (typically at least 1 month), a large number of message being sent to each harvested spamtrapped 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).

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 sent to each harvested addresses, and fraud based (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. In this process, they use e-mail addresses harvesting software like: advanced e-mail extractor pro, extreme e-mail extractor. Since most of the available email clients support emails separator with the comma (,), another software is introduced in the process. This software allows the criminals to separate their harvested email addresses with the comma character. A good software for this purpose is the e-mail extractor lite1.4.

2 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 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.

The term "warez" describes commercial software, movies and games that has been modified by a cracker and made freely available to the public on the Internet. The word came from the word "wares" but, as with "phishing", the hacker/cracker community altered the original word just enough to claim it as its own.

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 cybercrime may be the hardest of all to curb as the common man also seems to be benefiting from the crime. A typical Africa person would stop at nothing to download "free software, musicals, movie" or related items. The reason is that, the taxation system in most African countries is ineffective and people grow up to believe paying tax and other bills are a way the government use to oppress the poor citizens.

THE VICTIMS

Victimology is a very important branch of criminal psychology. It is as important, if not more, to

know whom the criminal is likely to target. Preemptive action can only be taken by the law if they know who is likely to commit crime as well as who is likely to be targeted. All criminals – at least the intelligent ones – will only attack those who exhibit certain vulnerabilities. Just as a robber will never think of robbing someone who is armed, so are cybercriminals careful about the personalities of those they choose to prey on.
I have identified four levels of cybercrime victims. They are;
1. Gullible
2. Desperados
3. Inexperienced
4. Unlucky people

1. The Gullible
There is no doubt that cybercriminals are most fond of people who are easy to deceive. During the period of this research, I interviewed some cyber criminals in four cyber cafes in Nigeria and what I was told was this "yahoo-yahoo business is all about deceipt, if you are gullible, then you become my mahi.." On a more obvious level, phishers are best able to fool such people into buying their scams or being drawn into legal traps. Spammers send multiple e-mail messages to harvested email addresses and the gullible fall prey to the contents of the email. Usually older people are prone to being scammed as they are more trusting and helpful towards others.
On a more dangerous level, however, many especially children believe that the people they meet on the net are as friendly and worthy of trust as real people. Almost all victims of cyberstalkers are prone to trusting people and making friends easily.

2. Desperados and greedy people
Many internet users are desperate for easy ways to make cash. Hence, they easily fall for emails that say things like "Get rich fast!", "CONGRATULATIONS ON YOUR LOTTO WINNING" and all of those stuffs. Come to think of it if you did not take part in any lottery program, how come someone is telling you congratulations for winning? Greedy and desperate people will always fall to this level of scam and follow the instructions in the emails which most others are likely to treat as junk. They are almost definitely being led to legal and financial entanglements out of which only the perpetrator will make profits. There are others who are attracted to advertisements related to improving one's physical image. Ridiculous products such as "cheap, effective breast enlargements" etc. claim to boost their self-esteem at minimum cost. This explains why there are so many of such emails in circulation these days. These adverts are almost certainly nothing more than means to extract credit card numbers and render the reader bankrupt.

3. Unskilled and Inexperienced
There are a lot of people in the world today whose knowledge of the Net is just enough to chat with their friends and maybe get information from here and there. They are ignorant of the fact that most people they meet online are criminals who hide under the shades of the internet to perpetrate different crimes. Lots of people have been raped by sex seeking individuals on the internet. That's reminds me, I remember an instance during my work in one of the most populous cyber café in Benin City, the capital of Edo State, a particular lady would come to the café and request for private system, when I monitored her activities, I discovered she was just an unskilled and inexperienced lady who was deceived by an American guy to always go naked for him and show herself in a web cam and she always did. What a shame!

4. Unlucky people
There are also people who fulfill none of these categories but are just unlucky enough to be at the wrong place at the wrong time, in cyberspace that is. These categories of victims believe they are meeting legitimate business associates only to be deceived by the variants. Also, a full-scale of attack or a self-replicating and highly advanced virus can cause great damage to networks or PCs

and the individual may not in anyway be blame.

PREVENTION
Apart from his own mentality and the strength of his motivations, the criminal also 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. The fight against cybercrime must start with preventing it in the first place.

Users
The individual should be proactive, not reactive. You do not have to remain at the receiving end of crime forever. The fight against cybercrime starts in your very own home. Individuals should not reply any e-mail from unknown persons, they should learn to report spam mails to the e-mail server or any know cybercrime research sites. If there is one thing that makes committing cybercrime lucrative, it is the fact that victims rarely have the required knowledge or presence of mind to handle the situation.

Law update
One of the biggest challenges the African government and other nations faced is the enactment of adequate cyberspace laws. For instance, the government of Nigeria under the leadership of President Olusegun Obasanjo, has gone a long way to fighting cybercrimes and offline crimes. The Economic and Financial Crime Commission (EFCC) of Nigeria since its establishment has been on top of the game of fighting crimes. Several of these criminals have been trapped down by the EFCC and many are also declared wanted by the commission. But the EFCC should be fast in the cybercrime laws they earlier sent to the National Assembly for review. Another major challenge faced by government bodies today with regard to cybercrime is the fact that laws and statutes are by nature rigid and long-standing. Cybercrime is evolving every single day and even if new laws are created to tackle a particular crime, it can be circumvented in a matter of weeks. But some countries have made a head start in this area, Australia for example have updated laws that include cyber crimes.

The Nigerian Cybercrime facts
When efforts are being made to remove the rebellious shoot of the proverbial tump, it obstinately sprouts another. So is cybercrime, which has continued to grow by leaps and bounds, just as the government frantically keeps on fighting financial crimes. Cybercrime has continued to dent the image of Nigeria abroad. When the internet was been introduced some years back, we were told of great opportunities it will bring to Nigeria and Nigerians, but now we only see and read in papers how the internet has reduced Nigeria reputable internationally. Recently a report indicated that Nigeria is losing about $80 million (N11.2 billion) yearly to software piracy. When you come across phrases like “Nigerian scam”, the assumption that crosses your mind is that all (or conservatively, most) scam email originate from Nigeria or Nigerians. It is even alarming to know that 80% of perpetrators in Nigeria are students in various Higher Institutions who maybe were distracted by some hidden factors. I noticed one common characteristic among most of the cybercriminals I interviewed (indirectly) during the period of gathering materials for this work… it is their desire for “cars” and “powerful camera phones”.

Like I do teach people, the best way to fight crime is to be at the scene of crime. Cybercrime is not “armed robbery”, not “pen and paper crime” and should not be handle as such. Fighting Cybercrime requires intelligent knowledge and that has to be IT intelligence. What I mean is this, men of the regular Police force should not be allowed to investigate crimes committed over the internet. IT experts should be recruited into law enforcement agencies to assist in the fight.

Finally, apart from updating laws of nations, I advocate that if United Nations could set millennium goals for countries in the world, the same should be done in the areas of cybercrime. UN should make it mandatory for countries affected by cybercrimes to update their laws to include cybercrimes and other internet (high-tech) related misconducts. It should now be publicly acknowledged by academics, participating law enforcement officials and business representatives that a range of threats including specific kinds of malicious activities undertaken by insiders, hackers, virus writers need to be globally criminalized. More importantly, this range of criminalized activity has to be extended to organized crime and internal corruption within the law enforcement itself. It is always important to take note of the fact that the best of laws are useless and can even be counterproductive and dangerous if they are not fairly and effectively enforced. United Nations and other organizations should support laws that could be implemented across national borders.

CONCLUSION

Cybercrime is indeed getting the recognition it deserves. Internet (cybercrime) seems to be yielding much to developing nations, so it is not going to be curbed that easily. Offline crime rates have reduced in most developing nations because the offline criminals have gone high-tech and are making “huge money” from the business. In fact, it is highly likely that cybercrime and its perpetrators will continue developing and upgrading to stay ahead of the law.

Aghatise E. Joseph is a final year (HND II) Computer Science student of Auchi Polytechnic, Auchi, Edo State, Nigeria, the founder of the group “JUST iT TEAM” a campus based IT group. His HND project work was entitled “Level of awareness of Internet Intermediary Liability”. He has worked with several cyber cafes in his state and has experience in a number of cybercrimes. He lectures (Part-Time) computing at OSE-ICTi Ltd, Nigeria. His research areas include: Information Systems Security, Networking, and Web Technologies.

REFERENCES

Aghatise E. J. (2006): Level of Awareness of Internet Intermediaries Liability. (HND Project work) Unpublished. Auchi Polytechnic, Auchi, Edo State, Nigeria.

Longe, O.B. (2004): Proprietary Software Protection and Copyright issues in contemporary Information Technology. (M.Sc Thesis) Unpublished. Federal University of Technology, Akure, Nigeria.

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 (republished in The Reformer February 2000, pp. 17-19).

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