Cybercrime: The Downside of the Global Internet

Percy Okae
Assist Lecturer, Computer Engineering Dept
University of Ghana, Accra, Ghana
pokae@ug.edu.gh, perokae@hotmail.com

Abstract - Although, the Internet had existed for many decades as the ARPANET since 1969, it was only after 1991 when the British MIT professor, Sir Tim Beners-Lee, invented the World Wide Web (WWW), which also runs on the Internet that the Internet attained the heights it has to this end. This major technological breakthrough helped cement the Internet in the annals of technology history because of the way it has impacted the World in information dissemination. Today, at the click of a computer mouse, one reaches a friend or family member thousands of miles away because of this extraordinary breakthrough. However, notwithstanding these positives, our confidential files and even our individual lives have become a target for would-be criminals who have specialized in the art of hacking into people's computers or intercepting people's electronic messages. These kinds of crimes are simply termed as cybercrimes. Through cybercrimes, criminals have been able to intercept people's credit card details and used them to withdraw their monies. Others have also stolen people's identities and managed to escape the long arms of the law for many years whilst the victims of such crimes fought very hard to prove their innocence. The World and indeed all who use the computer in one way or the other are at risk from these incorrigible social deviants who go to all lengths to rob people in cyberspace. This paper seeks to investigate the causes of these types of crimes and prescribe recommendations for their global combat.

Keywords- Internet, World Wide Web (WWW), cybercrimes.

1. INTRODUCTION

Cybercrime has become a very important issue since the WWW took the center stage of the technological revolution that has recently swept our World. The threat posed to every computer user as a consequence is very real and huge. There are now people all over the planet who have specialized in the art of stalking computer users and using all sorts of highly sophisticated software to prey on otherwise unsuspecting netizens. Today, most especially in the developing World, cybercrime has become more or less a lucrative 'business" for so many young men and women who should otherwise focus their energies on productive ventures. Currently, for instance, one typical example of cybercrime is what people call "advanced fee fraud" which is also known as "419".

Cybercrime is simply the art of committing a crime such as hacking into somebody's computer without his or her permission and using the information obtained thereof to engage in unlawful acts. Such unlawful acts include:

- cyberstalking,
- fraud and identity theft,
- information warfare,
- phishing scams,
- dissemination of offensive materials

Recently, the American government has accused the Chinese government of hacking into its computers, a claim China denies. According to the report released by the American cyber security firm Mandiant, it had linked hundreds of data breaches since 2004 to a Chinese hacking team traced to the site of a military unit in Shanghai [1]. The report asserted that China was stealing intelligence information on US diplomatic, economic, and defence sectors which could benefit China's own defence programme. To this end, America for one, has said that cyber attacks and cyber espionage had supplanted terrorism as the top security threat it faced. The bottom line is that whether these allegations and counter allegations are true or not, cybercrime and cyber security have become a major concern such that even every now and again, suspicions could be raised by one nation against the other. If indeed this canker has assumed such alarming proportions, then it presupposes that every effort ought to be made at curbing this menace [15, 16]. Thus this research work is geared towards some of the landmark examples of cyber attacks and the recommended alternatives measures that could be taken by governments and individual alike to curtail them.

2. METHODOLOGY OF RESEARCH

The objective of this research is to review the modus operandi adopted by cyber criminals and make recommendations as to how this perennial canker can be reduced to the barest minimum, if not completely uprooted from our respective communities and the entire World at large. Most specifically, we list typical examples of how various individuals have been scammed through various schemes to the extent that some unfortunate victims ended up losing their lives. We also present tabular poll results (surveys) carried out to identify victims who have in one way or the other fallen prey to this perennial canker.

2.1 METHODS ADOPTED BY CYBER THIEVES

Cyber thieves adopt many strategies including but not limited to all the acts listed above against their unsuspecting victims depending on the geographical location of the criminal [2]. These cybercrimes are not limited only to certain geographic areas of the globe, but rather happen in almost all parts of the World.

2.1.1 A TYPICAL CASE OF FRAUD AND IDENTITY THEFT

These heinous crimes are perpetrated mostly by the youth who steal the identities of people they do not even know from Adam and deceive their would-be victims into believing that they are the people whose identities and particulars they have stolen [3, 4, 5]. These kinds of frauds are mainly perpetrated through online dating where they almost on a daily basis engage their unsuspecting victims in chats at various Internet cafes and gradually dupe them of their entire lifetime savings. The local term they have assigned to this kind of fraud in Ghana for instance, is "SAKAWA". Normally, most of their victims are white women from Western countries in the age bracket of 45 – 60 years who have been widowed or are divorced and are therefore seeking to build a new love life. Out of such desperations, these women are usually too easily deceived by these scammers and by the time they would have realized it was all a scam; it would simply be too late as they would have wired so much hard currency away to these fraudsters. I have personally been to various Internet cafes in Accra, Ghana, where these scammers, some of them teenagers, engage these white women far way in their countries in chats online whilst via webcam the identities of the people they are using will be live right there and then for the other party to see. As these conversations and interactions develop and mature and some level of trust is built, these scammers then start making demands from these unsuspecting women usually from small demands until they fabricate a big lie to pull off a rather big payday from these women and then from thence, they cease of forms of communications with the victim [6, 7, 8]. In Ghana, the case of the British businesswoman Mary Little in 2009 is the most prominent of these scams. As usual, she was also looking for love on the dating site, Match.com. She happened to meet a supposed retiring American colonel by name Frederick Stalke who was returning from duty in Iraq and was in the process of fixing his home in New York. Mary claimed she had built a relationship with the supposed Stalke for seven months and so when the supposed veteran demanded a $100,000 from her to help fix the house in New York where they could move into very soon, Mary, was convinced and wired almost all her entire lifetime savings to her prospective husband. The story actually cooked up by the supposed Stalke was that he had arrived in Accra, Ghana, to retrieve some valuables of his wrongly shipped to Accra and so he was to be back in the USA in two weeks. The story went on that Mary was to wire the money to a prominent bank in Ghana as soon as possible as Stalke had had problems with the police in Ghana and needed this huge amount badly to sort himself out and also complete the house in New York. Trusting him, Mary did send the money to Ghana and with the help of a staff of this prominent bank; these scammers withdrew the money in local currency in three tranches. When after receiving the money Mary had not heard from her prospective husband, she rang the hotel where he was supposed to be residing and was told all sorts of lies. After a lull of almost three months, Mary was contacted by a woman claiming to be the daughter of the fake Stalke who claimed that Stalke had suddenly died. She also claimed that she was a student in California and that she had returned to Accra to find out the cause of her father's death. Consequently, she needed £3,000 to undertake that task. Based on advice from the UK Fraud Department, Mary was asked to send the money by courier and the Ghana police were immediately alerted. At the designated place and time, the young lady turned up to retrieve the £3,000 and was immediately arrested by officers who had taken positions. She subsequently led them to the hideouts of all those involved in the syndicate. Mary followed up to Ghana to see to the prosecution of these social deviants and also sued the bank for not doing due diligence before releasing the money to the fraudsters. Speaking to the Ghanaian media Mary had said she did not want to commit suicide as some in similar situations in the UK had done but was determined to fish out these criminals to serve as a deterrent to would-be scammers. Asked why she wired such a huge amount to someone she had never met before, Mary insisted that all her life in the UK, she had lived among trustworthy people and that she felt the same applied to the very man she had been dating online [9, 10].

2.1.2 ADVANCE FEE FRAUD ("419")

The type of cybercrime known as advance fee fraud or "419" has indeed assumed global proportions. As a matter of fact, the number 419 refers to the article in the Nigerian Criminal Code dealing with fraud. In this kind of fraud, one will for instance, out of the blue receive an e-mail message from someone he does not know at all

informing him or her of a prize money he or she has won [11, 12]. Then they would advise that you confirm whether you are the person in question. When you fall for it and confirm your identity, they will then ask that you pay money upfront to them so that they can service the prize money you are supposed to receive and this is usually in millions of dollars. Usually they request that you wire the money through either Western Union Money Transfer or Money Gram, as these are instant services and also not traceable once they retrieve the money and abscond. I have personally received quite a number of e-mails every now and again informing me of a lottery win or prize money that I stand to get if I did what they directed me to do in the e-mail. In one particular instance, I was been addressed by a supposed widow of a wealthy Nigerian and she wanted me to advance an amount of $5,000 to her to help her secure a whopping amount of $55,000,000 from a trust in which the money was kept and my eventual share of the trust was going to be 25 %. I knew there and then that it was a scam in the sense that how could this person who did not know me from anywhere get to know that I was even rich enough to have $5,000 to lend? Also, how could I give my bank account number to a total stranger as she requested in the e-mail as well so that she could eventually deposit my share of the booty into? However, it is not all people who are able to read between the lines to detect the modus operandi of these fraudsters so as to stop them in their tracks as I do by totally ignoring these messages anytime I receive them.

2.1.3 INVITATION TO MEET THE SCAMMERS

Much as cyber fraud is concerned, there have also been occasions when people who did not exercise enough caution have paid the ultimate price with their own lives. In one particular case that took place on 22 July, 2012, a Nigerian graduate student by name Cynthia Udoka Osokogu, 24, paid the ultimate price with her life in Lagos, Nigeria when she agreed to meet two male friends she had met on the social networking site “Facebook”. On the said appointed date, the lady arrived at the hotel in Lagos by name Cosmila Suites and Hotels to meet her Facebook friends and lo and behold, they rather held her captive over there, drugged and sexually abused her and eventually strangled her and fled because she could not fulfill their cash demands on her.

There is also the murder case of the 29 year old Greek national George Makronalli who was lured to South Africa by scammers to complete a lucrative business deal in 2006. When he got there and realized it was a scam and wanted to back out, his supposed business allies refused to accept his wish. This resulted in bitter exchanges with his hosts and they subsequently kidnapped him and tortured him to death when his family back in Greece refused to pay a ransom of $160,000 his kidnappers demanded.

Cases like the two examples above do happen every now again when most of the victims least suspect that these so-called friends rather generally have ulterior motives for inviting them [13].

3. PRECAUTIONS TO TAKE TO OUTWIT SCAMMERS

The observation made through the examples of cybercrimes cited so far indicates a case of undeserved trust accorded their would-be scammers by the victims. The proposition we make here is that given the level of skill and tools applied by potential criminals, all computer users review their mode of making friends online [14]. Even one has to meet an online friend at all; it should be in open places where lots of people are around. Online friends meeting for the first time should not forget to take along a friend or family member. Moreover, they should not board each other’s private cars but insist on traveling by public transport such as taxis or buses. Another proposition we make is that people should not within a short time of meeting a complete stranger online agree to meet them in anyway and also resist the temptation to part with money. As a matter of fact, once a potential friend starts making financial demands, there is every likelihood that that individual is a scammer and one has to quickly cease communications with such people.

4. SURVEY RESPONSES FROM VICTIMS OF CYBERCRIME

Interesting results are obtained from surveys that aim to identify victims of cybercrime. The mode of questioning was simply by sampling the views of a cross-section of people at various forums who regularly work with computers as to whether they may have fallen victim to cyber crime before.

Table 1: Responses of 45 people in various professions about falling victim to cyber fraud

Type of cybercrime	Type of responses			
	Yes respondents	No respondents	Yes (%)	No (%)
Phishing	22	23	48.9 %	51.1 %
Identity theft	6	39	13.3 %	86.7 %
Fee fraud such as “419” schemes through e-mail	33	12	73.3 %	26.7 %

4.1 DISCUSSION OF SURVEY RESULTS (Table 1)

The responses show a pattern which invariably conforms to international scam patterns. Those who have experienced phishing scams- this is the process by which Internet users are lured into revealing personal information such as usernames, passwords, accounts information etc. by creating a site similar to that of the victim's bank. This particularly is a type of cybercrime that is on the ascendancy and thus the high percentage of people who responded yes to the survey is in order. In the case of "419"-like scams, it is so commonplace and no wonder it has the highest number of victims among the three types of cybercrimes the survey conducted on.

Table 2: Responses of 137 people concerning whether they prefer a World of ICT services or not

Type of question	Type of response			
	Yes respondents	No respondents	Yes (%)	No (%)
Do you use an Internet-enabled computer at work?	121	16	88.3 %	11.7 %
Do you prefer an Internet-enabled computer either at home or at work?	114	23	83.2 %	16.8 %
Does having ICT tools at work enhance your delivery at work?	125	12	91.2 %	8.8 %

4.2 DISCUSSION OF SURVEY RESULTS (Table 2)

The results from above are an overwhelming approval for ICT services which facilitate work both at home and at the workplace. Almost all current educated people are taking ICT skills very seriously and even the older generations are also upgrading their knowledge so as not to be left behind. Even as at now, many mobile phone subscribers all over the world have learnt how to access the Internet on their cell phones and have become so accustomed to it that they cannot do away with these new habits. We can only keep improving our skills in utilizing the software tools that rolled out each passing day by various multination companies. Through that, we can also grow confident enough with experience to be able to avoid the many traps scammers set. If the responses of Table 2 are anything to go by, then we can propose a model whereby in every organization or institution, a section of the ICT department is dedicated to ensuring the integrity of their computing systems by ever upgrading their skills levels so as not to be overtaken by events.

5. CONCLUSIONS

Cybercrime has come to stay with us in as much as technology keeps growing with each passing day. They days are long gone when one could just use a computer without as a minimum having a tool that prevents information theft on it. As the sophistry of technology grows, so are the incorrigible fraudsters also varying their styles and focus. Presently, there are networks of individuals who have formed more or less conglomerates with the singular purpose of hacking into computers especially those of businesses and governments with the aim of stealing information which they use eventually to amass illegal wealth. However, every concerned person has to play a role in the combat of this global canker. Governments should as a matter of ICT policy tackle this major threat head-on so as not to compromise on state security. There have been instances where cybercrimes have affected various government machineries grinding an entire national administration to a halt for some time.

However, all is not lost. Be it as it may, the benefits one gains using ICT services far outweigh the demerits such as cybercrime. Today, there are over 6 billion cellular phone subscribers all over the World thus facilitating communications among people even in different geographic places on the globe [6]. Years back, especially in the underdeveloped World, the main modes of communicating to a friend or family member whether far or near were through snail mail or by traveling. Now e-mails, text messaging, instant chatting, to mention just these three, have replaced the old forms of communication and consequently enhanced our lives. Today, one can also see loved ones who have been away for a long time live from wherever they are through technologies such as web cam. Thus the merits of ICT tools in our everyday lives and their concomitant failings are all there to savor.

6. RECOMMENDATIONS ON HOW TO COMBAT CYBERCRIME

i. Various organizations should as a matter of priority organize in-house training for their employees regularly to sensitize them well enough on the threats posed to them both at work and in the home as they work on their computers.

ii. If an employee usually has to complete office work at home, then the organization should allow such employees to use the company laptops at home since they have the right sophisticated software installed to prevent confidential information leakages.

iii. There is a need for all computers users to be constantly alert and not be tempted in the least to even respond to strange e-mails let alone part with money.

iv. If possible, people should make provision for anti-virus installation on their personal computers as a minimum to ensure a certain level of cyber security.

v. In the extreme case where unsolicited mails are received and one is unsure of what to do with it, a good line of action to take will be to consult an ICT professional who could help.

vi. People who engage in online banking should as much as possible try to avoid open spaces where people could be spying on them whilst they enter their bank details online. Sometimes at Internet cafes for instance, people hide cameras around which can capture activities that take place there.

vii. Those who frequent Internet cafes can contribute their quotas to fighting cybercrime by being on the lookout for people who come to cafes mainly to chat with people several miles away with the sole aim of lying to them and eventually duping them. One can quietly sneak out to inform law enforcement if such a situation is detected.

viii. At the national level, governments should as a matter of priority, implement ICT legislative policies to combat cybercrimes by forming various task forces trained in ICT skills to educate the citizenry on the basics and the places to seek help and also report suspicious characters.

ix. Internet cafes should be properly licensed before they can operate and those who acquire the undesirable track record of cyber crimes can be tracked down and delicensed.

x. Severe punishments should be meted out by all governments to perpetrators of cyber attacks so that they will serve as deterrents to would-be fraudsters.

xi. Real-time security should be deployed at Internet cafes and public ICT parks who will monitor the activities of patrons and hopefully arrest potential criminals.

REFERENCES

[1] US accuse China government and military of cyber-spying, 7th May, 2013, available at http://www.bbc.co.uk/news/world-asia-china-22430224.

[2] Understanding Cybercrime: Phenomena, Challenges, and Legal Response, ITU, Sept 2012

[3] Comprehensive Study on Cybercrime, United Nations, New York, February, 2013.

[4] Cybercrime presents a major challenge for law enforcement, EUROPOL, January, 2011.

[5] The cost of cybercrime, Detica, February, 2011.

[6] Threat of mobile cybercrime on the increase, FT.com, February 8, 2011.

[7] Ramona R. Rantala, Cybercrime Against Businesses, 2005, Bureau of Justice Statistics, U.S. Department of Justice, NCJ221943, Sept , 2008, http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

[8] Internet Crime Complaint Center, http://www.ic3.gov/about/default.aspx.

[9] E. Gabriella Coleman, "Anonymous: From the Lulz to Collective Action," The New Everyday, April 6, 2011

[10] "HBGary Federal Hacked by Anonymous," KrebsOnSecurity, February 7, 2011.

[11] The Indian Law Institute. Introduction to the cyber world and cyber Law. 2010.

[12] U.S. Department of Justice, "International Hacker Arraigned After Extradition," press release, August 6, 2010, http://www.justice.gov/usao/gan/press/2010/08-06-10.pdf.

[13] Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

[14] [14] David L. Speer, "Redefining Borders: The Challenges of Cybercrime," Crime, Law and Social Change, vol. 34, no. 3 (October 2000), p. 260.

[15] U.S. Department of Justice, "Organized Romanian Criminal Groups Targeted by DOJ and Romanian Law Enforcement," press release, July 15, 2011, http://www.justice.gov/opa/pr/2011/July/11-crm-926.html.

[16] Dominic Rushe, "FBI Fights Back Against Cybercrime," The Guardian, August 24, 2011, http://www.guardian.co.uk/technology/2011/aug/24/us-agency-fights-back-against-cybercrime.