Journal of Information Technology Impact
Vol. 11, No. 3, pp. 169-182, 2011

Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective

Paul Danquah [1]
Accra Institute of Technology
Ghana

O. B. Longe [1]
University of Ibadan
Nigeria

Abstract

Using a combination of ethnographic study of criminals and victims in combination with secondary published text that highlights cyber deception and theft we seek to determine the schemes and plots of cyber deception in Ghana. We provide a detailed report on the primary data collected from criminals and victims on the ploys used for cyber deception and theft viz-a-viz the content and schemes found in secondary data documentations. Findings from this research showed that the typical Ghanaian cyber criminal is hardly ever involved in spoofing, page-jacking and auction/merchandize frauds. Evidently, social engineering is syndicated and has become a prominent feature in cyber deception and theft in Ghana. Unfortunately, timely and reliable statistical data on cyber deception and theft are not readily available from the Ghanaian law enforcement agencies. We conclude by providing insights into disturbing scenarios in public internet access points and recommendations for legal actions as well as law enforcement

Keywords: Social engineering, fraud, law enforcement.

Introduction

The users of the internet are involved in a spectrum of activities ranging from mere consumers, business competitors and many other reasons, one cannot rule out the fact that these users are capable of engaging in various forms of cyber crime like stealing intellectual property or services amongst others. Some users tend to perform crimes like fraud, releasing malicious code, terrorism, website defacement, theft and many others Noting the increasing dependence of many societies on the internet, Dana (2001) reported that a sizeable number of users in the cyber space are well behaved, engage the web for productive purposes and are law-abiding. There is however a fraction as is the same in the conventional space who act inappropriately, break the law and use illicit means to take advantage of others in cyberspace.

We direct our efforts in this work towards providing a descriptive assessment of cyber deception and theft as engaged in Ghana by cyber criminals by discussing evidence collected via interviews of criminals and victims as well as secondary data from documentary evidence. The intention is to provide a basal understanding of the ploy and strategies the cyber criminal employ to successfully victimize and deceive unsuspecting victims. The research ultimately seeks to better educate users of cyber space in Ghana viz-a-viz globally and empower them as the last line of defense against cyber victimization.

The remaining part of the paper is organized as follows. The next section traces cyber criminality and discusses in cyber crime typologies. This is followed by a section on problem statement and research design. Next we reported findings from the ethnographic study. The paper concludes in the final section with recommendation for policy and practices

Cyber Crime Trace and Cyber Crime Typologies

Crime threatens social order and cyber crime is a subset of crime that is committed by use of computer technology, either alone or in conjunction with real-world acts and actors. (Brenner, et al, 2004; Picker, 2004). cyber crime started gaining prominence in 1971 Wavefront (n.d). Notable cyber crimes committed over previous decades include the 1973 incidence where a Teller at New York's Dime Savings Bank used a computer to embezzle over $2 million Wavefront (n.d). In 1981 Mr. Ian Murphy also known as "Captain Zap“ was convicted of a computer crime after breaking into AT&T‟ s computers and changed the billing clock so that people received discounted rates during normal business hours Slatalla(2003). The most notable cyber crimes in the 80s were those which occurred in 1988, when Kevin Mitnick secretly monitored the e-mail of security officials, he was convicted and sentenced to a year in jail Wavefront (n.d) . In the same year First National Bank of Chicago was the victim of $70-million computer theft. Robert T. Morris a graduate student at Cornell University launched a self-replicating worm (the Morris Worm) on the government's ARPAnet and the worm spread to over 6000 networked computers, clogging government and university systems. Morris was dismissed from Cornell, sentenced to three years' probation, and fined $10,000.Zuley et al (2003)

In the 90s the rate of cyber crime increased significantly with the most notable ones occurring in 1994 and 1999 respectively. In 1994, a 16-year-old student, nicknamed “Data Stream”, was arrested by UK police for penetrating computers at the Korean Atomic Research Institute, NASA and several US government agencies Zuley et al (2003). Five members of the Aum Shinri Kyo cult's Ministry of Intelligence broke into Mitsubishi Heavy Industry's mainframe and stole Megabytes of sensitive data Wavefront (n.d). In 1999, the Melissa worm was released and it turned out to be the most costly malware outbreak ever. US Defense Dept. acknowledged 60-80 attacks per day. In the 2000s, the rate of cyber crime has even grown higher with numerous cyber crimes reported Wavefront (n.d).

Notable crimes occurring in the last decade include among many others, in 2001 Microsoft falling victim of a new type of attack against domain name servers, corrupting the DNS paths users take to Microsoft's Web sites Wavefront (n.d). This is a Denial of Service (DoS) attack. The hack was detected within hours, but prevented millions of users from reaching Microsoft Web pages for two days. The year 2004 saw Brian Salcedo sentenced to 9 years for hacking into Lowe's home improvement stores and attempting to steal customer credit card information. Prosecutors said three men tapped into the wireless network of a Lowe's store and used that connection to enter the chain's central computer system in North Carolina, installing a program to capture credit card information Spylogic (2008). In 2008, MySpace and FaceBook private pictures were exposed on-line using URL manipulation in January and March. Furthermore, hackers stole 4.2M card numbers of Hannaford shoppers, resulting in over 2000 fraud cases BroadbandDSL (2008). The United States Internet crime Complaints Centre has provided statistics over the last year of higher dollar losses due to cyber deception and theft from advance fee fraud mail. In particular, these schemes are traced to West African Countries and tagged 419 activities (IC3, 2010).

In its various forms, cyber crimes was categorized by Yar (2005) as:

- Cyber-Trespass: This involves crossing boundaries into other people's property and/or causing damage, i.e - hacking, defacement and viruses
- Cyber-Deceptions and Theft: This type of cyber crime involves stealing (money, property), i.e - credit card fraud, intellectual property violation, piracy
- Cyber-Pornography: These are activities that breach laws on obscenity and decency
- Cyber Violence: This involves causing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person. i.e. - hate speech.

We focus on cyber deception and theft in this discourse.

Cyber-Deception and Theft

Cyber-deception and theft involves deception and stealing with the use of technology. Typical examples are credit card fraud, intellectual property violation and piracy. Cyber deception and theft comes in various forms, some of which are outlined below;

Identity Theft

This refers to the wrongful acquisition and use of someone else’s personal data in some way that involves fraud or deception, typically for economic gain. (Schmalleger,2008)

Spoofing or page-jacking

This involves the use of fake or fraudulent websites to extract personal information. This involves the insertion of keywords and meta-tags from other websites to be used by search engines. This is eventually used to misdirect users to fraudulent sites either through Domain Name System(DNS) hijacking or poisoning. (Dinev 2006)

Credit Card Schemes

This refers to the use of unlawful methods to obtain credit card numbers to order goods and services over the Internet. For example, “sellers” will offer victims expensive items, such as video cameras at a very attractive price. When the victim contacts the seller, they will even be promised that the item would be shipped prior to payment. Naturally victims tend to agree. The “seller” then uses the victim’s real name, without the victim’s knowledge, together with a credit card number belonging to another person, to buy the item online. (Schmalleger, 2008)

General Merchandise and Auctions

Auctions are schemes from online retail goods where victims are made to pay for their successful bids but never receive any items in return. (Kouri 2006) describes the international fraud scheme based in Romania had 21 defendants obtain over $5 million via internet fraud schemes where victims were made to believe they were purchasing items listed for sale on the internet.

Advance Fee Fraud

These scams are typically advance fee fraud mails (referred to as ”419” mails a nomenclature borrowed from the Section 419 of the Nigerian Criminal Act . These scams that are purported to originate from the West African countries, especially Nigeria, require victims to pay a series of fees to process a transaction that supposedly enables the victim claim a large sum of money. These fees would usually cover duty, stamp and form charges. (Cukier et al, 2007). In 2011, Longe & Osofisan reported a research carried out over a two year period using freeware e-mail and internet protocol address tracers that deviates from the generally held believes about the origins of advance fee fraud e-mails.

Phishing

Phishing is aimed at acquiring confidential financial information such as account numbers and passwords (Anti-Phishing Working Group 2007). The number of phishing websites was detected to be over 55,000 as at 2007 by Anti-Phishing Working Group.

Problem Statement

One major challenge with treatment and apprehension of cyber criminals is the issue of jurisdiction and the ability of existing legal frameworks to prosecute cybercriminals. In Ghana, the government passed the Electronic Transactions Act (Act 772) which addresses cyber crime issues but as indicated in Boateng et al (2010) the police still rely on conventional crime laws on false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Crimes committed under these laws are bailable offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber offences.

Obviously these laws provide a vent for the criminal as the weight of judgment is not in any commensurate to the depth of cyber criminal activities. It is therefore not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law. Most lawyers capitalize on such technicalities and have their clients acquitted (Boateng et al, 2011). The laws under which the suspects are charged are the existing laws on fraud established in 1960 which gives room for defense lawyers to often win when the prosecution presents poor evidence.

Premised on these issues are the fact also that cyber criminality is not well understood. As the internet expands, opportunities for unethical use will continue to increase if nothing is done in terms of understanding the modus operandi of the cyber criminal and the methods of victimization. This is reflected in the routine activity theory which posited that crime can be motivated by opportunities provided in routine activities. Incidentally, the use of the web falls perfectly into the domain of routine activities howbeit on a global scale. (Cohen & Felson, 1979).

Also ccorrelating level of education and poverty with cyber crime as a major factor for causation may not capture the entire picture and could be misleading. Research is therefore warranted to investigate cyber crime ploys and plots as a way of providing an insight into cyber victimization – particular cyber deception and theft which is becoming very common in Ghana.

Research Design

We collected primary data via the use of interviews and observation of cyber criminals and victims within Ghana but not restricted to Ghanaians. Close-ended and open-ended questions are asked using randomization via interviews to solicit information. The sampling technique used is simple random sampling. We further reviewed secondary data, published text that tends to highlight cyber deception and theft from a Ghanaian perspective.

Research Instrument

Interview questions were designed and validated by experts in the cyber crime field of study. The analysis of data collected is done qualitatively via an attempt to compare the findings from the primary data with the meanings derived from the secondary text for the purpose of using it to optimize the conceptualization of cyber deception and theft from the Ghanaian perspective.

Study Population

Specifically, 10 Internet Cafes known for cyber crime activities were visited and upon a socially engineered discussion with some observed perpetrators, interviews were granted. All the internet cafes were located within the Accra metropolis. Subsequently, a victim who had publicly discussed her case was approached for further interview as well one victim who had assisted the Ghanaian police in the arrest of her culprit. Despite the ten Internet cafes visited it was only four self acclaimed and practicing cybercriminals that opted to grant an interview for this research. A close observation was made to authenticate their stories for the purpose of determining the reliability of their responses. Furthermore, two perpetrators who are prosecuted and convicted cyber criminals are considered and discussed. Interview questions are provided in the appendix section.

Presentation of Information from Ethnographic Study

Responses from the interviews showed that several varying approaches were used by the culprits to socially engineer their way into defrauding victims. These ranged from scams of donations to orphanages, non existing Non-Governmental Organizations, business men and contractors with fake pictures of ministers awarding contracts as newspaper items with evidence of documents. Below are typical examples of the process culprits used to defraud a victim. For the purpose of ensuring privacy, names of culprits have been altered. What follows are extracts from the study

Cases from Non-convicted Criminals

The Case of Asare

The cyber criminal here is Asare, a 25 year old University student who posed as a 57 year old UK based Ghanaian in the construction industry. He convinced the victim that he was also a gold dealer. The victim was a 53 year old Philipino woman who worked with the Philippines Government Treasury Office.Asare successfully convinced the Philipino that he was based in United Kingdom (UK) though he was actually resident in Ghana. He achieved this by using "sucks", an application that routes telephone calls toll free with private number hence she was unable to determine the location from where a call was made. He also successfully acquired a legitimate UK telephone number via which calls were routed to Ghana whenever he received a call from the Philipino woman. This obviously gave the victim a false impression that the culprit was really in the UK. Asare explained that new dating websites with free services are the best sites to meet vulnerable clients.

Asare did not achieve all these on a silver platter though, he initially had major challenges accessing the dating site where the victim was available, and this was as a result of most Ghanaian Internet Protocol (IP) addresses that were blacklisted hence denied access. He therefore routed all his access via www.pagewash.com (pagewash). This website provides anonymous (Proxy) surfing that allows users to surf the net without having to worry about people knowing what they have done and where they have been. From pagewash, the web could be surfed safely and anonymously by entering the URL (website address) into the web address box and click the begin browsing button.

The site does not learn or know who the user is, does not save any cookies or track codes, makes it possible to surf anonymously and protect your privacy and security, and ensures fast and uncensored access at any time. The services are provided without warranty of any kind, expressed or implied, including warranty of merchantability or fitness for a particular purpose. Asare also had to overcome the hurdle of having live webcam chats with the victim. This he successfully achieved by the use of the "fakewebcam" application which enables a user record webcam clips and playbacks as if it is live. After successfully gaining the trust of the victim via regular chats, e-mail and telephone conversations Asare proposed a business deal which was agreed to by the victim. He proposed that he could export gold from Ghana to the Philippines for sale via a local Philipino company. His victim therefore decided to assist with the necessary processing using her credentials. The implication here was Asare would travel to Ghana and subsequently to Philippines with the gold for sale. All this was to be done with the victim's credentials as a major party to any brokered deal.

Asare further blackmailed the victim by then pretending to have arrived in Ghana and to have been arrested while attempting to travel to Philippines with the gold. The arrest was supposedly due to cocaine found in the gold without Asare knowing. With the Philipino woman's name being in the centre of affairs she was indirectly then implicated and therefore had co-operate with Asare and his legal advisors to clear his name. This then began a series demands for financial remittance as legal charges by the local legal team here in Ghana to help clear her name to avoid notification of the Philipino government. Asare in total defrauded his victim of a total sum of $1000 in chunks of $500, $200 and $300 over a three month period.

The Case of Dela

Dela is a Junior High School male dropout who patterned his approach after Asare's for a couple of months without success. He indicated that after several failed attempts and a subsequent visit to the "Malam" (fetish priest/ black magician), he has gotten a committed victim to remit $1500 per week. He explained his "Malam" is paid a mandatory 10% of every transaction. He explained that he was given a ring to wear and that made all the difference in succeeding. He explained all he had to do was to wear the ring every time he is communicating with the victim to request for any form of remittance.

The Cases of Nii and Nana

Two other males who are also Junior High School dropouts confirmed that after numerous failures and a subsequent visit to the "malam" (fetish priest/ black magician), they posed as female with contracted ladies showing their bodies during web cam chats to successfully defraud some victims online. They are together remitted an average of about $500 per week. They admitted that their remittances had started declining possibly due to increasing awareness of victims.

Cases from Prosecuted and Convicted Culprits

The Case of Collins and Onos

As reported on Yahoo Plus (2010), Collins and his accomplice Onos who were 23 and 25 years respectively were unemployed and resided in Nungua, Accra. They both thought they had the perfect format to swindle a Swede. In one of their e-mails to the Swede, they claimed that under their supervision as the Inspector-General of Police and a senior police officer respectively, they arrested five men at Ghana's Kotoka International Airport trying to illegally export a box containing $5 million and 50 kilograms of gold. They added that following investigation, it was discovered that the gold and money belonged to the Swede. They then advised the Swede to send some money so they could reward the arresting police officers in Ghana and ship the consignment from Ghana to Sweden.

Suspecting foul play, the Swede asked them to send copies of their identity cards and passport to show that they were real. They then sent copies of forged police identity card with number GPS 2216 H and biometric data page of passport number H 1527864, all bearing the pictures of the Inspector-General. The Swede alerted his friend, a retired police officer in Ghana, to his ordeal and the Ghanaian police swung into action. Both Collins and Onos have been prosecuted and convicted.

Victims of Cyber Crime

The Case of Karen

Karen is a British business woman who planned retiring into a new life with her new found internet lover and was defrauded of $100,000.She developed a relationship with a supposed retiring American Colonel via phone, text messages and internet chat after meeting on a dating website www.match.com. They planned to use the money to prepare a New York house for Karen to move in. She was supposed to meet him for the first time in New York and possibly start a new future together, it turned out the money went into a cedi account at reputable bank in Accra and with the help of an employee of the bank, the amount was withdrawn in three tranches by the fraudsters. Karen explained that the Colonel claimed he was part of the soldiers withdrawn by the United States government from Baghdad and was to take care of some properties wrongly shipped to Accra and would return to United States in two weeks.

Whilst in Accra, the Colonel allegedly got into some problems with the police and needed part of the amount to resolve the issues and invest the remaining in the property in the United States as agreed by the two of them. He requested that the money be paid to his lawyer who was litigating the case for him. Karen upon cross-checking from the Fraud Department of the United Kingdom Bank confirmed the existence of the account in Ghana before she transferred the money into an account at reputable bank in Accra, Ghana. With the help of an employee of the bank, the amount was withdrawn in three tranches. Karen never heard from the Colonel from that moment onwards and decided to take legal action against the bank for not doing enough due-diligence before the money was withdrawn. Her basis for legal action was how the Branch manager in Accra did not suspect how an 18 months old account owned by a trader could receive such a hefty amount, the first of its kind, without following the necessary banking procedures before releasing the amount in less than two days.

Five persons, the account holder, an employee of the bank and three others including a woman have been arrested by the police. They are currently being prosecuted at an Accra High Court.

There is no trace, at least not yet of the Colonel. It is still not clear if he was party to this sophisticated scam, or was impersonated. Karen cannot also confirm if he was indeed part of the United States Army. Narrating how the whole scam was uncovered, Karen said she had to liaise with the United Kingdom Fraud Department where she was told to be on the alert, that fraudsters are always selfish and would come back for more. According to her, a lady purporting to be the daughter of the missing Colonel contacted her after several weeks to announce the death of her lover. She claimed to be schooling in California but had to come to Accra to find out what had happened to her father. She wanted an amount of £3,000 to take care of the search for the father. Karen said she was advised by the Fraud office in UK to send the money via courier. Together with the Ghana police the fraudsters were arrested.

The Case of Anita

Anita is an Australian High School teacher who was defrauded through a dating website which involves money sent to a person in Ghana and not returned. The supposed fraudster was supposed to pay the money back upon arrival at Australia after having had over $24,745 in over ten transfer transactions. The culprit claimed to be a Canadian archaeologist based in London but happened to be working in Ghana and in conjunction with a Chief in Ghana who was sponsoring the dig. The National Museum in Accra Ghana was mentioned as part of the archaeological work. Anita communicated with the supposed Canadian in the United Kingdom over the Internet, phone and text messages. Subsequent investigation proved that all e-mail communication was from Ghana even when the culprit claimed to be in the United Kingdom. The implication is that even calls that she made to a legitimate United Kingdom number were diverted to Ghana as well. The culprit here was arrested when the law enforcement agencies were alerted of some more funds being transferred to via a money transfer service to a specific location at a specific time.

Concluding Remarks

The findings above clearly shows that the typical Ghanaian cyber criminal is hardly ever involved in spoofing or page-jacking, general merchandise and auctions. It is quite evident from the accounts of victims and perpetrators that the use of social engineering skills in a syndicate form tends to be a prominent feature in cyber deception and theft. Some unique observations that are worth drawing attention to are discussed below:

The Black Magic Factor

An interesting factor which came up during the interviews was the influence or effect of Black Magic on the success of cyber crime. It was believed by some culprits that black magic had played a significant role in the success of their cyber crime exploits. This phenomenon definitely would require proof to ascertain its authenticity. The perpetrators tend to believe that Black Magic can be used to hypnotize victims into parting with their money without a careful thought. It is also believed it can be used obtain unconditional sympathy from victims of cyber deception and theft.

The VIP Sections

A feature that was common with most of the Internet cafes was a special section referred to as the Very Important Person (VIP) section within the Internet cafes. It was a section reserved strictly for members of a certain category. The criteria for determining who deserves to be a VIP member was not very clear, it was also observed that most VIP members patronized the cafes at night and usually worked in groups.

Key Loggers

A disturbing observation that was made at four Internet cafes out of the 10 was the prevalence of installed key loggers which run in stealth mode. One needed to be relatively technical to detect its existence. The implication of key loggers at these cafes is that every key struck on the keyboard is recorded and can be read/known after a visiting customer had left the café.

Recommendations for Policy and Practices

Cyber deceptions and theft can be mitigated by a combination of pragmatic measures. Laws will have to be put in place mandating all Internet Cafes to adhere to specific standards set by the National Standards Board. The standards must clearly include normatives that provide guidelines for setting up internet cafes with strict enforcement. The purpose of this is to aid investigators in their search for electronic evidence. Law enforcement agencies must provide their computer crime investigators with the technology required to conduct complex technology based investigations. Besides access to technology, law enforcement agencies must also be given forensic computer support as many computer crimes leave "footprints" on the computer as well as on the Internet. Most prosecutors also lack the training and specialization to focus on the prosecution of criminals who use computer-based and Internet system as a means of committing crimes. Thus, they must have a working knowledge of computer-based and Internet investigations if they are to handle these crimes effectively.

There must be a task force from the government to investigate the activities of the Internet Cafes especially those with VIP sections that do not have clearly defined criteria for membership and usage of the VIP sections. Awareness in Information Security for the general public must increase with possible inclusion of information security practices in modern day school curriculum.

References

Boateng, R., Longe, O., Mbarikaz, V., Avevor, I., & Isabalija, R. (2010). Cyber Crime and Criminality in Ghana, Its Forms and Implications Americas Conference on Information Systems (AMCIS), In *Proceeding of the Sixteenth Americas Conference on Information Systems*, Lima, Peru.

Boateng, R., Longe, O.B, Isabalija, R., & Budu, J. (2011). Sakawa - Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact, 11*(2), 85-100.

Brennar, S. W., & Clarke, L. L**.** (2004). Distributed Security: A new Model of Law Enforcement. John Marshall Journal of Computer & Information Law, Forthcoming. Available at SSRN: http://ssrn.com/abstract=845085

Broadband DSLReports. Retrieved on July 2011, from http://www.dslreports.com/forum/r20184245-42-Million-HannafordSweetbay-Credit-Card-Numbers-Stolen.

Camp, L.J. (2009). Mental Models of Security, *IEEE Technology & Society*, *3*(28), 3-28. Taylor & Francis 2008.

CitiFM online news, Retrieved September 9, 2010, from http://www.citifmonline.com/site/news/news/view/11099/1.

Cohen, L.E., & M. Felson. (1979). Social Change and Crime Rate Trends: A routine activity approach. *American Sociological Review, 44*, 588-608

Dana, D.A. (2001). Rethinking the puzzle of escalating penalties for repeat offenders, *Yale Law Journal*, *110*, 733–783

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, *17*(1), 61–80.

Felson, M., & Clarke, R. (1998). *Opportunity Makes the Thief*. Policing and Reducing Crime Unit, Research, Development and Statistics Directorate Unit, Paper 98. London. Home Office

Grady, M. F., & Parisi, F. (2006). *The Law and Economics of CyberSecurity*, Cambridge University Press.

IC3 (2010). *Internet Crime Complaint Centre Report (2006-2010)*. Retrieved from http://www.ic3.gov/media/annualreports.aspx

Jahankhani, H., & Al-Nemrat, A. (2010). Examination of Cyber-criminal Behaviour. *International Journal of Information Science and Management*, 41-48.

Longe, O.B., & Osofisan, O.A. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. *The African Journal of Information Systems, 3*(1). Retrieved from http://digitalcommons.kennesaw.edu/ajis/vol3/iss1/2

Lovett, G. (2009). Fighting cybercrime: technical, juridical and ethical challenges. In Proceedings of the 2009 Virus Bulletin Conference, 63-

Paller, A. (n.d.). Predicting the future of cybercrime and security. British Computer Society. Retrieved May 2010, from http://www.bcs.org/server.php?show=conWebDoc.8126

Picker, R.C., (2004). *Cyber Security: Of Heterogeneity and Autarky*. U Chicago Law & Economics, Working Paper No. 223 (2D Series).

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet*, Pearson Prentice Hall.

Slatalla, M. (n.d.). A Brief History of Hacking. Online. Discovery Communications, 28 Oct. 2003. Retrieved from http://tlc.discovery.com/convergence/hackers/articles/history.html.

Spylogic.net (2008). *Lesons learned from the Lowe's hacker Brian Salcedo*. Retrieved July 2011, from http://www.spylogic.net/2008/05/lessons-learned-from-the-lowes-hacker-brian-salcedo

Wavefront Consulting Group (n.d.). A Brief History of Cybercrime. Retrieved May 2010, from http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime-4.html.

Wired.com, (2011). Crazy-Long Hacker Sentenced Upheld. Retrieved July 2011, from http://www.wired.com/science/discoveries/news/2006/07/71358 [Accessed July 2011]

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Yahoo Plus (2010, July). The New Face of 419. Retrieved July 2011, from http://thenewsafrica.com/2010/07/21/yahoo-plus-the-new-face-of-419.

Zuley C., Clawson J., Cordell M. (2003). A brief history of hacking, LCC 6316: Historical Approaches to Digital Media, p.6

APPENDIX

Extracts from the Questionnaire Administered to Non-convicted Criminals

How old are you?

What is your nationality?

What is your highest level of education?

Are you gainfully employed? If so what is your level of income?

How did you get involved with this business? (Cyber deception and theft)

How do you go about the deception and theft from your victims?

What is your main motivation for being involved in this business?

Have you been hired by someone to do this as a paid job?

How much money do you make and how often do you make the money?

Some of your colleagues believe their success in this job depends on supernatural powers; do you share the same view?

Do you think your victim ever had doubts about your credibility at some point? If so how did you succeed in persuading them to be convinced that you were genuine?

Is there any secret to your success in cyber deception and theft?

Extracts from the Questionnaire Administered to Victims of Cyber Crime.

How old are you?

What is you nationality?

What is your highest level of education?

Are you gainfully employed? If so what is your level of income?

How did you become a victim to cyber deception and theft?

Can you explain in details how they(culprit) successfully defrauded you?

Why did you remit money to the culprit?

How did you remit money to the culprit?

How much money did you remit and how often did you remit the money?

Did you think you were hypnotized by the culprit(s) in anyway?

Did you at any point have doubts about the credibility of the culprit?

[1] Mr. Paul Danquah is a Lecturer with the Faculty of Information Technology, Pentecost University College and currently a PhD Candidate at the Accra Institute of Technology. His holds a MSc in Information Security from Anglia Ruskin University (UK), a BSc (Hons) in Computing from the University of Greenwich (UK), a Graduate Diploma in MIS, and the professional certifications MCSE and CCNP with over 8 years industry experience.

[2] Dr. Olumide Babatope Longe is the consulting director for cyber crime research at the PearlRichards Foundation. His research interests include cybercrime causation, apprehension, treatment, prevention using social theories and information security models. He is a Fellow at the Massachusetts Institute of Technology Science & Technology Initiatives and also on faculty at the Department of Computer Science, University of Ibadan, Ibadan, Nigeria. He can be reached at longeolumide@ieee.org or longe@mit.edu; Phone: Nigeria +2348024071175 and USA +1(857) 207-8409.