Beyond E-Mail Headers: An Ethnography-Based Model for Counteracting Socially Engineered Cyber Deception

P. Danquah
Deputy Director of IT Infrastructure and Engineering
University of Professional Studies, Accra, Ghana
padanquah@ait.edu.gh

O.D. Ogunsanwo
Department of Computer Science
D.S. Adegbenro ICT Polytechnic
Itori-Ewekoro
Ogun State, Nigeria.
jidos1@hotmail.com, jidos2@yahoo.com

O.B. Longe
Department of Computer Science
Adeleke University
Ede, State of Osun, Nigeria
longeolumide@fulbrightmail.org

ABSTRACT

Cyber-Deception and Theft is a type of cyber crime that involves stealing (money, property), typical examples include credit card fraud, intellectual property violation and piracy, page-jacking, general merchandise, auctions, advance fee fraud, and phishing. A peculiar and prominent feature in Ghana has been the use of social engineering skills to successfully defraud unsuspecting victims. This research uses an ethnographic study of criminals and secondary published text that highlights cyber deception and theft to determine the consistent behaviour of perpetrators of cyber deception and theft in Ghana. Based on the consistent behaviour observed, a model is proposed to counteract the socially engineered approach to cyber deception and theft. The model does not apply to the types that exclude social engineering such as intellectual property violation and piracy.

Keywords: Cyber crime, deception, ethnographic, page jacking, theft, cyber criminals and security.

African Journal of Computing & ICT Reference Format:

1. INTRODUCTION

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. Cyber-Deceptions and Theft is a type of cyber crime that involves stealing (money, property), typical examples include credit card fraud, intellectual property violation and piracy.

Cyber deception and theft comes in various forms, some of which are identity theft, [16], Spoofing or Page-jacking [11], Credit Card Schemes [14], General Merchandise and Auctions [15], Advance Fee Fraud [8] and Phishing. Longe and Danquah ([16] showed in their findings that the typical Ghanaian cyber criminal is hardly ever involved in spoofing or page-jacking, general merchandise and auctions.
Evidence from the accounts of victims and perpetrators showed that the use of socially engineering skills in a syndicate form tends to be a prominent feature in cyber deception and theft. Longe and Danquah [16] also explained further a unique observation that is worth drawing attention to. This was The Black Magic Factor which definitely would require further research and proof to ascertain its authenticity. The perpetrators of this 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 the cyber deception and theft.

This research uses an ethnographic study of criminals and secondary published text that highlights cyber deception to determine the consistent behavior of perpetrators of cyber deception and theft in Ghana. 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 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 remaining part of the paper is organized as follows. The subsequent sections address the methodology, relevant theories, findings and analysis, model to displace cyber deception and theft.

2. RELEVANT LITERATURE

There are numerous theories advanced to explain the commission of crime as a whole, these theories tend to approach the subject from various fields of study which range from legal, social science, psychology and even technology. The section of theoretical framework discusses theories from all the above mentioned fields of study and attempts to relate these theories to cyber crime. Below is an elaboration of two relevant theories considered.

2.1 Routine Activity Theory (Crime Theory)
The Routine Activity Theory is a criminological theory that was propounded by Cohen and Felson in 1979, the theory presupposes that for a crime to be committed, the following must be concurrently present:

(a) A suitable target is available: The suitable target here refers to a person, object or place.
(b) There is lack of a suitable guardian to prevent the crime from occurring: The capable or suitable guardian refers to a deterrent like police patrols, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems.
(c) A motivated offender is present: This presupposes that there can be no victim without the intentional actions of another individual.

This theory definitely applies to cyber crime regardless of the category. It must be emphasized that a crime must occur when there is the opportunity for the crime to be committed. Opportunity is the cause of crime and indeed root cause of crime. For cyber crime to be successfully committed, the opportunity for crime is multiplied by the simple fact that the criminal is no longer "place-bound". The routine activity theory was confirmed by Bossler and Holt in their 2009 publication On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory.

2.2 Crime Displacement
Cox, Johnson & Richards [6] The primary focus of crime reduction is opportunity reduction. The logical question is whether or not such efforts simply displace or move the crime to another locale. Crime Displacement may involve the following:

(a) Geographical: Moving Crime from one location to the other.
(b) Temporal: Moving Crime from one time to the other
(c) Target: Moving Crime from one target to the other
(d) Tactical: Changing the approach to committing the crime from one to the other
(e) Crime type: Changing the type of crime that is to be committed (Felson and Clarke 1998)

The use of Crime Displacement as a method of reducing crime may have varying outcomes, these are;

(a) Positive: A crime is displaced to a less serious damage. It represents a success since it produces a net gain.
(b) Negative: A crime is displaced to a more serious crime with greater reward or greater social cost.
(c) Neutral: A crime is displaced to one of the same seriousness, of the same risk, rewards and damage.
(d) Even-Handed: Prevention is concentrated on those who are repeatedly victimized in order to achieve a more equitable distribution of crime.
(e) Attractive: Activities and/or places attract crime from other areas or activities (eg-red light districts attract customers from other areas, as well as other criminal activities)

2.3 Industry Experts’ Perspective
Upon sampling publications on the perception of industry experts, industry players are in agreement regarding the need for real-time, behavior-based security. Gartner [21]
The network, in order to examine their contents using that intercept these packets as they are travelling through a network of computers, until they reach their destination, where they are assembled back into a message (emails, images, videos, web pages, files, etc.) are required to be available for unimpeded real-time monitoring by the American Federal law enforcement agencies. CALEA (n.d)

Computer surveillance is the act of performing surveillance of computer activity, and of data stored on a hard drive or being transferred over the Internet. Computer surveillance programs are widespread today, and almost all Internet traffic is closely monitored for clues of illegal activity.

Surveillance Software is a computer monitoring program to secretly monitor and record user's activities on computer. Spylab (n.d). In terms of the legality of its usage, according to the Spy Act passed in October 5th 2004 by US houses, installation of advertising or data gathering spyware without authorization or the computer owner's consent is prohibited. Main part of the Spy Act is about adware and spyware related software and website which use to gather user information for advertisement.

Much as monitoring all Internet traffic is important for security reasons, concerns over privacy and the possibility of a totalitarian state where the government aggressively uses electronic technologies to record, organize, search and distribute forensic evidence against its citizens. The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. Diffie, Whitfield and Landau [10] In the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by the American Federal law enforcement agencies. CALEA (n.d)

One such technologies that is used to achieve surveillance is packet sniffing, packet sniffing is the monitoring of data traffic on a computer network. Computers communicate over the Internet by breaking up messages (emails, images, videos, web pages, files, etc.) into small chunks called "packets", which are routed through a network of computers, until they reach their destination, where they are assembled back into a complete "message" again. Packet sniffers are programs that intercept these packets as they are travelling through the network, in order to examine their contents using other programs [7].

The United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system considers accountability as fundamental and significant requirement for securing systems. The Trusted Computer System Evaluation Criteria (TCSEC) is used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information [9].

The antecedents to accountability in this context are:

1) Identification - The process used to recognize an individual user.
2) Authentication - The verification of an individual user's authorization to specific categories of information.
3) Auditing - Audit information must be selectively kept and protected so that actions affecting security can be traced to the authenticated individual.

In the article “The Growing Web Threat”, it is explained that URL Filtering was primarily designed to monitor employees Internet activity and enforce acceptable usage policy in order to avoid hostile workplace litigation.

However URL Filtering suffers a fundamental flaw to be an effective security filter; it does not monitor threats in real-time.” Furthermore, “Malware filtering is increasingly important and provides an immediate return on investment (ROI) [17]. Other statements from industry experts that tend to buttress the need for behavior based security are outlined below.

- “The evolution of the threats has made protection based on behavioral detection techniques indispensable” [12].
- “Based on signatures, anti-virus software is dying - we need Behavior-based Interception,” John Pescatore, Gartner Analyst at Network World
- ”Behavioural-based anti-malware with smart algorithms is the best way to detect and block such attacks on Web 2.0 sites,” Nigel Stanley, Bloor Research - IT Week, Nov 30, 2006
- “The consensus seems to be either don't let your employees use these [Web 2.0] sites at work, or make sure you have some form of real time, behaviour-based content security in place,” Phil Muncaster - IT Week blog, November 30, 2006

opined that “Traditional signature-based antivirus products can no longer protect companies from malicious code attacks. Vendors must execute product and business strategies to meet the new market requirements for broader malicious code protection”. Clyde [4] also emphasized that “Reactive, signature-based protection is becoming less effective. The time from software patch to exploit is dropping below the time needed for companies to install the patch. Even if you start when the patch is released, most IT departments will take 30 days to test and patch a system and hackers are faster than that now. Therefore we need more proactive security, behavior-blocking looks promising”.

...
The above extracts show the gaping need for proactive research into determining the behavioural patterns of cyber criminals and crime ware. It however needs to be emphasized that an attempt to monitor behavioural patterns of cyber criminals is very likely to infringe on the privacy of computer users.

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.

3. METHODOLOGY

Primary data is collected via the use of interviews and observation of cyber criminals after obtaining police clearance to carry out ethnographic study (under cover). The perpetrators are all within Ghana but not restricted to Ghanaians, close-ended and open-ended questions are asked via interviews to solicit information. The sampling technique used is simple random sampling. Secondary data that tends to highlight cyber deception and theft from a Ghanaian perspective is further reviewed. The interview questions were designed and validated by experts in the cyber crime field of study.

The study population involved three non-convicted self acclaimed and practicing cybercriminals that opted to grant an interview for this research. A close observation (ethnographic) was made to authenticate their stories for the purpose of determining the reliability of their responses.

4. FINDINGS

The Case of BKS:

<table>
<thead>
<tr>
<th>Interview with BKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question:</strong> I am aware you do a lot of credit card hacking and usage online, how exactly do you get it done?</td>
</tr>
<tr>
<td><strong>Answer:</strong> I either access a website that sells credit cards or I use a hacker to provide me with the needed credit card and the details. I usually use the hacker, I get access to the hacker through the internet sites like the hacker s’ lounge at <a href="http://www.yahoo.com">www.yahoo.com</a> etc. One essential requirement from our part of the world is to have a liberty reserve, this is an online account that enables make payments for services rendered by the hackers. Once you have successfully stashed your liberty account with the money needed, then you purchase the credit card from the hacker with money in that account. Prices of the cards vary depending on what type of credit card you intend to buy. American Express and Discovery are the relatively expensive cards, cards like Mastercard and Visa are usually fairly moderate in price. There are also company cards that usually have quite a lot of money. Some of these hackers are just in to rip us off our money, some of them collect the money but never offer any service. Sometimes they rather give us bad credit cards. You can also access site like ww.cardexstore.com to purchase a credit card, again you may have to pay with liberty reserves, that is more reliable but the sites really change often. There is a network of dealers who circulate the new site addresses to each other.</td>
</tr>
<tr>
<td><strong>Question:</strong> How do you successfully receive the items you buy with the credit cards?</td>
</tr>
<tr>
<td><strong>Answer:</strong> Usually, you must have developed a relationship with someone you can trust, you can then use the person’s address as the receiving address of the items purchased. The person then in turn would send the items to you. Usually it is not safe for you to receive the items in person so you have to work it out with some custom official. A few times I have picked up the items myself. Take note, the supposed friend who sends you the items must be someone with whom you have built a friendship of trust over a period. That is usually done by buying the individual presents occasionally over a long period like six months and over. One other thing, some of the credit cards are what is called “verified by data”, those ones usually have passwords and payment with those are usually declined. It is important you these so you don't choose the wrong type.</td>
</tr>
<tr>
<td><strong>Question:</strong> How much do you usually pay for the credit cards?</td>
</tr>
<tr>
<td><strong>Answer:</strong> About $3 to $5 per credit card. Some of the sites expect you to register, those ones usually charge $50 and over before they provide any services.</td>
</tr>
</tbody>
</table>
Question: Have been successful in this endeavour?

Answer: I have been able to purchase a lot of items with the use of this method, I have purchased laptops, Ipads, even my shirt and slippers.

Question: What tools or software do you use to assist you with this endeavour?

Answer: Well, before you can hack or buy something online, you must get a VPN and a very strong one, you need to hide your identity or location by going to vpn.com or hidemyass.com to change your IP address to make it reflect as if you in the US or some other part of the world.

Question: Have you ever been successful not going through the proxy server, I mean going directly to buy items online?

Answer: No no, the system won't allow you.

The Case of Dodoo

Interview with Dodoo: Dodoo is a final year University student, studying Information Technology.

Question: How are you able to successfully gain access to credit cards?

Answer: There is a payment service called liberty reserves, I usually pay money into a liberty account and then I use the reserves in the liberty account to pay for services of hackers who can gain access to the credit card details. When I register with liberty, I am provided with a login, password and the master key which is the identification number of my liberty card. This payment service can be used to conduct legitimate business payments, it just so happens that a lot of the online scammers are the ones who use it.

Question: Once you pay for the hacking services and successfully obtain the credit card details, how do you purchase items and ensure you have received them?

Answer: The key is finding someone you can trust, you need to have built a relationship with that person to establish that trust. When the items are purchased, they are delivered at that person's address and then it is subsequently mailed to you here in Ghana. In Ghana it important to also have an insider at the port who will assist you with clearing without you being indicted. Most of the time you don't use have to use your real name to obtain the items.

Question: When you communicate with the hackers and also make purchases online, do you do that directly from your PC or you use proxy servers?

Answer: No, I dont go directly, there are tools like "hide my ass" and "anchor" which enable you change your IP address to make it seem as if you are from another country of even sometimes unknown. Once you make the change, you can confirm by accessing a site like "whatismyip.com" to confirm the change.

A Chronological analysis of Dodoo's screenshots are provided below;
Figure 1: Original Network Configuration Check (ipconfig /all) at 3.00pm on 12th March, 2012
Source: Field Study

Figure 2: IP Address is: 10.128.125.169
Source: Field Study
Figure 3: Enabling AnchorFree Software’s VPN Tunnel at 3.01pm on 12th March, 2012
Source: Field Study

Figure 4: Confirmation of VPN Tunnel Connection via AnchorFree Software at 3.02pm on 12th March, 2012
Source: Field Study
Figure 5: Confirmation of Network Configuration after VPN creation (ipconfig /all) at 3.03pm on 12th March, 2012
Source: Field Study

Figure 6: IP Address is still: 10.128.125.169 but Tunnel Interfaces/adapters have been created.
Source: Field Study
Figure 7: Confirmation of Public IP Address while on AnchorFree VPN Internet Connection at (www.whatismyip.com) at 3.05pm on 12th March, 2012
Public IP Address is: 216.172.135.126 from California, US
Source: Field Study

Results above and below shows a consistent hop from private address 10.93.96.41 through two other private IP addresses to public address 41.190.88.225 before any other route is used. A subsequent confirmation of Public IP Address while on disconnected from AnchorFree VPN Internet Connection at (www.whatismyip.com) at 3.17pm on 12th March, 2012 showed the public IP Address is: 41.190.90.37 from Ghana.
The Case of Yaw

Yaw is a University student who was also quite open with providing information about his activities. He therefore granted an interview of which the salient responses are transcribed below. He comes from a seemingly disciplined background with a very keen interest in technology. He is an IT student in his final year at the University. He came across as quite sincere with his responses; he did not hesitate at all.

Question: How have you been successful in internet fraud activities?
Answer: I first had the idea when learned about key loggers and what they could be used for, I became curious and one thing led to another. I must say that I am not into defrauding people online. I search for usable credit card numbers online and use them to purchase downloadable (soft copy) products like books, journals, movies and music. I cannot be sure if delivering a tangible item to a physical address somewhere. It may put the recipient in trouble hence I use my online identification.

Question: What exactly do you do to get access to these credit card numbers?
Answer: You go online and search for credit card numbers, one key word that has been very helpful is “discard”. Once I am successful in finding some numbers, I then need to look for a valid address to be used for the card. On average if I find 10 card numbers and five valid addresses I am able to shop satisfactorily. There are different types of cards like Visa, Master Card, Discovery etc. They all have specific sites where they are usable and vice versa.

Question: How sure are you that no one knows you are being tracked and could be arrested?
Answer: I make sure I always cover my tracks by using a proxy server most of the time. I know those servers usually go out as anonymous, but I sometimes have to resort to a direct access since the proxy does not seem to be accepted by all websites.

Question: You mentioned key loggers, what about it? Tell me how you use them.
Answer: Well, I know some Internet Cafes use them to obtain vital information for accessing people’s accounts. I just happen to know how it works but I have never used it to collect anyone’s confidential information.

Longe an Danquah (2011) gave a classic case of cyber deception and theft as follows;
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 Filipino woman who worked with the Philippines Government Treasury Office. Asare successfully convinced the Filipino 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 Filipino 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, 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, 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 Filipino 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 Filipino woman’s name being in the center of affairs she was indirectly then implicated and therefore had cooperate 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 Filipino 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.

4.1 Inferences from Findings
A consistent behaviour deduced in the approach of the interviewed perpetrators is as elaborated below, a review of Longe and Danquah [16] and Warner [19] which both focused on approach to cyber crime in Ghana tends to confirm the ensuing outlined behavior;
Perpetrators of Cyber Deception and Theft typically engage in the following:

1. Attract Attention: The perpetrator attracts the attention of the victim via chat, text messaging or e-mail.
2. Collect/Exchange Information: The perpetrator exchanges some information with the would-be-victim over a period of time.
3. Develop Cordial Relationship: The perpetrator builds a relationship with the victim by regular communication which develops over time into a convivial relationship.
4. Establish Trust: Trust is established after a cordial relationship has been built, the trust is developed via various means, most of which emanates from buying of gifts for the victim and introducing victim to supposed close pals and family.
5. Trigger a bait/ Access Victim: With the established trust, victims tend to be willing to offer varying forms of assistance or sacrifice to the perpetrator.
6. Commit Offense: This usually provides the ideal opportunity for the perpetrator to launch the attack.
7. Clear Tracks (Optional): Some perpetrators tend to disappear from the cyber world after successfully committing their offense whereas others continue until their victims are of no benefit to them again.
As indicated earlier, this is typical of cyber deception and theft. A striking indication is that social engineering is prominent. Social engineering, in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. Goodchild [13]. The perpetrators, in this context tend to be deceptive mostly from step one all the way to the step seven. One distinct type of cyber theft which does not adhere to this modus is Cyber piracy, this involves the use of technology in unauthorized ways to reproduce copies of proprietary software and proprietary information, or to distribute proprietary information (in digital form) across a computer network. Cyber piracy must be addressed separately in future research.

Upon observations made, tests carried out as shown with screen shots in findings and responses from interviews, it is evident that it is quite simple to fake one’s location and identity to buttress the whole deception and theft agenda. This is the case because users with very little technical knowledge can use tools like “hide my ip” or “hide my ass” to pretend they originate from locations that are untrue. This is by virtue of the fact that locations are tracked with the use of Internet Protocol (IP) addresses, these addresses are captured usually in headers of applications used to communicate via mail.

Once content of these headers are compromised, the deception agenda is successfully achieved. This tends to render all IMAP based mailing systems quite limited in determining location accurately, this is because they are centralized and their source addresses do not depict the real location users. The use of various tools to create Virtual Private Network communication between remote proxy servers and the destination servers they communicate with tends to successfully conceal their locations even better. There also does not seem to be any absolute identity verification solution on the internet, this facilitates perpetrators’ anonymity or false pretense activities.

Users of mailing, chat and social network systems tend to easily provide false information about their identity and that is ultimately used to deceive the victims. Industry experts have propounded various approaches to dealing with cyber security, some of which were discussed under the “Industry Experts Perspective” section. These approaches range from permission based, accountability based and behavioural based, in all these they suggestively emphasize the essence of ensuring the key security requirements are implemented. These requirements are namely; access, identification, authentication, authorization, privacy and non-repudiation.

4.2 Analysis of Findings

Having deduced this pattern of behaviour as typical of the cyber deception and theft perpetrators, the obvious objective is to determine ways of combating this menace. This triggers the usefulness and relevance of the crime displacement theory and the respective security requirements. The various stages of behavior are considered individually;

1. Attract Attention: This behavior involves the perpetrator attracting the attention of the victim via some form communication using chat, text messaging, e-mail or social networking site. At this stage, the perpetrator is inherently fortified by the right to privacy, the deception may not necessarily originate here however, there is that obvious potential of a false pretense.

2. Collect/Exchange Information: This stage where the perpetrator exchanges some information with the would-be-victim over a period of time. Typically as evidently enumerated under the findings section, this information includes personal information. At this stage, a perpetrator who has a pre-conditioned mind would be deceptive at this stage. This is the stage where perpetrators provide false identities and false information about their location.

3. Develop Cordial Relationship: When it comes to the building of relationships with the victim by regular communication which develops over time into a convivial relationship, the perpetrator has every right to privacy. There is however the tendency that the deception would continue, one obvious trait observed with most perpetrators was their almost tremendous availability for communication during this stage.

4. Establish Trust: The development of the cordial relationship evolves into trust after perpetrators have consistently fuelled the relationship with reliable communication, buying of gifts for the victim and introducing victim to supposed close pals and family. At this stage in the development of the relationship development, the perpetrator again has every right to absolute privacy in communication.

5. Trigger a bait/ Access Victim: Within this context, the cyber criminal thrives on the established trust to either create an indicting situation for victims or they appeal to victims to offer varying forms of assistance or sacrifice to the perpetrator. At this stage the perpetrator again has every right to absolute privacy in communication; however, this is where the deception virtually culminates into theft.

6. Commit Offense: At this stage the perpetrator successfully steals. Based on the findings, most offenders tend to pretend a change in location or routine as they maintain their false pretense.
7. Clear Tracks (Optional): At this stage, perpetrators use their discretion to decide how to continue with the relationship. They may disappear from the cyber world with that specific identity after successfully committing their offense or continue to exploit their victims. Warner [19] accurately explained the significant difference between Nigerian fraudsters and the Ghanaian. It was explained that Nigerians typically would keep going until victims are totally depleted whereas Ghanaians tend to end their exploits after just one or two successes.

4.3 Technical Analysis

Figure 4.4 and shows Original Network Configuration Check (ipconfig /all) at 3.00pm on 12th March, 2012 and shows the IP address of the PPP adapter to be 10.128.125.169. Figure 4.6 and 4.7 shows the Enabling of the AnchorFree Software’s VPN Tunnel at 3.01pm on 12th March, 2012 and a confirmation of VPN Tunnel Connection via AnchorFree Software at 3.02pm on 12th March, 2012. Upon confirmation of Network Configuration after VPN creation (ipconfig /all) at 3.03pm on 12th March, 2012, IP Address is still: 10.128.125.169 but Tunnel Interfaces/adapters have been created.

Figure 4.9: Confirms the Public IP Address while on AchorFree VPN Internet Connection at (www.whatismyip.com) at 3.05pm on 12th March, 2012 to be 216.172.135.126 from California, US Figure 4.10: An attempt to trace the path to destination via (tracert) to www.hp.com and www.bbc.co.uk while on AchorFree VPN Internet Connection at 3.10pm on 12th March, 2012. Results in Figure 4.11 shows a hop from private address 10.90.112.1 to public address 174.115.1.11 before any other route is used.

Upon termination of VPN connection via AnchorFree is terminated at 3.12pm as shown in Figure 4.12, a confirmation of path to destination via (tracert) to www.hp.com and www.bbc.co.uk while disconnected from AchorFree VPN Internet Connection at 3.16pm on 12th March, 2012 in Figure 4.13 showed a consistent hop from private address 10.93.96.41 through two other private IP addresses to public address 41.190.88.225 before any other route is used.

A subsequent confirmation of Public IP Address while on disconnected from AnchorFree VPN Internet Connection at (www.whatismyip.com) at 3.17pm on 12th March, 2012 showed the public IP Address is: 41.190.90.37 from Ghana (shown in figure 4.15). The deduction from the chronology of events tracked implies the tool in question (AnchorFree) enables one deceptively pretend to be at another geographical location without the victim’s knowledge. One peculiar finding is that the original IP address of the perpetrator’s computer (PPP, Ethernet or Wireless) tends to remain the same as a new tunnel adapter is created with the new fake IP address assigned. A trace route also shows different hop paths for the VPN and non VPN links respectively.

The implication is that the only sure way to know a remote user’s real IP address is to invoke a local command to determine the real locally assigned IP address to the Ethernet, PPP or Wireless Adapters. It needs to be mentioned here that these addresses may not necessarily always be public address hence a tracing of path would serve as an assistant to determining the real address. These deductions prompted a further fundamental investigation with free online mail services; an experiment was carried out to determine if the use of a VPN tunnel influences the determination of source addresses of users.

The experiment involved e-mails being sent from a test account on yahoo.com to itself and an assessment of how the mail server records the source IP address. The results showed as exhibited on the next page.
Test Mail to Self without VPN Tunnel via Ethernet Adapter
Received: from [80.87.82.194] by web121703.mail.ne1.yahoo.com via HTTP; Mon, 16 Apr 2012 10:46:23 PDT

Test Mail to Self with VPN Tunnel via PPP Adapter

- **Inbox Copy Header:**
  Received: from [209.73.137.168] by web121701.mail.ne1.yahoo.com via HTTP; Mon, 16 Apr 2012 11:52:11 PDT

- **Sent Items Copy Header:**
  From Test Account Mon Apr 16 11:52:11 2012
  X-Apparently-To: testaccount@yahoo.com via 98.138.91.218; Mon, 16 Apr 2012 11:52:11 -0700

- **Local Network Configuration Check**
  PPP adapter Zain Internet:
  IPv4 Address. . . . . . . . . . . : 10.128.43.176(Preferred)
  Subnet Mask . . . . . . . . . . . : 255.255.255.255
  Default Gateway . . . . . . . . . : 0.0.0.0
  DNS Servers . . . . . . . . . . . : 10.93.86.248
  10.93.86.249
  Connection-specific DNS Suffix . : hshld.com
  Description . . . . . . . . . . . : Anchorfree HSS Adapter
  Physical Address. . . . . . . . . . : 00-FF-D3-77-49-E1
  DHCP Enabled. . . . . . . . . . . : Yes

Auto configuration Enabled . . . . : Yes
DHCP Server . . . . . . . . . . . : 10.37.23.254
DNS Servers . . . . . . . . . . . : 10.37.16.1

Test Mail to Self without VPN Tunnel via PPP Adapter

- **Inbox Copy Header:**
  Received: from [41.190.88.245] by web121703.mail.ne1.yahoo.com via HTTP; Mon, 16 Apr 2012 12:02:47 PDT

- **Sent Items Folder:**
  From Test Account Mon Apr 16 12:02:47 2012
  X-Apparently-To: testaccount@yahoo.com via 98.138.90.192; Mon, 16 Apr 2012 12:02:48 -0700

- **Local Network Configuration Check**
  PPP adapter:
  IPv4 Address. . . . . . . . . . . : 10.128.43.176(Preferred)
  Subnet Mask . . . . . . . . . . . : 255.255.255.255
  Default Gateway . . . . . . . . . : 0.0.0.0
  DNS Servers . . . . . . . . . . . : 10.93.86.248
  10.93.86.249
  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix . : hshld.com
  Description . . . . . . . . . . . : Anchorfree HSS Adapter
  Physical Address. . . . . . . . . . : 00-FF-D3-77-49-E1
  DHCP Enabled. . . . . . . . . . . : Yes
  Auto configuration Enabled . . . . : Yes

The results above shows that again, the use of the VPN tunnel creates a false impression of the source of IP addresses used to access this remote mail server. As established, this approach is a common trend with numerous tools being available for such activities.

4.4 Analysis in Perspective
The determination of source addresses of users is generally determined via data captured in headers of transmitted packets. The IP addresses that are shown in free mail headers for instance are obviously obtained from a layer 3 activity that reads the source address of the packet being transmitted; this makes it possible for an encapsulated packet to provide an address that may not be the actual original source of the user. Besides, mail servers running the IMAP protocol serve as both client and server hence they tend to provide themselves as the source address. This again does not provide very accurate header information as to the real source of the mailing system’s user. The above presupposes that there is a fundamental security limitation in the software communication services used over the internet, the element if identification and authentication lapses demonstrated, makes it vulnerable to being exploited by perpetrators of cyber deception and theft via social engineering methods.
An evident phenomenon derived from the findings is the false pretense and impersonation or identity theft, this factor tends to be successful via sophisticated syndicates where technical expertise is required in conjunction with cyber trespass activities. To avoid being tracked down, perpetrators have a highly spatio-temporal nature where they offer services (technical expertise) for very limited amounts of time and with continually changing addresses.

5. MODEL TO COUNTER ACTIVITIES

This model leverages on the Crime Displacement Theory, fundamental security requirements and recommendations from Industry experts. The crime displacement emphasizes that displacing crime from one locale to the other is an effective crime control method, the displacements could be target based, time based, location based, approach based or type based. Also fundamental to the provision of efficient and effective security are the requirements access, identification, authentication, authorization, privacy and non-repudiation. Industry experts have also advanced several approaches to enhancing security amongst which are permission based, accountability based, behavioural based and surveillance. The model below tends to leverage on all the above stated recommendations to recommend an effective and efficient method to deal with this phenomenon of socially engineered cyber deception and theft.

![Fig. 1: Model To Counteract Socially Engineered Cyber Deception and Theft](image-url)
Table 1: Below are antecedents to the various components of the model:

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Antecedents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission</td>
<td>• Access</td>
</tr>
<tr>
<td></td>
<td>• Identification</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Authorization</td>
</tr>
<tr>
<td></td>
<td>• Privacy</td>
</tr>
<tr>
<td></td>
<td>• Non-repudiation</td>
</tr>
<tr>
<td>Accountability</td>
<td>• Identification</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Auditing</td>
</tr>
<tr>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td>• Access Mode</td>
</tr>
<tr>
<td>Surveillance</td>
<td>• Content</td>
</tr>
<tr>
<td></td>
<td>• Motive</td>
</tr>
<tr>
<td>Behaviour</td>
<td>• Regularity of:</td>
</tr>
<tr>
<td></td>
<td>• Identification Access</td>
</tr>
<tr>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td>• Content</td>
</tr>
<tr>
<td></td>
<td>• Motive</td>
</tr>
<tr>
<td></td>
<td>• Change</td>
</tr>
</tbody>
</table>

Definition of Antecedent

- **Access**: Ability to permit or deny the use of an information asset, resource or facility
- **Identification**: How a user tells a system who he, she or it is, the basic requirements for identification are uniquely identify, should not reflect position and should avoid using shared accounts
- **Authentication**: The process of verifying an identity, this may something you know, have, are or do
- **Authorization**: Defines a user’s right and permissions on a system. Ability to determine rights, roles and privileges specific to the authenticated identity. Roles refer to who you are in context, privileges refer what you can do and eligibility is what you can have.
- **Privacy**: Privacy is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes.
- **Non-repudiation**: Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message
- **Access Mode**: Connection point of the user and the adapter (together with the configuration parameters eg-MAC address, IP address, Gateway address, DNS server etc) on the user’s local machine used to connect to the network or internet.
- **Content**: Content refers to web content which may be text, audio, images, videos and animations. Primarily it the information transmitted over the internet.
- **Motive**: Reason for access and specific activities online.
- **Location**: This refers to the geographical location of the user. This location is derived from the true and authentic source IP address of the user. This is further explained under the “Tracking Actual Geographic Locations” section.
- **Change**: Variation in activities online from specific identities, locations and all relevant antecedents.
5.1 Discussion on Model and Privacy
The entire model operates within relevant policy, in the absence of relevant policy, this model will be extremely difficult to implement. The prevention of socially engineered cyber deception and theft would require a combination of permission based security, accountability based security, surveillance and behavior based security. As explained in the table above, all the respective antecedents are required for efficient implementation. Permission and accountability based security are fundamental to ensuring users don’t commit crime, the accountability aspect ensures they can always be tracked should there be any form of suspicion with their activities. The permission component actually restricts privileges based on the policy in place. An extension of these is the surveillance component, arguments may be advanced to advocate the need for privacy, while this is just, the reserved right to review content and motive must always be included in policy to ensure the state always has some level of ultimate control to investigate threatened social order and optimize security. The combination of the success of security measures for socially engineered cyber deception and theft would serve as an input for behavioural patterns of this category of cyber criminals, the known behavior would subsequently inform the amendment of policy and optimization of the various model components.

5.2 Tracking Actual Geographic Locations
Evidence from the interviews and the research results show that majority of the culprits rely on VPN tunnels created to perpetrate their deception and theft. These VPN tunnels as shown in figure 4.11 prove to rely on private IP addresses issued to end users, this implies that even when a path tracing (eg-“tracert” on Ms Windows) command is issued at the source, there tends to be a leap to some remote anonymous proxy server which subsequently sends requests on behalf of the user. However, the use of a command to check the local network (eg- icaconfig /all) configuration of the user’s machine provides the real and accurate configuration of the access mode (as described in table 1).

This implies the automated tracking of the real geographical address of users would require more than just header information of applications used. Given the possibility of this information not providing the user’s authentic source address, it is imperative that either a technical tool is embedded in the application to retrieve the “access mode” information or a local command is invoked on the user’s machine to provide the real “access mode” information. Once the accurate public IPv4 address is retrieved and reference is made to the global IP registration database to determine the allocated region or country.

6. FINAL REMARKS
The model unifies various approaches to implementing cyber security, much as it is inductive, its development was based on deduced consistent behaviour. It is important to emphasize that the model does not apply to the types of cyber deception and theft that exclude social engineering such as intellectual property violation and piracy. The model leverages on a combination of permission, accountability, surveillance and behavior based security to counteract the menace.

REFERENCES


Authors’s Profile

Paul Asante Danquah is a Deputy Director of IT Infrastructure and Engineering at the University of Professional Studies Accra, he has a background of MSc Information Security from Anglia Ruskin University (UK), BSc HONs in Computing from the University of Greenwich (UK), Graduate Diploma in MIS and the professional certifications CEH, MCSE and CCNP. He is a PhD candidate under the supervision of Dr. Longe Olumide at the Accra Institute of Technology, Ghana. His research has focused on Cyber Crime and Information Security. He can be reached at paul.danquah@upsa.edu.gh

Ogunsanwo Olajide Damilola is on Faculty at the Department of Computer Science, D.S Adegbenro ICT Polytechnic, iitori-Ewekoro Ogun State Nigeria He had a BSC Computer Science at Ambrose Alli University, Ekpoma, Edo State in 2004. MSc Computer and Information Science from the Lead City University Ibadan, Nigeria. He has other professional qualifications such as CWNA, Oracle Certified Data Base Administrator (OCA9i, OCA10g and OCP). He can be reached at jidos2@yahoo.com

Dr. Longe Olumide is on Faculty at the Department of Computer & Information Systems, Adeleke University, Ede, State of Osun, Nigeria. He obtained a BSC Computer Science at the University of Benin, Benin City, Nigeria in 1998, a Master of Technology Degree in Computer Science at the Federal University of Technology, Akure in 2005 and a PhD Degree in Computer Science from the University of Benin, Benin City, Nigeria in 2010. His research has focused on using social theories, machine learning and computer security models to design cyber security systems and explain cyber victimization. He can be reached by phone on +18572078409 and through E-mail longeolumide@fulbrightmail.org