Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.5, 2015

The Risks and Countermeasures of Social Engineering in Ghanaian Universal Banks

Wolali Ametepe- Lecturer
Faculty of Computing and Information Technology (CIT) Department of Business Computing
Wisconsin International University College-Ghana P.O. BOX LG 751, ACCRA-LEGON.
E-mail of the corresponding author: wametepe@wiuc-ghana.edu.gh/ametepef@gmail.com

Dwumfour Abdullai
Faculty of computing and information technology (CIT)
Wisconsin international university college
abdullai.dwumfour@wiuc-ghana.edu.gh

Nana Kofi Annan-Head of IT Department.
Faculty of Computing and Information Technology (CIT) Department of Business Computing
Wisconsin International University College-Ghana P.O. BOX LG 751, ACCRA-LEGON.
nk.annan@wiuc-ghana.edu.gh

Abstract
Ever since the evolution of banking, there have always been a number of unscrupulous individuals who have tried to breach its defenses in order to gain access to valuables. In the course of time, the physical attacks have become slowly less necessary because banking has steadily gained an online presence. Formerly, it was impossible to authorize a transaction through a mobile phone using the Internet. However, now that is more than possible, it is an extremely popular way of having transactions. As a result, security within financial institutions has shifted focus from physical to virtual measures. The most important component of a good financial IT security infrastructure is security Karishma (2010). In this scenario, the need for ensuring that information is kept confidential, adhering to accepted norms of privacy and making it available to authorized users at the appropriate time, assumes great significance. This is particularly valid for the banking sector where day-to-day operations are centered on information and information processing, which in turn is highly dependent on technology. Banking as a business involves the management of risks based on a repository of trust extended by the customers, If this objective has to be accomplished, it becomes imperative for all security concerns especially customer sensitive data to be addressed in an effective way so as to ensure that the trust levels are well preserved and information assets perform the role that they are supposed to according to Chakrabarty (2010). The research conducted on the Ghanaian banks concerning information security breaches within the banking and financial institutions has shown that majority of the banks are very much concerned with both internal and external security breaches and also all the Ghanaian banks have in one way or the other experienced information security breaches before, according to Tobin and Danquah (2011).The current and the future bank institution in Ghana need to provide social engineering measures to secure their information and that of their customers. Because a lot off banks in Ghana and Nigeria has being attacked unaware due to the social engineering effect, this research investigates social engineering effect in Ghanaian Banks, and also identifies how Information and Communication Technology is managed. It also creates awareness on social engineering and it countermeasures of stakeholders, Contributes to development of policy to enhance and secure quality banking.
Keywords: Information Security , Social Engineering , Countermeasures, Creation of Awareness, Mitigation.

1.Introduction

Human nature is the social engineer's greatest exploit. As part of human nature, people generally trust easily and get satisfaction out of helping those in need. In order to gain information, such as a phone number or a password, the attacker must first establish trust with the individual that he or she hopes to gain information from to perform his or her task. (Mitnick,et al 2004).

Security of information systems is being highly challenged by the recent banks in the world including electronic commerce and a variety of information brokering services. It is imperative that security of an information system should, by design, protect the confidentiality, integrity, and availability of the system. Given the information-intensive characteristics of the modern global economy dominated by the internet and the World Wide Web, it should be no surprise to learn that information security is a growing spending priority among most companies and government agencies. Most hackers engaging in the manipulation of users in this way follow a similar pattern in their planned exploitation, first starting by conducting their own research into the type of social engineering tricks that may work and on which targets. Then it is important for them to develop rapport and trust with the users, perhaps through fake web-sites (with highly realistic designs). They will then exploit the trust

they have fostered and use the information for their own ends (e.g. obtaining money from bank accounts) (Mitnick, 2002). In a test carried out at a Texas University, over 90% of students parted with their authentication details after being sent spoofed e-mails and web pages, which looked like those of their University's IT department (Vijayan, 2005). This seems to suggest that using social engineering tricks is an effective mechanism for hackers to gain access to confidential information even in the groups in society which one would expect to be more cautious.

Security is all about trust. Trust in protection and authenticity, despite the humungous security threat posed by social Engineering, very little is ever highlighted about it. Primary reason for the lack of discussion about social Engineering can be attributed to shame. Most employees in banking environment see social Engineering as an attack on their intelligence and wit, no one wants to be considered ignorant or dumb to have been duped. This is why social Engineering gets hidden in the closet as a "Taboo' subject, whereas the fact is that no matter who a person is he/she may be susceptible to a social Engineering attack. This research intends to put value on the challenges facing Ghanaian banks vis-à-vis to the social engineering; physical, telephone based and computer based social engineering and also to identify

2. Objectives

The general objective of the proposed research is to create awareness of social engineering as security measures for both employees and customers of banking centers in Ghana and also to stop the social engineers from succeeding or even damaging the Ghanaian banks assets.

3. Literature Review

3.1 Social Engineering define

Social Engineering' is a threat, often overlooked but regularly exploited; to take advantage of what has long been considered the 'weakest link' in the security chain of an organization -- the 'human facto '(Malcolm ,2007).As Rusch stated in (Rusch, 1999) it is a well-recognized rule of social interaction that if someone gives us something, we feel inclination to provide something in return, i.e. reciprocate. It is quite natural to help someone in belief that we may need help in the future and can rely on people we have helped before. This is especially true in corporate environments as, for example, Kevin Mitnick, a famous hacker, has perceived (Fraber & Mitmick, 2001). Similar behaviour can also be observed in the case of first making a larger request and then getting a more favourable response towards a smaller request (Gragg, 2002).

People have a tendency of trying their best to fulfill the commitments they have made, especially in their workplaces (Gragg, 2002). If they do not succeed in doing what they have promised, it can cause a feeling of guilt, even though a user evaluation might reveal that doing it might be foolish. Additional thing is that the people have a tendency to believe that people are expressing their true attitudes, i.e. the first reaction is not to suspect a lie unless there is strong evidence to the contrary. Also, some may feel it is their moral duty to proceed with actions that they believe to be important and failing them could lead to dire consequences their to the company or to a supposed work colleague. Social proof means that in bigger crowds the people are likely to observe more what others are doing and saying, thus letting others influence their own decisions. (Harl, 1997).

3.2 Employees Awareness of Social Engineering

The security awareness program should create continuous awareness of the social engineering risk among the organization's employees and their (personal) responsibility in protecting the organization's assets (Gragg, 2002). The program should consist of (interactive) trainings with clear reference books discussing the security policies and procedures of the organization, the tactics and psychological principles used by social engineers and the targeted information (and value thereof). This security awareness training teaches the trainees to recognize an attack when it occurs and prevent it from causing harm by following policy and set procedures (Gragg,and Mitnick, 2002).

Even if an attack is detected later on, this recognition can help with the recovery. The training should also discuss information and attributes –e.g. uniforms and letterheads- an attacker may already have. This awareness can be used to refute the tendency to trust a person having certain information or attributes. And finally the consequences of an attack to the organization, the organizational environment –e.g. suppliers and clients- and the employee personally should be addressed to generate support for the security architecture. Next to training on the social engineering attacks employees should also get technical training on the information systems they use, to make them aware that the technical security features on these systems do not protect the organization's assets by themselves and that they should question the credibility of requests for actions on them (Stonebuener et al 2002).

This increases the chance of detecting illegitimate requests by a social engineer or co-worker and recovery from an attack. The profundity of the training depends on the access rights of the employee –e.g. systems' administrators- and level of contact with the public –e.g. helpdesk personnel and receptionists-, but all

personnel internal and external –e.g. security guards and cleaners- need to get basic security training on social engineering (Gragg,2002). Therefore distinct training programs should be created for the different groups, some more focused on the technical systems security, others more on the physical security (Mitnick, 2002).

3.3 Impersonation

Social engineering usually requires some form of impersonation in order to win the trust of the target. Quite often used tactic is to impersonate an IT support person, who is "checking the network" and asks for a password or asks to install a piece of software. Other support staff, like janitors and repairmen, also does not catch the eye of the unwary and can be quite successful in finding interesting pieces of information. Someone could also pose as a manager and rely on the peoples' trust on authorities. Posing as a fellow colleague in trouble might earn the attacker's sympathy enough to gain access to the desired information. Impersonation often is preceded with an identity theft, which can be simple as acquiring an official looking company badge (fake one will usually do), a company t-shirt, or carefully gathered collection of personal information of a person. Identity theft in itself is an increasing cause for worry that has direct economical consequences as many cases have shown (see, for example, (Durhan, 2001), (Mercuri, 2006)). Nowadays companies are eagerly outsourcing their non core functions, so it is not so surprising to see strange faces at the work facilities.

3.4.Countermeasures of Stakeholders

The very nature of social engineering suggests that the most effective way of preventing it from happening is through the user training. This should be accompanied with relevant policies that dictate the user actions in potential abuse circumstances.

Security needs several layers, i.e. defense in depth that can mitigate the effectiveness of an attack, if one of the security measures fails, like when people give out too much information or allow unauthorized people to roam the premises. In other words, one needs to have breakpoints, either policy or technology based, in the phases of the attack cycle depicted in Figure 2.2. Additionally, the security design of any system should not be a separate design activity, but should take an integrated approach right from the start of the whole design process (Yee ,2004). This should also ensure that security is an embedded feature, not something you turn off in the name of usability when shipping the final products.

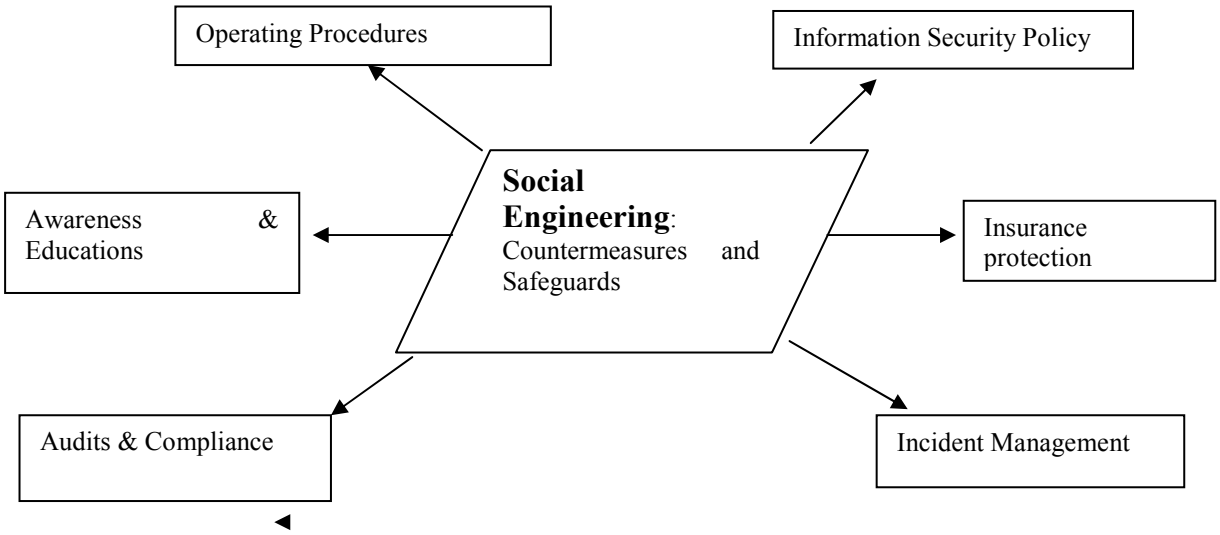

Figure 1 Diagram showing Social Engineering Countermeasures and Safeguards.
Source: White paper "Social Engineering " An attack vector most intricate to table.

4. Methodology

The research design used to carry out this study was mixed method research design which covers both qualitative and quantitative analyses. We use the mixed method research design because our work or research contained both qualitative and quantitative analyses, and the appropriate design for qualitative and quantitative analyses is the mixed method research design, the researcher intended to conduct the study in order to determine the current status in terms of availability, adequacy and use of the human and material resources.The population for the study was all the 1568 staff of all its 60 branches and agencies. Stratified random sampling and quota sampling techniques were used to collect data. In all 180 people from 36 branches were selected. Primary data was gathered from the field through the use of questionnaires and interviews were conducted for workers of some of the Universal banks in Greater Accra Region in Ghana.

5. Results of the study

5.1 Methods of Social Engineering Based Attacks Spotted in Some Selected Ghanaian Universal Banks.

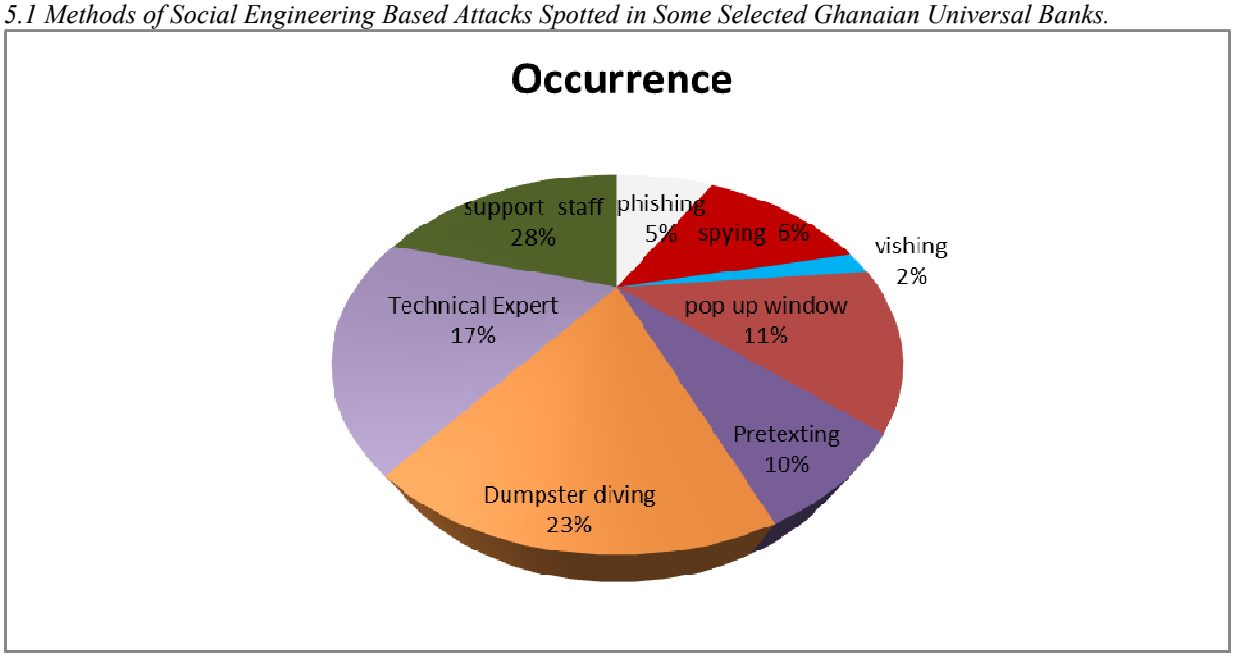

Figure 2 Methods of Social Engineering Based Attacks Spotted In The Selected Ghanaian Banks. from 2007 to 2013

Source: Field Study.

Out of about Eighteen (18) different social engineering attacks, only 8 of them have occurred in the Ghanaian Universal Banks as at February 2012. Those experienced by the universal banks in Ghana are: support staff, phishing, spying, vishing pop up windows, Technical Expert, pretexting and Dumpster Diving. As at now, some of the attack vectors have not yet occurred in the various banks contacted. There are Hoaxing, authoritative voice, Interesting software and spam mails. After analyzing the chat above, it has been realized that the support staff contributes up to twenty-eight (28%) of the attacks. The way the Intruder attempts acquiring information such as usernames, passwords, VISA and credit card details by masquerading as a trustworthy entity in an electronic communication known as finishing, has occurred up to five percent (5%), vishing represents two percent (2%). We also have the situation where technical expert of social engineering attack represents seventeen percent (17%). It is discovered that individuals lie to obtain privileged data (pretexting). A pretext is a false motive and it is found in the Ghanaian universal banks; it rates up to ten percent (10%). We have pop up window that a social engineer uses to get information from system users from the various banks. This is also used to attack banks and it rates up to eleven percent(11%). Investigation shows that some people's job is to sift through commercial or residential trash to find items that have been discarded by their owners, but that may prove useful to the dumpster dive. Dumpster Diving have also gone up in the Universal banks up to twenty three percent (23%), and six percent of spying (6%) also show in the banks.

Table 1 Security vulnerabilities that can be exploited by Social Engineering-based attacks.

Types activities	Average Monthly Rate of Occurrence (Hours)	Average Monthly Downtime (Hours)	Average Monthly Man Hours Lost
Misdirected mail	6	6	4
Vandalism	8	4	3
Phishing / web site defacement	14	2	2
Password compromising	5	7	6
Information taken by rogue employees	8	6	2
Laptop or Computer Stolen	7	7	5
Unauthorised access to private information	9	8	7
Employees divulged customer account to anybody	12	8	8
Total	**69**	**48**	**37**

The Ghanaian universal banks tend to be subject to various threats of the social engineering breaches, downtime or breakdown, and personal hours lost affecting their activities. An average of sixty-nine (69) represents monthly hour's rate of occurrence from the usual threats, forty-eight (48) monthly downtime hours on

average, and thirty-seven (37) average of monthly man hours lost.

5.2 Systems in Place to Minimize Social Engineering Risks

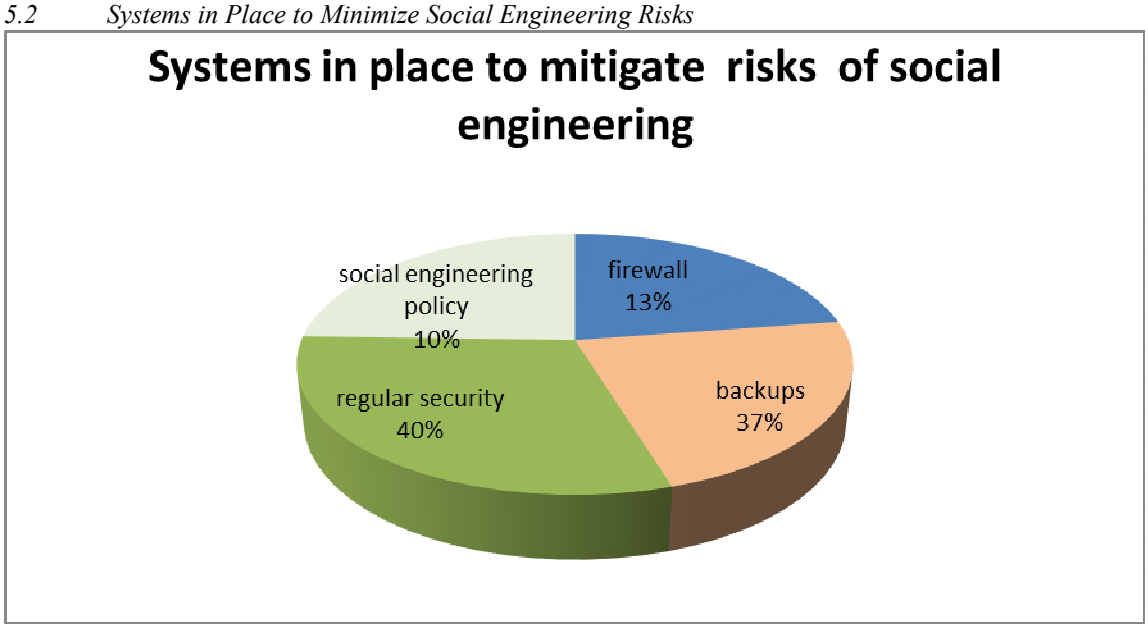

Figure 3 Average systems in place to minimize social engineering risk.
Source: Field Study

To minimize social engineering breaches, the responses indicate that almost all the banks had some mitigation measures in place to minimize information security breach that always occur to their database or information systems. Social engineering policy has occupied ten persent (10%) of the all the mitigation measures ,thirty five percent (37%) of the banks have secured backups procedure for recovery in case a system fail ,Thirteen percent(13%) also a strong firewall as security measure and all other regular security has also taken up to forty percent(40).

6. Conclusion

This study shows or reveals various security vulnerabilities that are due to compromising activities encountered in the banks such as fishing and website defacement that create awareness about the practices of social engineering will help mitigate this vice in and against our universal banks. This involves also the effective working of the regular security practices and measures put in place So every financial institution in Ghana need to be aware of evil practices by the attackers.

7. Recommendations.

- Physical pieces of information should be kept behind locked doors or in a fault.
- Server rooms should also be locked and hard disks with confidential information should be kept behind locked doors as well.
- Audits should be performed on the adherence to policy and procedures.
- Authorization management should be implemented.

8.References.

Farber D. and M (2001).*Mitnick on Mitnick: "Why I'm going legit" (part two).Kevin Mitnick interview by CNET Networks,. Retrieved December 11, 2011,* from http://www.silicon.com/a55864 .

Durham-Vichr D.,(2001). *Online Con Artist Steals Identities of World's Richest News Factor*

Gragg, D., (2002) *A multi-level defense against social engineering, in GSEC practical assignment, SANS Institute: Washington.*

Granger, S (2000*). Social Engineering Fundamentals, Part I: Hacker Tactics* last updated December 18, 2001

Harl.(1997), *People Hacking: The Psychology of Social Engineering. Talk atAccess All Areas III, Harl. People Hacking: The Psychology of Social Engineering. Talk at Access All Areas III, 1997. Retrieved December 11,2011,* from http://bak.spc.org/dms/archive/aaatalk.html (accessed 08/2006).

Harl. (Nov, 2011). *People Hacking: The Psychology of Social Engineering. Talk at Access All Areas III, 1997. Retrieved December 11,2011,* from http://bak.spc.org/dms/archive/aaatalk.html

Karishma Sundaram (2010). *Information Security for Banks •Edited by: Lamar Stonecypher Published May 17,*

2010. Retrieved December 11,2011, from *http://www.brighthub.com/computing/enterprise-security/articles*.

Mercuri R.T. (2006).*Security watch: Scoping identity theft. Communications of the ACM, Volume 49.*

Mitnick, K.D. & Fraber (2001). *The art of intrusion: The real stories behind the exploits of hackers, intruders, & deceivers., Wiley: Indianapolis. xvii, 270p.*

Mitnick, K.D. & Graged (2002), The *art of deception: controlling the human Element of security. Wiley: Indianapolis. xvi, 352p.*

Mitnick, Kevin D., Simon, William L.(2003) The art of deception Controlling the Human Element of Security

Rusch J. (1999). *The Social Engineering of Internet Fraud. Proceedings of 9th Annual Conference of the Internet Society (INET'99). Retrieved December 11,2011 from* http://www.silicon.com/a55864 (December,2011)

Stoneburner et al, (2002), Risk *management guide for information technology systems, in Computer security. National* Institute of Standards and Technology: Gaithersburg.

Tobbin, P., and Danquah, P. (2011). *The Impact on Information Security Breaches on Banking Information Systems from the year 2000 to 2009:* PentVars Business Journal, Vol. 5, No. 3, July September, 2011. ISSN 0855-9163.

Vijayan, J. (2005), "*Targeted Attacks Pose New Security Challenge", Computerworld, Vol 39, No 26.*

Yee K. (May, 2004). *Aligning Security and Usability, IEEE Security and Privacy,Volume 2,*

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar