Analysis of the Awareness and Safeguarding Against Social Engineering: A Case Study of Federal Polytechnic Ilaro

Fagoyinbo, I. S.
Akinbo, R. Y.
Ajibode, I. A.

*Department of Mathematics and Statistics,
Federal Polytechnic, Ilaro,Ogun State, Nigeria*

Dosunmu, A. O.

*Department of Computer Science,
All-Over Central Polytechnic,Sango,Ogun State,Nigeria*

Abstract *This paper attempts to discuss the concept, forms and safeguarding against social engineering attacks as a means of security measures to individuals, organisation and governmental functions. Illustrations were made on how social engineering attacks can be lunched prevented and also reduced to the barest minimum. The paper also exposes various ways of perpetrating the evil and how such menace could be detected, security measures to be put in place and educating people through seminars and workshop on the existence of social engineering attacks, the menace in careless handling of vital information as well as procedures for avoiding information leakages. It also summarizes the relevance of security in day to activities and how to improve on security lapses as a means of safeguarding against social engineering attacks so that it can benefit the society at large. Data was collected on social awareness by the top, middle and lower management staff of Federal Polytechnic Ilaro. From the analysis it was observed that social engineering attacks was still in the awareness stage, the preparation involved the management staff only and the commitment varies and increases from the staff union to officer, to management staff and finally the senior staff.*

Introduction

Security is as old as the creation of the world itself, in the olden days, it was not as important as it is today due to the development of modern technologies and the ability to beat security by the technology so developed. Social engineering is a strategy for obtaining information people wouldn't normally divulge, or prompting an action people normally wouldn't perform, by preying on their natural curiosity and/or willingness to trust. Perpetrators of scams and other malicious individuals combine social engineering with email in a number of ways. Many advanced countries pay more attention to their securities; in spite of these, social engineers still operate and succeed in such environments; a typical example is the world trade centre attack carried out on the September, 2001, in the United State of American. New policies are in place for online business transactions and focusing their attention on security, it was also extended to the health care system so that they could be held accountable for patients protected health information. This was backed up with an Act HIPAA (Health Insurance and Portability and Accountability Act). Also in United States' schools must be adhere to FERMA (Family Educational Rights and Privacy Act) this Act protects the privacy of students education records. It is paramount to every organisation and individual to have adequate security measures for all vital records and transactions.

According to the Federal Trade Commission (FTC) reported in 2005 that "more than one million consumer fraud and identify theft complains that have been fitted with Federal, State and Local law enforcement agencies and private organisations. The survey released on April 2, 2006 by the United States Department of Justice about 3.1 percent of American household became victims of identity theft in 2004. The survey revealed that now, more than before, individuals are at a high risk of having personal information stolen and used by criminals for their self aggrandisements. The land mark are debt, bad credit, higher interest rates and charges that are criminal in nature, the victims are not free until they are prove innocent. Recovering from this menace could take years or even a life time. Sufferers of this theft are left with a permanent stain to wipe off.

Moreover, in order to protect confidential information, all possible security measures shall be put in place, for an individual, organisation or governmental Agents/Agencies the security measures to be adopted emanates from the use of passwords to access electronic data equipment; also unauthorised personnel should not be allowed entrance to a work place where clasified information or equipment is located. Packet sniffing – the act of encrypting data to prevent malicious intruders should also be put into place. Privatising records are essential to prevent spying or break – in from the outside, this can be done by using intrusion preventing systems, access control lists, anti – spyware software and the use of firewalls. It is evident that for individuals, organisations and agencies there should be protection of personal electronic information by using passwords for access and having security tools in place, at home or workplace sensitive electronic data can be used through the process of authentication, authorization and accounting methods.

Finally, no matter the type of security measure put in place, an individual, organisation or agencies are still at risk of having their information stolen. Grander (2006) pointed out that "by merely trying to prevent infiltration on a technical level and ignoring the physical – social level, we are leaving ourselves wide open to attack". Although many security systems have been developed to prevent intruders from accessing high value systems, an organisation cannot be totally free of social engineering.

Social engineering is the name given to a category of security attacks in which someone manipulates others into revealing information that can be used to steal data, access to systems, access to cellular phones, money or even your own identity. Such attacks can be very simple or very complex. Gaining access to information over the phone or through websites that you visit has added a new dimension to the role of the social engineer. Basically social engineering is the acquisition of sensitive information or in appropriate access privilege by outsider, based upon the building of an appropriate trust relationship with insiders. The goal of social engineering is to trick someone into providing valuable information or access to that information. It is the act of manipulating people into speaking or acting contrary to their normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. They prey on human behaviour, such as:

- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble

The sign of a truly successful social engineer is that they receive information without raising any suspicious as to what they are doing. People are usually the weakest link in the security chain. They employed different methods to persuade and influence others in other to achieve their objectives of obtaining unauthorized information so as to perpetrate fraud, network intrusion, industrial espionage, identity theft, or simple to disrupt the system or network (Granger, 2001). A few examples of tactics used include impersonation, phishing and dumpster diving.

Social engineering can be broken into two viz: Human based and computer based. Human- based refers to person-to-person interactions to retrieve the desired information, whereas the computer based refers to having computer software that attempts to retrieve the desired information. Huber et al (2009) noted that Automated Social Engineering uses artificial conversations where the human victims talk to a computer program that mimics human behaviour. Automated Social Engineering (ASE) is the process of automatically executing social engineering attacks. Social engineering targets human weaknesses of the user instead of vulnerably of a technical system. As an example of ASE, Robert Epstein reports in the Scientific American Mind (2007) how he was fooled for a considerable amount of time by a computer program that pretended to be a Russian woman. The human based includes:

Impersonation

This is the greatest techniques used by social engineers to deceive people e.g. pretending to be an employee of an organisation tricks are often used by pretending to be in the information technology (IT) department so as to obtain information. A simple phone call requesting an employee's password is usually an easy way to get access to information; by assuming that the phone call comes from the IT department, employee disclose the password willingly without question, especially after that employee has been told, what seems to be a legitimate reason for the request.

The human tendency to be helpful, trusting others and having tendency to protect themselves as well as fear of getting into trouble makes the use of impersonation very well for social engineers. The ability to be highly responsive to assertions of authority, even in the absence of the person in the position of authority (Rush, 1999). For instance, a low cadre, help desk employee may be intimidated by a phone call from someone claiming to be the secretary of marketing demanding a rest or adjustment in his passwords so that he may log in to the system immediately. Due to fear the help desk might not ask for proper credentials of the caller before abiding to the request.

Phone is a universal device used to conduct social engineering attack, it is a device used to obtain information from people at home. People can receive phone calls at home from banks requesting for information about their credit card and their accounts details. This makes people to divulge information concerning their accounts to someone over the phone that claims to represent the bank. Such phone calls could lead to releasing the following vital information; credit card number, social security number, bank account number. This vital information is released to the social engineer by either offering something of value to the card holder or the fear of some problems in the account of the victim.

Phishing

Wilkepedia (2005) defines phishing as, the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. It is the most common online social engineering; it includes e-mail spoofs (Grander, 2006). The e-mail directs the user to visit a website where they are asked to update personal information. The website is set up only to steal the user's information. Phishing is similar to impersonation but instead of face to face contact; the contact is through e-mail or other online mechanism.

Dumpster Diving

This occurs when people are not aware of the value of information they possess and are careless about protecting it. It involves careless throwing away of vital documents such as policy manuals of a company as well as company's phone book. Although the information obtained through these documents could be used for foot printing. Granger (2006) defines foot printing as "the art of gathering information (or pre-hacking).... it's commonly done to research a predetermined target and determines the best opportunities for exploitation".

The individuals at home are just a vulnerable to dumpster driving as an organisation. Many people throw away vital information such as credit card statements, bank statements, and other mails containing personal information without hesitation. Such information might not be used immediately to suit the required purpose but can be used for foot printing; impersonating a representative of a credit card company is a lot easier for a social engineer when he or she posses the cardholder's account information.

Protection Against Social Engineering

Social engineering attacks are almost an incurable disease since it involves the human element. Grander (2001) defines security as "security is all about trust, trust in protection and authenticity. Generally agree upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack". There are common defences that may be put in place such as:

- Everyone that enters the building (contractors, business partners, vendors, employees) must show identification.
- Passwords are never spoken over the phone.
- Passwords are not to be left lying around.
- The use of ID technology.
- Invest in shredders.

An organisation should also provide training programs for all categories of workers including security guards, receptionists, help desk employees and management on various forms of social engineering attacks their preventive measures and actions to be taken so as not to release vital and confidential information to an unknown visitor. There should be sound policies and procedure in place to cover the following areas:

Account set up, password change policy; help desk procedures, access privileges, violations, unique user identification, confidential information handling, modem usage and acquisition, secure sensitive areas, privacy policy, centralized security, focus point etc.

People in top management posts should be guided by rules and regulations not to give orders that are sensitive in nature to their subordinates e.g. commanding a help desk employee on phone to reset password by the vice president of marketing. The help desk employee could insist on receiving proper credentials before obeying such instructions i.e. there should be documented procedures.

On the other hand, seminars and workshops to employers will serve as a guide to social engineering attacks and this will enable them to use their best judgement as a defence mechanism. Somebody who is aware of social engineering attack receiving an email from a company requesting that an individual must update his or her account information will definitely know it is phishing attack and would not consent to a possible bogus company's website through a link on that email. That person would either go directly to the company's website through a separate browser window, or call the company to verify that the email was in fact legitimate. Awareness through seminar and workshops would also allow people to be more careful of what they throw away in the trash. When people recognise the value of information they possess, they will handle it with care. Appropriate cautions will also be put in place against all forms of attack such as "dumpster dive" for valuable information, recognition should be given to the use of shredder to do away with confidential information and give proper monitoring to those who dispose of trash.

Finally, if you feel you have thwarted or perhaps been victimised by an attempt at social engineering, report the incident to your manager and to the security personnel immediately.

Summary of Findings

From the field survey we conducted in Federal Polytechnic, Ilaro with fourty staff of the institution who responded to our questionnaire and interviews we find out that the implementation of safeguarding against social engineering in Federal Polytechnic, Ilaro, is still in the AWARENESS STAGE, with strength value of 3.50. On the other hand the actual implementation was found to be significantly less than advanced with value of 1.85 sharing that the implementation stage is still very low especially in the educational institution like ours, some institutions are yet to be aware. The level of thoroughness of preparation stood at 3.70 which was a little above average level.

Moreover, the finding also shows that the C.E.O., management staff and senior staff are very committed to the ideas of safeguarding against social engineering particularly its application in Educational institutions.

However, the staff unions are comparatively less committed.

A reward and Recognition system in place tends to reward individual more than team achievement. This trend if sustained could weaken team spirit and threaten the success of safeguarding against social engineering attack training for awareness at all levels.

- Training for awareness at all levels.
- Top Management commitment.
- Incorporating safeguarding into corporate strategy.
- Choice of safeguarding coordinator.
- Setting up of a safeguarding steering committee.
- The corporate culture.
- Sustenance of the programme for continuity.

We found that the identified factors to be in line with the prescriptions of the literature on the subject. We are not surprise at this trend as Nigerians are known to be avid readers and knowledge seekers.

Recommendations

It is recommended that: the continuous social engineering education should be undertaken at all levels, even for those sectors that have already acquired a high degree of awareness. Educational institutions should integrate safeguarding against social engineering attack resulting into their reward systems. Appraisal systems should be similarly treated.

Safeguarding against social engineering should form part of the induction training for new staff so as to give them an early orientation; since attitudes once formed, are difficult to influence.

Finally, Management should be patient with problem staff of long tenure, who have developed resistance to change. Training on 'Management of Change' should be done pari pasu with social engineering education.

Conclusion

In this study, we carried out a survey of extent of implementation of safeguarding against social engineering by questionnaire and interviewing 40 staff of Federal Polytechnic, Ilaro.

Based on our findings it is still very much at the awareness stage and more effort and commitment is required to get it beyond that stage.

From the findings reported in this paper more attention should be paid to creating awareness of safeguarding against social engineering so that we can attain a higher level of curbing the menace before the next millennium.

Organisations must protect vast information so as to prevent consumer fraud and identity theft. The discoveries of modern and advanced technologies increases security risks and this led to attacking more importance to security for individuals, companies and even government. Social engineering is a technique used by hackers and other criminals to persuade people to divulge confidential information, or allow unauthorised access, for their personal gain or for malicious purposes. Various techniques exist for social engineering attack this includes impersonation, phishing and dumpster diving and are used to achieve their goals. These attacks are difficult to control but can only be reduced or minimized because it involves human effort, training through seminars and workshops against the menace of social engineering attacks is a better means of minimizing the menace by various organisations.

Moreover, individual and organisations can try to protect their confidential information by storing their data on a system that requires password-only access, putting the system in a secure room that allows only authorised admission, and spending much money as possible on security tools to protect the data through that does not mean that the data is not vulnerable to social engineering attack.

Finally, training people which includes formal education against the menace of social engineering attack and organising seminars and workshops will prevent social engineering attacks from thriving in any organisation. Other ways of preventing this attack includes the generation of overall awareness, once people are aware of the critical data they posses; the need to protect it for possibility of exploitation this will lead to building a strong defence against social engineering attack thereby leading to its decline.

References

Facts and Statistics (2005): Insurance Information Institute.
Damle, Pramod (2002): Social Engineering: A Tip of the Iceberg.
Gaudin, Shann (2002): Social Engineering: The Human Side of Hacking. Earth web.
Grander, Sarah (2006): Social Engineering Reloaded: Security Focus.
Lemos, Robert (2006): Survey: Identity Theft Hits Three Percent. Security Focus.
Palmer, C.C. (2001): Ethical Hacking, IBM Systems Journal Volume 40, Number 3.
Phishing (2005): Webopedia
Social Engineering (2005): Search Security.com definitions.
Collen Rhodes (2007): Running Head: Safe-guarding Against Social Engineering.
Fagoyinbo I.S. (2004): Applied Statistics for Tertiary Institutions.