The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

Impact of Social Engineering on knowledge Community

Mohammed H. Shalhoub
King Abdulaziz University
shalhoub@live.com

Abdula Bataweel
Jeddah, Saudi Arabia

Hassan A. Alsereihy

***Abstract* — The main objective of this article is to examine the overall information security by addressing the readiness of some more efficient attacks and attacks against the human race. This was achieved through studying the previous work in the field of information security and other relevant research areas. Also, we'll discuss using social engineering techniques against enterprise users. Through the application of methods of social engineering, we will discuss how to bridging the gap between the user and information security group. Let the best security awareness, and improve compliance with information security policy, and the least difficulties in user acceptance. We concluded that training should be given on information security awareness for all employees in the organization .**

I. INTRODUCTION

This template Information security is one of the most important and least popular administrations in most companies. The information security group is to be involved download the project and be blamed for the first set when something goes the error in the information technology infrastructure of the organization. Social engineering can go a long way toward solving a lot of problems, and improve the relationship between information security and the rest of the organization. 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. One of the main differences between the areas of staff development, security organizations that believe in accepting risks. Although it's hard to accept, in some cases, businesses really need not trump security. In cases that do not need, but driving ease, the "trump" Override. The initial argument that you need to copy is safe. In order to protect confidential information, all possible security measures shall be put in place, for an individual, organization or governmental Agents/Agencies the security measures to be adopted emanates from the use of passwords to access electronic data equipment; also unauthorized personnel should not be allowed entrance to a work place where classified information or equipment is located. Packet sniffing – the act of encrypting data to prevent malicious intruders should also be put into place. Privatizing 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, organizations 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. As it is well known, only a small percentage of information security is maintained by technical security measures, while its greater percentage depends on the user. Individuals in charge of information security in an organization are all of the organizational staff, with the foremost being the owner of the information and the IT personnel.

II. HUMAN BASED SOCIAL ENGINEERING

The human based social engineering includes [7]:-

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

A. *Impersonation:*This is the greatest techniques used by social engineers to deceive people e.g. pretending to be an employee of an organization 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.

B. *PHISHING:* phishing is 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 [8]. 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.

2. *UMPSTER *IVING: 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 [9] 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".

III. PROTECTION AGAINST SOCIAL ENGINEERING

Social engineering attacks are almost an incurable disease since it involves the human element. Grander [9] 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 defenses that may be put in place such as [7]:

- 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 organization 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.

IV. IMPORTANT ,ACTS ABOUT ATTACK

Now that we have our social engineer's hat on, we can begin the attack. Start with a single group within the organization. Pay attention to their habits. Where do they go for lunch? What do they do during breaks? What do they talk about when they're slacking off? Pay attention to the way they speak to each other, and work on emulating it. Once we have the answers to a few of these questions, we can use that information to infiltrate the group. Find out what the group's focus is, what they need to accomplish, and use that information to formulate your security arguments, and tailor them to the target's needs.

So how do we infiltrate? To infiltrate a group, we must be able to blend in. This can

be tricky for many infosec people. The problem is that the first step in blending in is appearance, and that can mean a dramatic change from the normal appearance of our information security team. We need to pay attention to the way our target group dresses, and emulate them. This may mean moving from jeans and a t-shirt to slacks and a polo shirt. It could be more extreme and involve wearing a suit. This tends to be the biggest point of contention among information security teams, but a truly strange thing happens when the security team interacts with a user group while dressed the same way. The users begin to talk to the team as equals, and actual information can be exchanged.

Stranger still, if our team can manage to dress better than our target group, we may be seen as authority figures. Once we have blended in, re-examine the target. Pay close attention, not just to what they do, but how they do it. People are nearly always willing to talk about what they do to an interested peer, become one. Listen to them, find out where the group talks, and what they talk about. Get an idea of what is important to them, and never forget to use their names in conversation. At this point, the recon phase of the attack is complete. We've learned enough about the target to blend in. If we've done things correctly, we are no longer the Security Dude(ette), we have instead become

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

our name here. In other words, we're now human in the eyes of our users. Continue speaking to them in their terms, but gradually turn the conversation to items relevant to security. Don't override the conversation, but start adding topics. Talk to them about how infosec impacts them. Explain what a breach could do to them personally.
Explain what a breach in their section could do to the company. Tell them what they
can do to help, and ask them to do it. While we're talking to the users about security, don't forget to listen. Remember, at this point, we are not the infosec team dictating from on high, we are just another employee, and communication must be two-way. Find out what the users need. Listen to the stories of how security gets in the way, and examine them for inconsistencies in our policies. If we find an inconsistent policy, then it needs to be changed. From a user perspective, if one of our policies is inconsistent, then all of our policies are. Listen to what the users are complaining about and act on it when possible. If it isn't possible to change something, explain to the user why it can't be changed. Make sure to couch the explanation in terms that are relevant to the target group.
Lastly, examine our policies again, and loosen any that are overly restrictive. If our
social engineering exercise was successful, we will begin to see changes in the organizational attitude. We'll get a few more requests to change processes, and policies. We shall also see a more positive reception to new security policies. The key here is that the users now feel as though they have some say in what happens to them, and in how they work during their time at the office. As the users become more comfortable with the infosec people, they will become much more willing to listen to arguments brought up by the security team. The security team will be brought in at the beginning of projects rather than the end, and you will likely start hearing more about your team in a positive light.

V. METHODS OF SOCIAL ENGINEERING

The arsenal of the social engineer is large and very well established. This is mainly because social engineering amounts to a variation on confidence trickery, an art that goes back as far as human history can recall. One might argue that Homer's Iliad contains the first record of a social engineering attack in the form of the Trojan horse [10].

A. Direct requests

Many social-engineering methods are complex and require significant planning. However, there is a simple and effective method that is often just as effective. The social engineer contacts his or her target and simply asks for the information.

B. Preying on trust and emotion

Social engineering is a method of gaining information through the persuasion of human sources, based on the abuse of trust and the manipulation of emotion. In his book, The art of deception, Mitnick makes the argument that once a social engineer has established the trust of a contact, then all security is effectively voided and the social engineer can gather whatever information is required. The most common method of targeting computer end-users is through the manipulation of gratitude

C. Impersonation

Because forming trust relationships with their victims is critical to a social engineering attack, it is not surprising that social engineers often pretend to be someone or something that they are not. Two of the major tools of impersonation (1) Speaking the language of the victim institution and (F) knowledge of personnel and policy. To allay suspicion, a social engineer needs to know and be able to use an institution's terminology. Being unable to do so would cause the victim to suspect, rather than trust, the social engineer.

D. Research

To establish trust in their victims, social engineers use research as a tool. This comes in two forms, background research and cumulative research. Background research is the process by which a social engineer uses publicly available resources to learn what to ask for, how to ask for it, and whom to ask it of. While the intent and goal of this research differs from the techniques used by students, librarians, and other members of the population, the actual process is the same.

VI. SUMMARY OF ,INDINGS AND RECOMMENDATIONS

From the field survey we conducted in Federal Polytechnic [7], Ilaro with forty 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 G.H0. On the other hand the actual implementation was found to be significantly less than advanced with value of 1.8H 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 G.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

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

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 program for continuity.

Regarding the management cautions for assuring a secure community, we divided these requirements into two classes: non-Technical management tends to be similar to the normal end users. For this group, metrics showing why x is better than y tend to be more persuasive than arguments over which specific technology to purchase. These managers can be some of our best sources of information about their groups. Their attitudes are typically reflections of their department's attitudes. Listen to their objections in the same way we did during the main portion of the engagement. They can bring information to our that gives us a better overall picture of the workflow in their group. When presenting this group with new information, we will still need to keep things concise. They are not generally interested in the technical details, but rather in the way our changes will impact them, their employees, and the business. Once again, Regulatory requirements can be used to sway this group.

On the other side, technical management tends to be the easiest group for information security to talk to. These are the managers that teams deal with daily. Frequently, these managers act as an insulator for the security team, shielding them from the upper levels of management, and acting as the faces of the organization's information technology group. When presenting to this group, we can be significantly more detailed. Provide them with a clear definition of the problem. It frequently helps to provide technical managers with multiple potential solutions alongside the problem. Be prepared to answer questions, and possibly even defend both our definition of the problem, and our proposed solution. Give these managers details, such as the likelihood of a given vulnerability being exploited. Help them to prepare to bring our findings to other groups.

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. Naturally it is expected that the administrative and physical security is taken care of and the company has meaningful security and data management policies [1F]. The user training can be made more effective through audits, which can be conducted by outside auditors. This could be, for example, simulated attacks that could reveal the weak points and also teach people who fall for them.

Personal experience is likely to be more effective learning method than sitting at
lectures or reading policy documents. Online auditing itself may not reveal the real culprit as some form of impersonation probably is taking place, but it mitigates the possibility of malicious insiders through deterrence. Of course there might the problem of proving whether the insider was malicious or just a victim of social engineering. But as Bruce Schneier has stated, in the end the organization is at the mercy of its people [1G]. This is backed by estimates, which state that around 70-80% of information thefts are conducted by insiders. However, sometimes it is not even known that some information has leaked.

The companies should also pay attention to what sort of information they are revealing about themselves and their employees on public channels like Internet, so the personal information should be kept to minimum and it is better to use role names than the actual names of the persons. It is also important to take care of the proper disposal of the material that is no longer needed. This applies to paper, electronic information, and hardware as well. The advances in feature matching and similar algorithms may require a more complete destruction of paper documents than mere shredding [1K]. The hardware, especially hard disks and such, should be destroyed rather than rely on erasing the contents, which still can leave traces of information. There are companies that offer this kind of services, but one needs to be certain that they employ due procedures, otherwise they could be real gold mines for information diggers.

VII. CONCLUSION

Due to a lack of awareness regarding social engineering, executives should first implement security awareness programs such as training sessions for all employees. Next, put tips onto the intranet and keep employees updated. Following, implement physical security measures and use audit testing to ensure data is not easily revealed to external users. Auditors should perform internal controls testing to ensure companies are implementing appropriate security policies in their companies. Overall, penetration tests will help the company finds its weakest access points and develop defenses to prevent confidential information from being stolen. Now, the technology changes the way people build social structures and networking, and providing new opportunities lobately affect people. Therefore, the most effective way to combat social Engineering is the training of users. Otherwise, carefully crafted security policies seem elusive to daily working, who cares only to do his or her job, but can still feel compassion with a colleague in

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

distress. And holistic approach can design help to mitigate the threats, which may result from decisions based on usability factors alone. In other words, should not be treated as a separate function from the security system but as the sum of all parts

REFERENCES

[1] Tolga MATARACIOGLU and Sevgi OZKAN, "User Awareness Measurement Through Social Engineering", International Journal of Managing Value and Supply Chains (IJMVSC) Vol. 1, No. F, December F010

[2] [F] T. Mataracioglu, "Social Engineering: Attack and Protection Methods", Tubitak

[3] Uekae", Department of Information Systems Security – Course Notes, Oct. F009. [G] K. D. Mitnick and W. L. Simon, The Art of Deception. Wiley Publishing, F00F.

[4] [K] M. B. Arslantas, "Methods Used in Internet Crime", MEB Head Office of Information Technologies. Nov. F00K : http://egitek.meb.gov.tr/EgitekHaber/EgitekHaber/s7H/bQlsQmsuclarQ.htm

[5] T. Mataracioglu, "Analysis of Social Engineering Attacks in Turkey", Journal of National Research Institute of Electronics and Cryptology (UEKAE), p. 88-9H, Vol. F, No. K, F01

[6] [I] M. Hasan, N. Prajapati, S. Vohara, "Case Study on Social Engineering Techniques for Persuasion", International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, Vol. F, No. F, Jun. F010.

[7] Fagoyinbo, I. S. Akinbo, R. Y. Ajibode, I. A., Analysis of the Awareness and Safeguarding Against Social Engineering: A Case Study of Federal Polytechnic Ilaro, Journal of Educational and Social Research Vol. 1 (F) September F011

[8] Lemos, Robert : Survey: Identity Theft Hits Three Percent. Security Focus, F00I.

[9] Grander Sarah: Social Engineering Reloaded: Security Focus, F00I

[10] Samuel T. C. Thompson, Helping the Hacker? Library Information, Security, and Social Engineering, Information Technology and Libraries, December F00I

[11] Dimensional Research, " The Risk of Social Engineering on Information

Security: A Survey of IT Professionals. September F011

[1F] Whitman M.E. Enemy at the gate: Threats to Information Security. Communications of the ACM, Volume KI, Issue 8, F00G.

[1G] Schneier B. Secret and Lies. Wiley Computer Publishing, F000.

[1K] Justino E., Oliveira L.S., Freitas C. Reconstructing shredded documents through feature matching. Forensic Science International Volume 1I0, Issues F-G, F00I.