INCREASING INFORMATION SECURITY INSIDE ORGANIZATIONS THROUGH AWARENESS LEARNING FOR EMPLOYEES

MOHAMMAD BTOUSH*, ABDULSALAM ALARABEYAT, MALIK ZBOON, OMAR RYATI, MUNEER HASSAN, SULIEMAN AHMAD
Al-Balqa Applied University, Salt, Jordan.
* *Corresponding author. Email* m.hjouj@bau.edu.jo

ABSTRACT

Social Engineering is the use of non-technical means to gain unauthorized access to information or systems. Instead of using vulnerabilities and exploit scripts, the hacker uses human nature. *Social Engineering* provides the potential for the most complete penetration of a target, but it does take time and talent. Generally, it is only used by hackers who are targeting a specific organization. *Social Engineering* is represented as in ability of building improper trust relationships with people who are working inside the organization to get unauthorized access privileges or gaining sensitive information such as (usernames, passwords, and personal identification codes(PINS)) which are needed to gain unauthorized access/see the organization's systems and information. Hackers have applied numerous methods to bypass the security measures, for instance using psychological tricks on legitimate users of a computer system to gaining unauthorized access to the information or systems. Many organizations like (companies, banks, universities) around the world are used set of(software and hardware Implementations)to protect them from this fatal attack. there is real fact every one you must takes in yours mind, are you can find one computer system in the world is not depend on human element inside it?, there will always be people who used to provide information and maintenance inside the organizations. many people are using social skills in some forms of our life since the beginning of our life on the universe, because most of us are want to be helpful and trusting source for others that it is from human nature which can not be change it easily. Inside my short paper WE attempt discussing the critical need for security issue in my organization (Petra University), as well as for an individuals (lecturers and Employees), then, WE will describe some of the methods that are used by *Social Engineers* to infiltrate security measures which are applied inside my university in an effort to ascertain confidential information and use it for malicious purposes. To end with, this paper WE will explain the importance of awareness learning against Social Engineering *attack*, and describe how the people should incorporate to safeguard and fighting against *Social Engineering* threats by giving some suggested solutions.

Keywords : *Awareness learning, Dumpster Diving, Impersonation, Phishing, Social Engineering*.

1. INTRODUCTION

Many organizations around the world depend today on reliable information to perform their daily tasks additionally the information needs to be timely, accurate, complete, valid, consistent and relevant to be of any use for the organization.
Today work in security issues typically focuses on the more technical aspects of information security, for instance firewalls and antivirus software. The more non-technical aspects of information security are vary often neglected [1].

There is one way of circumvent the technical protection mechanisms is *Social Engineering* once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software implementations. And present it's the hardest form of attack to defend against because hardware and software components alone won't stop it [2].
The main impression is that organizations are not only overlook the problem but there is a lack of awareness and knowledge about *Social Engineering* attack. Many organizations deal with it as a phenomenon so, a defense against Social

Engineering must take into account what is known about the psychology of persuasion for employees staff and develop that knowledge to understand the persuasive attack [3].

There are several ways to cope with *Social Engineering*, but the best way is by educating your employees that are need to be aware of the risks and remain vigilant against any new threats that can appear from inside or outside the organization [4].

Following from my abstract, the introduction talk about general information you must know about *Social Engineering* attack, and explain the ways to prevent it. Background and related works looks at *Social Engineering* attack from different aspects: its definition, uses, methods of attack, and classification. The main work talk about main process and tactics that are used from the hackers to penetrate of the organization and discuss how to safeguard against *Social Engineering* attack by suggested some physical or technical procedures that can used or applied to enforce it and give immunity for organization from negative impact of this attack. Finally my conclusions will explain with a short view of the problem, and suggest proposed solution for this problem from practical perspective.

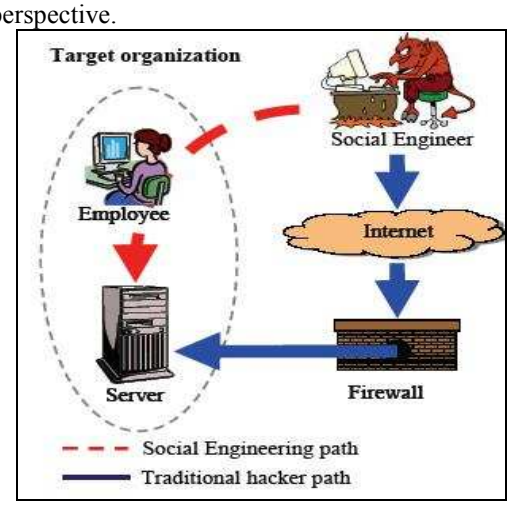

Figure 1

2. BACKGROUND

Many researchers and specialists over the world talk about *Social Engineering* attack from different dimensions and analyzing this fatal attack from practical perspectives. For example, Mr. Gaudin Sharon look for the *Social Engineering* as the human side of breaking into a shared networks. The hacker will not have any luck trying to convince a firewall or access control of the organization to give him or her will find easier way by persuading a person to allow him or her access to a secure area or even to make known confidential information [5].

Mr. Damle Pramod he considered the *Social Engineering* represented as in ability of hackers for gaining sensitive information. He also described the *Social Engineering* as the art if manipulating people into speaking/acting contrary to their Normal manner and he think the primary goal of the *Social Engineering* is to fool someone into providing valuable information or access to that information by preying on human behavior, such as the desire to be helpful, and trust source for the people. when you receive any sensitive information without any doubt you can say the *Social Engineering* attack is done successfully [6].

Social Engineers use many different strategies to persuade and influence others in order to accomplish their goal of gaining unauthorized access to systems or information in order to disrupt the system or network there is a few examples of these strategies include *impersonation*, *phishing*, and *dumpster diving* [7].

All specialists unanimously agreed considered the *Social Engineering* attack as the serious threat to most secure computers systems, networks, and organizations. Because it depend human factor which considered as the weakest point in any organization so, it is not easy to defend against it [8].

This basically means you can find very skilled *Social Engineers* have ability to gain access to any desired computer system or information in spite of the hardware and software protection mechanisms implemented to protect them. Therefore *Social Engineering* is essentially based on finding a way or means to bypass technology security mechanisms implemented in a system by manipulating people who have access to the desired system or information [9].

Figures 1 Illustrates how the *Social Engineers* uses humans inside the organization to acquire desired information, and uses social skills instead of using traditional hacking techniques to gain access to the target organization. Finally all specialists and researchers who are works in FCC (FederalCommunicationsCommission) Center in USA are unanimously agreed after comprehensive study for the *Social Engineering* attack that exist very little number of people have ability to talk about what happened for it from *Social Engineering* attack so, all thinks the primary reason for the lack of discussion about *Social Engineering* can be attributable to shame

from others. Most of people see *Social Engineering* as an attack on their intelligence, and no one wants to be considered as "ignorant" person enough to have been duped this is why *Social Engineering* gets put in the closet as a "taboo" subject. My dear you are, vulnerable to a *Social Engineering* attack in any time [10].

3. MAIN WORK

A few years ago the university was working out a series of deliberate sabotage by one of the employees who hold senior positions-Director of Computer Center– this is sabotage to disrupt many of the systems used within the university such as the admission and registration of students, the accounting system, this offensive action was an unpleasant surprise to the university administration and academic and administrative staff of both this act of vandalism has left a negative impact for the majority of workers, which prompted me to search for the cause of the problem and the motives and methods used and search for better ways to prevent the recurrence of this act of vandalism again. This attack confirms to me no doubt one percent if there is no risk there is no need for security this risk can be come from vulnerabilities in physical/technical procedures that applied inside my university or real threats that come from internal/external environments so, the security has never been important as it is today.

The essential need for security in not only apparent in every organization, but also for the individuals this means individuals are at a high level of risk when having their personal information stolen and used by attackers for their own personal again. Many security procedures for the Organizations are needed to protect confidential information, and all possible security precautions must be taken.

For organization, these safety measures should include password requirements for access to electronic records. In addition, only authorized personnel should be allowed entrance to a workplace where classified information or equipment is located. And when transmitting data across the network, it should be encrypted to prevent malicious intruders from capturing and analyzing it. To further secure private records, there are many tools such as firewalls, access control lists, and intrusion prevention systems, can be used to prevent from this fatal attack.

It is just as important that an individual should protect his or her personal electronic information by using passwords for access and having security tools in work place.

4. THE PROCESS OF THE SOCIAL ENGINEERING ATTACK

Even though *Social Engineering* attack can be performed in many various ways a common pattern has emerged according to Gartner. This pattern is analyzed and divided into four common steps that are performed in a *Social Engineering* attack.

Each steps is dependent of the completion and success of the previous steps therefore their position in the process is fixed this chart is show these steps.

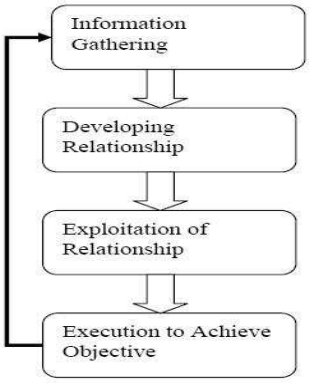

Figure2 [7]: The process of *Social Engineering* attacks

The *Social Engineers* makes use of different techniques to gather information about specific target.The information is then used to build relation with the target by developing a relationship; attackers place themselves in a position of trust, which can then be exploited. The attacker exploits the target into revealing information this information or action can be the end objective or can be used to stage the next attack /phase of attack. The attacker can be executes this process many times to achieve the end objective often an attack includes a number of these cycles to achieve the end objective.

The iteration arrow in the figure above shows that the process can be repeated a number of times until the attacker has gathered the information needed to perform a more serious attack. In this way the attacker achieves enough information about the organization and its employees to be able to, for instance, act as an employee in the organization in this way the attacker can be convince the target to reveal information needed to compromise the organization security [7].

The *Social Engineers* uses many different strategies to persuade and influence others to achieve their goal. A few examples of these tactics include *impersonation*, *phishing*, and *dumpster diving*.

5. IMPERSONATION

Impersonation is arguably the greatest technique used by *Social Engineers* to swindle many people, such as posing as an employee of the same organization. "Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his or her badge" [13]. In particular, a *Social Engineer* finds that pretending to be an employee in the information Technology (IT) department is typically useful guise. A simple phone call requesting an employees password is usually an easy way to get access to information. Once an employee learns that the call is originating from the it department, he or she will usually disclose the password willingly and without question, especially after that employee has been told, what seems to be, a legitimate reasons for the request. Using the phone is not only frequently used at the workplace to conduct a Social Engineering attack, but its also a mean for obtaining private information from people at home.

6. PHISHING

"Phishing is the most common from of *social engineering* online and most notably includes e-mail spoofs." [12]. webopedia [15] 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. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, and bank account numbers that the legitimate organization already has. The Web site however, is bogus and set up only to steal the user's information. Phishing can be considered a form of impersonation except that instead of the intruder masquerading as an authorized individual, the social engineering attack comes in the form of an email or other online mechanism.

7. DUMPSTER DIVING

Although it might not be the most sophisticated manner for a hacker to ascertain information, dumpster diving tends to be a valuable *Social Engineering* attack method. Search Security [16] reveals that "*Social Engineers* rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it." Most employees would probably not think twice about throwing away a company phone book or company policy manuals. It's commonly done to research a predetermined target and determine the best opportunities for exploitation. Dumpsters are usually not locked or exist in not protected areas as a result, this makes them very attractive to hackers. The individual at home is just as vulnerable to dumpster diving as an organization.

8. HOW TO DEAL WITH SOCIAL ENGINEERING

Today there is no particular approach to be absolutely protected against any security threat. This clearly applies to *Social Engineering* attack as well. It is even harder to protect yourself against *Social Engineering* attack then to protect your self against for virus attacks since a virus has limited ways to accomplish while a *Social Engineer* can act in mainly endless ways. There is however ways to reduce the likelihood of successful *Social Engineering* attacks. Many researchers that discuss different defensive measures against *Social Engineering* attack, education and training of employees is often mentioned as the most effective and sometimes even as the only protection there is against *Social Engineering*. To go as far as to say that it is the only way to cope with the problem is a fairly risky thing to involve, nevertheless one can agree that education is an important area in the combat against social engineering. Although the emphasis in this paper lies on the educational and training part it is important to mention other additional countermeasures Mr. Malcolm Allen suggest many countermeasures, besides education, to combat against *Social Engineering* like the following [8] :

Security policy : Te security policy clearly states what is expected from the personnel within n organization. It is important that employees knows to what extent they re allowed to give out information**.**
Good security architecture: The key issue here is to keep it simple so that personnel can concentrate on more important tasks.
Management buy in: It is important that the management are well aware of what type of security rotection is needed and why, in order for efficient

protective measures to be taken to counter the risks.
Limit data leakage: To make it hard for the Social Engineer to achieve desired information about a organization it is a good idea to decrease the amount of data available in public on for instance websites**.**
Incident response strategy: Clear rules on how to handle information requests is important when stressed situations occur for the employees**.**

There are many other suggestions on countermeasures presented throughout the articles that deal with this issue. For example Mr. Gartner [7] suggests specific solution for this problem by removing human's element from the authentication process he considered this solution is the best way to deal with troubles that happen when humans authenticate other humans. The purpose with showing these countermeasures is not to claim that these are somehow best practice. The purpose is to show that other means that education are both available and necessary to be able to cope with the problem of *Social Engineering* attack.

9. HOW TO SAFEGUARD AGAINST SOCIAL ENGINEERING

Mr. Granger considered the *Social Engineering* attacks are one of the hardest threats to defend against because they involve the human element. Mr. Granger [7] successfully puts it, "Security is all about trust. Trust in defense and authentic generally agreed upon as the weakest link in the security chain, the natural human motivation to accept someone at his or her word leaves many of us vulnerable to attack."

In the world today *Social Engineering* attacks may be unavoidable for the basis that humans are such easy targets, nevertheless, that does not mean that they are unpreventable. "Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how *Social Engineers* function." [16].

Absolutely employees training and awareness learning for them is needed for any organizations, or an individuals who works inside it, to protect them from against *Social Engineering* attack. *Social Engineers* not only succeed on people's ignorance of the importance of the information they possess, but also of the fact that they are unaware to the possible attacks against themselves.An organization should provide well prepared training programs to all employees, security guards, Help Desk employees, and organization's management. This training programs should highlight the need for security and inform people of the different *Social Engineering* attacks, as well as the actions they can take to prevent accidentally giving out confidential information. Businesses, such as credit card companies and banks, should also educate its' customers by supplying them information and instruction on *Social Engineering* attacks so that they, too, will be aware of the possible security risks associated with the individual at home.

Security measures must work in conjunction with other training and awareness programs which are applying inside the organization, to defense against *Social Engineering* attacks. These procedures should be documented clearly in an organization' policies. This Documentation will help support these programs not only by increasing awareness, but by providing a reliable manner in which employees should act. The employee will know that by acting according to the rules, he or she does not have to fear any possible repercussions.

Once people are aware of potential *Social Engineering* attacks, they are able to use their best decision as a defense mechanism. In the case where an email is received from a company requesting that an individual update his or her account information, a person who is knowledgeable of phishing attacks would not permission to being directed to a possible trick website through a link on that email. That person would either go directly to the company's web site through a divide browser window, or call the company to confirm that the email was in fact legitimate.

Awareness learning for employees inside any organization in the world would also allow people who work inside it to be more heedful of what they throw away in the trash. When people are mindful of the value of the information they own, they will be more careful of how they handle it. Furthermore, when people are heedful that there are hackers eager to go through their trash and "dumpster dive" for this valuable information, then they will take the proper precautions of disposing of the trash properly.

The Following Table Lists Some suggestions for hackers Tactics And combat Strategies that can be used from organizations, or an individuals For Prevention from *Social Engineering* attack: [14].

Area of Risk	Hacker Tactic	Combat Strategy
Phone (Help Desk)	Impersonation and persuasion	Train employees/help desk to never give out passwords or other confidential info by phone
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Office	Shoulder surfing	Don't type in passwords with anyone else present (or if you must, do it quickly!)
Phone (Help Desk)	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support
Office	Wandering through halls looking for open offices	Require all guests to be escorted
Mail room	Insertion of forged memos	Lock & monitor mail room
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Phone	Stealing phone toll access	Control overseas & long-distance calls, trace calls, refuse transfers
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
Intranet-Internet	Creation & insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
Office	Stealing sensitive documents	Mark documents as confidential & require those documents to be locked
General-Psychological	Impersonation & persuasion	Keep employees on their toes through continued awareness and training programs

10. CONCLUSION

The information security has never been as important as it is today for the business organizations and individuals alike. So, the information confidentiality is measured as main topic for many organization around the world that attempt to find the best way to protect them from hackers attacks for instance *Social Engineering* attack, which considered for many specialists and researchers as a safest attack that can be happen with simplest ways comparison with other technical attacks Which need from attackers good knowledge and experience. *Social Engineering* is a technique used by hackers to convince people to reveal confidential information, or allow unauthorized access, for their personal gain or for malicious purposes. Hackers techniques and strategies such as *impersonation*, *phishing* and *dumpster diving* are used by *Social Engineers* to accomplish their goals. Although *Social Engineering* attacks are not easy to defend against because they involve the human element, it is possible for organizations and individuals to guard themselves by being skilled on the importance of security and gaining awareness of the possible *Social Engineering* attacks that they may encounter.

Individuals and many organizations in the world can try to protect their confidential information by storing their data on a system that requires password-only access, putting that system in a secure room that allows only authorized entrance, and by spending as much money as possible on security tools to protect that data. After implementing all of these essential safety measures, they are still vulnerable to *Social Engineering* attacks because every security measure involves some kind of human intrusion.

While many organizations in the world attempt to training people on diverse methods used by *Social Engineers* will help prevent some attacks from being successful, these methods can be change and countless other schemes can be used. The only practical solution to protecting against these threats is by generating overall awareness. Many people are aware of the important data that they possess, the critical need to protect it, along with the strong likelihood of exploitation, then a strong defense will be built and *Social Engineering* attacks will begin to decline.

REFERENCES:

[1] *R. Sheiman*, "A balanced approach to information security", Last access November 3, 2008 from http://www.infoscreen.com/publications/InfoScreen_balanced_approach.pdf

[2] *A. Wendy*, "A proactive defense to Social Engineering", Last access November 5, 2008 from http://www.sans.org/rr/paper.php?id=511

[3] *D. Gragg*, "A multi-level defense against Social Engineering", Last access November 5, 2008 from http://www.sans.org/rr/papers/51/920.pdf

[4] *R. Barber*, "Social Engineering: A people problem?" Network security magazine, volume 2001, issue 7, 1 July 2001

[5] *S. Gaudin*, "Social Engineering:The Human Side of Hacking", Last access November 14, 2008 from http://itmanagement.earthweb.com/secu/article.php/1040881

[6] *P. Damle*, "Social Engineering: A Tip of the Iceburg", Information Systems Control Journal (2002), Last access November 5, 2008 from http://www.iii.org/media/facts/statsbyissue/idtheft/

[7] *S. Granger*, "Social Engineering Fundamentals, Part I:Hacker Tactics", Last access November 3, 2008 from http://www.securityfocus.com/print/infocus/1527

[8] *M. Allen*, "The use of "Social Engineering" as a means of violating computer systems" Last access November 30, 2008 from http://www.sans.org/rr/paper.php?id=529

[9] *J. Hiner*, "Change your company's culture to combat Social Engineering attacks" Last access November 25, 2008 from http://techrepublic.com.com/5100-6264-1047991.html

[10] *Federal Communications Commission*, "FCC computer security notice week 2002" Last access November 18, 2008 from http://intranet.fcc.gov/omd/itc/csg/index.html

[11] *M. Gartner*, "Information Security Strategies Research Note TU-14-5662" Last access November 28, 2008 from http://www3.gartner.com/gc/webletter/security/issue1

[12] *S. Granger2006*, "Social Engineering Reloaded" Last access November 3, 2008 from http://www.securityfocus.com/print/infocus/1860

[13] *C. Palmer*, "Ethical Hacking" IBM Systems Journal, Volume 40, Number 3 Last access November 8, 2008 from http://www.research.ibm.com/journal/sj/403/palmer.html

[14] *K. Mitnick*, "The art of deception" Wiley Publishing, Inc. 2003

[15] *Webopedia*, "Hacker Tactic's: Phishing" Last access November 10, 2008 from http://www.webopedia.com/TERM/p/phishing.html

[16] *Social Engineering*, "Security Definitions" Last access November 10, 2008 from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html