Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(11): 15-19

Review Article ISSN: 2394 - 658X

Social Engineering Threats and Awareness: A Survey

Anshul Kumar, Mansi Chaudhary and Nagresh Kumar

Department of Computer Science & Engineering,
Meerut Institute of Engineering and Technology, Meerut, Uttar Pradesh, India
rana.anshul2010@gmail.com

ABSTRACT

This paper defines social engineering and explains how one can use the human mind for capturing useful information about organizations or individuals. It also provides recommendations on how to defend and protect against attackers using social engineering techniques. Social engineering is a non-technical method of intrusion hacker's use that relies heavily on human interaction and often involves tricking people into breaking normal security procedure. Since there is neither hardware nor software available to protect an enterprise or individual against social engineering, it is essential that good practices be implemented. The overall purpose of this survey is to highlight the different social engineering attacks and how they can prevented.

Key words: Social Engineering, Intrusion, Hacker, Attack

INTRODUCTION

In today's information age, cyber threats are very real and will continue to be a concern for organizations or individuals. Cyber threats expose vulnerabilities in an organization's security infrastructure to gain valuable information, usually for financial gain. Cyber attacks can cause system disturbance [1] and uncover information such as credit card numbers, passwords, and proprietary documents that can cost individuals and organizations from hundreds to billions of dollars. Sometimes cyber attacks are motivated by a personal vendetta or retaliation. The Internet is evolving into a medium that is beyond just web search. Social networking, micro blogging, etc. are some of the next generation services that have gained prominence. Users of these services have real time two-way interaction (e.g. Facebook [2], MySpace [3], Twitter) as well as non real-time communication (e.g. Craigslist [3]).

This survey explains how one can use human beings for capturing useful information about the organization. In this paper we have described various techniques used for performing social engineering attack, various qualities required for social engineer and the counter measures for a social engineering attack. This survey defines social engineering and discusses how it negatively affects organizations or individuals. It also provides recommendations on how to defend and protect against attackers using social engineering techniques. The objective of this paper is to present and demonstrate an analytical approach towards Social Engineering and its presence in India. Analysis of the collected responses guided us to construct a more refined model of Social Engineering based attacks. The paper begins types of social engineering followed by preventive method of Social Engineering attacks. The paper ends with some suggestions to protect Social Engineering based attacks.

What is Social Engineering?

Social engineering is the art of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception for the purpose of information gathering, fraud, identity theft, or computer system access. Social engineering attacks that include interpersonal interaction involve direct communication (such as in person or by telephone) or interaction that is mediated through electronic means (e.g., electronic media, email, and Internet).

Social engineering is the act of gaining either unauthorized access to a system or sensitive information, such as passwords, through the use of trust and relationship building with those who have access to such information. A social engineer uses human psychology to exploit people for his or her own use. The most common method for gaining unauthorized access into a company's network is simply by calling specific personnel within the company. This generally involves convincing people over the phone into giving them information through persuasion with tools such as fear, imitation, and compassion [4].

Why Social Engineering?

Social engineering is a non-technical method of intrusion hacker's use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineering attacks are more challenging to manage since they depend on human behaviour and involve taking advantage of vulnerable employees. Businesses today must utilize a combination of technology solutions and user awareness to help protect corporate information.

HUMAN BASED METHODS

Human Based

Human based social engineering [5] needs interaction with humans; it means person-to-person contact and then retrieving the desired information. People use human based social engineering techniques in different ways; here I am sharing the top popular methods.

a) **Impersonation:** In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system [5-8]. A hacker can gain physical access by pretending to be a janitor, employee, or contractor.

b) **Posing as an important user:** In this type of attack, the hacker pretends to be a VIP or high-level manager who has the authority to use computer systems or files. Most of the time, low-level employees don't ask any questions of someone who appears in this position.

c) **Being a third party:** In this attack, the hacker pretends to have permission from an authorized person to use the computer system. It works when the authorized person is unavailable for some time.

d) **Desktop support:** Calling tech support for assistance is a classic social-engineering technique. Help desk and technical support personnel are trained to help users [9], which makes them good prey for social engineering attacks.

COMPUTER BASED METHODS

Computer Based

Computer-based social engineering [5] uses computer software that attempts to retrieve the desired information.

a) **Phishing:** An exploit generally defined as a phisher impersonating a trusted third party to gain access to private data. Typically, the phisher sends an email that appears to come from a legitimate business or individual [5], [10] (e.g., a bank, credit card company, or fellow employee) requesting verification of information and warning of dire consequence if it is not provided. The email usually contains a link to a fraudulent web page that appears legitimate—sometimes with company logos [11] and content—and requests private information (e.g., Social Security number, bank account number, banking PIN).

b) **Baiting:** Baiting involves dangling something you want to entice you to take an action the criminal desires [7]. It can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labeled "Executive Salary Summary Q1 2013" left out in the open for you to find. Then, once the device is used or downloaded, the person or company's computer is infected with malicious software allowing the criminal to advance into your system.

c) **On-line scams:** Emails sent by scammers may have attachments [5] that include malicious code inside the attachment. Those attachments can include key loggers to capture users' passwords, viruses, Trojans, or worms. Sometimes pop-up windows can also be used in social engineering attacks. Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

d) **Pop-up windows**: A window will appear on the screen telling the user that the network connection has been lost. The user is prompted to reenter their user name and password. A program previously installed by the intruder [8] will then email the information back to a remote site. Users are directed to sites that claim to offer help or more information but are really designed to plant Trojan horse programs on their computers which the hackers later use to gain access to their computers and the networks to which they are connected.

e) **E-Mail attachments:** Programs can be hidden in email attachments that can spread viruses or cause damage to computer networks [8]. This includes malicious software such as viruses, worms and Trojan horses. In order to entice users to open the attachments, they are given names that raise curiosity and interest. The first example of this combination of traditional worms along with a social engineering component was the "I Love You" worms. Another recent example is the "Anna Kournikova" worms. The user assumes that by opening the attachment, they will see a picture of Anna Kournikova. This particular worm also employs another social engineering tactic "Designers of the virus attempt to hide the file extension by giving the attachment a long file name. In this case, the attachment is named Anna Kournikova.jpg.vbs. Often when displayed the name is truncated so it looks like a harmless jpeg file when it really has a .vbs extension.

f) **Email scams:** Email scams [5] are becoming more prevalent. One recent example claims that you have won a trip to the Bahamas and requests "basic information" from the user so that the prize can be awarded. Initially they request relatively harmless information such as name, address and phone number; however, in a subsequent email, credit card information is requested in order to hold your spot on the "free" trip.

g) **Chain Letters and Hoaxes:** These nuisance emails rely on Social Engineering to continue their spread. While they do not usually cause any physical damage or loss of information, they cause a loss of productivity and also use an organization's valuable network resources.

h) Websites: A common ploy is to offer something free or a chance to win a sweepstakes on a Website. To win the user must enter an email address and a password. Many employees will enter the same password that they use at work, so the Social Engineer now has a valid user name and password to enter an organization's network.

PREVENTION OF SOCIAL ENGINEERING ATTACKS

Tools and techniques have been designed to prevent social engineering attack. Using these tools make the organizations less vulnerable [5-6]. According to Douglas Twitchell, there are currently three ways commonly suggested to defend against social engineering attacks: education, training and awareness; policies; and enforcement through auditing.

- Organization's employees or individuals can be educated through training and awareness which can make them more reluctant to disclose personal information. In depth security training of the employees should be conducted. This reduces the risk of social engineering attack and makes the organization less vulnerable.
- Policies should be made which provides instructions to the employees on proper handling of company's or personnel information and user data.
- Audits must be conducted in order to ensure that the employees of the organization are following the policies and procedures.
- Hard copies of organizational data, records, or personal information must be destroyed before being discarded. Common effective methods for destroying hard copy information include shredders and incinerators [6].
- Employees or individuals should be trained to question the credentials of the person who is calling himself to be in authoritative position in that organization.
- Organizations should be careful about what they are posting on their company's website. Company's details like names of people on authority and contact numbers should be avoided.

The most important thing that we can do to prevent being a victim of an attacker is to be aware of common tricks like those I have mention in this paper. Never give out any confidential information or even seemingly non-confidential information about you or your company-whether it's over the phone, online, or in person, unless you can first verify the identity of the person asking and the need for that person to have that information. You get a call from your credit card company saying your card has been compromised? Say okay, you'll call them back, and call the number on your credit card rather than speaking to whoever called you. Always remember that real IT departments and your financial services will never ask for your password or other confidential information over the phone. Also, make good use of your shredder and dispose of your digital data properly.

You can protect yourself from phishers [7],[12], scammers, and identity thieves, but there's only so much you can do if a service you use is compromised or someone manages to convince a company they're you. You can, however, take a couple of preventive measures yourself.

- **Use different logins for each service and secure your passwords**: Never use the same password for all services. And make sure your passwords are strong and complex so they're difficult to guess.
- **Use two-factor authentication**: This makes it harder for thieves to get into your account, even if your username and password are compromised.
- **Get creative with security questions**: The additional security questions websites ask you to fill in are supposed to be another line of defence, but often these questions are easily guessed or discoverable (e.g. where you were born).
- **Use credit cards wisely**: Credit cards are the safest way to pay online (better than debit cards or online payment systems like Papal), because of their strong protections. If you use a debit card and a hacker gets access to the number, your entire bank account could be drained. You can further secure your credit card by not storing card numbers on websites or using disposable or virtual card numbers.
- **Frequently monitor your accounts and personal data**: To be on the lookout for both identity theft and credit card fraud, check in with your account balances and credit score regularly. Several services offer free ID theft monitoring, credit monitoring, and questionable credit charges. You can even use Goggle Alerts as an identity theft watchdog.
- **Remove your info from public information databases**: Sites like ZabaSearch and People Finders publish our private information (like address and date of birth) online for all to see. Remove yourself from these lists with this resource.

These steps won't prevent your account from being compromised if a service provider falls for a social engineering hack and hands your account over to the attacker, but they may at least minimize the damage possible and also give you more peace of mind that you're doing as much as you can to protect yourself.

Since there is neither hardware nor software available to protect an enterprise or individual against social engineering, it is essential that good practices be implemented. Some of those practices might include:

- Require anyone there to perform service to show proper identification [9]. Make certain that the reception area has been trained to verify all service personnel and that there are procedures in place for the receptionist to summon assistance quickly.
- Establish a standard that passwords are never to be spoken over the phone. When contacting the help desk to have a password reset, the organization should establish a set of phrases or words known only by the user. The help desk can then reset the password to one of those words.
- Implement a standard that forbids passwords from being left lying about. Because employees now average around eight access accounts and passwords (information technology employees average twenty accounts), it is no longer possible to forbid the writing down of accounts and passwords. The new requirement should place the emphasis on the classification of passwords and confidential information and require the employees to treat them accordingly.
- Implement caller ID technology for the Help Desk and other support functions. Many facilities have different ring tones based on inter-office phone calls as opposed to calls that originate from outside. Employees need to be trained to not forward outside calls. Take down the name and number of the call and forward the message on to the proper person.
- Invest in shredders [9] and have one on every floor. Every work area needs a shredder. The size of the shredder should be based on how much confidential information is present in the office area. Eliminate confidential information collection bins. Require shredding, not storing.

Policies, procedures and standards are an important part of an overall anti-social engineering campaign [9]. To be effective a policy should be:

- It should not contain standards or directives that may not be attainable. When creating standards work with the user community to establish what can be accomplished immediately. Once these actions have been implemented, then every six months assess the process and act accordingly.
- They should stress what can be done and stay away from isn't allowed as much as possible. Enumerate to the employees what they can and should do. Requirements that begin with "Thou shall not . . ." have a tendency to turn people off to the standard.
- They should be brief and concise. Our employees don't have a lot of spare time. Tell them what is required and leave the rationalizations to the security awareness program.
- The need to be reviewed on a regular basis and kept current. Nothing lasts forever. As we discussed above, every six months assess the process and make adjustments as required.
- The message and standards should be easily attainable by the employees and available via the company intranet. Keep the user base informed. Use an internal web site to answer questions and give advice.

Employee Education Is the Key

To be effective, policies, procedures and standards must be taught and reinforced to the employees. This process must be ongoing and must not exceed three months between reinforcement times. It is not enough to just publish policies and expect them to read, understand and implement what is required [9]. They need to be taught to emphasize what is important and how it will help them do their job. This training should begin at new employee orientation and continue through employment. When an person becomes an ex-employee, a final time of reinforcement should be done during the exit interview process. Another method to keep employees informed and educated is to have a web page dedicated to security. It should be updated regularly and should contain new social engineering ploys. It could contain a "security tip of the day" and remind employees to look for typical social engineering signs. These signs might include such behaviors as: Refusal to give contact information, rushing the process, Name-dropping, Intimidation, Small mistakes, Requesting forbidden information or accesses etc.

As part of this training or education process, reinforce a good catch. When an employee does the right thing, make sure they receive proper recognition. Train the employees on who to call if they suspect they are being social engineered. Apply technology where you can. Consider implementing trace calls if possible or at least caller ID where available. Control overseas long distance services to most phones. Ensure that physical security for the building and sensitive areas are effective.

FINAL THOUGHTS

A social engineer with enough time, patience and resolve will eventually exploit some weakness in the control environment of an enterprise. Employee awareness and acceptance of safeguard measures will become our first line of defense in this battle against the attackers. The best defense against social engineering requires that employees be tested and that the bar of acceptance be raised regularly. Security professionals can begin this process by making available to all personnel a broad range of supporting documentation. Many employees respond positively to anecdotes relating to social engineering attacks and hoaxes. Keep the message fresh and accurate.

Include details about the consequences of successful attacks. Do not discuss these attacks in terms of how security was circumvented, but on their impact to the business or mission of the enterprise. These attacks can lead to a loss of customer confidence, market share, and jobs. Employees at all levels of the enterprise need to understand and believe that they are important to the overall protection strategy. Without all employees being part of the team, the enterprise, its assets, and its employees will be open to attack from external and internal social engineers. With training and support, we can lessen the impact of these kinds of attacks.

RESULTS AND DISCUSSION

A fundamental question is: how much privacy is enough? Social media companies have to balance the need for user privacy with law enforcement needs. Facebook, in its 2010 policy guide states that falsifying profile information will lead to disabling of the user account. But, checking the veracity of the profile information for each of the several hundred million users is an impossible task. Craigslist allows its users to flag a posting into one of several categories, if they choose to. One of these categories is spam. While policies and practices have been defined in India, U.S. and many other countries, this is not true globally. This may be because of low Internet penetration, blocking of all or many social media sites, close government monitoring of Internet user activities, etc. But with the growth of cellular networks Internet access is becoming more prevalent and cheaper in many countries. This means that in a few years countries that do not have well defined social media security policies have to rethink this issue to fill the policy gap. Even although people had participated in some form of training, many were still willing to share their passwords. Unfortunately, our other options for improving security are limited. Password strength may be improved through technical means and system requirements. However people are people and are often the weakest link in the security process.

CONCLUSION

On conducting a survey on the social engineering techniques and the art of deception, we can conclude that even after using the best and even the most expensive security technologies, an organization or a company or an individual is completely vulnerable. It means it is very easy for a good attacker to gather information about that organization just by gaining trust and being friendly with the user.

Social engineering technique of capturing information is being used since long time but it came into notice just some time before. Before people and organizations were not much aware of these security breach practices and techniques for securing information but nowadays information security is the main concern of the corporate world.

A key mechanism for combating social engineering must be the education of potential victims, in order to raise their awareness of the techniques and how to spot them. To protect the Social Engineering, employee or individual education, training & awareness is the key. Policies, procedures and standards are an important part of an overall anti-social engineering campaign.

REFERENCES

[1] Jessica C Flack and Raissa M D'souza, The Digital Age and the Future of Social Network Science and Engineering, *Proceedings of the IEEE*, **2014,** 102 (12), 1873 – 1877.

[2] Megha Gupta and Sameer Agarwal, A Survey on Social Engineering and the Art of Deception, *International Journal of Information and Education Technology*, **2012,** 1 (1), 31 – 35.

[3] Joseph A Cazier and Christopher M Botelho, Social Engineering's Threat to Public Privacy, *Proceedings of the 6th Annual Security Conference*, Las Vegas, NV, **2007**.

[4] Anubhav Chitrey, Dharmendra Singh and Vrijendra Singh, A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model, *International Journal of Information and Network Security*, **2012**, 1(2), 45 – 53.

[5] Jeremy R Strozer, Sholom Cohen, AP Moore, David Mundie and Jennifer Cowley, Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits, *IEEE Security and Privacy Workshops*, **2014**.

[6] Devin Luco, The Art of Social Engineering: A Research Note, *http://anniesearle.com/* **2015**.

[7] L J Janczewski and Lingyan (Rene) Fu, Social Engineering Based Attacks: Model and New Zealand Perspective, *Proceedings of the International Multiconference on Computer Science and Information Technology*, **2010**.

[8] Thomas R Peltier, *Social Engineering: Concepts and Solutions, Information Systems Security*, **2006**.

[9] Mahmoud Khonji, Youssef Iraqi, Andrew Jones, Phishing Detection: A Literature Survey, *IEEE Communications Surveys & Tutorials*, **2013**, 15(4), 2091-2121.

[10] R Chandramouli, Emerging Social Media Threats: Technology and Policy Perspectives, *Cyber Security Summit*, **2011**.

[11] Ugiomo Odaro and Benjamin Sanders, Social Engineering: Phishing for a Solution, A Research Note *http://www.kaspersky.co.in*/ **2015**.

[12] A Karakasiliotis, M Papadaki and SM Furnell, Assessing End-User Awareness of Social Engineering and Phishing, *Proceedings of the 7th Australian Information Warfare and Security Conference*, **2006**.