International Journal of Engineering Research & Management Technology ISSN: 2348-4039
January-2016 Volume 3, Issue-1
Email: editor@ijermt.org www.ijermt.org

Social Engineering in Social Networking Sites: A Survey

Mansi Choudhary , Anshul Kumar ,Nagresh Kumar
Department of Computer Science & Engineering
Meerut Institute of Engineering & Technology
Meerut

ABSTRACT

This paper defines social engineering in social networking sites and explains how one can use the human mind for capturing useful information about organizations or individuals.Social networking sites such as Facebook and Twitter have gained more popularity in recent years. Because of its large user base, and large amount of information, they become a potential channel for attackers to exploit. Many social networking sites try to prevent those exploitations, but many attackers are still able to overcome those security countermeasures by using different techniques. Social network users may not be aware of such threats. Therefore, this paper will present a survey on different privacy and security issues in online social networks. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats.

KEYWORDS: Social Engineering (S.E), Social Networking Sites, Attackers

INTRODUCTION:

The popularity of online social networking sites has increased the amount of personal data which is distributed on the net. This is supported by the fact that social networking sites have overtaken email in terms of usage[2]. Online social networking sites contain user profiles which consist of personal data. Those profiles are semi-structured [8] and the profile data or structure may change in an unpredictable way. This fits in nicely with the way online social networks operate. Social network profiles change all the time not just in structure but content as well. More research needs to be done into the extraction from semi-structured pages in terms of online social networking profiles. Our goal is to extract the relevant profile data so it can be mined in the future to find attributes that can cause the profile owner to be vulnerable to social engineering attacks. In terms of online social networks our research will allow us in the future to investigate the friends of a profile and see if any of the friends have profiles on other online social networks. This links into the transitivity concept where e.g. A and B are friends on one online social network but B and C are also friends on another online social network. The question is: will A and C become friends and if so how great will the strength of their friendship be. The question posed fits with theory[7] about weak ties and how they can provide an alternative information source to the ones associated with the strong ties.

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. Often the social engineer, or attacker, never come face-to face with the victim. The social engineer uses impersonation via phone, fax, Internet, messaging or e-mail- basically any form of communication.

WHY SOCIAL ENGINEERING?

Social engineering is a non-technical method of intrusion hackers 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 behavior and involve taking advantage of vulnerable employees. Businesses today must utilize a combination of technology solutions and user awareness to help protect corporate information.This generally involves convincing people over the phone into giving them information through persuasion with tools such as fear, imitation, and compassion [4].

ONLINE SOCIAL ENGINEERING:

Social engineering (SE) is the art of deceiving or tricking or may have been mastered before the invention of technology and computers, the Internet is a fertile ground for social engineers looking to gather valuable information. With the proliferation of poorly-secured computers on the Internet and publicly known security holes, the majority of security compromises are done by exploiting vulnerable computers. Computer attacks that do not use social engineering is commonly termed **hacking**. This is a more direct attack using hardware and software methods and programming tricks to break a security feature on the system itself. Generally, hacking requires above-average computer skills and takes much longer than simply obtaining an authorized user's ID and password. Social engineering for online information often focuses on obtaining passwords. While the typical social engineering attempt would be to gain trust and just ask for them password, many technical methods can also be used to gain password information without the owner's permission. An ongoing weakness that makes these attacks successful is that many users often repeat the use of one simple password on every Internet account, even their financial institutions. Several methods can gain password information.[3].

1.2.1 AWARDS:

Another way in which attackers can obtain personal information is through online forms that solicit information: Attackers can send out enticing offers or "awards" and ask the user to enter their name, e-mail address, and even account passwords.

1.2.2 POP-UP WINDOWS:

Pop-up windows can be installed by attackers to look like part of the network and request that the user reenter his username and password to fix some sort of problem.

1.2.3. NETWORK SNIFFING:

Sniffing means examining network traffic for passwords A person doing sniffing generally gains the confidence of someone who has authorized access to the network, to help reveal information that compromises that networks security. Then, the attacker can monitor a screen until an unsuspecting target types in their account information.

1.2.4. EMAIL:

Email can be used for more direct means of gaining access to a system. For instance, mail attachments can carry malicious software that can gather personal information without the user knowing. Trojan horses, viruses, and worms can be slipped into the e-mail body or attachments to solicit usernames and passwords.

1.2.5. PHISHING:

Phishing is a form of social engineering which involves using e-mail and websites designed to look like those of well-known legitimate businesses, financial institutions, and government agencies, to deceive users into disclosing their account information. These phony websites are simulations that appear to be login screens, but are not.Graphics and format can be copied from legitimate sites to make them highly

convincing. Once trust is established, a phisher tries to obtain sensitive personal, financial, corporate or network information. Many attackers target financial or retail organizations, but military targets are increasing (especially highly targeted phishing called "spear phishing"). Phishing can try to lure consumers into revealing their personal and financial data such as social-security numbers, bank and credit-card account information, and details of online accounts and passwords. A spoofed e-mail could ask you for billing information or other personal records, supposedly from a high-ranking employee. The attacker could e-mail thousands of online customers as the head of a corporation asking them to send in their passwords because some files were lost. Phishing can also be very
Useful to an state-level adversary for spying or sabotage.

1.2.6. HARVESTING NETWORKS:

Another tactic of social engineering is to use social-network websites such as myspace.com and friendster.com to harvest freely available personal data about participants, and then use the data in scams such as fraud and money laundering.[1]

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.

1. Organization’s employees or an in dividuals 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.
2. Policies should be made which provides instructions to the employees on proper handling of company’s or personnel information and user data.
3. Audits must be conducted in order to ensure that the employees of the organization are following the policies and procedures.
4. 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 in cinerators [6].
5. Employees or individuals should be trained to question the credentials of the person who is calling himself to be in authoritive position in that organization.
6. 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. As we saw recently, some (poor) security systems can be bypassed with just the info found on a pizza delivery receipt.

You can protect yourself from phishers [7,10], 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.

1. **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.

2. **USE TWO-FACTOR AUTHENTICATION**:

This makes it harder for thieves to get into your account, even if your username and password are compromised.

3. **GET CREATIVE WITH SECURITY QUESTIONS**:

The additional security questions websites ask you to fill in are supposed to be another line of defense, but often these questions are easily guessed or discoverable (e.g., where you were born). You can shift the letters into uppercase and lowercase and use numbers also to create a leet word to make sure only you know those security answers.

4. **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.

5. **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.

6. **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:

1. 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.
2. 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.
3. 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.

4. 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.
5. 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]n. To be effective a policy should be:

1. 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.
2. 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 ro turn people off to the standard.
3. 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.
4. 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.
5. 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 advise.

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 6 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 behaviours as:

1. Refusal to give contact information
2. Rushing the process
3. Name-dropping
4. Intimidation
5. Small mistakes
6. Requesting forbidden information or accesses

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 form 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. Social engineering techniques can be physical or psychological. Physical techniques do not require any type of persuasive power or good communication skills. These basically include checking out dumps and trashes in organizations. Psychological techniques include persuasion and impersonation. That is to imitate as someone in authority. These techniques require a lot of confidence and very good communication skills.

To protect the S.E, 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. http://en.wikipedia.org/wiki/Social_engineering_%28security%29
2. BBC, “Social sites eclipse e-mail use,” 2009. [Online] available from http://news.bbc.co.uk/1/hi/technology/7932515.stm, last Accessed 4th April 2009
3. AlgarniAbdullah, XuYue, Chan Taizan“Social Engineering in Social Networking Sites:The Art of Impersonation” Science and Engineering Faculty Queensland University of Technology Brisbane,IEEE International Conference on Services Computing,2014
4. AnubhavChitrey, 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. J. Widom, “Data Management for XML: Research Directions,” IEEE, IEEE Data Engineering Bulletin,Special Issue on XML, vol. 22, no. 3, 1999, pp. 44-52
9. Mahmoud Khonji, Youssef Iraqi, Andrew Jones, Phishing Detection: A Literature Survey, IEEE Communications Surveys & Tutorials, **2013**, 15(4), 2091-2121.
10. 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**.