THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Social Engineering Attacks and Prevention: A Mirror Review

AqibHafiz
School of Computer Science Engineering
Lovely Professional University
Phagwara,India
aqib.guleria@gmail.com

Ranbir Singh Batth
School of Computer Science Engineering
Lovely Professional University
Phagwara,India
Ranbir.21123@lpu.co.in

Jyoti
School of Computer Applications
Lovely Professional University
Phagwara,India
Dhanjujyoti1080@gmail.com

***Abstract*—** With the increase in the use of technology, the priority of every company and individual is rapidly shifting to data privacy and security. As it is well known in this area of digitalization that information is of high importance and so everyone's desire is for their information to be secure and out of reach to anyone except the authorized persons. Unfortunately, despite of every effort made by companies and individuals to keep their data secure, data can never be 100% secure as there will always be vulnerability. However, been as it is that there is no 100% security when it comes to data, it doesn't mean that we can't level up the security of our data, so in the paper we will be looking at one very important and easily exploited vulnerability the 'Human been', the kind of attack we are looking at is called Social Engineering which is defined as exploiting human flaws for malicious purposes. With the increase in system security attackers are finding it easier to exploit people than computer systems which makes people the greatest vulnerably of information.

I. INTRODUCTION

Unauthorized access and or alteration of data in an organization is due to some vulnerabilities present in the organization. However, not all vulnerabilities are in the technical department. People like computers are vulnerable to exploitation, which makes them a vulnerability to information, as they can be used to extract confidential information. As the technical world is evolving so are the security precautions and measures in terms of information security and privacy, making it even more difficult for unauthorized users to access the information. With been the case a Social Engineering came into picture. In cyber-security, social engineering refers to the manipulation of individuals order to induce them to carry out specific tasks or to give away information that can be of use by an attacker. Social engineering doesn't require much of technical knowledge in order to be successful. Instead, social engineering takes advantage of the common aspects of human psychology such as curiosity, courtesy, gullibility, empathy, greed, etc.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

II. DIFFERENT TYPES OF SOCIAL ENGINEERING CATEGORIES

Social engineering can be categorized in two possible ways.

1. HUNTING:

Hunting as it sounds means to hunt your target without creating a relationship with him. It is done by having minimal interaction with the target. Once the objectives which were meant to be achieved are completed the communication with the target is terminated, this is the most likely approach of doing a cyber attack which only involves a single encounter.

2. FARMING:

Social engineering farming is not the traditional way of using social engineering attacks, but sometimes it is used. In this, the target looks to establish a long term relationship with the victim in order to get the information out from him for a longer duration of time. This information can later be used to bribe and to blackmail the target which resorts to traditional criminal behavior.

III. DIFFERENT TYPE OF SOCIAL ENGINEERING ATTACKS

1. Eavesdropping:

Eavesdropping can be explained with an example easily like within a company someone simply discusses some classified information loudly and the attacker simply being present at the right place at a right time uses this classified information to breach the security. It is the most common example but there are other ways to eavesdrop a conversation like pro-actively listening to emails and telephonic communication.

2. Tailgating:

Tailgating can be explained as following a person who has access to the restricted area through some secure access point. The attacker can simply follow the person closely and can enter the door before it closes.

3. Impersonating:

As the name defines in this the attacker assumes a false name and identity to carry out malicious activities like impersonating as an authority figure or a trustworthy person, The attacker attempts to exploit and gain access to important credentials and personal information.

4. Shoulder Surfing:

Shoulder surfing can be explained as when a person tries to collect information by looking from directly over someone's shoulder. It is typically used to extract the credential details or ATM pins

5. Dumpster Diving:

It can be explained as when the attacker tries to look for sensitive information through the garbage from their target. Because often organizations do not dispose of their documents thoroughly this makes it easier for attackers to retrieve confidential information.

6. Phishing:

Phishing is used to extract personal information using digital means, the attacker creates a fake phishing email which looks almost genuine, once the target opens the link present in the email it redirects the user to the fake counterfeit website and once the target enters its credentials the attacker gets those credentials. Phishing has certain another type also known as spear phishing. Spear-phishing can only be done if the attacker has done some initial research on the target on which this phishing attack is to be implemented.

7. Baiting:

In this the attacker may infect a storage device and leave it at a place where it can be found by the targeted party and once the targeted party ends up finding it and connecting it. It will automatically infect the target's system.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

8. Reverse Social Engineering:

It is a type of attack in which the attacker creates some sort of trust between him and the target. In this, the attacker creates a situation in which the target ends up needing his help for that purpose and he can get the credentials from the target which he can later use against him for his personal use.

9. Water holing:

It can be described as when the attacker compromises a website that is most likely to be visited by the target and then waits for the target to visit the website.

		Phishing	Shoulder Surfing	Dumpster Diving	Reverse Social Engineering	Waterholing	Advanced Persistent Threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant messenger	✓			✓			
	Telephone,VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Software	✓	✓	✓	✓			✓
	Human	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio technical	✓			✓	✓	✓	✓

Table1: Types of social engineering attacks

1. Phishing: Phishing can use various channels which are email, messages telephone, social network, cloud, and website, physical.
2. Shoulder surfing: Shoulder surfing only using physical channel for exploitation.
3. Dumpster Diving: Dumpster diving also uses Physical Channel for getting the information on a target.
4. Reverse Social Engineering: Reverse Social Engineering uses Emails, Instant messaging, Telephone, and Social- network, physical as a means to get to the target.
5. Water holing: Water holing uses the website as a means to attack the target.
6. Baiting: Baiting uses physical means to bait the target.

IV. TYPES IN WHICH SOCIAL ENGINEERING ATTEMPTS CAN BE CLASSIFIED

Social engineering attempts can be classified in such a way like

a. **Computer-Based Deception**: In which the target ends up believing that he is interacting

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

with an actual computer rather than a human being.

b. **Human-based deception**: In this, the attacker takes advantage of the nature of human beings in which every human wants to take the help of the person they like.

V. STAGES OF SOCIAL ENGINEERING

There are certain steps which are used by Attackers to get the information on the target so that they can perform social engineering attacks without raising any suspicion on them. A successful Social Engineering attack requires a Four-step sequence which includes, information gathering, establishing relationship and rapport, exploitation, and execution. However, depending on the nature of the attack and the target of this sequence or some of the steps in the sequence can be repeated multiple times.

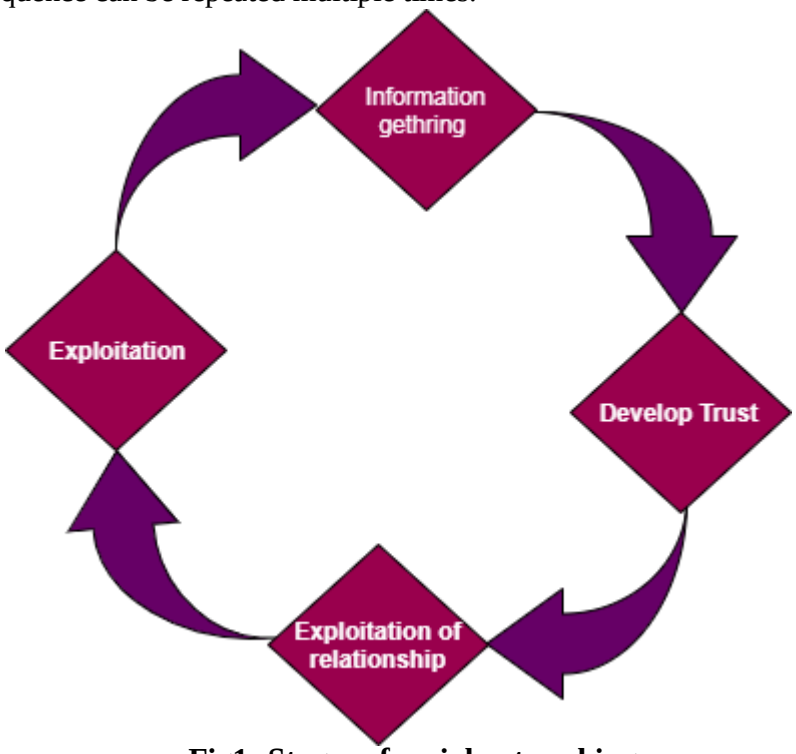

Fig1: Stages of social networking

1. Gathering information for social engineering:

From the near past, all big threats have generally taken place through social engineering attacks. People all around the globe end up using facebook, twitter where they generally post everything which is going in their life without thinking about the consequences which may later come to haunt them. Attackers use this information for their personal use they gather information like.

A. Personal information
B. Photos
C. Friends information
D. Location
E. Business information
F. Likes
G. Dislikes

All this information creates an ample amount of source of information for an attacker which they can use to get a clear picture of the individual and the things which he does. With all this information the attacker can use this data to create a perfect impersonation of the individual.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

2. **Develop Trust with The Target:**
Attacker can develop trust with the target like in the case of organization the attacker can present himself as the more senior member of the organization, we humans tend to easily trust someone if we think that person is trustworthy, we will never doubt that person until that person does something to break our trust . if someone tells us that they are that person we humans end up believing until we know that person personally .

3. **The exploitation of relationship:**
In this phase, the attacker tries to use the trust which he gained earlier without doing anything suspicious. he uses Psychological tricks to get the target in a certain state of mind where that person is most vulnerable and he does require some sort help from the attackers and by believing him he ends up giving the information asked by the attacker in the name of the trust in him which he can use for his own personal benefit.

4. **Exploitation:**
In this step, the attacker starts his exploitation without causing any kind of noise which will alert the target that he is under attack. After the exploitation is complete the attacker can choose to stay in contact for further exploitation or to end all sorts of bonds with the target.

Principal	Description	Example
Authority	Directed by someone imperonating authority figure or falesly citing their authority	"I 'm the CEO calling"
Intimidation	TO frighten and coerce by threat	"If you don't reset my password,I will call you supervisor."
Consensusl/social proof	Influenced by what others do	"I called last week and your colleague reset my password"
Scarcity	Something is in short supply	"I can't waste my time here"
Urgency	Immediate action is needed	"My meeting with the board starts in 5 minutes."
Familiarity/liking	Victim is well-known and well-received	"I remember reading a good evaluation on you."
Trust	Confidence	" you know who I am."

Table 2 Defines Social engineering effectiveness.

It tells about the effectiveness of a different type of attributes that are used by the attacker during the time of performing a social engineering attack like impersonating himself as someone of higher authority and etc.

The Fear Attack Vector:
It is most commonly used by the attackers during social engineering attacks. It means that attacking the target in such a way that he ends up giving information to the attacker by putting the target in the state of stress, anxiety, fear.

For Whom Social Engineering Attack Is Most suited For: Social engineers have a habit of studying people. Those who are completely committed to social engineering are better

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

actors rather being complete computer nerds. They have a great amount of knowledge on the body language of the person they habit of picking up even subtle details in a personal expression which a normal person cannot catch. They learn how to make someone believe in them. How to deal with people who have different personalities. They learn how to bluff so that they can gain the trust of a person. If a person can gain the trust of a group at will he is most suited for the task of the social engineer.

VI. PREVENTION OF SOCIAL ENGINEERING ATTACKS

There are various tools and techniques which are present so that social engineering attacks can be prevented or minimized. If we start to use these techniques it will make us less vulnerable. There are three ways with which we can prevent ourselves from being a victim of social engineering attack which are education, training, and awareness.

The most important way with which we can prevent ourselves from being a victim by knowing some common tricks which the attackers use to gain the information from us. We need to know the need of keeping our credential information a secret, we need to learn the fact to doubt others if we don't know about them we need to learn that we cannot trust anyone blindly, we need to know that before giving someone information about you we have to check whether the person who is asking for the information is genuine or not. Always remember that whenever you receive a telephonic call where they are asking about your information, you need to verify whether that call is really from your organization or not, If someone is asking for the details related to the password you should never give those details to them as in organizations no one ever asks for credential of a system over a phone call

1. You need to create a secure password for creating a secure password always use something complex so that even if someone tries to look at your credentials using shoulder surfing he should not be able to remember it because of its complexity. Always use different passwords for different credential details so that even if one of your accounts gets compromised you can minimize the loss.
2. By using two-factor authentication you can keep the thieves at bay even if they get your account id and password they will not be able to login to your account.

It is not possible to keep your data safe hundred percent as there is no software or hardware which will prevent and individual for falling into the trap of social Engineering attack. To prevent and to minimize the effect of social engineering good practices are needed to be followed.

If we talk about the organizational point of view it is necessary to educate your employees as they are the most valuable as well as the most vulnerable assets of the company. Employees must be taught all the policies, procedures and standards. It is necessary to understand what the policies say, it is necessary to implement whatever is written in the policies. Giving positive reinforcement to the employees is a good way to keep them in check, whenever an employee does something good, give them some sort of incentive so that they can do even better next time. If they end up finding something wrong going on tells them where to report it so that the problem can be solved before it is escalated. Ensure that the physical security for the building is effective there are no security gaps that an attacker can use for his advantage.

VII. CONCLUSION

In this research paper people see that over the years social engineering attacks have rapidly

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

increases and this as said in the report is due to the increase in system security leaving people to be the greatest vulnerability, apparently people are now more vulnerable to exploitation compared to computer, but this can change with enough education regarding social engineering attack, how it's performed and how it can be avoided. I believe that it is correct to conclude that social engineering attacks are successful because of ignorance on the victim's side.

REFERENCES

[1] Flack, Jessica C., and Raissa M. D'Souza. "The digital age and the future of social network science and engineering." Proceedings of the IEEE 102, no. 12 (2014): 1873-1877.

[2] Kumar, Anshul, Mansi Chaudhary, and Naresh Kumar. "Social engineering threats and awareness: a survey." European Journal of Advances in Engineering and Technology 2, no. 11 (2015): 15-19.

[3] Cazier, Joseph A., and Christopher M. Botelho. "Social Engineering's Threat to Public Privacy." In the 6th Security Conference, Las Vegas, Nevada: The Information Institute. 2007.

[4] Huang, Hsiu-Chuan, Zhi-Kai Zhang, Hao-Wen Cheng, and Shiuhpyng Winston Shieh. "Web application security: threats, countermeasures, and pitfalls." Computer 6 (2017): 81-85.

[5] Patel, Kushal, Brijesh Patel, Mihir Mishra, and Nilesh Patel. "Privacy issues in big data." In 2017 2nd International Conference for Convergence in Technology (I2CT), pp. 259-264. IEEE, 2017.

[6] Cullen, Andrea, and Lorna Armitage. "The social engineering attack spiral (SEAS)." In 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), pp. 1-6. IEEE, 2016.

[7] Atkins, Brandon, and Wilson Huang. "A study of social engineering in online frauds." Open Journal of Social Sciences 1, no. 03 (2013): 23.

[8] Ianelli, Nicholas, and Aaron Hackworth. "Botnets as a vehicle for online crime." CERT Coordination Center 1, no. 1 (2005): 28.

[9] Breda, F., H. Barbosa, and T. Morais. "Social engineering and cybersecurity." In Proceedings of the International Conference on Technology, Education and Development, Valencia, Spain, pp. 6-8. 2017.

[10] Ilangakoon, Sriendra Deshan, and JADC Anuradha Jayakody. "Awareness of Sri Lankan internet users on web browsing related threats and vulnerabilities." In 2016 IEEE International Conference on Information and Automation for Sustainability (ICIAfS), pp. 1-6. IEEE, 2016.