CHAPTER 15

Social Engineering

Introduction

Social Engineering attacks are increasing in our well-connected world. One of the main reasons for this is the availability of personal information on the Internet. For example, social media websites such as Facebook are used by attackers to collect information about people, which in turn can be used in their attacks, or can be used to initiate attacks. Hackers can uncover significant information about their targets—be they people or companies—by simply searching the Internet, or by searching social media sites such as Facebook or LinkedIn. Many of the images posted on social media, like family photos or photos of the company picnic, can reveal lots of information that is otherwise unavailable to the outside world. Using the information collected about the individuals, further information can be collected from their relatives and friends. The bits and pieces of the information collected from all such means can become substantial information about people and companies, which can be effectively used by attackers to initiate the attacks. Unlike in other attacks, the targets here are not primarily computers but human beings.

These social engineering attacks are based on the following premises:

- Human beings are helpful by nature and want to help out people in distress or in difficult situations
- Human beings by instinct trust others
- Human beings tend to obey the orders of their superiors or persons with authority in their organization
- Human beings by nature are afraid of consequences of not having followed the rules/orders of the company, particularly of losing their jobs

Social engineering attacks are initiated typically in two ways:

- By the attackers personally
- Through the use of computers[1]

Such attacks often may be initiated by attackers personally and once they are successful in collecting significant and sufficient information; further attacks may be initiated through computers. Both these types of attacks are part of social engineering attacks.

Such social engineering attacks may be targeted at:

- Individuals
- Organizations

In the case of attacks on individuals, the target of exploitation is their banking accounts or financial accounts and the intention is mostly monetary gain. Sometimes, it may be to initiate attacks on people, with some ulterior motives. In the case of attacks on companies, it may be to benefit their competitors, to take revenge, or to initiate distrust in such

companies by leading to their loss of reputation, and so on. The means used may be leaking of sensitive information, modifying the integrity of the information, leaking strategic and confidential information to the competitors, and so on.

The initial information collected can be used to initiate physical security attacks and / or network security attacks and / or host security attacks depending upon the information at the hands of the attackers. This depends upon the intentions of the attackers and the information available to them through social engineering to further initiate attacks. The auto dialing facility using computers, other such utilities, and so on, have made the use of telephonic lines one of the easier methods to be used to connect to people from anywhere anonymously.

Even after somebody is duped or conned to provide the information pertaining to himself / herself or others, the person so duped or conned may not even know that he/she has been duped and so the information collected may be misused. This is the modus operandi of social engineering attacks as authority, trust, or fear is used most of the time for ensuring the effectiveness of such attacks. Technical attacks can be understood and avoided using technical countermeasures. However, social engineering attacks have much less propensity to be dealt with through technical countermeasures. Policies, awareness, and trainings are the only major means of ensuring that the people are not easily duped or conned through social engineering attacks.

Social engineering attacks start mostly as passive foot printing activities and ultimately culminate in active social engineering / technical attacks. The risks of social engineering are high as you cannot monitor each employee in the organization and the transactions they carry out and you cannot analyze the logs of the activities carried out by each employee. It requires concerted efforts on the part of the organization to reduce these risks. Security Policies and awareness and trainings on information security on a regular basis are the main means of reducing the risk. However, this risk cannot be completely avoided.

The typical Social Engineering Attack Life Cycle is illustrated in Figure 15-1.

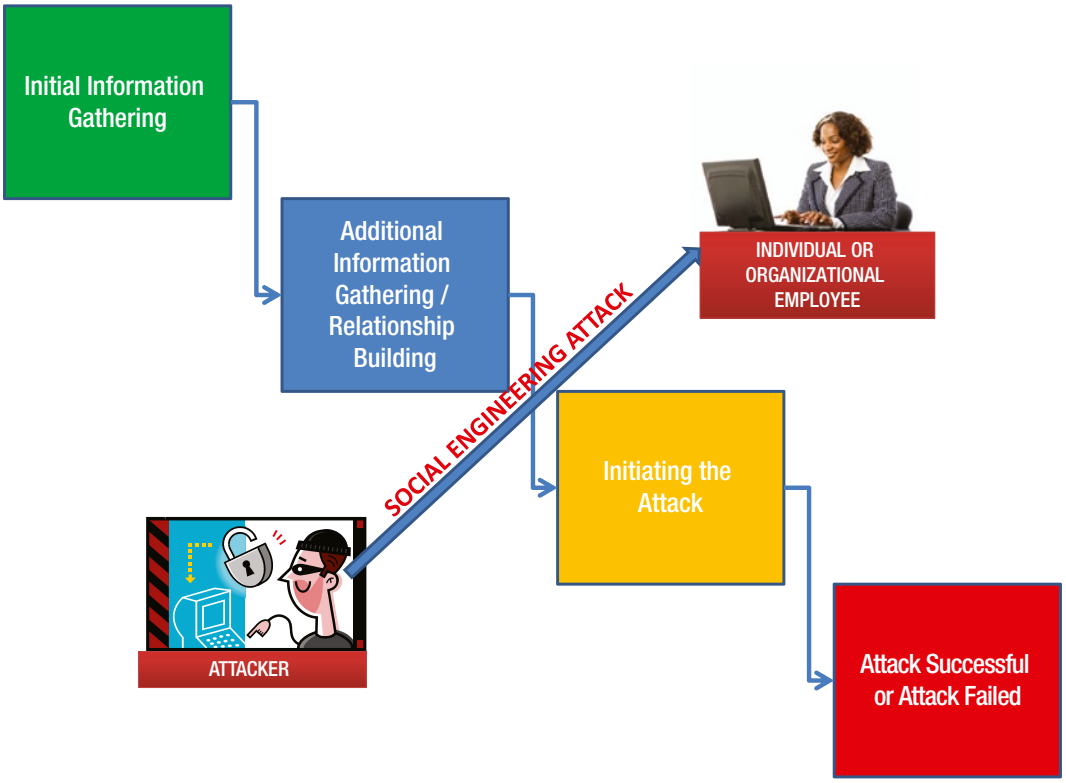

Figure 15-1. *Typical Social Engineering Attack Life Cycle*

Social Engineering Attacks: How They Exploit Human Nature

As discussed social engineering is an attack on / through human nature; attackers exploit this nature in several ways in order to collect the information, which subsequently may be used by them to initiate the attacks:

- Helping nature
- Trusting nature
- Obeying the authority
- Fear

The only thing the attacker needs to do is to imagine the scenarios through which he can exploit the above nature, such as those described in the following sections.

Helping Nature

Imagine you are working in the technical support function of your organization which is a big multi-national company. You get a call on your support desk number from an international number. The scenario goes something like the following:

Caller: Hi, I am Robin from Sales & Marketing department. I work for Tim.

You at technical help desk: Hi, I am Fred. How can I help you?

Caller: Thanks. I am working on a new proposal to acquire a multi-national prospect and millions of dollars are at stake. The prospective client had just now called me and wants some urgent information. I need to connect to the sales server to get the information. I am in Paris and I need to catch my flight in 30 minutes. I am required to send the information to the prospect before boarding my flight. But, my password is not working. Can you help me out by quickly resetting my password? Hurry up fast. Otherwise, I will be fired by Tim.

You at technical help desk: Ok. Ok. I understand. You are….

Caller: Robin, Robin Hogg from the Sales & Marketing. The fat man. Hurry up, please.

You at technical help desk: Ok. Now, your password is reset. It is RoSe123!! – Capital R for Rome, small o for orange, capital S for Sweet, small e for English, numerals 1 2 3 and exclamation mark two times. You need to reset the password upon first login.

Caller: Thanks a lot Fred. You saved my day. (Hangs up the call)

Precursor to the call: the attacker had understood through the social media account that Robin Hogg works in the Sales & Marketing department of the company. He also knows from the social media that Robin Hogg is known as "the fat man" within his company because of his huge body size. He had some other credible information about Robin Hogg from the social media if Fred had asked him. He also knows from the social media that his boss is Tim who is a very strict disciplinarian. The attacker had easily obtained the help desk number from the website of the company.

The following things worked in favor of the attacker:

- Fred had been chosen to work on the help desk as he was very helpful and was quick at solving other's problems.
- Fred did not go beyond verifying the basic details like name of the employee, boss's name in the database as there was an "urgency" in the attacker's voice as he did not have much time at his disposal.
- The additional details provided by the attacker like he works for Tim, that he will be fired by Tim, and that he is known as "the fat man," made Fred believe that the caller is a genuine employee. He had heard about some fat man in the Sales & Marketing department and he knew that Tim who headed the department was a strict disciplinarian.
- The fear that the new prospect and the millions of dollars of business may be lost also added to the fear and responsibility Fred felt not wanting to be responsible for losing the deal.

Even though other factors did help the attacker, in this case the primary factor that worked in his favor was the "helpful nature" of Fred which is also true with most of us as we want, by nature, to be helpful.

Trusting Nature

Imagine you are the receptionist at a medium-sized company and are at the desk. You get a call on your mobile number. The scenario goes on like the following:

Caller: Hi, I am Rose Mary, Secretary to the CEO.

You: Good Morning, Rose Mary. Jennie here. How can I help you?

Caller: Good Morning, Jennie. As you may be aware, my boss, Mr. Smith is at SFO today. He has forgotten his Standard Chartered Bank card CVV. It is written in my diary which is available on the side cabinet. You can get the key to the cabinet from Thomas or any of the security guards on duty. I am on vacation and the boss called me. I need to pass on this information urgently to him. I will hold for the information.

You: Ok. Sure. I will do it right now.

Jennie walks across to the security guard and informs him that Rose Mary had called her for some information and she needs to open Rose Mary's side cabinet. The security guard trusts Jennie, even though she has been the receptionist only for the past 6 months, as she is known for hard and sincere work. He hands over the key to Jennie.

Jennie opens the side cabinet, gets the CVV number and passes it on to the caller trusting that the caller is Rose Mary.

Precursor to the call: The attacker had met Rose Mary at her desk as a person representing one of the professional bodies of secretaries. She had interviewed Rose Mary on the best practices she follows to ensure that her boss is supported effectively. During this conversation, the attacker had understood that Rose Mary has a practice of noting all the important details about her boss including the credit card, debit card, and CVVs in a diary. Further, through the social media, the attacker also knew that Rose Mary is on a vacation.

The following things worked in favor of the attacker:

- Jennie trusted people easily
- Security guards trusted Jennie
- Jennie knew that Rose Mary was on vacation and that was confirmed by the caller who posed as Rose Mary
- The mention of the diary and the availability of the information therein, made the call more authentic

Even though other factors helped the attacker, the primary factor which worked in her favor in this scenario was the "trusting nature" of Jennie as well as that of the security guard. But, this normally would be applicable to most of us as most of us, by nature, trust others easily.

Obeying the Authority

By nature, human beings are obedient to their superiors and obey their orders without hesitation / much thinking. Imagine a situation where you are one of the trusted and loyal seniors in the finance and accounts department. You are well respected and the management people, including your boss, the CFO, rely on you for most of the information, including historical information / records of the company, or during the audits. Your boss was recently fired by the company and you had just started reporting to the COO. You also like to be respected, and get elated by this respect.

It is 10am in the morning. Your phone rings. The conversation goes as follows:

Caller: Hi David. Good morning. This is Parker, your COO.

You: Good Morning Mr. Parker. What can I do for you?

Caller: David, listen to me carefully. This is most important. There is an important external audit a customer wants us to undergo. Mr. King from Management Consultants X & X will be there at our office in another half an hour. You need to provide him with all the information and connect him to other departments as required. You are empowered by me to do this. I need not tell you, but ensure that the auditor is respected. Remember, he is representing one of our important customers.

You: No issues Sir. I will take care of it.

Caller: Ok. Thanks. I need to move on to another meeting. I will be busy in meetings throughout the day.

About one hour after the above call, a tall, smart gentleman in professional attire arrives at the reception and introduces himself as Mr. King from X & X and is warmly welcomed and led to Mr. David of the finance and accounts department. David warmly welcomes him. Mr. King mentions that he is acting on behalf of M/s. XYZ Inc., one of the large customers of the company and that he is provided with the charter to study the information security practices of the company. Mr. King praises the loyalty of David and mentions that the COO had high praise for David. David provides Mr. King with all the information required by him as well as connects him to the other departments as required by Mr. King. Mr. King has detailed discussions with the IT Manager and leaves by 6 pm. While leaving, Mr. King congratulates David again for being an asset to the company and appreciates his loyalty.

Precursor to the call: The attackers had collected the details of the board members and the executive management from the web-site which had more details about them than required. Most of them maintained a presence on social and other media, and it was easy to learn the COO's "voice." David, on social media, had highlighted his achievements at the company and the awards he had won. They had understood that he is working in the finance and accounts department. In discussion with some of the employees during some of the recent conferences, the attackers had corroborated on the fact that David at the finance and accounts section is well respected, is well recognized for loyalty and has been working there in the company for a long time and is also well known in Management circles of the company. The attackers also had details about the customers of the company and the services with which they are being provided from the website of the company. Another important fact was that the CFO was recently fired by the company and it was well published in all the newspapers.

The following factors worked in favor of the attackers:

- The authority with which the order was conveyed to David. There was no other option for David but to carry out the orders.
- Lots of details about the company and the customers available on the website of the company and social media
- The details posted by David about his achievements on the social media
- The fact that Mr. King appreciated David at the outset elated David and led to his cooperation
- Very familiar and reputed name of the Management consultancy organization
- The internal network created by David and the respect he earned because of his knowledge and loyalty helped him connect to the other departments easily

Even though other factors helped the attacker, the primary factor which worked in favor of the attackers in this scenario was the "nature of obeying the superior" of David. But, normally this will be applicable to most of us as most of us, by nature, are obedient to our superiors.

Fear

Fear of losing a job or fear of being reprimanded by the boss later on is one of the reasons to act on any requests, even though one may become suspicious of such requests. Sometimes, the employees may be blackmailed by the attackers using their personal knowledge about certain unwanted behavior or relationships of the employee outside the business. For example imagine the following scenario:

You are part of the purchasing department and handle important contract negotiations. You report to the CFO directly. You get a call at around 2 pm.

Caller: Good afternoon, Betsey. I am Stewart King, Senior Partner from AXYZ Consultants. We have been directed by your CFO to conduct a quick study of the current contracts in the pipeline and suggest strategies for better negotiations as the board has directed the CFO to cut some costs. Your CFO called us this morning from SFO where he is on vacation and instructed us to make this exercise a top priority this week. Please print out of all the current contracts under negotiation. Your CFO has instructed us to keep this work highly confidential.

You at Purchase department: Good afternoon, Mr. King. I understand your request for these details, but how can I send these details without authorization?

Caller: Betsey (voice is hardened, stern), I do not think you have any other options. Your CFO has ordered us today from SFO where he is on vacation. You can imagine the urgency. This work has to be completed this week and we do not have much time. He has specifically authorized us to collect the details from you. Consequences of not honoring his orders may be grave for you. You may be fired once he returns from vacation if you do not follow his instructions. And, you know very well that your boss does not like anybody who does not take their work seriously. Further, the board also may not take your disobedience lightly as this work is at their request. It is up to you. Anyhow, in an hour's time, our person will be at your reception. Please hurry up.

You at Purchase department: Ok, Mr. King. Your person can collect the printouts in an hour.

Precursor to the call: The vacation of the CFO is well published by him on social media. He is also posting the photos as he moves from one place to another. His tour program is also published on social media by him. Further, the details of the purchasing department contacts including Betsey is well known to all the vendors. The attackers have found the details about Betsey from one of the vendors of the company without raising any doubts.

The following factors worked in favor of the attackers:

- The fact that the CFO was on vacation
- The urgency of the work highlighted by the attacker
- The fear created by the attacker in Betsey
- Reputed name of the consultancy organization
- The weight in the voice of the caller as a senior person with lots of knowledge

Even though other factors helped the attacker, the primary factor which worked in favor of the attackers in this scenario was the "fear" incited by the attacker in Betsey. But, normally this will be applicable to most of us as most of us, by nature, are afraid of what can happen to us, particularly we dread the thought of losing our job.

Social Engineering: Attacks Caused by Human Beings

Most social engineering attacks are initiated and carried out by the attackers personally (i.e., without the use of computers).

Some of the attacks that are perpetrated by using human beings are:

- By impersonation as an employee or contractor or vendor – mostly pretending to be in distress, a difficult situation, or urgency – calling the technical help desk or calling any specific targeted department or person
- By exerting authority as a superior or a management person
- By exerting authority of a management person by invoking the authorization of such a person
- By posing as a very important person like a customer or a legal authority or an outsourced entity doing a critical job for the company

Let us look into some of the probable scenarios related to the above. In the earlier section 1.1, we looked at how an impersonation works. We have looked at impersonation as an employee and as a top management person. We also looked into the scenario where a third party calls as authorized by the top management person. We will look at some more relevant scenarios here in the following section.

You are working in the technical support department and you are manning the technical help desk and your phone rings (it is late in the evening and most of your staff are away from work).

Caller: Good evening. This is Michael, IT Manager from XYZ Ltd., which is, as you know, one of your privileged customers (commanding voice, hurry and anxiety evident in the voice).

You at technical help desk: Good evening, Michael. I am Rajan. How can I help you out?

Caller: (commanding voice, hurry and anxiety in the voice continues) We have a major information security incident at our end. We have a serious virus attack. This virus is known to use existing user ids and passwords. We need to reset all passwords. Please reset all the user credentials belonging to persons from our organization on your systems. This is urgent. Otherwise, there is a risk that virus may spread to your network too. As my official id is at risk, please change the passwords and send them to following personal id …

You at technical help desk: Ok, Michael. Thanks. We'll get right on this. However, before that I have to get permission from my IT Manager.

Caller: Rajan, listen (commanding voice, anxiety continues). No need to get additional permission. I have already informed your IT Manager, Mr. Johnson, and he is fine with it. We do not have much time to salvage the situation. Please do this immediately. You know we have provided huge business to your organization.

Precursor to the call: The attacker obtained the number of the technical help desk from the company website, and details about the client from publicly available brochures. Further details about the client company, including the name of the IT Manager, are obtained from the client company's website. Additional details about the IT Manager were obtained by the attacker from social media. The attacker had further details about the current ongoing projects from the website of the client company and also from some resources within the client company.

These characteristics worked in favor of the attacker:

- Commanding voice of the attacker
- Importance of the customer and the quantum of business they provide to this organization
- The possibility of virus spreading to this organization if not acted upon immediately
- Additional details known by the attacker like the IT Manager's name of this organization
- Main factor which acted in favor of the attacker was the importance of the customer and the quantum of business they provide to this organization

Consider another situation. You are the second in the finance and accounts department. Your department head is on leave and you are at your desk. A heavy weighed voice announces:

Caller: Good Morning, Mr. Alexis. I am John Madtha from Export Control Office of the Department of Commerce. Listen to me carefully. I am directed by the President to carry out a highly confidential urgent investigation, on some of the export irregularities on behalf of the federal government. The probe covers many companies. We know that your department head Mr. Joseph is not available, which is why we're calling you directly.

Alexis: Good Morning, Mr. Madtha what can I do for you?

Caller: (continues) The probe is not on your company but covers some of your customer companies. We will be faxing you an authorization letter from our department in the next 5 minutes. We want certain details regarding some of your customers. Keep in mind, it is highly confidential and nobody else should know about it. You need to fax me the details within the next hour.

Alexis: Ok, Sir.

Caller: Thanks, Alexis. But, remember. This is highly confidential and you need to keep this confidential.

Alexis: Ok, Mr. Madtha. I will. (call cut from the other side)

In next five minutes he gets an authorization letter from the Export Control of Department of Commerce (on the surface nobody can make out that it is fake). As an obedient citizen Alexis faxes the details required to the number provided on the fax received by him.

Precursor to the call: The attacker has studied the details of the customers of the company through their website. Some of those companies are big names and the company was providing them certain critical services as mentioned in the website of the company. The attacker knew through various accounting forums that Alexis is working there in the accounts department as second in command. The attacker had chatted with Alexis on one of those forums and understood that he was a law-abiding loyal citizen with a mild personality. Additionally, the attacker through one of the persons known to him from the company understood that the department head is on leave.

What worked in favor of the attacker:

- Attacker's commanding voice which sounded like that of the senior officers from the government
- Attacker reached Alexis's desk directly and addressed him as Alexis which confirmed the belief of Alexis that because the call is from law enforcing department they should know his name
- The department head who was handling the legal matters was on leave
- The letter of authorization faxed was a look alike of any government letter with all the appropriate formatting, symbols, and so on.
- Law-abiding nature of Alexis

But what worked the most was the law-abiding nature of Mr. Alexis in this specific context. This applies to most of us as we are all law-abiding citizens and consider it is a privilege to be of use to the government at any point of time.

Social Engineering: Attacks Caused by Computers or Other Automated Means

The other ways of perpetrating social engineering attacks are by using computers or automated means.[2]

One way of attacking is through fake websites, which are easily created. Websites which look like the legitimate sites also can be created very easily. One very popular type of social engineering attack is done by offering free downloads or very high discounts and encouraging them to use their official ids. The persons may be lured and provide substantial details in the process. Sometimes, the employees may reuse the same password as that of their official ids. The information collected will be used for further attacks.

Through Popup Windows: Interesting popup windows with irresistible offers can again lure the people to share substantial but unwanted details requested to be keyed in. These popup windows may announce that you have won a lottery or laptop or jackpot and may want you to provide details about yourself including sometimes your banking details so that the amount can be credited to your banking account or the gift can be sent to you.

Through E-mails: Again, interesting and irresistible offers can be made to you through e-mails. These e-mails may again request urgent intervention on a technical glitch as a user of e-mail, verification of credit card details, banking account details, and so on due to technical issues or resetting of credentials required on account of the upgrade of the systems of the bank to make them more secure for the customers, and so on. These e-mails provide the links to fake websites. Sometimes, these e-mails can have attachments which can download malicious software like keyloggers or screen capture tools or viruses, and so on which will make all the details keyed in by the users available to the attacker. Such e-mails also sometimes declare that the attachments or the links are to anti-spyware whereas they may be in fact installing spyware. Similarly, they may lure you with useful software while they may install actually useful software they may additionally install malware without your knowledge. Such e-mails can bring to you so called useful utilities, interesting games, and interesting reports and entice you to download them leading to malware infection of your system [Ref 5]. Such attacks are many times targeted at you knowing your specific interests.

Again the scenarios which can be created are only limited by the imagination of the attacker. Let's consider a hypothetical situation.

One recent—and highly publicized—attack on a retail giant during the holiday season resulted in the compromising of the details of millions of credit card accounts. Your bank name is also part of the list of the banks whose card details were leaked out. You get an e-mail message purported to be from your bank (with all the logo and style similar to that of the e-mails you normally get from your bank) that in order to ensure the security of your credit cards you need to reset your PINs. You click the link, provide your old PIN and then create a new PIN. You provide all the details sought in the process without observing whether they are required or not as you feel the urgency and necessity to be secure. When you complete the process you feel secure but actually your PIN is compromised and lots of details about you are in the hands of the attacker. You do not even know that you are attacked and the attack was successful.

Let's consider another scenario.

You get a job interview call from one of the African countries through an e-mail (it can come through other means like telephonic calls also). The position and the compensation offered sound very lucrative (it also sounds unreasonable – but because it has come to you, you do not believe so as you believe that you deserve such a position and compensation and feel happy somebody has noticed your talent). The link is provided to the company website. You go to the link, the company is a great company with excellent spread of branches and with great performance. You feel happy that you are privileged to be considered for the position. You anticipate the interview and prepare well. On the date and time mentioned, the interview is telephonically conducted. There may be some technical questions but the questions also remotely ascertain your or your parents' monetary status. You have done well in the interview.

Promptly after the interview, you get a communication that you have been selected and you get your offer letter. You are excited as you got an offer which is five times your current salary and there are also additional perquisites. But, they have also requested a good amount of money be remitted to them towards Resident Permit / VISA charges, and so on. But, it does not sound very big when compared to the potential salary! You do not waste time, you go to your bank and remit the amount promptly. The recruiter is in touch with you either through phone or through e-mail. They come back to you again and inform you that there are some issues with your Resident Permit / VISA and to clear the issues you need to remit some more amount to them expeditiously. The amount is specified in the message or communication from your recruiter. You are excited to join the company as early as possible (not a surprise if you already resigned from your current job) and hence expeditiously remit the amount.

Then these requests may be followed by similar requests citing one reason or the other but the amount requested to be remitted may be smaller than the earlier one but still substantial. You will continue to remit the amount till you feel something is "fishy". Now you start exploring. You do not find anything "fishy" in the website. You go through the offer letter, everything sounds fine. However, you may find, if you observe closely that either they have not provided any telephone number or address of the office in the offer letter or the number provided does not exist or is a wrong number. You go to the local police and file a complaint. They inform you that this may be fraud.

Now, if you had written to either your embassy at that country or that country's embassy at your country, you may have been fortunate to get a reply that "The Company does not have an office at the address and location specified in the letter." Again, such a reply will also caution you not to fall prey to fraudulent attacks. Now, you realize that your craze to get huge compensation has not only made you lose your current job, but also has made you spend a substantial amount without any return. Maybe you would have borrowed those funds from others. Now, your excitement turns into sorrow.

Some of the other scenarios are:

- You get an e-mail announcing that you have won a lottery or jackpot of a huge sum like Euro 2,500,000. This also has a request to send your details. Once this information is provided by you, you may get the request to send your bank account details. Along with this request you may also be requested to remit them a sum of for example: Euro 10,000. Compared to the amount you are going to get you feel the amount to be remitted is nothing. You pool all your savings or borrow from others and arrange for this amount and remit it to them. You may get further messages citing some trouble in processing and requesting additional money to clear the hurdle, and so on.

- You get an e-mail from somebody that she came to know of you through one of your common friends and that she has bequeathed a huge sum of money from her husband after his death and that she is ready to share that huge amount with you, but in return she wants a small favor. She wants you to send her an amount to fight the legal hurdle to repatriate the amount to your country. You believe her and remit the money. Subsequent requests will follow for additional money citing some more unanticipated hurdles which need to be cleared before being able to get the amount released. As you have already invested some amount you may remit the amount as requested the second time. But, as more and more requests for remittances pour in, you start getting doubts. When you enquire with friends, one of your friends informs you that these are all fraudulent messages.

Many more instances can be cited but, the variety of social engineering is only limited by the imagination of the attacker!

Social Engineering: Methods that are Used for Attacks

Different methods are used by the attackers when it comes to social engineering attacks. However, use of some of these methods depends upon the completion of collection of contextual data or building based on the currently collected contextual data. The initial attacks will be to collect useful data like bank account details including user id, password or bank account number, or collection of personal information like name, social security number, address, and date of birth. If the primary attacks to collect useful data do not fetch the expected details, using the details collected during the initial attacks, subsequent calls or attacks will be used to try to collect further data. Hence, the required data to initiate a strong attack may be collected in one or more attacks by the attackers.

The following methods are commonly used:

- Pretexting
- Phishing
- Spear Phishing
- Vishing
- Baiting
- Tailgating
- E-mail attachments

Pretexting

Pretexting originates from the word “pretext”. “Pretext” means “for some reason” and most of the times a reason which is not genuine. This involves the use of intelligently thought out well-crafted lies with the bad intention of collecting information about an individual or organization to initiate the attacks. These pretexting attacks build on information already available to the attacker, or through multiple, gradual attacks that continue until the intended objective is achieved.

Pretexting for privacy information or financial / banking information is prohibited by the acts of law in some of the countries of the world.

Phishing

Phishing is possibly the most heard of terminology particularly among those who use online means of dealing with the banking and financial related transactions. The bankers or financial institutions keep on cautioning their customers against the “phishing” activities. “Phishing” typically means “fishing," that is, “fishing” for useful personal information about the user which will be used by the attacker for identity theft.

Phishing attacks are usually carried out through links in the email attachments. E-mail seems to be from the legitimate bank or financial institution or electronic payment organization or similar organization but is not actually from the legitimate bank or financial institution or electronic payment organization. These attacks target primarily the obtaining of login credentials of the users like user ids and passwords, and so on or other personal information like social security number, banking account number, credit card / debit card details, and so on. Some of the reasons that are cited in such e-mails are:

- Crash of one of the servers or corruption of data which necessitates resetting of the passwords and allows for resetting the passwords (in the process capturing your current login credentials)
- Security reasons like suspicious transactions noticed in your account and the need to verify your current credentials (in the process capturing your current login credentials). These may be related to your bank accounts or credit or debit cards.
- Overcharge on the account which need to be reversed and to carry out the same they want the account details to be verified (in the process seeking such information which will lead to identify theft).

The logo of the bank or financial institution, style of the contents are typically copied from or are in close resemblance to that of the bank and therefore does not induce the thinking in the minds of the users that these may not be genuine. Further, the words like “to ensure security of your account” introduce the anxiety / urgency in the minds of the users to act on them. As such most of the users blindly believe such e-mails and act on them.

Even though banks and financial institutions keep on advising their customers not to fall prey to phishing attacks still many do not understand what phishing is and the implications of the phishing, and fall prey to such e-mails.

As more people have started using their mobile smartphones for carrying out their financial or banking transactions the risk of the phishing has also grown. People who use mobile devices without ever having used a computer may not be aware that computer security issues are equally applicable to mobile devices. Furthermore, sometimes these phishing messages seem to originate from trusted mobile apps. Because you trust these apps, your natural inclination is to assume these messages are genuine, and to divulge personal or banking credentials when prompted by them. This leads to further identity theft.

Most of these links take you to a URL that, again, looks like a legitimate website, and asks you to enter not only your user credentials, but also other personal data such as your social security number and mailing address, which is already on file with your financial institution. A genuine bank / financial institution never asks for the information it already has unless as a part of the telephonic verification to ensure that the person contacting them is the person who owns that particular account or credit card or debit card the details of which he is trying to obtain or on which he is transacting upon. Any website which asks for such details should be suspected.

Unfortunately to the disadvantage of the user, the user goes by the words mentioned in the mail like “if you do not respond operations on your account may be suspended.” Ideally, when any user gets a message which looks like a phishing message he has to promptly delete it or forward it to the concerned authorities in their countries. They should not act on the instructions in such mails or even click on the links in such mails. Still in case of doubt that it may be from the bank or financial institution or electronic payment organization, the person should directly contact them at the original contact numbers available with him or on their official websites and confirm that the concerned organization has not sought such details and it is likely most of the times it has not.

These phishing e-mails are normally spams which are sent to large numbers of users. The target list may also have the users who are not customers of the bank or financial institution who is spoofed. Normally most of them will ignore such e-mails. Some of the knowledgeable or information security aware users may ignore them even though they have accounts in such bank or financial institution. Some others who are not well aware of phishing or who are normally "anxious" or who become easily "weary" are the persons who will fall prey to such attacks. Attackers are fine even if they get the required information from some of the mailers sent as they can use such information to initiate further attacks.

Spear Phishing

Spear phishing differs slightly from phishing. The intention of the phishing attack remains the same. However, the phishing message is normally not from outside organizations, but from somebody with sufficient seniority and position, normally who is well respected and considered to be a reliable person in the organization. The attack is directed at a particular target organization. The spear phishing mails request the employees to update certain critical personal details or reset some critical user ids and passwords. Again, such mails are drafted very intelligently by the attackers. As the mail seems to be from the legitimate person many employees are likely to act upon the request and in the process lots of personal data which can lead to identity theft or banking or financial frauds are made available to the attacker.

Vishing

Vishing is short for "Voice Phishing." Here, normally the call is made to the number of the user instead of sending an e-mail with the link and a message is left to the user to call a particular number. These calls seem to be from the legitimate organizations like banks or financial institutions. These calls are normally initiated through automated means. When you call the number specified in the recorded message, you will be redirected to a voice response system and you are led to provide the information like in the case of the normal phishing attacks. These may be passwords and other personal information. The intention of the attacker is the same as that of the normal phishing attacks, such as identity theft and use of the information gathered for further attacks.

Baiting

Baiting is an attack where physical drives like CDs, DVDs, or USB drives are used instead of the emails. These drives are loaded with malicious software by the attacker. Intention of the attack is to maliciously infect the computers which use them and then the network, thus providing access to all the information on the computer and network to the attacker.

Normal scenarios of baiting works like this: usually a few copies of the CDs, DVDs, or USB drives infected with malicious software are placed by the attacker in such places as rest rooms or walkways or reception area or elevators or parking lots, and so on. These CDs, DVDs, or USB drives are labeled intelligently with interesting name / content tags. Such CDs, DVDs, or USB drives are then placed or dropped outside / nearer to the target company premises including many times at reception or waiting lounges. The employees who find them normally want to explore what is there inside the drives and when they insert them into their computers, without their even being aware of it, their systems are infected with malicious software which does the further part of the work required by the attacker like passing on the targeted information to the attacker. Even if these are found by a good employee and returned to the company IT staff, again when the IT staff inserts them into his / her computer or other authorized person takes possession and analyses the same by inserting into his computer, his computer is highly likely to get infected. As the malicious software is intentionally written by the attacker, it may not be even detected by the anti-virus software on the machine where it is used.

Tailgating

Tailgating is also sometimes known as "piggybacking." When this occurs, a legitimate user is followed by an attacker through authenticated gates like the ones where access is allowed by using access cards or fingerprints. Normally most of the employees do not want such an employee (because the person is entering they feel that he is also an employee – sometimes such attacker may wear a fake badge so that they are not doubted) closely following them struck by the doors and hold the doors open for them to come in. Sometimes such attackers may request other employees to allow them inside in the pretext that they have forgotten to bring their ID card or they have lost the card and requested a duplicate card and the other employee may open the door for them. Once within the organization such attackers can initiate attacks like inserting malicious software through USB drives on unlocked unattended computers (user may be away temporarily) or by shoulder surfing or by dumpster driving find out useful information like passwords, and so on. Again the courteous nature of human beings and the nature which does not like to see colleagues in distress help out the attackers, in good faith but with negligence.

E-mail Attachments

E-mails with interesting subjects always bring an urge in the employee to open them. Normally these have attachments with interesting names. The employee opens the attachments and malicious software is downloaded even without his knowledge. The attachment may also contain sometimes the matter of interest to the employee. However, it also does infect the user's system and in turn the network. Now, the user's system and other infected systems can be accessed easily by the attacker. Sometimes, the emails seem to have originated from government authorities and again carry serious subjects like mistake in the return filed by him which forces the employee to open the attachment and again his system is infected with malicious software. Some of these e-mails also may warn the employee that there is a virus attack and the solution is provided in the attachment, if he clicks and installs the solution his system will be trouble free and a virus will not attack it. Obviously to avoid any virus issues, he clicks and installs the so-called solution which is nothing but the malicious software.

Social Engineering: Other Important Attack Methods

In addition to the previous descriptions of attacks, there are also important attack methods that are often employed by the attackers:

- Find an employee in the target organization who hates his organization strongly: It is easy to find out through other employees remotely as to who in their organization always talks negatively and does not like the management. The reasons for that employee's hatred of the companies may be many, such as repeatedly denied promotion, continual recognition as low performer, sidelined by the management even though good at performance, intentionally one or more of the management persons ridicule his views, and so on. Such an employee when offered either some monetary benefits or alternative job may be ready to carry out any work you tell him particularly anything he has to do against his current company which he hates. He will be ready to carry out such attacks even though he knows that he is not doing something ethical or good but at that point in time the only thing that prevails upon him is that he has to take revenge against his company which has not taken care of his aspirations or has not looked after him well.
- Plant your person as an employee of the target company by getting him recruited by the target company and for a crucial position. Once he is within the target company get the credentials required for the attack through him and carry out the attacks or get him to carry out the attacks intelligently like malicious infection of the computers of one of the key employees, and so on. This person may instead identify a disgruntled employee and get the work carried out through such a person.

- The attacker may identify the weaknesses of some of the employees from the information collected through various sources like neighbors, and other employees and collect relevant information to blackmail such employees and use them to collect the information required by the attacker to initiate attacks.
- Look for the notebooks wherein the employees take notes as some people have the habit of writing their passwords in the first or last pages of their notebook. When the employee is not around and the notebooks used by the employee are around, the attacker may search into these notebooks or steal these notebooks and later check for the written passwords, if any.
- Once the attacker is inside the organization the attacker may use shoulder surfing to learn the password when the password is typed by the employee. There are even instances wherein a PIN entered by an ATM user is observed with the help of binoculars or telescopes and is copied.
- Once the attacker is inside the organization he may also check the dustbins for any written down passwords.
- Once inside the organization the attacker can listen to the conversations going on around gathering some of the confidential information or be able to read the files or messages from the systems switched on but unattended at that point of time.
- Today we are in the world of mobile smartphones and tablets. Some of the malicious apps may be sold through online stores with the same name or similar name to that of a popular mobile app. Users downloading and using them will get infected with malicious software which will perform the activities intended by the attacker.

Social Engineering: How to Reduce the Possibility of Falling Prey to Attacks

In a real and practical sense, it is very difficult and nearly impossible to eliminate social engineering completely as no software or hardware can stop these types of attacks. Further, human nature, particularly of every employee differs from that of the other and is very difficult to make out and devise countermeasures. However, that does not mean that we should not do something. Definitely organizations as well as the individuals should consciously work against social engineering attacks and try to avoid falling prey to them.

Some of the important measures that need to be taken by the organization in this regard are:

- Clearly define, document, and describe your organization's security policies. Make it clear in these policies what is expected from the employees, vendors and customers in the organization. Also, specify clearly what is not acceptable from the employees, vendors and customers in the organization. Circulate these policies among all the employees, vendors and customers (as applicable) so that they are aware of them.
- Include important do's and don'ts with respect to information security and the expectations from the vendors related to information security in the contracts / agreements with them and clearly mention the consequences of the breach of these. Also, again ensure that the vendors in turn, train their staff, who are involved in dealing with / working for your organization, about these information security related responsibilities.
- Include important do's and don'ts and adherence to the security policies as a mandatory aspect in the employee agreements with the organization (like employee appointment letter or Terms and Conditions of Employment) and make the employees sign such undertakings after consciously understanding the information security related responsibilities. Include in these also the responsibilities which will survive beyond the termination of their service.

- Carry out regular and detailed information security awareness trainings with clearly specified do's and don'ts related to information security with clear information as to what can go wrong if they do not follow the good practices of information security. They should also be informed of the consequences of the breach of information security by them and how it attracts disciplinary action. Such trainings are to be conducted first during the joining of the employee and then whenever key changes are made to the security policies or information technology infrastructure / tools as the risks undergo change. Also, periodical and regular refresher trainings need to be carried out at least at a minimum of once a year. Also, again when the employees leave the organization they should be apprised of the continuation of some of their information security responsibilities which survive beyond their termination. Such information security awareness trainings also should cover social engineering attacks and how to avoid them.
- Information security awareness trainings as described above have to be provided to the contract employees as well as vendor employees.
- Clearly defined information security event and incident reporting mechanism which is easy to use should be set up. All the information security events have to be regularly analyzed and if turned out to be incidents have to be analyzed further for the causes and appropriate corrective actions have to be drawn up. It is most necessary to ensure that drawn up corrective actions are actually executed too within the targeted timeframe. Corrective actions, if require employee training, the same has to be ensured across the organization.
- All access control / authorizations have to be periodically reviewed and revised on need-to-do and need-to-know basis. Authorizations have to be kept at the lowest level possible, but it has to be ensured that the work of the employees is not adversely impacted. Where such reviews throw up issues such as people granted temporary access to some of the folders or applications are still holding them, the access has to be removed immediately. Some of the authorizations earlier valid but are not required in view of the current role and responsibility of the employee have to be removed accordingly. The need for change of the authorizations during the promotions, and transfers have to be considered during such changes and authorizations have to be appropriately set. Earlier permissions if not required being continued have to be removed.
- All the highly confidential data has to be secured appropriately and authorizations should be strictly controlled. Access to such data has to be monitored. If possible, such confidential data is also segregated appropriately.
- All the data needs to be appropriately classified and labeled so that all are aware of the sensitivity and know whether there are restrictions on them being shared with others.
- All the employees should be sensitized to ensure that they do not divulge under any circumstances their passwords or PINs or such other credentials including the badges, smart cards etc. to anybody else even to a co-worker. All should use their own badges. They should be clearly made to know that their user ids and passwords are not required by technical help desk for any work.
- Background checks of all the employees including those of outsourced contractors have to be conducted. The background checks have to be assigned to an organization with repute and capability. Some of the organizations do not carry out the background checks of key resources like outsourced security guards, outsourced housekeeping personnel, outsourced IT resources, and so on. This can turn out to be a serious omission on the part of the organization.

- The systems should force employees to use only strong passwords. Weak passwords should not be accepted by the systems. The access to the systems should be barred after a specified number of failed login attempts.
- Areas within the organizations have to be additionally secured depending upon the sensitivity of the information handled. For example, data centers have to be additionally secured with the lock and key or additional layer of access control so that only few authorized persons are allowed inside.
- All the employees should be invariably issued badges and it should be made mandatory that they display the badges on their person invariably when they are within the organization. This enables somebody to differentiate an employee from an external visitor.
- Visitor Policy should be clear. Visitors should be always escorted by an employee when he / she is within the organization.
- All the unwanted papers have to be shred invariably. They should not be allowed to be dumped in the dust bins.
- Strict policies on clear screen and clear desk should be issued and employees should be made aware of the same.
- Employees should be trained as to how to ensure that the voice is kept low when they take confidential calls from their desks. Or, they should be advised to take such calls from closed rooms.
- Multi-factor authentication can be introduced for sensitive servers or network equipment so that password compromise does not lead to any issue.
- All permissions for additional access have to be reviewed thoroughly and should be considered only as per the Access Control Policy and based on the need for such information access to such an employee, vendor, or customer.
- Strong anti-virus software with strong anti-spyware / strong anti-malware capability should be installed by the organization. Organization should always ensure that the signatures are maintained up-to-date.
- Ensure that the organization follows all the employee exit procedures. Where an employee has administrative access to some of the applications or servers, such rights are revoked and the administrative passwords known to such employee are modified invariably. Also, all his access / authorizations are disabled.
- Employee registration / de-registration process is strictly followed to ensure that access systems do not allow any ex-employee to still authenticate and get into the organization.
- Carry out regular internal audits on the adherence to information security policies. All the issues found need to be fixed immediately.
- At least once a year carryout Penetration Testing on Social Engineering, understand the vulnerabilities and take appropriate corrective actions.

Some of the measures that individuals have to take to avoid becoming prey to social engineering attacks are:

- Do not publish any of your personal information
- Do not give your personal information over the phone unless you know for sure the other party to whom you are talking. Look at the need for the other party to know your personal information. Banks for example have all your information with them and may require little information to validate you if you have called them.

- Do not believe in any request for your personal information. When in doubt, notify the bank or financial institution named in the request via an official phone number gleaned from a verified legitimate source.
- Always create strong passwords. Never have same passwords for various systems. Ensure that you invariably change your passwords periodically.
- Do not write down your passwords anywhere.
- Ensure to cover up if you have to type your passwords / PIN in front of others. Ensure that your screen is clear or is locked when you have to discuss with strangers at your desk.
- Verify regularly your banking account statement or credit card statement to ensure that no unauthorized transactions are reflected thereon.
- Ensure that any personal information written down by you or unwanted copies of the applications with personal information are completely destroyed.

Chapter Summary

- We introduced social engineering and specified how social engineering attacks are carried out by taking disadvantage of the human nature like helping nature, trusting others, obeying the orders of the superiors, and fear of losing a job. We also talked about the social engineering attacks initiated personally and social engineering attacks initiated through computers. We also classified the attacks as attacks on the organizations and attacks on the individuals. We explored the risks of social engineering and mentioned that the risks of social engineering are high but are difficult to easily contain the same. We highlighted the importance of security policies, building awareness and conducting information security related trainings as most important aspects to reduce the extent of social engineering attacks.
- We offered different suitable scenarios as to how social engineering attacks exploit various aspects of human nature like helpfulness, trusting nature, superior's order obeying nature, and fear. In this section, we explored as to how these are exploited by other human beings (attackers) personally. For each of the scenario we also gave precursor information and analyzed as to how and why the attack was made possible.
- We discussed how social engineering attacks are carried out using computers. We looked into how through fake websites, through popup windows and through emails with links or attachments these attacks are carried out. Again we explored some of the relevant scenarios.
- We described various methods used in social engineering attacks like pretexting, phishing, spear phishing, vishing, baiting, tailgating, and e-mail attachments.
- We explored other social engineering attack possibilities such as attacks by planting an employee in the target organization (through recruitment process) or identifying a disgruntled employee from the target organization who hates the organization. We also looked at how such attacks can be carried out.
- We provided an approach and measures that organizations and individuals need to take to ensure that their propensity to fall prey to social engineering attacks is substantially reduced. We highlighted the necessity to have strong information security awareness training focus among others.