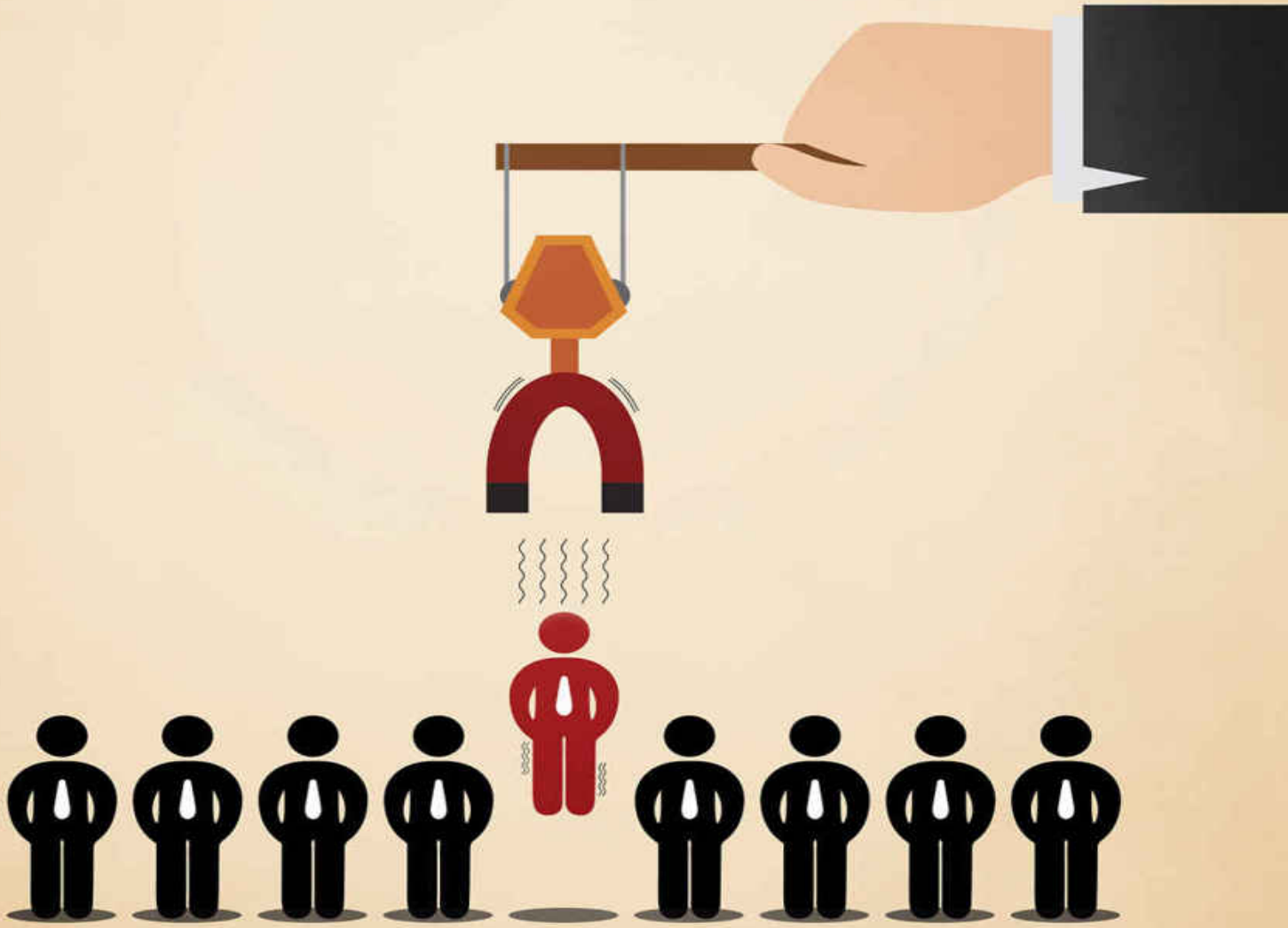
SOCIAL ENGINEERING

The Art Of Psychological Warfare, Human Hacking, Persuasion & Deception



VINCE REYNOLDS

Social Engineering

The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception

Table of Contents

and are the owned by the owners themselves, not affiliated with this document.

Introduction

Nowadays, a huge number of people have become too acquainted with hackers who exploit sensitive data and protected computer systems of various organizations, including banks, businesses, and even government agencies. More often than not, you will hear about hackers and become motivated to forestall their ploys. Most organizations counter the exploits of hackers through investments in new and up-to-date technologies to strengthen their defenses.

On the other hand, there is a new breed of attackers who use their expertise to go past the solutions and tools of organizations. This new breed of attackers is referred to as social engineers, who are likewise known as hackers; however, their primary objective is to tap into one's weakness, that is, human psychology. Social engineers make use of media such as phone calls as well as social media to trick people so that they can gain access to important and sensitive information.

Social engineering involves a wide range of malicious activities, which are executed in various ways such as pretexting, phishing, quid pro quo, baiting, and tailgating among others.

Pretexting is a form of social engineering in which attackers create a fabricated situation or good pretext, which they use to steal one's personal information. More often than not, attackers who use pretexting are mistaken as scammers who usually pretend that they need personal information for confirming their target's identity.

Attackers who have advanced skills in social engineering using pretexting try to persuade their targets to do certain actions in order to gain access to an organization and exploit its structural flaws. For instance, an attacker may take the form of an external IT services auditor to try and manipulate the physical security staff of an organization so that he/she can gain access to the building.

Social engineering attacks via pretexting depend on the creation of a delusive sense of trust with the target. The attacker is required to create a

credible story, leaving little or no room for doubt on his/her target; thus, the attacker can gain information that is both sensitive and non-sensitive. There was a case wherein a group of attackers took the form of modeling agency representatives and invented fabricated stories as well as interview questions. The attackers targeted women whom they manipulated to sending nude photos of themselves.

Phishing is considered as the most common type of social engineering, which attackers use today. Phishing scams have distinct characteristics such as obtaining personal information, including names, social security numbers, and addresses of targets; incorporating fear, a sense of urgency, and threats to manipulate targets to act fast; and using embed links or link shorteners to redirect targets to suspicious websites through URLs that may appear authorized or legit.

Although some phishing emails are crafted poorly, that is, the messages include grammatical errors and misspelled words, they can still direct targets to fake websites. Phishing emails are intended to steal the login credentials and other personal information of targets.

More often than not, attackers who use phishing emails pair malware with their phishing ploys in order to obtain users' information. For instance, a reported scam involved attackers who sent phishing emails to targets. The targets were prompted to install cracked APK files from Google Play Books. However, the files were already pre-loaded with malware.

Quid pro quo is another form of social engineering. It involves a promise from the attackers that the target will receive a benefit in exchange for a particular piece of information. The benefit that attackers promise their targets is in the form of services instead of goods.

More often than not, attackers who use quid pro quo ploys pose as fraudsters who act as people for IT services. The attackers usually make as many spam calls as possible to direct numbers from an organization and offer their targets IT assistance. They will then promise a quick fix of a certain IT issue while prompting their targets to disable their AV program. Once the targets agree, the fraudsters install malware that take the form of software updates on the computers of their targets.

There are also cases wherein attackers use less sophisticated ploys of quid pro quo. For instance, attackers know that many people, specifically office workers, would be willing to share their passwords in exchange for a bar of chocolate or even a cheap pen.

Another form of social engineering is baiting, which is similar to phishing and quid pro quo in many ways. Attackers who use baiting employ online schemes that entice their targets to surrender their login credentials to a suspicious website in exchange for a good or an item. More often than not, attackers offer their targets with free movie or music downloads.

However, baiting is not limited to online schemes. Attackers who use this type of social engineering can also exploit the human curiosity through physical media. There was a case in which a founder of an organization along with his team infected and dispersed a number of USBs with a Trojan virus around the parking lot of his organization. Most of the employees picked up and plugged the USBs into their gadgets such as computers, laptops, and tablets out of curiosity. Once they plugged the USBs, a keylogger was activated and the founder was able to access the login credentials of his employees.

Tailgating, also known as “piggybacking,” is a social engineering form that involves attackers who have no proper authentication in an organization. The attackers follow employees to obtain access in a restricted area.

A tailgating attack often involves attackers who pose as delivery drivers waiting at an organization's parking lot. When the attackers see an employee gaining the security's approval, the attackers who usually carry “goods for delivery” ask the employee to hold the door. Thus, they gain access from someone who is authorized to get into the building.

Social engineers often use tailgating in small organizations or companies given that most large companies require employees to swipe their identification cards. However, in the case of small to mid-sized companies, attackers can easily converse with employees to show the security a sense of familiarity, getting past the latter as well as the front desk.

A known security consultant used tailgating to access into several floors of a building, including one that housed the data room of a financial firm. The

consultant was able to access the building's third floor meeting room wherein he worked for a few days in order to obtain information.

Clearly, social engineering attacks are far-flung and considered as an enormous threat to various organizations. Social engineering can cost targets thousands, if not, millions of dollars annually as it attacks people with access or knowledge to an organization's sensitive information. Today, most attackers leverage various tactics and social networking schemes in order to obtain professional and personal information of their targets. The people who are most susceptible to social engineering attackers are the new employees, followed by contractors, human resources, executive assistants, IT personnel, and business leaders.

Unfortunately, some organizations do not have an awareness and prevention program to counter social engineering. In addition, there are organizations who do not have security policies or employee training that prevent tactics of social engineering.

This book offers valuable information about social engineering. In the first chapter, you will learn what social engineering is and what social engineers want as well as the different ploys that attackers use. The second chapter of this book offers pertinent information on the basic psychological tactics that attackers use to implement their social engineering schemes.

Chapter 1: What is Social Engineering?

Social engineering is a method of gaining access to systems, data, or buildings through the exploitation of the human psychology. Instead of using technical techniques or breaking in, social engineering involves non-technical schemes that attackers employ. For instance, an attacker may call a target or an employee and disguise as an IT support person instead of finding a software vulnerability in the target's company. The attacker will then trick the target into giving his/her password. The primary objective of social engineers is to gain the trust of as many targets as possible in a certain company.

In the '90s, Kevin Mitnick, a famous hacker, popularized the term “social engineering,” although the concept of tricking a person into divulging sensitive information has already been around for many years.

Types of Social Engineers

There are many forms of social engineering. It is either friendly or malicious and can build up and tear down a target. It is important to have knowledge on the different types of social engineers to determine how one can deal with them.

Hackers

Hackers are considered the most popular and prominent type of social engineers. Even if software vendors develop hardened and more difficult to break software systems, hackers are able to hit on them. Network and software attack variables, including hacking, are fast becoming a part of social engineering skills. More often than not, this type of social engineers use a combination of personal and hardware skills and use hacking in either minor or major breaches across the globe.

Penetration Testers

Skilled penetration testers or pentesters are quite similar to hackers as they use hacking skills to penetrate a company's or target's security system. Pentesters are those who have malicious black hat skills; however, they do not use the information they have obtained to harm a target or for personal interest.

Identity Thieves

Identity theft refers to the utilizing information of an individual's name, address, bank account numbers, social security number, and birth date without the knowledge of the owner. This is a crime that ranges from wearing a uniform to impersonating an individual to more complicated attacks. Identity thieves carry out a number of social engineering skills. Today, identity thieves have become more creative and unique in the ploys they carry out.

Spies

Spies are those who use the skills of social engineering as a substantial part of their lives. They usually employ the principles of social engineering in their ploys. Spies are considered science experts as they are taught various

methods of tricking or fooling their targets into believing something that they are not. Furthermore, spies from all over the world are taught and trained with the skills of social engineering so that they can build credibility and successfully inquire about their targets.

Disgruntled Employees

More often than not, members of organizations who become dissatisfied or disgruntled likewise become rebellious toward their employers. Furthermore, most employers are unable to determine the dissatisfaction of their employees as the latter naturally hides their concerns to protect their jobs. As such, the relationship between employers and employees is one-sided. Regrettably, employees who have become tremendously disgruntled with their employers or the organization find it easier to execute malicious acts such as theft, vandalism, security breach, and other offenses.

There are some signals that employers can use when it comes to discerning whether a member of their staff becomes disgruntled and inclined to carrying out social engineering ploys.

1. Disgruntled employees are well-informed and aware that those who frequently call in sick, file leave of absence a lot, and go home on a half-day among others are likely to be the usual suspects of wrongdoings in organizations. Hence, disgruntled employees are inclined to initiating extra work, task, or duty, working for long hours, or simply attempting to catch the attention of the higher-ups in the organization. This type of behavior is referred to as the protective behavior pattern.

2. If employees become upset over minor or major things that threaten to ruin their fraud or scam, they are indeed disgruntled and likely to lead into social engineering ploys. They may also say negative statements regarding the organization or management so that co-workers would sympathize with them once they are caught committing their misdeeds. For instance, disgruntled employees may say that the top management is corrupt, unfair, or unappreciative and try to encourage other employees. Once the disgruntled employees are caught, they would simply say that their

misdeed is nothing compared to the inequity of the top management towards its employees.

3. Disgruntled employees are likely to demonstrate the antisocial loner personality. While this personality may or may not be inherent, disgruntled employees tend to become loners as they think, plan, and execute their crimes. Again, these employees would often blame all their misdeeds to the organization or top management. This personality is developed when an employee constantly complains about the workplace, co-employees, or the top management. Eventually, this would lead them into thinking that they are alone, hence, becomes antisocial. They become impersonal and cold towards their colleagues.

4. *Disgruntled employees are likely to change their lifestyle inappropriately. They may have a sudden increase in their assets, travel a lot, purchase luxurious items, and even open offshore bank accounts, which do not add up to their actual salary. In this case, employers should take note of how these employees can afford such lifestyle. Furthermore, disgruntled employees who carry out social engineering ploys are primarily motivated by ego and money.*

Executive Recruiters

Recruiters are required to master the aspects and skills of social engineering. They need to become experts in the skill of elicitation along with the various psychological social engineering principles. As such, they are proficient in understanding and discerning what motivates their targets. More often than not, recruiters attack both the job poster and the job seeker.

Scam Artist

Scam artists, also known as con artists, take on greed as well as other principles that may attract their target's desires and beliefs to make money. Scam artists have the ability to discern the signals, which make their targets a good prey. They are adept in establishing situations that are irresistible and full of “opportunities” for their targets.

Governments

Governments are often overlooked as social engineers; yet, they are proficient in controlling the people they govern and the messages they convey. Most governments make use of authority, social proof, and scarcity to ensure that they are able to control their targets. On the other hand, this social engineering skill is not always considered negative given that some of the messages relayed are beneficial for the targets. In addition, governments make use of social engineering elements to make the message more convincing, appealing, and accepted.

Salespeople

Salespeople are similar to recruiters because they are also experts in a number of people skills. According to most sales gurus, an effective salesperson does not control people, but make use of their skills to determine the needs of their clients and find out if they would be able to fill those needs. The art of sales involves various social engineering skills, including elicitation, information gathering, psychological principles, and influence among others.

Psychologists, Doctors, and Lawyers

Most people might be surprised to know that people in these career fields belong to the types of social engineers. This group carries out similar techniques used by the other types of social engineers. For instance, this group uses elicitation, psychological principles, interrogation, and proper interview tactics to obtain as well as manipulate their clients or targets into the direction they want to lead.

Therefore, people can find an aspect of social engineering in various kinds of field, whether or not they may appear as well-educated professionals such as doctors and lawyers. This goes to show that social engineering is also a science, involving equations that exist to allow a person to apply social engineering skills that result in their objectives. One equation may be translated as: pretext + attachment to greed + manipulation = target victimized.

Goals of Social Engineers

The main goal of most social engineers is to possess a target's personal information, which can lead them to identity or financial theft or get them ready for a more intensive attack. More often than not, social engineers find ways to install malware into a company's system in order to gain access to computer accounts, personal data, and other sensitive information. In some cases, social engineers look for ways that translate to competitive advantage. Some of the most common items that are valuable to social engineers include passwords, keys, account numbers, access cards, identity badges, any personal information, details of computer systems, phone lists, information about non-public URLs, servers, intranet, servers, and names of targets with access privileges among others.

Social Engineering Ploys

Unfortunately, there is a great number of exploits associated with social engineering. Attackers may trick their targets into visiting a fake Web page, leaving a door open for them, downloading a document that includes malicious code, or even inserting a USB in the computer so that they could gain access to the targets' corporate network. Some of the typical ploys related to social engineering include:

Friending. This ploy involves a social engineer gaining the trust of their target and prompts to click on attachments or links, which contain malware. This malware usually includes a threat that is detrimental to a corporate system. Once the social engineer gains access to the corporate system and finds its weakness through the malware, they may begin to exploit. For instance, the social engineer may start an online conversation with targets and impel them to divulge useful and sensitive information.

Impersonal or Social Network Squatting. This ploy involves a social engineer tweeting their target and the target's friends or other contacts using the name of someone whom that target knows. The social engineer then asks the target for a favor, such as providing data from work or sending a spreadsheet. It is important to take note that social engineers can manipulate or spoof anything seen on a computer system.

Posing as an Insider. This ploy involves a social engineer posing as an IT help desk contractor or worker in order to obtain information such as passwords from targets. In a study for vulnerability assessments that involved employees from a certain company, 90% of the workforce trusted the accomplices who posed as co-employees. As such, the accomplices were able to obtain personal information and other sensitive information about the company.

Chapter 2: Social Engineering – Basic Psychological Tactics

Social engineering involves basic psychological tactics that attackers employ for gaining the trust of their targets as well as getting what they want. It is necessary that you know the social engineering underlying principles so that it could be easier to recognize when you are being targeted by an attacker.

A social engineer exudes control and confidence. Naturally, people who are into carrying out something misleading or deceptive act confidently and in control. For instance, a social engineer may try to pose as an individual from a service company or even forge a badge just to gain access in a secure building. The social engineer simply needs to act as if they belong there. Thus, as a social engineer conveys control and confidence, they are able to put others in the building at ease.

Take the case of the security people in concerts. The security people do not look for badges when they allow people to enter inside a venue. They look for unusual postures. For instance, security people can determine whether a fan is sneaking back to have a glimpse of the star. They also know the people who are working for the event.

A social engineer may also strike up a conversation in order to gain the upper hand. Consequently, when they are able to ask questions to the target, they are able to control the conversation. More often than not, social engineers start a conversation with a question, which can put the target immediately on the defense. Thus, the target feels a social pressure to provide an appropriate or correct response.

In the event that someone conveys control and confidence both offline and online, the key is not to become too comfortable. For instance, companies should advise employees to be keen when it comes to allowing outsides

enter the building. Guests and even service providers should be checked thoroughly for credentials regardless if their faces may be familiar.

A social engineer offer favors or free gifts. One of the human impulses that social engineers use is reciprocation. More often than not, when people are given gifts or favors, they feel the need to give in return whether or not they like the person giving something to them. A social engineer may offer to hold the door for an individual who belongs in a company or offer cookies to a receptionist to gain access to the building.

Most social engineers know that the time delay between offering a gift and asking for a favor is crucial. This is because the target might take the gift as a bribe when the social engineer immediately asks for a favor. The target is likely to act uncomfortably when they perceive the gift as a bribe. As such, a social engineer is inclined to giving a gift, say, to a guard or receptionist of a building in the morning and come back in the afternoon. The social engineer may claim a mix-up, such as pretending that there was a confusion with an item or than an item was left in one of the rooms of the building after a meeting. The guard or receptionist is likely to let the social engineer enter the building as an act of reciprocation for the latter's gift.

To prevent something like this from happening, employees should be skeptical, specifically when someone is trying to offer them a gift. In most cases, social engineers spend weeks in order to lay the foundation to establish a reciprocal relationship with their targets, leading them to access to secure or sensitive areas.

A social engineer makes use of humor. In general, people enjoy the company of other individuals with a good sense of humor. This fact does not escape the knowledge of most social engineers. They know that they can use humor to gain information, get out of trouble, or win over a gatekeeper. For instance, a social engineer may simply convey an upbeat impression to a security guard questioning them. Social engineers usually give their targets the impression that they are not worried with the questioning.

In addition, social engineers may try to strike up a conversation in order to obtain information from their target. For instance, a social engineer may pose as an IT person and fake a call, asking for the target's password. The social engineer may use humor during the call as the target is likely to volunteer sensitive information when the conversation is comfortable and fun.

A social engineer always states a reason. A recent study was conducted involving 2 groups of participants. The first group was waiting in line to use a library's copy machine. The second group was tasked to cut the line so they can use the machine first. The study found out that people are inclined to concede to individuals when they hear the work “because.” In the said study, the second group cut in line to use a copy machine saying the following: “Excuse me, may I use the copy machine because I have five pages and I am in a hurry?” This statement made 94% of the first group concede, allowing the individual to skip the line.

In another scenario, an individual in the second group used the line, “Excuse me, may I use the copy machine? I have five pages.” This statement made 60% of the first group concede. In the final scenario, the second group used the line, “Excuse me, may I use the copy machine because I have five pages and I need to have copies?” While the reason may be absurd, 93% of the first group allowed the line-cutter.

Consequently, the magic word in the study was “because.” Social engineers know this. As they try to blend with the people in a specific building and march around as if they own the place, other people would think that they truly belong there. In the same way, a social engineer who uses the word “because” is likely to convey to the target that they have a legitimate reason. Most people are likely to cooperate when they are given a perception of a reason, regardless if such reason is sensible or not.

Given that social engineers can work in any type of environment, people should take time to know what is going on around them and what is being said to them. More often than not, people who have a hectic day are likely to give up information right away just to end the day and rest. Social

engineers scout for targets who may seem stressed out as they know these people are likely to lose their awareness as well as presence of mind.

Elicitation

Elicitation refers to drawing or bringing out, or arriving at a truth or conclusion through logic. It is also referred to as a stimulation, which draws forth or calls up a specific class of behaviors.

In the context of social engineering, elicitation is used to draw targets out through a set of questions that stimulate them, leading them to the behavior that the social engineers want. In social engineering, the attackers fashion their words and questions as well as enhance their skill to a higher level. Social engineers who are adept in eliciting information can make their target want to answer every question or request that they ask for.

Most governments warn and educate their employees about elicitation given that this psychological variable is used by spies across the globe. For instance, the National Security Agency of the United States government has defined elicitation in its training materials as “the subtle extraction of information during an apparently normal and innocent conversation.” The conversations referred in this definition can transpire anywhere, such as in a daycare, a restaurant, the gym, or just about any place where the target is.

Given that elicitation is low risk and extremely difficult to detect, it works well with other aspects of social engineering. More often than not, targets never know where the information leak about them comes from. Regardless if there is suspicion, targets usually pass it off as just a question that they should or should not answer.

There are several reasons why elicitation works well with social engineering.

1. Most people want to be polite even to strangers.
2. When people are praised, they are likely to talk and divulge more information about themselves.
3. Professionals desire to exude intelligence and superiority in their fields.
4. Most people respond as pleasantly as possible to people who appear to have concern about them.
5. Most people do not lie just because they want to lie.

These are significant factors that social engineers consider in the targets they are dealing with. Social engineers know that these factors are usually inherent in every individual, making elicitation work well with their ploys. Thus, they are able to get people to talk about any information about them.

More often than not, social engineers employ light and simple conversation to get the most relevant information out of their targets. However, prior to doing so, they ensure that they are clear with their goals in order to obtain the optimal results from elicitation. On the other hand, social engineers do not utilize elicitation just for obtaining information. They use it to make their pretext more credible and gain access to the information they want.

The Goals of Elicitation

Based on the definition of elicitation presented above, social engineers are provided with a clear path of what their goals are. Social engineers want their target to act regardless if the action is as simple as replying to their questions or as elaborate as accessing a specific restricted area. In order to get their target to act in accordance to their intention, social engineers are inclined to asking several questions or simply keep a conversation, which would stimulate their target to the path that they are leading.

The key to effective elicitation is information. The more social engineers are able to gather information, the more successful their ploy would be. Given that elicitation is low risk, it does not pose a threat to targets. For instance, people have numerous conversations with others at coffee shops, stores, or elsewhere regardless if they are significant or meaningless. Thus, the entire concept of keeping a conversation is immersed in elicitation, utilizing it in an inauspicious manner. This is why keeping a conversation is significant in elicitation.

Irrespective of the method used, the goal of elicitation is to gain access to information and use it to stimulate targets to a path in which social engineers lead them. This is why people should be able to discern between a "normal" conversation and elicitation as it can be difficult to differentiate.

In addition, social engineers are masters when it comes to the art of conversation. They have become proficient in the three main steps of conversing with their targets.

The first step is being natural. Social engineers can create and keep a conversation by being natural in the way they speak and act while dealing with their targets. For instance, they are able to have a conversation with their target about something they are experts with. As such, they are able to stand comfortably and convey their knowledge without spilling out a hint of malice to their target. Social engineers exude naturalness and confidence. Not only have they mastered the way they speak, but also the nonverbal factors of a conversation.

The second step is education. Social engineers are equipped with knowledge about what they are talking about to their targets. They avoid

pretending more than they can be believed that they are. This means that if they want to obtain information, say, from a marketing company and their target is an advanced marketer, their elicitation approach should involve something about what interests the target. Social engineers research, practice, and prepare before choosing to converse with their target. They come in with adequate knowledge so that they can speak about a specific topic intelligently.

The third and final step is not being greedy. This step may be contradicting the motives of social engineers. However, the objective in creating and keeping a conversation is to obtain information, get answers, and be provided the key to the target's arena. As such, when conversing with their targets, social engineers avoid being greedy with information. Instead, they apply the concept of reciprocation, making the conversation a give and take process rather than a one-way street. They also allow their targets to dominate the conversation. Even if the conversation leads them to obtaining few information, social engineers are patient enough not to be greedy by going deeper and raising a red flag on the part of their targets.

These steps to a successful conversation are also keys to a successful elicitation. It can change the way social engineers converse with their targets.

Key Elements of a Successful Elicitation

Social engineers apply the principle of elicitation firstly by lacking the fear to communicate with their targets and being in circumstances that are not regarded as normal.

As part of training its agents, the United States Department of Homeland Security (DHS) has developed an internal pamphlet on elicitation. It is a brochure containing some significant pointers on how to identify the difference between a normal conversation and elicitation. It also contains measures on how their agents can avoid elicitation.

In one of the scenarios in the pamphlet, the attacker tells the target, “Your job must be important... that is why others think very highly of you.” The target then replies, “Thank you, buy my job is not that important. All I do

is...” This avoidance technique into a possible elicitation is simple yet effective although it generally appeals to the target's ego.

Social engineers tend to strike at their target's ego without overdoing it. They usually do it with utmost sincerity without stalking their targets. Social engineers do not say things that might lead to calling the security upon them.

Social engineers use ego appeals as subtly as possible. They instill flattery in their conversations without making their approach overly done or obvious.

In another scenario in the DHS pamphlet, the attacker says, “You have a background in compliance databases? You should see the model that I have created, which is designed for a reporting engine to assist with a certification. I can surely get you a copy of it.” Then, the target answers, “I'd love to see it. Our company has been indulging with the idea of an additional reporting engine to the system.”

This tactic of the attacker is expressing mutual interest, which is considered as an important elicitation aspect. This is a tactic that is more powerful and effective than appealing to the target's ego. This is because when there is mutual interest, the relationship is extended beyond the initial attempt to converse. In this scenario, the social engineer was able to make the target agree to further contact by acknowledging the offer of the attacker and expressing interest in the plans discussed for the company's system in the future. This alone can lead into a huge system breach.

In this scenario, the social engineer already has full control of the target. This means that the social engineer has control over the next steps as well as what, when, and how much information is released. Naturally, once the social engineer establishes a long-term engagement, they would be able to build rapport and trust with the target and make the latter feel a sense of obligation.

Another scenario in the DHS pamphlet presented the creation of a deliberate false statement. While this tactic may be inclined to backfiring, it is just as a powerful tool as any other social engineering tactic.

For instance, the attacker says, “Everyone is aware that ABC company yielded the highest selling software for this particular type of widget across the globe.” The target then replies, “That is not true, actually. Our company began selling the same product in 1996 and our sales records have not been beaten since then.”

The social engineer's statement is a form of elicitation wherein they can make the target respond with real facts. More often than not, people are likely to correct a wrong information or statement once they hear them. It is as if they are being challenged to prove otherwise. It is inherent in people to appear knowledgeable, inform others, and be unwilling to tolerate misstatements. Most social engineers know this and use it to bring out real facts from their targets.

The DHS pamphlet also has a scenario wherein the attacker volunteers information. Once a social engineer is able to offer information into a conversation with the target, the latter becomes compelled to provide an equally valuable data. People are likely to share similar views, information, or news. Social engineers use this fact to set the mood or tone of the conversation while instilling a sense of obligation to their target.

Another manipulation tool that is discussed in the DHS pamphlet is assumed knowledge. When people assume that someone is knowledgeable in a particular topic or situation, it is alright to discuss it with them. Social engineers are able to exploit this human trait deliberately by appearing to be knowledgeable in a topic, then using elicitation to establish a conversation. Social engineers are good in producing information, which is as if they own such information and continue to build around it to keep a conversation.

Elicitation and Intelligent Questions

The goal of social engineering with elicitation is to obtain small and apparently invaluable information and later build a clear picture of the answers they want to get from their targets. Asking intelligent questions to their target provides social engineers to have a clear path of their goals. There are various types of questions they use in order to obtain answers that lead them to a successful attack.

An open-ended question is a type of question, which is not answerable by a simple yes or no. For instance, “It's a little hot today, huh?” leads to a “Yes.” However, asking “What can you say about the weather today?” leads to a real response of more than a yes or a no.

Social engineers know when to use open-ended questions through studying and analyzing prominent reporters. Naturally, good reporters use open-ended questions so that they can continue to elicit responses from their interviewee.

In the context of social engineering, open-ended questions using “how” and “why” are more powerful. This is because it compels the target to expand on his or her response. Furthermore, open-ended questions also compel targets to reveal other details that social engineers may find valuable.

In some cases, asking open-ended questions lead to some resistance. As such, social engineers use the pyramid approach where they begin with narrow questions and follow them up with broader ones. This technique is evident when asking teenagers.

For instance, when a teenager is asked with open-ended questions such as “How's school?” it will be replied with just an “Okay” and no more than that. However, if asked with a narrow question such as “What type of Math are you doing this year?” it will be answered with “Algebra.” Then, the narrow question may already be followed up with broader questions to get the teenager to talk more.

Another type of intelligent questions that social engineers use is closed-ended question. While it may be the complete opposite of open-ended questions, it is likewise efficient in leading targets where the social engineer wants them to be.

More often than not, the goal of closed-ended questions is to obtained detailed information instead of leading the target to the social engineer's goal. For instance, in an open-ended question, the social engineer might ask, “What relationship do you have with your manager?” In a closed-ended question, on the other hand, the social engineer asks, “Is your relationship with your manager good?” This type of questioning is obtaining direct yet detailed responses from the target.

Leading questions are those that combine the concepts of open- and closed-ended questions. This is because leading questions are similar to open-ended questions but leads to a hint towards the answer. This is apparent in courtrooms when lawyers ask questions to whoever is on the witness stand. For instance, “On July 5th at around 6:30am, you were at the XYZ restaurant, weren't you, Mr. Phoenix?” In this line of questioning, the lawyer leads the witness to where they want to and at the same time provides the witness the opportunity to express their response. In addition, this type of question preloads the witness with the idea of how the lawyer acquired knowledge of the events.

A leading question is usually answered with a simple yes or no; however, it is equipped with more information, which makes the answer more informative as well. Social engineers use leading questions to state facts, making the target either agree or disagree.

Assumptive questions are also intelligent questions where social engineers already assume that the target possesses valuable information. Through asking assumptive question, the target responds in an affirmative or disconcerting way.

For instance, in a scenario where a law enforcement officer questions a target to know where Mr. X resides. The officer asks, “Where does Mr. X live?” The response will allow the officer to determine whether or not the target knows Mr. X.

In the context of social engineering, attackers utilize assumptive questions without giving the whole picture to the targets. This is because the target may control the environment and remove the ability of the social engineer to govern the situation.

More often than not, social engineers use assumptive questions when they have an idea of the facts, which they can utilize in the question. This means that social engineers inject as much real facts as possible to the assumptive question rather than including bogus information, which may turn off their target.

Pretexting

Pretexting is referred to as the act of making a manufactured scenario that causes a target to either do an action or divulge information. Pretexting goes beyond the concept of lying. There are situations wherein it can create an entire new identity and using such identity to control the information received. In the context of social engineering, pretexting may involve posing as people in a certain role or job, which the attackers never have done themselves.

On the other hand, pretexting is not as easy as it may seem even for social engineers. For instance, social engineers need to develop as many pretexts as they can over their career. While pretext may be different in one situation to another, their common factor is research. Time and again it has been mentioned in this book that having good information gathering methods can either make or break social engineer's ploy and even an excellent pretext. Take for example, a social engineer posing as a tech support representative. This act is futile if the social engineer does not utilize outside support.

As much as it is used in social engineering, there are other fields that make use of pretexting, including public speaking, sales, neurolinguistic programming (NLP) experts, so-called fortune tellers, therapists, doctors, and lawyers among others. All of them make use of pretexing in various forms. However, they also have to create a scenario in which clients or targets would be comfortable in divulging information that they would not normally share.

The only difference between social engineering and other fields that use pretexting is the intention or goal. This is to say that social engineers should live the persona until they achieve success in their ploys.

The quality of the pretext goes hand in hand with the quality of information social engineers are able to gather about their targets. This means that when a social engineer gathers more relevant and valuable information, the easier it would be to develop a pretext for a particular target.

Take for example a social engineer posing as a tech support person. The pretext of this type of impersonation would fail if the social engineer goes

to a company with either an internal or outsourced support. Social engineers find it as easy to employ their pretexts as one would converse naturally with a friend.

Principles of Pretexting

Just like any other skill, pretexing also involves principles that correspond to carrying out a task. Consequently, social engineers know these principles by heart, which is why they are exceptionally good at the skill.

The principles of pretexting substantiate the significance of pretexting. These include the following: the more research conducted, the better the chances of success; the involvement of personal interests increases success; practice of expressions or dialects; using the phone as a significant part of a social engineering ploy; the simpler pretexts are developed, the better the chances of success; pretexts should be spontaneous; and providing a follow through or logical conclusion for the target.

The more research conducted, the better the chances of success Although this principle may be self-explanatory, it is best to provide more details about it. Simply put, this principle associates the success level of a social engineering ploy to the depth and level of research that social engineers conduct. Information gathering is the most important factor to consider in a successful social engineering gig. This is to say that a social engineer holding more information about the target has better chances of success in developing an excellent pretext.

Social engineers refer to this principle in every action they take, specifically when developing pretexts. They are aware that even small details can make a difference in pretexting. In addition, they also know that any information gathered is relevant and useful.

There are ways that social engineers use when gathering information and as they do so, they also look for aspects, stories, and items associated with their targets. In some cases, they also look into the personal nature of their targets. Most social engineers use the emotional or personal attachments to allow them to get closer to their targets. For instance, finding out that every year, the CEO of a company donates a substantial amount of money to a cancer research center for children would allow the social engineer to inject a fund raising for such cause in his or her pretexts. It may seem heartless doing this, however, most social engineers would do anything just to achieve their goals. Furthermore, malicious social engineers make use of

pretexts, which are sustained by emotions without hesitation or second thoughts.

In 2011, after the terrorist attacks on the Twin Towers of the World Trade Center, numerous social engineers as well as malicious hackers used the losses of people for raising funds for themselves through emails and websites. These scammers targeted the computers of people and devised the accounts of legitimate fund raisers so that they can get the donations for themselves. Similarly, in 2010, after the earthquakes that occurred in Haiti and Chile, many scammers developed websites, which posed as providing information on the people who were lost, victims of the natural disaster, or the seismic activity. These websites were embedded with malicious code that enabled the social engineers to hack the computers of hundreds, if not, thousands of people.

Another common scenario in which social engineers take advantage of developing excellent pretexts is after the death of a music or movie star. Naturally, experts on marketing and search engine optimization (SEO) will set up the search engines pulling up stories about the star in just a few hours.

While these experts are doing their thing in their respective fields, social engineers take advantage of the increased attention given by people to search engines. Thus, they launch malicious websites, which feed upon a specific SEO. As people are drawn to these websites, the social engineers are able to gather information or infect the computers of people with viruses. Social engineers would then have better chances to research and gather information, making their chances of success in pretexting highly achievable. Sadly, there are people like malicious social engineers who take advantage of others' misfortune.

The involvement of personal interests increases success. Social engineers are likely to increase their chances of success in pretexting when they use their own personal interests. This may seem a simple tactic, but it can definitely convince targets that social engineers are credible. Trust and rapport are immediately ruined if a social engineer claims to be someone who is knowledgeable about a specific topic and then comes short of

information. For instance, if a social engineer posing as a tech support person has never seen a server room, yet continues to play the part can lead to ultimate failure. This is why most social engineers only include activities and topics in their pretexts that they are interested in. This provides them enough room to talk and display their intelligence and confidence to their targets. When social engineers exude with confidence, it is easier for them to convince their target that they are what they say.

In addition, there are certain pretexts that need more knowledge than others in order to be convincing; which is why research is a recurring thing for social engineers. When a pretext is uncomplicated, social engineers simply read a book or search on a few websites.

Regardless of how knowledge is obtained, social engineers usually research topics that they are personally interested in. Once they have chosen an interest, story, service, or aspect that they have adequate knowledge in, they determine if that angle is feasible.

When social engineers develop a pretext that lacks confidence, it creates dissonance, especially if the pretext necessitates that the social engineers should be automatically confident. Such dissonance results in red flags as well as impedes the establishment of trust and rapport between social engineers and their targets. Red flags and barriers can affect the behavior of a target who is anticipated to even out feelings of dissonance. These barriers also discard any possibility of the pretext to work.

In 1957, Dr. Leon Fe-stinger, a psychologist, instituted the theory of cognitive dissonance, stating that people are likely to look for consistency within their opinions, beliefs, and all cognition. When inconsistency is present between people's behaviors and attitudes, a change should be employed to eliminate the dissonance. According to Festinger, there are two factors that affects the intensity or level of dissonance. These are the number of dissonant beliefs and the importance of every belief.

Festinger stated that dissonance can be eliminated by adding more consonant beliefs, which prevail over dissonant beliefs; changing the dissonant beliefs to make them consistent; and reducing the importance of dissonant beliefs.

Skilled social engineers are able to change dissonant beliefs to make them consistent. This is one of their powerful yet tricky skills. For instance, a social engineer's appearance may not fit what the target has envisioned from the pretext; however, the social engineer can adjust with the beliefs of the target by his or her actions, attitudes, and knowledge of the pretext.

Practice of expressions or dialects. Most actors all over the world have dialect coaches who assist them in have the perfect target accent. Given that not all social engineers can afford dialect coaches, they simple learn from various publications that include valuable tips on the basics of putting an accent to their speech and expressions. These publications include native examples of the accent that social engineers want to learn. There are books that come with audiotapes in which social engineers listen to. They also speak along with audiotapes and practice sounding like the person speaking.

Once social engineers become confident in their accent, they record themselves to assess if they are convincing enough and correct any errors. More often than not, social engineers create a scenario with a partner so they can practice their new accent. They also try it on other people to check if their accent is believable.

Using the phone as a significant part of a social engineering ploy. Nowadays, the Internet dominates more social engineering aspects that are impersonal or objective. Back in the days, social engineers use the phone as an integral part of their ploys. Thus, the shift resulted in most social engineers to exert less effort or energy in using the phone. However, highly-skilled or advanced social engineers know that the phone remains as one of the most effective tools for their ploys and that using it should not be reduced due to the Internet's impersonal nature.

In some cases, social engineers who plan attacks using the phone may think differently as using the Internet is much easier to plan. Social engineering attacks that are phone-based are given the same level and depth of effort, information gathering, and research as with any other attacks. They are also of the same level of practice.

Social engineers usually practice and hone their phone-based skills by learning to deal with the “unknowns” or unexpected, specifically if they accidentally altered something in their script, throwing them of their base.

Social engineers, particularly those who work alone or do not have anybody to practice their phone-based skills with, are creative enough to ensure that they are able to hone such skills. For instance, they try to call their friends or family members to know how convincing they are and how far they would be able to trick them.

Social engineers who use the phone know that it is one of the quickest solutions to get close to their target. The phone gives them the opportunity to fake or “spoof” anything they want to tell their target.

Moreover, social engineers also spoof the information appearing in the target's caller ID. They use services or homegrown solutions to tell the target that they are calling from a local bank, a corporate headquarters, and even the White House. These types of services allow social engineers to spoof the number and make it appear that it is coming from anywhere all over the world.

Hence, the phone is a powerful social engineering tool that solidifies pretexting. Social engineers spend time in developing the habit of using the phone and treating it with respect as an efficient tool set for their pretext.

The simpler pretexts are developed, the better the chances of success. This is based on the principle, “the simpler, the better.” If a social engineer creates a pretext with too many details and forgets even one little detail, the social engineering act is likely to fail. In order to establish credibility, social engineers keep their facts, details, and story lines as simple as can be. In addition, it is highly impossible for social engineers to remember all the pretexts they created; as such, they keep pretexts simple, natural, and easy to remember.

Moreover, apart from remembering the facts, the details of a pretext should also be kept small. Social engineers know that keeping their pretexts simple paves the way for their story to grow as well as allow their target to fill the gaps using his/her imagination. Pretexts should not be elaborate.

More often than not, tiny details make the difference in the manner the target views the pretext.

Then again, there are some social engineers who deliberately make a few mistakes in their pretexts. Even famous con men and criminals purposely inject a few mistakes based on the premise that "nobody is perfect." In addition, most targets become more at ease when the person they are talking to makes even just little mistakes. It could be intimidating if social engineers are all too perfect for their target.

In social engineering, the types of mistakes that attackers decide to make are also calculated. While mistakes can complicate a pretext, they can also make it appear natural. The key of social engineers, whether or not they plan to inject mistakes, is to keep their pretexts simple.

Apart from creating a simple and uncomplicated storyline, social engineers back it up with appropriate tools and clothing, which can make the pretext more convincing. More often than not, the lack of detail makes a pretext workable and more believable.

For instance, a social engineer that makes use of the pretext of a tech support person is likely to wear a pair of khakis and polo shirt coupled with a small tool bag for fixing computers. In most cases, this actually works with the target, providing room for the social engineer to enter and move freely with minimal supervision.

Pretexts should be spontaneous. Creating a spontaneous pretext is comparable to using an outline over using a script. When a social engineer makes use of outlines, it provides him or her spontaneity and more freedom to edit as necessary. On the other hand, using a script makes a social engineer sound unnatural, even robotic.

Spontaneity in pretexts is also associated with using a storyline that the social engineer is personally interested in. Coming in to the target without knowledge about the pretext can compromise the credibility of the social engineer. For instance, if the target asks something or makes a statement, requiring the social engineer to think, the latter is likely to pause and start thinking deeply if he or she cannot reply with an intelligent answer.

Naturally, people think prior to speaking; however, social engineers know that it is not about being able to answer in just a second. It is having a reason or answer for not having the answer to the target's inquiry or statement.

Social engineers follow a certain guideline when it comes to the spontaneity of their pretexts. These include not thinking about how they feel; not taking themselves too seriously; discerning what is relevant; and seeking to gain experience.

When creating pretexts, social engineers are inclined to overthink and add emotion into their storyline. However, this can lead to anxiety, fear, or nervousness and ultimately, failure of the pretext. Some may not experience fear, but over-excitement. This likewise causes a social engineer to make numerous mistakes and again, lead to the failure of the pretext. As such, social engineers make sure that they do not think about how they feel while creating their pretexts.

Social engineers also avoid taking themselves too seriously. While their jobs are serious as it deals with security, social engineers are still able to laugh at their mistakes. This allows them to handle the bumps that may come in their way instead of feeling nervous or cramming up. This does not entail taking security as a laughing matter. However, social engineers know that if they become pressured or think of a potential failure as irreversible, the create fear within themselves. Thus, they know that minor failures are normal and that they have the capability to reverse them.

Social engineers also know how to discern what is relevant. For instance, social engineers usually plan ahead. If they miss out on one important detail, they have the ability to discern the relevant information or material around them. This may include the target's microexpressions, body language, or words spoken. Social engineers take in the information and employ it to their attack.

In addition, social engineers know that generally, people are able to identify if someone is not paying attention to what they are saying. Targets are often turned off if they feel that they are not being listened to. People like others who listen to even the insignificant statements they utter. As such, social engineers listen carefully and consistently to what their target is

saying. They pay attention while picking up relevant details that may help in the success of their attack.

Finally, social engineers always seek to gain experience through practice. This is because they know that practice can either make or break their pretext. As mentioned in the previous sections, social engineers who work alone practice their acts with friends and families. Some even try their tactics with strangers without causing any harm. Social engineers strike up conversations with other people to practice their spontaneity and improve as necessary until they become comfortable.

Providing a follow through or logical conclusion for the target. Although some may deny it, most people like it when they are told what to do. For instance, if a doctor walks in, checks over the patient, writes notes on his chart, and simply tells the patient, "See you in two weeks," it is unacceptable on the part of the patient. Naturally, the patient would want to know what is wrong and what he or she should do regardless if the prognosis is bad.

In the context of social engineering, the attackers do not merely leave their target alone. Social engineers either lead the target to take action or simply provide a conclusion. Regardless of the situation, social engineers give their target a follow-through so that he or she may fill the expected gaps or provide a conclusion for the target.

A great example would be the social engineer posing for a tech support person. If the social engineer simply walks out without saying a word to the target after exploiting the database, they social engineer leaves the target wondering what transpired. The target would possibly call another tech support company and ask what he or she needs to do. At any rate, social engineers do not simply walk away from their targets. Again, they either follow-through or provide a conclusion for their targets.

Influence and Persuasion

Apart from the four basic psychological tactics mentioned previously, there are other psychological techniques involved in social engineering. These include influence and persuasion.

Social engineering psychology, just like psychology in general, has a set of rules that produces a result when followed. It is both calculated and scientific. Persuasion and influence are psychological cognitive factors, which are backed up by science. While they are psychological results of perception, they also involve beliefs and emotions.

The art of influence and persuasion is a process of causing someone else to think, do, react, or believe in a manner that another individual wants them to. People use the art of influence and persuasion in their everyday dealings. Unfortunately, scammers, malicious attackers, and social engineers also use this art in their ploys.

More often than not, true influence is smooth and undetectable to individuals being influenced. When you are knowledgeable in the methods of influence, you will notice that billboards and commercials use the art. Probably the people who use the art of influence and persuasion most of the time come from groups of salespersons and marketing people. As you become aware of the art, you start to notice the terrible billboards and commercials while you drive along busy streets.

Prior to learning how social engineers utilize the art of influence and persuasion, it is proper to introduce you to some of the art's key elements as well as its five fundamentals that lead to obtaining success in influencing a target. The next section covers all pertinent information that you would need to understand how social engineers are able to use the art of influence and persuasion in their ploys.

Five Fundamentals of Influence and Persuasion

The five fundamentals that are significant in a successful ploy to influence a target include the following: set clear goals, build rapport, be observant of surroundings, be flexible, and get in touch with yourself.

The ultimate objective of social engineering is to be able to influence targets to carry out actions whether or not such actions would be in their best interest. Furthermore, social engineering not only influences targets to take action. The type of influence that social engineering uses is powerful that it makes targets "want" to take actions.

To understand how social engineering can have such powerful influence on their targets, go on to the next section.

Set Clear Goals. One of the most important aspects of the art of influence and persuasion is knowing what result you want to achieve out of your actions. In social engineering, attackers approach a target with a vivid knowledge of their goals as well as the indicators that they would achieve what they want. Once social engineers have set clear goals, they would be able to determine that path that they need to take to carry out their ploy. Having goals that are clearly defined could result in either the success or failure of the influence tactic. In addition, it can also make the next step easier to determine, master, and execute.

Build Rapport. In order to develop and establish rapport, you need to get the attention of the other individual you are targeting. In addition, you should be able to affect his unconscious mind. Social engineers have advanced skills in building rapport as it changes their entire methodology. They are aware that once they establish rapport with their targets, everything will flow smoothly with their dealings.

Be Observant. When it comes to being observant, it entails awareness of yourself as well as your sensory acuity or surroundings. When you are

observant, you have the ability to take note of the signs in the individual that you are targeting, which will indicate whether or not you are moving towards the right path. If you want to master the art of influence and persuasion, you need to be a master in observing and listening.

Social engineers avoid thinking about their next stage of their ploy when approaching the target. This is because they can miss out on what is truly going on between them and their target. Internal dialogues can stop potential conversations, which is why social engineers avoid them.

Be Flexible. One of the keys to a successful persuasion tactic is being flexible. In order to understand the concept of flexibility, think of it as being tasked to bend something like a steel rod or a branch of a sturdy tree. Many people would choose to bend the branch because it is easier to bend than the steel rod, making the task realizable. When it comes to persuading people, it is important to learn how to yield and be flexible.

Social engineers are flexible enough to adjust their objectives and tactics as necessary. While it may contradict the concept of planning, being flexible entails the ability to adapt when things are not going as planned. Inflexible social engineers may be viewed as insane and unreasonable individuals in the eyes of their targets; thus, they would not be able to achieve their goals.

Be in Touch with Yourself. In everything you do, your emotions take control. This is also true for all individuals you are dealing with. It is necessary to discern your emotions and be in touch with yourself so that you can determine the foundation for a successful influence and persuasion tactic.

For instance, if you have a smoking friend and you truly hate the smell of smoke, such hatred can affect your approach when trying to persuade her to quit the habit. Your hatred towards smoking can cause you to express, act, say, or do something that will stop your chance to persuade your friend. This is why it is important to be in touch with yourself and your emotions so as not to compromise your approach.

Social engineers are always in control of themselves and their emotions. This is because being in touch with themselves help them in establishing a clear path toward persuading their targets.

The five fundamentals of influence and persuasion are significant in understanding the art. The goal of persuasion is to establish an environment in which a target would want to perform what social engineers are requesting them to do. These five fundamentals are of enormous help in establishing such environment.

How Social Engineers Use the Fundamentals of Influence and Persuasion

In order to carry out their ploys successfully, social engineers should practice the art of influence and persuasion until it becomes habitual. They need not influence each and every individual they come in contact with; however, once they are able to turn the skill of persuasion on and off, it becomes a social engineer's powerful attribute.

There are various aspects of influence and persuasion that individuals could use, but eight techniques stand out as they are utilized frequently by politicians, media, government, scammers, con men, and social engineers.

Techniques of Influence and Persuasion

Reciprocation

The inherent expectation of people to be treated the way they treat others is referred to as reciprocity. For instance, if you open a door for someone, you expect him or her to say thank you while making sure you keep the door open as he or she comes in. It is important to know the rule of reciprocity given that returned favor is usually done unconsciously.

Social engineers are always looking for even small opportunities in which they will obtain valuable information. More often than not, they obtain information by making their target feel indebted to them. In addition, social engineers are extremely aware of what goes on around them as well as the little things that they can to make their targets act out of reciprocation. They act as natural as they can so that their targets would not sense anything unusual about them. Thus, reciprocity is a an effective tactic of influence and persuasion when carried out naturally.

Obligation

Obligation refers to a state of being wherein an individual is adhered to do something due to a sort of legal, social, or moral responsibility, contract, duty, or promise. In social engineering, obligation is much like reciprocation, only in a broader sense. For instance, simply holding an outer door for a target is a form of obligation in the context of social engineering. In turn, the target will be obligated to hold the inner door for the social engineer.

More often than not, social engineers use obligation as an attack factor, specifically when they are targeting individuals from customer service departments. They also use obligation for smart complimenting. For instance, a social engineer compliments the target and follows it up with a request for something. This is a technique, which can go wrong easily when the social engineer is inexperienced and misjudges the signals of the inner sense of the target. However, for advanced social engineers, obligation allows them to obtain event the tiniest bit of pertinent information as they carry out their ploys.

Concession

Concession refers to the act of yielding or conceding. It is similar to the act of admitting or acknowledging something. In the context of social engineering, concession is used to assist in touching a target's reciprocation instinct. In general, people may seem to have an inherent capacity that compels them to do something for others as others have done for them.

Social engineers use concession in their ploys based on the principle of “scratching the back of their targets as long as the latter scratches theirs.” Furthermore, social engineers follow some basic principles when applying concession to their attacks. These include labeling their concessions, demanding and defining reciprocity, making contingent concessions, and creating concessions in installment basis.

When it comes to labeling, social engineers make their targets aware of what and when they are conceding. This technique makes it harder for the

targets to dismiss the need to reciprocate. Social engineers usually use the statements “I will meet you halfway” or “I will give you this one” to show that they are conceding.

When it comes to demanding and defining reciprocity, social engineers start with a foundation of reciprocity in order to increase their chances of obtaining something in return from their targets. For instance, attackers may start through nonverbal communication with their targets to show their flexibility. While these may be little things, they can eventually lead to great results in terms of building a sense of reciprocation on the part of the targets.

When it comes to making contingent concessions, social engineers usually give in to something that their targets need or want without demanding something in return. Concessions such as this are “risk-free” and especially effective when social engineers need to let their targets know that they are ready to concede. It is a way to avoid making the targets feel that there is something the social engineers need from them.

Finally, when it comes to creating concessions in installment basis, social engineers give in a little during their first attempt and another over time so that their targets would continue to reciprocate. Given that reciprocity is inherent in people, they are usually obligated to give in when someone makes a concession, say, in a bargaining agreement or negotiation process.

It is important to know that social engineers as well as negotiators and salespeople use concessions almost instinctively. These people are able to use concessions by taking over the situation and resisting the manipulations that their targets place upon them.

Scarcity

In most cases, people find items and even opportunities more appealing if they are hard to obtain, rare, or scarce. People are likely to be attracted to messages in radio, television, and newspapers ads such as “3-Day Sale,” “Limited Time Only,” “Going Out of Business Forever,” and “Last Day.” Generally, these messages lure people to get a share of items, products, or opportunities, which may no longer be available. In the context of sales,

using scarcity is widely known with catch phrases such as “first 100 callers are entitled to a free widget” or “act now while supplies last.”

In the context of social engineering, scarcity is used to establish a sense of urgency when it comes to decision-making on the part of the target. Such urgency often allows social engineers to manipulate the decision-making as well as control the information they give to the target. Social engineers usually use a combination of the principles of scarcity and authority.

Take for example a social engineer posing as an IT technician targeting an assistant of a chief executive officer (CEO). The social engineer would claim that the CEO called him prior to leaving for the long weekend to fix an email problem. In addition, the social engineer tells the assistant that the CEO claimed of being sick and tired of the crashes and wanted the problem fixed by Monday. In this case, the social engineer creates a sense of urgency on the part of the target given that the CEO is unavailable. Furthermore, the scarce item is time given that the problem should be dealt before the CEO returns for work. Thus, scarcity establishes a desire, which leads a target to make a decision at once.

Authority

When people view someone as an authority, they tend to be more willing to abide by recommendations or directions given by that individual. For instance, children are instructed to obey their parents, teachers, nannies, and counselors among others because these people have authority over them. Furthermore, children are also taught that questioning or disobeying authority is disrespectful and that they will be rewarded for their obedience. These principles are carried over into adulthood. This is why people respect and avoid questioning orders and rules by authority figures.

Regrettably, this is the same principle that often leads many women and children into the hands of molesters and abusers. While the cause of molestation and abuse is not solely based on this principle, individuals who victimize children know that the latter are taught about authority. In the same way, social engineers make use of the principle of authority to carry out their ploys by manipulating their targets to take action, leading to a breach.

Commitment and Consistency

As much as people want to be consistent in their behavior, they also value the consistency of others. In general, people want congruency and consistency in words, deeds, and attitudes both of themselves and others. The need for reprocessing information and making complex decisions are reduced through having consistency.

Social engineers make use of consistency and commitment as powerful tools for carrying out their ploys. Once they establish a form of communication with their targets, they commit themselves entirely until they accomplish their goals. When social engineers sense that their targets are using gut feelings in making a decision, they work doubly hard using commitment and consistency. This is to discard any uncertainty that their targets might sense in them.

Liking

In general, when people like an individual, it is because that individual likes them, too. In the context of social engineering, liking is an extremely useful tool. One of the important attributes that social engineers should have is being likeable. In addition, as social engineers need to gain the trust of their targets, they appear to be interested in people in a genuine manner. For instance, in pretexting, social engineers become the individual that they are pretexting more than just playing out a belief or an idea. This makes it easier for them to be likable as their targets would conceive that they are genuinely interested in liking, assisting, or helping the targets.

Social Proof or Consensus

Social proof or consensus is referred to as a psychological state wherein people are ineffective in discerning the proper mode of behavior in social situations. When people are talking or acting in a certain way, it is safe to assume that their behavior is appropriate. Generally, social influence can result in conformity of large groups of people regardless if the choices are

correct or misguided. For instance, people who are in an unfamiliar situation, especially if they do not have a reference on how to act in the situation, tend to look for the behavior of others whom they know are already familiar and better informed of the situation. Furthermore, they mirror the behavior of those people with the assumption that it is the appropriate way to act.

In the context of social engineering, social proof is yet another powerful tool. Social engineers use social proof to provoke the compliance of their targets with a request through informing them that other individuals also took the same behavior or action. More often than not, social engineers refer to role models or prominent individuals in order to get their targets to do what they want.

Social engineers use social proof, especially when there is uncertainty and similarity in a specific situation. For instance, social engineers know when the targets are unsure due to an evasive situation because the targets tend to observe how others behave and assume such behavior as appropriate. Social engineers also know when the targets tend to mirror or follow the behavior of others in a specific situation. These conditions make it easier for social engineers to use social proof. They will appear to be more convincing when they tell their targets that many people before them have done the same action.

The influence tactics discussed above are just some of the powerful tools that social engineers use to carry out their ploys. These tactics provide social engineers the ability to stimulate and motivate people to act according to their objective. Thus, social engineers become in control of any situation.

In social engineering, the art of influence and persuasion is a process wherein social engineers get their targets into wanting to think, do, believe, and react in the manner they want them to.

Chapter 3: Social Engineering Tools

Apart from psychological principles, social engineering also uses a decent tool set that can make or break a social engineer's ability to achieve success in his or her ploy. Most productive social engineers have the adequate knowledge in use the tools, which closes in the break between failure and success.

It is important to take note that social engineers who merely possess the tools, even the best or most expensive ones, will not guarantee success in their ploys. The tools only allow social engineers to enhance their security practice, especially when they are executing their attacks.

Social engineering has three categories of tools, including physical tools, phone tools, and software-based tools.

Physical Tools

Physical security refers to measures, which people or companies utilize to keep them secure without the involvement of computers. It usually involves motion cameras, locks, and window sensors among others. In social engineering, it is important to understand how physical security works just as it is valuable for ordinary people to understand simply security mechanisms.

For instance, lock picking, as portrayed on television and in the movies is simply putting a lock pick in and the door opens instantly. Some people have knowledge in lock picking; however, most people learn how to do it slowly with countless attempts, frustration, and tension. A skill that is associated with lock picking is raking. It is using a raking tools and sliding it in and out of the lock gently with minimal pressure to the tension wrench. More often than not, lock picking coupled with raking works on most types of locks, making the breach as simple and effortless as possible. Social engineers learn the skills of lock picking and raking efficiently to conduct their ploys.

Today, a number of companies and organizations are using RFID, magnetic cards, and other types of electronic badges, making lock picks almost obsolete. For instance, in 2004, Wal-Mart has launched a pilot program by making use of radio frequency identification (RFID) technology in relation to its strategic plan of using inventory-tracking tags for its top suppliers. RFID is known as a type of automatic identification system, which enables data to be transmitted through a portable device referred to as a tag. The tag is read by an RFID reader and processed based on the needs of a particular application. The data transmitted by the tag may furnish identification or location information about the tagged product including date of purchase, color, and price among others. According to Wal-Mart, RFID will provide employees greater ability to locate products within a location and get them on shelves as customers need them. On the other hand, the use of RFID can also cause implications to its people, say, on their auditors. Certified public accountants and auditors will have to obtain the skills and knowledge to reassess accounting procedures, systems, and methods related to the use of RFID systems. In fact, they will have to be

skilled in assessing RFID system controls and note signs of inaccuracy or insufficiency of information such as partial inventory counts. Security of information may also be affected by the use of RFID systems. The illicit tracking of RFID tags has been a principal security concern of RFID technology. Tags pose risks to both personal location privacy and business security since they are world-readable. Thus, locks and lock picking are still used in many companies that do not have enough financial capability to install types of electronic access.

The problem in using locks is not due to the choice of locks, but the security plan that supports them. For instance, a company may have installed a heavy-duty lock that demands for biometrics as well as key access in order to enter the server room; however, the next door may have a single-paned glass window in which scammers, thieves, or social engineers can easily break and gain access with minimal effort.

Thus, locks alone are not enough security for companies and even homes regardless if the locks belong to the top of the line types. Social engineers know for a fact that security does not merely rely on a piece of hardware.

During a social engineering audit wherein a company patches its human infrastructure for more security, people are tested on their knowledge and skills about company security. However, the same principles are employed when social engineers carry out their ploys.

In general, people are unwilling to admit that they are inclined to being fooled or tricked by social engineers. In fact, most people would deny being fooled by a simple social engineering tactic due to fear of job repercussions as well as embarrassment. Recording devices can show proof that the trickery actually happened although they can also be used to train both employers and employees, specifically on what signals to watch out for.

Cameras and recording devices should never be used in getting employees to embarrassment or trouble. On the other hand, the information obtained from these devices provides valuable learning to show employees who fell for the pretexts and other scams of social engineers.

Most companies that use cameras and recording devices can obtain proof of a social engineer's successful hack. This can educate both employers and

employees on how they should deal with malicious attempts involved in social engineering.

Recording devices also provide companies the necessary protection against social engineering ploys, especially from advanced or highly-skilled social engineers. In camera recordings, for instance, the staff can see the facial gestures and other little details of social engineers. Thus, once the camera captures those details, the staff has something to analyze so as to be ready for a social engineering attack.

Phone Tools

The telephone is one of the oldest tools that social engineers use in carrying their ploys. With the advent of cell phones, homemade phone servers, and VoIP, social engineers are given a wide range of options to conduct their malicious schemes via the telephone.

Given that people are flooded with sales pitches, telemarketing calls, and sales advertisements, social engineers are compelled to be skillful when it comes to using the phone, leading to a successful ploy. As simple as it may seem, social engineers who use the phone as a tool can compromise a company's security in a matter of minutes.

Today, most people, if not all, are using cell phones and carry them both for personal and business conversations on subways, buses, and any other public places. In these places, social engineers are likely to eavesdrop or call their targets on their cell phones to obtain additional vectors, which may not be available during their previous malicious attempts.

As smart phones and hand-held phones that resemble computers are increasing in numbers, most people are inclined to storing personal data, passwords, and other private information in these devices. As such, social engineers are provided with yet another opportunity to carry out their ploys because they can have access to their targets as well as their data in various situations.

In addition, people have 24/7 access to their smart phones, which makes them more inclined to giving out information quickly when social engineers pose as “believable” callers. Take for example the caller Ids on cell phones, which indicates the identity of the person calling. When social engineers successfully access their targets through calling them from a corporate building, the targets are likely to give out information willingly without verifying the caller's identity. Certain applications in Android and iPhone smart phones are available for spoofing caller ID numbers to any number desired.

In the context of social engineering, the use of phones is categorized into two; the technology equipped on phones and the planning of the social engineers on what they would tell their targets.

Software-based Tools

One of the key aspects of social engineering is information gathering. Social engineers make it a point to spend time in gathering information about their objectives and targets to ensure success in their ploys. Today, there are various tools that can help social engineers in gathering, collecting, utilizing, and cataloging the data they have collected. This means that social engineers are no longer limited to what they can obtain from routine searches as online and software-based tools are already available.

Social Engineer Toolkit (SET)

While social engineers take most of their time in honing their skills, much of the variables for carrying out their ploys require the ability to generate PDFs and/or emails, which are embedded with malicious codes. Social engineers have developed the social engineer toolkit (SET), which provides them the ability to penetrate their targets easier and quicker through malicious codes.

Nowadays, SET is continuously expanding. In fact, recently, SET has proven its capability to handle attacks such as an infectious media generator in addition to spear phishing and website cloning. An infectious media generator allows a user to create a CD, DVD, or USB key, which is encoded with a malicious file. Then, the CD, DVD, or USB key is left or dropped at the office building of the target. Once it is inserted and ran in a computer, the generator will carry out its malicious payload, causing the computer of the target to be compromised.

SET also has the capability to produce a simple payload as well as a proper listener. For instance, if a social engineer wants to embed an EXE with a reversed shell connecting back to their servers, a USB key may be used to carry the payload and carry out their ploy. Once the social engineer finds a computer or any machine for remote access, they can insert the USB key and ran the payload file. This allows the social engineer a quick connection back to their servers.

SET creates the programming necessary for telling tiny boards what to do the moment they are plugged in. It also commands tiny boards to give reversed shells or set up listening ports.

As mentioned, SET also has a web interface feature in which a web server starts to host the SET automatically on a web page so the social engineer can use it easily. Thus, SET is an extremely powerful social engineering tool that allows attackers to test the weaknesses of targets, specifically in companies.

Password Profilers

Another tool set that social engineers use is password profilers. After obtaining information about their targets, social engineers create a profile of each of their target. This profile is used to plan out some attack strategies that social engineers deem fit for a specific target. A profile is also used to establish a list of potential passwords that social engineers can use in their ploys. Passwords can help social engineers in carrying out a hack, specifically when the situation presents such option.

There are several password profilers that are used in social engineering, which provide assistance in profiling potential passwords of a target or company. Some of these password profiling tools include Who's Your Daddy (WYD) and Common User Passwords Profiler (CUPP).

The number of people who fall prey to simple social engineering ploys is increasing every year in spite of various warnings issued by both private and government sectors. In addition, the number of individuals listing all types of information about themselves, their lives, and their families on the Internet is also rising.

Social engineers can profile and outline the entire life of their targets by simply using their tools and combining a profile established from social media usage. This works well on the part of social engineers given that most people choose their passwords. Fact is, most people use the same password for various Internet accounts such as emails and social networks. Worse, these people choose passwords that others can guess easily.

While social engineering tools are important to carry out malicious tactics, they do not guarantee the success of a social engineer. Tools are useless unless they are coupled with knowledge on their usage. Social engineers should also be able to maximize these tools in order to result in a successful ploy. As such, potential targets should also have knowledge about these tools as they are commonly used even by ordinary people.

Regardless of what tool social engineers use, whether it is a physical tool, phone tool, software tool, or a combination of tools, successful ploys are only possible if they have adequate knowledge of each tool. On the part of

targets, they should be doubly aware of the features of these tools so as not to become victims of social engineering.

Chapter 4: Pickup Lines of Social Engineers

As mentioned in the previous chapters of this book, some of the most common places for social engineering ploys include corporate offices, social networking sites, and just about anywhere on the Web. Social engineers are able to infiltrate corporate systems, hijack accounts, steal identities, and make money through employing different tactics, including the formulation of good pickup lines.

Pickup lines are used in social engineering to encourage communication between social engineers and their targets. Some of the most effective pickup lines used in social engineering will be discussed in the following section as well as how they work.

Pickup Lines on Social Networks

I'm here in New York traveling alone and I lost my wallet. Can you wire some money?

This pickup line works when a social engineer pretends to be a Facebook "friend" or a contact in other social networks. He or she sends a message to the target pretending to be in a foreign city and has no money due to lost wallet, robbery, or other unfortunate event. The social engineer then asks the target to wire money.

In this type of pickup line, people should be extra careful because most social engineers are able to hack accounts and pose as one of a target's contacts or friends. Thus, people cannot be guaranteed that the identities of those they are in contact with, specifically in social networks are genuine.

Check out this link!

This pickup line works when a social engineer sends a message or an email and encourages the target to click a link, which leads to a bogus site. The social engineer usually poses as a friend so that the target would likely read the message. Once the target clicks on the link, the bogus website, which may appear legitimate, asks the target for personal information such as account number or password.

For instance, there is a Twitter spam campaign that circulated. It has gone with a pickup line, "Have you seen this video of you?" A number of people with Twitter accounts fell for this line and led them to a fake Twitter website that required their passwords.

Someone has a secret infatuation on you! Find out who! Download this application.

This pickup line works, specifically in the numerous applications that users can download in Facebook and other social networking sites. This is because not all applications available in Facebook are safe. Social

engineers administer and control applications that install adware for launching pop-up ads. They also have applications in which personal information of targets are exposed to third parties.

Pickup Lines in the Office

This is Jack from technical services. I have been asked to check on your computer due to an infection.

This pickup line works when a social engineer poses as a technical support person, calling a target from a certain business or company. The social engineer tells the target that the computer is infected and offers to fix it. Then, the social engineer ratchets the technical difficulty intentionally as he or she plays on the fear and vulnerability of the target. As the target becomes more nervous, the social engineer takes advantage by letting the target reveal the password as "required" to finish the fix.

Hello, I am the rep from (name of company), and I am here to see (name of target).

This pickup line works when a social engineer poses as a client, service technician, or sales representative among others, making him/her a legitimate visitor. The social engineer will then use his/her knowledge about the company he/she is representing. Some social engineers even wear a shirt bearing the logo of the company. This tactic is effective in gaining the confidence or trust of the receptionist. Social engineers spend days, weeks, and even months to obtain adequate information about their targets. They take time in knowing who to ask for as well as how to dress and act when already inside the company.

Excuse me, can you hold the door for me? I left my access/key card in the car and I am late for a meeting.

This pickup line works when a social engineer waits outside the entryway of a company, usually the entry point of a smoking area or the front door. The social engineer then poses as one of the employees. More often than not, targets willingly hold the door open for social engineers in disguise. Thus, the attackers are able to access the building without being asked for their identities. Furthermore, social engineers get better when it comes to using high-end photography, specifically for printing genuine-looking

badges. As such, even when asked for credentials, social engineers simply present their self-made, fake badges.

Pickup Lines for Phishing

You recently won on eBay and you have not paid for the item yet. Please click here to pay.

This pickup line works when a social engineer sends a target an email that may seem to originate from prominent companies and organizations like eBay. The message tells the target that he or she won a bid and have not yet paid for the item. Social engineers know that targets who are into websites such as eBay give importance to their ratings and not being able to pay for a won item would result in a negative impact. As such, they are likely to click the link while the social engineer obtains the personal information of the target.

You have been let go. Click here for your severance pay.

This pickup line works when a social engineer takes advantage of increased digitization and economic uncertainty. The social engineer sends an email to the target containing a malicious link, which may appear as legitimate. The link may be supported by another pickup line such as “This year, we are sending out W-2 forms electronically. Click here.”

Targeted Social Engineering Attacks Using Pickup Lines

The tactics of social engineering is increasingly specific as attackers are inclined to targeting individual people for a larger payoff. There are more lucrative pickup lines that social engineers use to gain personal information of their targets and make more money.

Donate for the hurricane victims and recovery efforts!

This pickup line usually starts circulating shortly after a tsunami, major earthquake, or other disaster. Fake websites that social engineers manage target people who are deeply concerned about their loved ones in the disaster area. The website usually claims to have rescue efforts and other specialized resources to help in finding victims and their recovery. In order to solicit charitable donations, the website collects the names as well as contact information of those who are willing to donate. The social engineer then calls the victim who naturally has heightened emotions to obtain their account or credit card number. Thus, the social engineer would be equipped to commit identity theft with all the information obtained such as the target's name, address, account or credit card number, and a relative's name among others. Some social engineers even conduct a secondary attack by posing as a bank representative who requests for the Social Security number of the victim for the purpose of verifying the legitimacy of the donation.

This is Microsoft support; we want to help you.

This pickup line works when a social engineers poses as a Microsoft tech support individual. The social engineer claims to be notifying all licensed Windows users who are experiencing abnormal number of errors caused by a software bug. The target is instructed to access the event log, which is usually alarming for inexperienced users. More often than not, Windows event logs are able to record numerous yet small errors. The target is likely to do whatever is instructed of him by the social engineer, prompting to go

to a remote access service, such as Teamviewer.com. This service provides the social engineer control over the target's PC. Then, the social engineer installs malware, which will provide him/her continuous access to the target's PC.

@Twitterguy, what is your opinion about Obama's statement on #cybersecurity? Http://shar.es/HNGAt

This is one of the most common phishing lures used in social engineering. Attackers continuously observe the trends in Twitter in order to carry out their ploys. For instance, social engineers hijack legitimate hashtags to embed malicious links. Once the targets tweeted using the hashtags, the malware redirects them to a phishing site with the intent of launching more malware or stealing the targets' account information in Twitter. More often than not, social engineers look for targets in Twitter by learning about their interests. Then, the attackers send tweets that appear legitimate to entice targets to click the links that lead to phishing sites.

No new followers? Get more Twitter followers here!

This pickup line works when a social engineer sends a tweet, which promises targets an increase in their followers once they click a link. The link then leads the targets to a web service, which asks for their credentials in Twitter. For those who are knowledgeable, there is not legitimate third party that would request for Twitter credentials.

Subject: About your job application.

This pickup line works when a social engineer targets businesses and headhunters by embedding malware in their email responses to numerous job postings. Based on a warning released by the FBI, over $150,000 was stolen from a prominent business due to unauthorized wire transfer. The social engineer responds to a job posting on a specific employment website. Once the malware is installed, the social engineer obtains the target's credentials, specifically for online banking in order to carry out

financial transactions within the company. The social engineer redirects the wire transfers to his/her own accounts through making changes in the account settings. As this tactic became rampant, most companies and organizations use online forms for job seekers instead of accepting their cover letters and resumes in email attachments.

Chapter 5: Social Engineering Scams on Social Networks – Then and Now

Google and Its Chinese Hackers

In the beginning of 2010, Google made the headlines and revealed that Chinese hackers were able to breach a part of its system. Google claimed that some of its services were breached and that the perpetrators wanted to obtain access to Chinese human rights activists through their Gmail accounts. Apart from Google, these social engineers also targeted other prominent companies, including Symantec, Adobe Systems, and Yahoo.

The success of the social engineers was due to spending weeks and even months of scouting and targeting Google employees in order to obtain information. They began by using the information of employees found in social networks and other places. Once they got the necessary information, the social engineers sent messages to the employees that appeared legitimate and coming from a friend or contact. Thinking that the message truly came from their friends, the employees clicked on the links embedded with malware, resulting to the installation of spyware on their computers.

This attack on Google was planned and carried out for a considerable period. The social engineers took their time in gathering information and winning the confidence of the employees so that they could interact and elicit information.

Given that most companies make use of social networks as a part of the marketing strategy, social engineers find it easier to gather information about their targets. Apart from conveying their marketing tactics through social media, companies also expose their company structure, making the information needed by social engineers readily available.

Information Exposure on Wikileaks

Again, in 2010, highly classified government information was exposed on Wikileaks with the successful ploy of social engineers.

Bradley Manning, a U.S. Army soldier who was then assigned to a support battalion in Iraq, was accused of providing classified information to the founder of Wikileaks, Julian Assange.

Having access to the Secret Internet Protocol Router Network, which was used by the U.S. Department of State and Department of Defense for transmitting classified information, Manning was able to obtain the material.

Meanwhile, Adrian Lamo, a former hacker, reported Manning to the authorities, telling the officials that Manning downloaded the material from SIPRNet and saving it on CD-RWs. Manning was allegedly successful in fooling his colleagues that he was merely listening to music instead of accessing and downloading classified information.

Manning carried out his ploy by coming in with music on a CD-RW with a label, such as “Lady Gaga.” He erased the music, overwriting it with a compressed split file. Manning told Lamo in an online chat that nobody from his colleagues suspected anything as he listened and even lip-synched Lady Gaga's song, *Telephone*. While doing this, he “exfiltrated” probably the most magnanimous information spillage in the history of the United States.

Manning was able to play on the trust of his colleagues while keeping his cool. A social engineer like Manning is ruthless as he knew his action may result in a court martial, yet still pushed through with it.

Following the exposure of highly classified information on Wikileaks, other social engineers took advantage and sent out messages with a pickup line, “Do you want to read the file on Wikileaks? Click here.” Once users clicked on the link, it led them to a pdf file that allowed the social engineers to search the computer through a Javascript, determine the Adobe reader version on the computer, and launched their exploitation for such version. The victims did not mind if the pdf took time to load as they were expecting

a huge document. However, they also did not know that it was not the document that took time to load, but the malware, which the social engineers embedded.

Facebook Friend Request

The ploys used in social engineering are continuously evolving as various tools for obtaining information are made available. These tools are specifically designed for information gathering in social networking sites.

In 2011, a tool referred to as a Facebook profile dumper was developed by a group of security researchers who were based in Egypt. The tool was created to educate users on how people can get scammed easily on Facebook. This Java-based tool was released for general use. It automates the hidden Facebook profile data, which is collected from users and only accessible to friends in a network of a user. According to the developers, the tool enables a user to send friend requests to a number of Facebook profiles. The moment the recipient accepts the friend request, the tool dumps all his/her information, friend list, and photos to a local folder.

The developers claimed that a scammer or social engineer collects information from the Facebook profile of a user simply by creating a new account. The social engineer then adds all the user's friends through a “friending plugin” to ensure they share some common friends with the user.

Then, the social engineer uses a cloning plugin that allows them to choose one of the user's friends. The plugin clones the display name and picture of the chosen friend and lays it to the authenticated account.

The social engineer then sends a friend request to the user's account and once the latter accepts it, the tool begins to save all information, tags, images, and accessible HTML pages, allowing the attacker to examine them offline. While it may be too late, the user may unfriend the forged account in the event that he or she discovers that it is actually fake.

Given that the social engineer was able to penetrate into the user's information, they will be able to carry out a number of social engineering ploys. When social engineers are able to obtain more personal information, they are likely to carry out more convincing ploys. For instance, a target is likely inclined to open a malicious email attachment, which social engineers normally use in a spear-phishing attempt, if it seems to appear authentic.

The main goal of the tool's developers for releasing it is user awareness for what is transpiring in the world, specifically in social networks. The developers claimed that the tool will provide people awareness and be cautious of the actions they make online. For instance, accepting friend requests without verifying the authenticity of the profile is one of the wrong actions people make. Social engineers will be able to exploit user profiles even with the shortest period given.

The developers also hope that they can make people aware of the flawed user verification process of Facebook. They claim that it is advisable for Facebook to have stricter policies when it comes to verifying profiles who claim to be “friends” as well as filter out impersonating or fake accounts.

Chapter 6: Social Engineering – How to Prevent and Mitigate

Social Engineering Prevention

As foolish as it may sound, some companies and organizations think that they are resistant to the threat of social engineering. On the contrary, no organization is immune to social engineering, not even the White House or any other prominent system.

For instance, a contest was held at a security conference wherein the participants were asked to obtain information from target companies, which could be utilized for a hypothetical attack. Out of the 140 phone calls that were made to employees of the target companies, almost all the employees divulged information except for five, who refused to give out anything. In addition, 90% of the employees clicked on a URL, which was sent to them by the participants. These employees did not even bother knowing the person who sent it. This security conference concluded on how wide and dangerous the scope of social engineering is for all systems and organizations.

In this light, it is best to know some effective ways to prevent social engineering or merely minimize the risk in organizations.

Learn to Discern Social Engineering Attacks

Before any organization can prevent and mitigate social engineering, the first step is to learn how to determine whether or not an attack is a part of a social engineering ploy. Organizations do not need to know how to create the perfect con or plot a malicious attack. The key is to understand what transpires the moment a malicious PDF link is clicked as well as the signs to look for when identifying if an individual is into something deceptive. Organizations need to understand the threat of social engineering and how such threat applies to them.

Take for example, Mr. Z, who owns a house and lives with his family. Mr. Z values both his house and family; thus, he would want to protect them all the time from any harm or malicious acts. In order to do this, Mr. Z should not wait for a fire in his home to know how to prevent and mitigate the danger. What he should do is plan an escape path and install smoke detectors in case of a fire. Furthermore, Mr. Z should make his family members aware of the phrase, “stop, drop, and roll” so they would know what to do in case of fire. Teaching his family how to get to the door and avoid the smoke by staying low can mitigate the dangers of a fire. Mr. Z can apply all these methods in order to prevent and mitigate a fire.

The same rule applies in protecting an organization from the malicious attacks involved in social engineering. An organization should not wait for an attack to transpire before finding out destructive it can be.

The key in preventing and mitigating social engineering is to know more about how attacks are conducted. This way, it would be easier to determine the most appropriate solutions for an organization. Some of the factors that an organization should be aware of include the expressions, body language, and phrases used in a social engineering attempt.

Once an organization obtains adequate knowledge about social engineering attacks, the next step is to raise staff awareness along with establishing a security-minded culture.

Raising Staff Awareness

One of the most effective ways to combat social engineering attacks is raising staff awareness. In any type of organization, having a security-minded culture is essential as long as it becomes a standard that each member operates. Furthermore, concepts should be reinforced consistently.

There are various ways for organizations to build a security-minded culture as well as raise staff awareness on the destruction that social engineering brings.

1. Higher-ups of organizations should ensure that their people get interested in security. They should be armed with techniques for securing not only company information, but personal information as well. Organizations can provide their staff with security seminars to obtain tips on what needs to be locked up or shredded at home, how to secure home-based wireless networks, and how to manage personal passwords among others.

2. Higher-ups of organizations should initiate on making the message visible to their staff. For instance, posters can be put up at coffee rooms, smoking areas, fax machines, and even shred bins. The posters should be eye-catching so the staff would not miss out on it. In addition, the posters should be visible enough so that any employ who walks by can read and understand them clearly. The message should be changed at least once a month so that the staff has something new to learn about security. If an organization does not have an internal graphic artist, it can use security awareness vendors to avail ready-made posters.

3. Higher-ups of organizations should allow their security department to provide treats for the staff simply for doing their part. For instance, a security department can give employees donuts or cupcakes as a gesture of thanking them for doing their part in securing the organization.

4. Higher-ups of organizations should conduct random desk checks after office hours. Those who have no sensitive material left on their desks will receive a reward. This reward can be as simple as a

leaving a pack of gum or piece of chocolate with a note, “Thank you for leaving your desk clean” or “Thank you for doing your part.”

5. Organizations with a monthly newsletter may include a security article, providing vital information on the latest incidents that transpire in the same industry they are in. This newsletter may be supported with a monthly email to all the members of the organization with a catchy message about a relevant topic, such as “Emergency preparedness,” “PDA safety,” or simply a reminder of what number to call for suspicious or malicious events. It is also best for organizations to provide their staff with a security page in the intranet, which includes the list of security policies, links, and important contact information among others.

6. Higher-ups of organizations should conduct regular training programs that include interactive contests, exercises, give-aways, or games about security. The training program need not be time-consuming. The important thing is that the comprehension of the staff about security is tested.

7. Higher-ups of organizations should be able to walk the walk. This means that the leaders of organizations should be able to exhibit their interest in keeping the company secured.

The staff can make or break the security program of an organization. As such, every member of the organization should be engaged in the security process through suggestions and feedback.

Stop. Think. Connect.

In line with President Barack Obama's mandate, the Cyberspace Policy Review, many organizations have conceptualized a campaign with the message, “Stop, Think, Connect”, which aims to encourage people to think first before engaging in a potentially dangerous or destructive activity online. This message is proposed to be understood as well as carried out as easily as other widely-known slogans, such as “Stop, Look, and Listen” or “Click it or Ticket.” Meanwhile, President Obama's mandate called for the establishment of a national awareness campaign that focused on cyber security.

The message is simple, actionable, and applicable to anyone who connects to the Internet through various devices, including personal computers, laptops, gaming consoles, and the most common of all, smartphones.

Securing the End User

Although technology continues to change and evolve, its end user remains the same. According to Winn Schwartau, who is the founder of the Security Awareness Company, the person at the keyboard has always been the weakest link when it comes to security. Schwartau claimed that along with the changes in technology, social engineering has added new forms and players although its fundamental techniques are still the same.

Thus, the end users should never divulge personal information to anyone and take note that if someone asks for their credentials, that individual is not trustworthy.

A substantial part in any awareness training is the inclusion of specific instructions to not divulge personal information to anyone or any department. Organizations should teach their departments not to ask for personal information from other departments. If an organization plans to launch a new system, the key is to create new credentials. Anyone who comes up asking for the existing credentials is up to something malicious.

As mentioned, when someone asks for credentials, he or she could not be trusted. In the same way, a legitimate financial institution would never ask its client for credentials via email.

Keep Software Updated – All the Time

More often than not, businesses are obliged to give out information to both their clients and staff. For instance, a business should be able provide its phone numbers, web addresses, and emails. Some businesses are required to send as well as receive PDF files from suppliers, vendors, and clients. While it is discussed in this book that releasing information can be the loss of privacy and security, oftentimes, it cannot be helped.

However, there is an effective way to prevent social engineering attacks from invading an organization's security – keep software updated all the time. For instance, there are still companies and businesses that still use Adobe Acrobat 8 and Internet Explorer 6 when there are already new versions of these programs. Those using outdated software programs and systems are more vulnerable to social engineering attacks than those with updated versions.

When social engineers find out that a certain company still makes use of these two outdated applications, they would certainly plan their attacks even if the company has firewalls, IDs, and antivirus systems.

Therefore, it is important for all types of organizations to update their software regularly. More often than not, the newest software versions have already fixed their security holes. In addition, organizations should never use a software system that has negative track record as it will surely be vulnerable to malicious attacks.

Develop Scripts

Developing scripts that help employees be prepared, especially when the situation requires critical thinking is one of the most beneficial ways to prevent and mitigate social engineering attacks.

The scripts referred here are not the same as what Hollywood actors use during their film shoot. The scripts for countering social engineering ploys are merely outlines that can support employees in various scenarios.

For instance, how should an employee reply to someone claiming to work for the CEO and demands for their password? What should an employee do when someone who does not have an appointment but dresses and acts the role of a vendor, demands access to a secured part of the building?

These are scenarios wherein scripts can be of enormous help. Scripts can assist employees in identifying the proper answer, response, or reaction in certain situations. Scripts also make employees feel at ease.

An example of a script for a specific scenario is provided in the following section.

Scenario: Someone calls and claims to be from the office of the CEO and demands an employee to hand over internal data or information:

Script: 1) Ask the employee ID number and name of the person without answering any questions until you are given this information; 2) After obtaining the identification details, ask for the project ID number associated to the project that the person is claiming to manage or be a part of; 3) If you have obtained the information of steps 1 and 2 successfully, comply. If not, ask the person for his or her manager's requesting authorization and send it via email. Terminate the call.

In this scenario and script, an employee would know what to say, how to react, and what to do while being conscious of the company's security.

Understanding Social Engineering Audit

A social engineering audit involves a simulation of the malicious attacks carried out by social engineers. This simulation is administered by a professional security auditor whom a company hires for testing the policies, physical perimeter, and people of the company.

There are two primary differences between a professional security auditor and a malicious social engineer. One, a professional security auditor follows legal and moral guidelines and two, the goals of a professional security auditor is to help as opposed to that of a malicious social engineer, which is to harm, steal, or embarrass a target.

In order to fully understand the concept of a social engineering audit, it is best to establish the goals on why an organization wants to implement it.

A professional security auditor should carry out his behavior based on morally and ethically accepted principles while he stretches across the line, allowing him to pose as a malicious social engineer. In other words, he should take note of things, which he can use to obtain information or gain access to the weakness of a company. While he tries to expose the hole in the defenses of a company in the persona of a malicious social engineer, he still needs to behave in an appropriate manner.

On the part of the companies hiring a professional security auditor, they should be able to determine the security gaps and balance them with a concern for each employee. More often than not, companies who undergo a social engineering audit think that terminating the employee or employees who fell for the ploy is the solution to the problem and fixes the hole. However, companies should realize that once an audit is done, the employees who fell for the attack are probably the most secure employees in the building during that time. Consequently, a professional security auditor should also take actions in ensuring that the jobs of employees would not be jeopardized.

Conclusion

The primary purpose of this book is to open your eyes to the real world of social engineering. I hope it has helped you in maintaining or establishing a healthy dose of fear for the potential destruction that social engineering can bring, not only to companies or organizations, but also in your home and personal life. Thus, I hope you will continue to pay attention to possible malicious attacks as discussed in this book.

Rest assured that following and implementing the principles you have read in this book would enhance your capability to discern and converse more efficiently with the people around you.