Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Social Engineering: Manipulating the Source

A company has a duty to every employee to inform and prepare them for social engineering attacks. If it fails to do so, it WILL become a victim of such attacks. The methods described in this paper will detail methods you can use for your company s aversion of social engineers.

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Social Engineering: Manipulating the Source

GCIA Gold Certification

Author: Jared Kee, jkee@alertlogic.net

Adviser: Brent Deterding

Accepted: April 28th 2008

© SANS Institute 2008, Author retains full rights.

Outline

1. Introduction 4

1.1 What is social engineering?.....4

2. How social engineering is accomplished 5

2.1 Telephone

2.2 Online

2.3 Dumpster Diving

2.4 Shoulder Surfing

2.5 Reverse social engineering

2.6 Persuasion

3. Who is affected by social engineering attacks?.....6

3.1 General list of who should be trained in a company and why

4. Examples…….....…...7

4.1 Telephone

4.2 Online scams

4.3 Dumpster Diving

© SANS Institute 2008, Author retains full rights.

4.4 Shoulder Surfing

4.5 Reverse social engineering

4.6 Persuasion

5. Countermeasures for social engineering attacks……...13

5.1 Suggestions and countermeasures on the Telephone

5.2 Countermeasures for online attacks

5.3 Countermeasures for dumpster diving

5.4 Countermeasures for Reverse social engineering

5.5 Countermeasures for In-person persuasion attempts

6. Conclusion…….....19

7. References…….……..20

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

It's 2 AM and you get a phone call from what appears to be your companies IT department claiming that there has been a computer virus outbreak at your office that is

© SANS Institute 2008, Author retains full rights.

destroying everyone's personal files and they need your username and password immediately so they can copy all of your personal files to a safe location. The name and number on the caller ID matches your companies number, and you recognize the name that the caller claims to be, and he even mentions that highly classified project that you have been working on lately that ONLY "insiders" know about. What do you or anyone else at your company do?

1. What is social engineering?

Wikipedia defines social engineering as "the art of manipulating people into performing actions or divulging confidential information" (Wikipedia). Note that not all information gathered by a social engineer may be classified as confidential, but can still assist them in their attack. For example, a simple question like "What's your superiors name?" may bring a social engineer a step closer to stealing your superiors identity. Social engineering is most commonly referred to when talking about computer system and network security. In fact, most social engineers are also proficient at using computers (which isn't a requirement of being a social engineer) as well as being a skilled social engineer which can be a very lethal combination. Social engineering is derived because of a human characteristic to trust other people. People have a tendency to sympathize with anyone that claims to be in trouble or believing anyone who comes around claiming to be a trusted person without officially checking their credentials first. A social engineer knows this and anticipates this. When a social engineer attempts an attack on your company, a person may ask a couple of questions off the

© SANS Institute 2008, Author retains full rights.

top of their head that they believe will confirm this persons identity, but a social engineer has spent ample time anticipating your every question and move and is ready with a reply on hand. Are you and your company prepared?

This type of attack can be prevented by proper training to ALL associates of a company. A company has a duty to every employee to inform and prepare them for social engineering attacks. If it fails to do so, it WILL become a victim of such attacks. The methods described in this paper will detail methods you can use for your company's aversion of social engineers. Following is the stories of those who failed to recognize the ways of a social engineer and what we can do to prevent these stories from becoming a reality once again.

2. How social engineering is accomplished

Social engineering is accomplished through many feats including dumpster diving and persuasion. Social engineering includes:

- Telephone – Using telephones to contact individuals of a company to persuade them to divulge in confidential information.
- Online – Persuading or gathering information through the use of an online chat session, emails, or any other method that your company may use to interact online with the public.
- Dumpster Diving – Looking for information discarded by a companies employees

© SANS Institute 2008, Author retains full rights.

- Shoulder surfing – Simply looking over someone's shoulder while they are using a computer. This can be done in close range as well as long range using a pair of binoculars.
- Reverse social Engineering – This is a more advanced method of social engineering and is almost always successful. An attacker will have had to already done reconnaissance as well as already have some amount of luck with previous attacks (whether thru hacking or social engineering). Reverse social engineering is a method where an attacker can get their victims to call them back pertaining to something an attacker may have previously. Since a victim is calling the attacker, the victim is already at the attacker's mercy, and it is almost impossible for the victim to tell that they are being attacked if they have already legitimately made the call back to the attacker. A social engineer can use a combination of all of these methods to accomplish his final goal. In fact, most successful ploys will incorporate at least 2 of these methods.
- Persuasion – Persuading someone to give you confidential information either by convincing them you are someone who can be trusted or by simply just asking for it.

3. Who is affected by social engineering attacks?

© SANS Institute 2008, Author retains full rights.

Everyone in a company is responsible for a company's integrity. A company can spend billions of dollars on all kinds of security equipment, but it only takes one person for a company's security to be compromised. While a janitor may not need as much training as an IT helpdesk or secretary, it is important not to forget anyone in a company. A good training program should address issues such as Data retention (what can be thrown away vs. shredded) and data classification (What level of security do I need to treat this document as and what does this level of security mean to me?), Employee Identification and physical access protocols, as well as consequences to not following these procedures and who to contact if you have questions or need to report suspicious behavior. Training can be reinforced by doing role playing with employees so they can get interactive training that will help reinforce what they have learned. Below is a general list of employees a company may have and recommended training.

Training Levels

High – This level represents people who should be expecting social engineering attacks and/or have the privileges to significantly change or render the network useless. An I.T. helpdesk is a good example of this because they are used to helping people all day as well as having a fair amount (if not more) of network privileges that typically include adding or removing users as well as changing their passwords.

Medium – This level represents people who may have contact with the general public

© SANS Institute 2008, Author retains full rights.

and/or may have some level of access of network access. These people may not have the authority to make network changes, but they can certainly run commands or go to another computer and do a number of things from there. Training should be focused on confirming a person's identity before they give out any information or do any favors.

Low – This level includes people who have little or no network access. This includes security guards and janitors. The training at this level should include training on social engineering tactics, and in some situations may emphasize not letting anyone in after hours as well as not doing any favors for anyone for **ANY** reason. The training at this level may skip certain tactics if necessary that may not apply to everyone.

A company will obviously have to have a social engineering training plan made to fit the company's needs and positions since no 2 companies are just alike. For a lot of positions where the employee may not work for a highly targeted department and may not do any work remotely, a low to medium strategy may be all that is needed, however do not forget to reinforce the training they do receive. A great social engineering strategy plan may be short lived if it is not reinforced with occasional mock social engineering attempts or short little tips emailed or posted regularly in a bulletin that everyone receives.

- **Helpdesk –** A helpdesk should be trained thoroughly in thwarting social

© SANS Institute 2008, Author retains full rights.

engineering attempts. A busy helpdesk may get many requests and inquiries through email, IM, in-person, or telephone and at any time, a social engineer can attempt to persuade them that they are a legitimate user and need some sort of assistance. A helpdesk's main goal is to help, and that is exactly what a social engineer will be looking for. The helpdesk should be trained to be friendly while at the same time using good judgment and skepticism before proceeding to assist a user. Before they start assigning usernames and privileges, they should be asking themselves if the user is who they claim to be and why and if this user NEEDS these privileges or information.

- **I.T. Administrator –** While IT Administrators may not get as many phone calls as a busy helpdesk, they can still be prime targets because they can control the entire network, and if there's one person a social engineer would like to have running commands and transferring files on a network, it would be the administrator which is why they should have a high amount of social engineering training. Administrators are generally more aware of computer based tactics because they understand the intricacies of a computer network and how devastating one command can be, but they are still vulnerable when it comes to other types of social engineering tactics such as simply just calling and asking for something.

© SANS Institute 2008, Author retains full rights.

- **Receptionist –** A receptionist is a broad term when it comes to responsibilities and a training plan will have to be made to fit their job. If they are at a company's front door and answering calls all day, they should probably be trained more for in-person persuasion tactics and phone tactics. If they are a personal secretary for a CEO and do a lot of online work and emails, they should probably be trained more for online tactics as well as phone calls where someone needs a favor because the CEO told them to call the secretary for that information. Depending on the job function, a medium amount of training should be sufficient for a receptionist.
- **Telecommuter –** A telecommuter should be moderately to very well trained for social engineering attacks simply because their home network is simpler and because of that, it is a lot simpler for someone to compromise the corporate network remotely as well as a higher chance of success and remaining anonymous due to the telecommuters lack of high-end networking equipment that would exist if that user were to be at the office instead.
- **HR department –** The HR department holds personal information for every employee and even if not everyone in the company wishes to actively protect their company from a social engineer, they should have an interest in

© SANS Institute 2008, Author retains full rights.

protecting their own personal information from being stolen. Not only is this a good point to make in any company training on this subject, the HR department should safeguard their employees data at all costs and pointing out how everyone's personal data is protected should motivate employees to do the same. The HR department may or may not be in regular communication with other departments sending classified information but if they are, there should be a procedure to follow before giving out any information. This department should be highly trained for social engineer attacks and should have procedures to confirm who is requesting data from this department.

- **R&D department –** While a R&D department won't be answering phone calls and responding to emails from unknown users all day, they will however be a prime target for those people who are wanting to see what the company is up to. The department should have very secure servers and possibly a VPN, it is recommended that the R&D department should at least be aware of scams and how someone can use social engineering to get into their servers and steal their blueprints and files. A moderate amount of training should be sufficient, possibly less depending on the situation.
- **Company Executives –** Company executives can take a lot of forms. Some may

© SANS Institute 2008, Author retains full rights.

need a lot of training, some may only need a minimal amount of training. Some may not even wish to be bothered by this, but you have to remind them that this involves the entire company and can affect them directly. A moderate amount of training should be sufficient for executives, but it varies greatly on the role that these people play.

4. Examples

In this chapter, I will show examples of many ways a social engineer can infiltrate your organization and get what they want and have almost no chance of having their true identity compromised.

- Telephone

Our first example is how easily a social engineer can use the telephone to achieve their goals. A lot of attacks will use the telephone because they are used so much in our daily routine and people who use the telephone often to communicate with clients they may not know personally tend to trust people a little easier than most and all a social engineer may really have to do is learn a few key words or jargon and may be able to talk a person into giving out information that the general public shouldn't have. Another reason people may give for trusting people on the phone so quickly is they do not want to seem rude or bothersome to that customer if it turns out their credentials are valid. However, it is quite the opposite, that

© SANS Institute 2008, Author retains full rights.

person will feel more secure knowing that your company is checking for credentials instead of just taking anyone who calls in claiming to be them at face value.

This example is one that I have heard of personally happening locally and it didn't take much more than a short google search (or possibly the local white pages might have worked too.) and a short phone call.

Paul had the desire to get into someone's hotmail account that he knew but had little technical knowledge. He only needed to get in there once or twice and didn't really care too much about them knowing that their email had been broken into. He knew a little information already on that person but nothing more than a name and an email address. The first thing Paul did was go to the local college that provided free internet access to anyone who could walk up to a console and hit enter as to remain somewhat anonymous. Next he went to Hotmail and clicked on "forgot your password?" (as a lot of times people will have security questions that really do not serve them well.) and it asked for some verification like city/town, zip code which he had already and if not, it could have probably been easily Googled. After that step it asked the security question "What is your pet's name?" Oh simple. He went on Google, pulled up the person's phone number, went to a quiet payphone and dialed them up. When they answered Paul said "Hi, I am a local biology student doing a term paper on household pets and I just have a couple questions. I am on the last part of the paper and I only have a few more pieces of data to gather before I am finished. Can you help me?" A

© SANS Institute 2008, Author retains full rights.

couple of seconds of silence passed and she said “Sure, fire away” The first question was how many pets do you own and what kind of pets are they? She answered 3 dogs 2 cats immediately. Next Paul asked “What are their names?” a few seconds passed and he continued with “My paper has a chapter on the most popular animal names in it.” She answered promptly and he asked the final question “and what are their ages?” to reduce the likeliness of her remembering the question that he asked that he was interested. After she answered that question, Paul thanked her for her time and she shockingly said “Oh that was easy” as if she was prepared to give out more information. Paul wasn’t completely stupid and waited a couple of days to pass before attempting the names then anxiously came home from work one day and attempted the names. The first 2 didn’t work and as he was thinking oh crap, time to come up with a Plan B, he typed in the 3rd name and success he was at the reset password screen which also gave him a temporary password to login.

The moral of this story: Be careful what you give out, it may seem innocent and innocuous, but it can be just what a social engineer needs to break into your system.

On a side note, I don’t like security questions. There are times that I use them, but not for everything, simply put they annoy me, I am password responsible, and if I had not heard about the above, I am likely to make up something vulnerable that someone could Google. Every time I help someone setting up an email or something similar, they always ask “what is a security question and why do I care?” and a lot of times they will initially make up something

© SANS Institute 2008, Author retains full rights.

just as vulnerable until I intervene. As for myself, I am not too bad at remembering passwords, so I make cryptic security questions if I absolutely have to, otherwise I say, “if I can’t remember the password, it probably wasn’t that important.“ This may or may not work with everyone, but just being aware of what can happen will naturally make the next security question you have to make more secure.

Another example is one I saw while reading Kevin Mitnick’s The Art of Deception.

The First Call:

Andrea Lopez answered the phone at the video rental store where she worked, and in a moment was smiling: It's always a pleasure when a customer takes the trouble to say he's happy about the service. This caller said he had had a very good experience dealing with the store, and he wanted to send the manager a letter about it. He asked for the manager's name and the mailing address, and she told him it was Tommy Allison, and gave him the address. As he was about to hang up, he had another idea and said, "I might want to write to your company headquarters, too. What's your store number?" She gave him that information, as well. He said thanks, added something pleasant about how helpful she had been, and said goodbye. "A call like that," she thought, "always seems to make the shift go by faster. How nice it would be if people did that more often."

© SANS Institute 2008, Author retains full rights.

The Second Call:

"Thanks for calling Studio Video. This is Ginny, how can I help you?" "Hi, Ginny," the caller said enthusiastically, sounding as if he talked to Ginny every week or so. "It's Tommy Allison, manager at Forest Park, Store 863. We have a customer in here who wants to rent Rocky 5 and we're all out of copies. Can you check on what you've got?" She came back on the line after a few moments and said, "Yeah, we've got three copies." "Okay, I'll see if he wants to drive over there. Listen, thanks. If you ever need any help from our store, just call and ask for Tommy. I'll be glad to do whatever I can for you."

Three or four times over the next couple of weeks, Ginny got calls from Tommy for help with one thing or another. They were seemingly legitimate requests, and he was always very friendly without sounding like he was trying to come on to her. He was a little chatty along the way, as well -"Did you hear about the big fire in Oak Park? Bunch of streets closed over there," and the like. The calls were a little break from the routine of the day, and Ginny was always glad to hear from him.

One day Tommy called sounding stressed. He asked, "Have you guys been having trouble with your computers?" "No," Ginny answered. "Why?" "Some guy crashed his car into a telephone pole, and the phone company repairman says a whole part of the city will lose their phones and Internet connection till they get this fixed." "Oh, no. Was

© SANS Institute 2008, Author retains full rights.

the man hurt?" "They took him away in an ambulance. Anyway, I could use a little help. I've got a customer of yours here who wants to rent Godfather II and doesn't have his card with him. Could you verify his information for me?" "Yeah, sure." Tommy gave the customer's name and address, and Ginny found him in the computer. She gave Tommy the account number. "Any late returns or balance owed?" Tommy asked. "Nothing showing." "Okay, great. I'll sign him up by hand for an account here and put it in our database later on when the computers come back up again. And he wants to put this charge on the Visa card he uses at your store, and he doesn't have it with him. What's the card number and expiration date?" She gave it to him, along with the expiration date. Tommy said, "Hey, thanks for the help. Talk to you soon," and hung up. (Mitnick, 2002)

- Online

The next example is about social engineering using phishing and popups online. Public awareness has risen over the past few years regarding phishing and popups. While most of them can be disregarded just by using a decent spell checker and a popup blocker, some can be more convincing. Be aware of the information that you give out online. I have noticed that this section will be more applicable to people who do not use their computer often, as a lot of regular computer users can spot an average online scam in about 10 seconds or less.

Bob was surfing the web on a nice sunny afternoon and had noticed a recent barrage of

© SANS Institute 2008, Author retains full rights.

pop-ups in which one of them said “Your computer is infected with Spyware, click here for a free scan”. Well it looked like a legitimate windows message because it had the XP theme and a red X at the top, so it must be legitimate he thought so he clicked it. It took him to a page and asked him to fill out some information like name, email, phone, etc. Soon after a scan began which claimed to clean out all spyware on the computer, but the popups continued and soon enough his inbox was filled with junk.

On the same day, Joe was checking his email and had noticed that one of them was from security saying that they had detected that his email had a virus and that he needed to download the attachment and run it to get rid of this virus. It was very colorful and had a lot of “WARNINGS” and “IMMEDIATE ATTENTION REQUIRED” labels all over. Without a second glance (not noticing who the email was from, or why they were emailing him, or even the misspellings in the email), Joe panicked and download the attachment and ran it. The attachment said the virus had been deleted and he went about his business feeling proud that he fixed his email problem and that no emails were lost.

When I used to do technical support, I would have to do a lot of house calls that had to do with this type of situation. Usually I would inform them about email scams and popups, refer them to a good antivirus and spyware scanner, and help them solve their immediate problem. Most of them had no idea about what was really going on, but after I trained them and pointed them in the right direction, they were grateful and I usually never had to make

© SANS Institute 2008, Author retains full rights.

another house call for them again. Training and awareness of these types of scams are key. Knowing what to look for in emails to tell if its authentic or not, and not clicking on any popups and why will greatly improve awareness of this type of attack.

- Dumpster Diving

In this example, a social engineer will prove that someone else's trash is another mans treasure. If your trash could be used against you or your company, dispose of properly.

Since dumpster diving is more passive and can actually be done while you are asleep, this is more of a description of what can happen.

A social engineer was out behind a company he was profiling poking around in their dumpster. The dumpster was in the open and had no lock on it so he looked down in the trash can and found a bag that appeared to have lots of documents inside. Inside were invoices, bills, and other important documents. The company earlier that week had some repair done on a laser printer as an invoice stated. That social engineer can now call the company he is going after claiming that he works with the repair company which opens the door for a number of attacks he can use. If the social engineer found a customer list or even a bill to another company, he can call up posing as a customer and get classified information that only the real customer should have. Furthermore, should he have found network diagrams or usernames and passwords, he could do even more damage, possibly without any further attacks.

© SANS Institute 2008, Author retains full rights.

- Shoulder Surfing

Shoulder surfing is when a social engineer watches what you are doing and can also be done remotely (both by cameras and software). This is also a mostly passive technique, as I wouldn't expect anyone to be coming up to you while you were at the coffee shop sending emails, sit down next to you, and say "Hey, mind if I watch you for a while?" I don't suggest going out into the public doing business on your laptop in clear sight, but sometimes it may be unavoidable and you need to be aware of your surroundings. For instance, if you work in a public place and have to operate a computer of some sort (like a POS register) anyone can watch you enter your employee ID and password to get on the register. Also, if you are in a public place with a laptop, be careful of what's on your laptop as well. It may be obvious, but some people leave usernames and passwords taped to their laptop, and not only can that be seen in public, if the laptop gets stolen, they already have credentials. ATMs are also used a great deal and sometimes may not always be as secluded as we all think. A social engineer with a pair of binoculars may be hiding in the bushes watching you enter your pin, and may happen to get a glimpse of your name. If you happen to be in a computer lab, there will probably be computer cameras around. For all you know, those cameras could be public and anyone with an internet connection can logon, zoom in, and see what anyone in the room is doing. The best thing to do is be aware of your surroundings; you never know who may be watching you.

© SANS Institute 2008, Author retains full rights.

- Reverse Social Engineering

Reverse social engineering is a more advanced method of social engineering and requires some reconnaissance before a successful attack is employed. It involves the user asking for assistance from the attacker so the victim is at the mercy of the social engineer. This is one of the hardest types of attacks to detect because when a victim contacts the social engineer, they have no doubt they are who they say they are and will most likely not question them at all. There are many ways that a social engineer may be able to get a user to contact them for help but here is one example.

This particular social engineer had managed to gain access to a small switch inside a company that connected a couple of users. The social engineer then might contact those users and introduce themselves and say that if they ever have any network connectivity problems to call them immediately. Sometime in the near future the attacker would then kill connectivity to that switch and wait for one of the users to give them a call. At this point, the social engineer is in control and can control the victim in whatever way the social engineer desires. If successful, the end result will be that the victim will have given away some piece of information (server name, username/password, network topology), the social engineer will have fixed whatever problem they have caused, and the user's problem will have been corrected without the victim even considering that they may have just given out some confidential data.

© SANS Institute 2008, Author retains full rights.

- Persuasion

Persuasion is This example is from the Official Certified Ethical Hacker Review Guide chapter on social engineering.

The facilitator of a live Computer Security Institute demonstration showed the vulnerability of help desks when he dialed up a phone company, got transferred around, and reached the help desk. “Who’s the supervisor on duty tonight?” “Oh, it’s Betty.” “Let me talk to Betty.” [He’s transferred.] “Hi Betty, having a bad day?” “No, why?…Your systems are down.” She said, “my systems aren’t down, we’re running fine.” He said, “you better sign off.” She signed off. He said, “now sign on again.” She signed on again. He said, “we didn’t even show a blip, we show no change.” He said, “sign off again.” She did. “Betty, I’m going to have to sign on as you here to figure out what’s happening with your ID. Let me have your user ID and password.” So this senior supervisor at the help desk tells him her user ID and password. (Graves, 2007)

5. Countermeasures for social engineering attacks

This chapter will address some practices that you can adopt to prevent a social engineer from making the best out of your company. No matter what the situation, always be sure to verify who the person is and their need to know. Using the telephone is usually a social engineer’s best friend simply because it can help them exploit your company with the

© SANS Institute 2008, Author retains full rights.

least chance of compromising their true identity.

- Countermeasures for telephone attacks

If your company has at least one telephone with someone answering calls all day, your company is at risk for a telephone based social engineer attack. Most social engineers are usually proficient with computer systems and how they work which also includes telephone systems and caller ID. Not only can a social engineer fool a person with the tactics mentioned above, but they can also mask their name and number on a caller ID to make their story seem even more legitimate. This can also apply to internal extensions as well, especially if they have access to your phone system. All it may take is a little reconnaissance to find out what phone system your company uses and who your phone system support is (if support is not done internally) and they may be able to impersonate a phone support technician doing some "maintenance" or upgrades, and they can have complete access to your phone system. That may be a little off topic but beware that that caller ID that is ever so popular today may not always be telling the truth. In fact, the only recommended verification when using the phone is if you personally know the person and can personally vouch for them. However, in a high volume call center, that's nearly impossible, so your company will need to have a pretty solid policy for handling calls. If your call center is handling calls from multiple clients, one method of handling them is to give each client a pass phrase or a 2 part question and answer like "What's crunchy and delicious? Tortilla chips." Of course this can still be circumvented,

© SANS Institute 2008, Author retains full rights.

especially if your client is not too concerned with security. When initially discussing security issues with your clients, be sure to emphasize that passwords, answers, or any important information that anyone can use against your company should not be written down or handed out to anyone who isn't authorized to access information that your company has. Also, setup some verified means of communication with the client so that if they need something immediately or there is a dispute on who the caller is, there can be some verifiable means of communication so that there will be less of a chance of a successful social engineering attack.

If your company is a little more flexible and only have a few people answering calls, it may not be feasible to have a high security protocol for handling calls. That does not mean that security shouldn't be taken seriously though. The call center should still at least try to verify name and number and ALWAYS be aware of the situation, IE. A caller should not be calling asking for internal forms or saying that they need some piece of information immediately but do not have access to any verified numbers or email addresses.

- Countermeasures for online attacks

A lot of recommended countermeasures for any kind of attack online, most people in IT in general will be familiar with. Everyday, I get loads of emails about winning the UK lottery, or some person needing my bank account number for whatever reason and it is very apparent to me that this is a scam but it may not be so obvious for people who aren't online everyday for their job. With emails, you can usually tell just by looking at all the misspelled words, and

© SANS Institute 2008, Author retains full rights.

oddly phrased sentences, or the fact that 99% of them have nothing to do with you whatsoever. A lot of online attacks can be counteracted by just being aware. If you do not know who the sender is and if the topic is not something relating to you, it is recommended that those emails be deleted to prevent anything being maliciously downloaded to your computer.

Utilizing the Web is also another avenue a social engineer can get into a system. By getting a user to click on a certain page that may download a script or enter credentials for a phony webpage, a social engineer can make quick work out of anyone not properly trained in what to look for on WebPages or how to tell if something strange is going on with their browser. SOME of these exploits and attacks can be thwarted by utilizing, antivirus, anti spyware, and popup blockers, but the user will still need to be aware of other things like phony pages that a program may not be able to detect. There are a number of ways that a social engineer may be able to direct someone to a phony webpage, but a user will have to be aware of the situation and if they believe that the page is a phony, close immediately, and if they are uncertain if there computer was infected, have someone who can tell (obviously, someone they know) if there pc has in fact been infected. A good training session is also recommended for users who will need to be online regularly for their job.

- <u>Countermeasures for dumpster diving</u>

Countermeasures for dumpster diving are pretty simple and easy for most people.

© SANS Institute 2008, Author retains full rights.

Don't leave important pieces of information lying around or in the trash unshredded. Not all companies may be able to, but if your company can, it is recommended to get a dumpster that has a lock, and possibly a structure around it so only authorized people can even get near the dumpster. An alternative to that is to have a 3rd party company take care of your important documents. Aside from corporate documents, most people can do their part by just throwing important documents (or any document that can possibly be used against them) into a paper shredder (Cross cut shredders is recommended). This even applies to your home life when checking your mail. You wouldn't leave a credit card application with your name on it on top of the trash pile out in the dumpster or on the side of the street for anyone to pick up and send away for, being responsible with your company's documents is just as important.

- Countermeasures for reverse social engineering

Reverse social engineering is a multi part attack. It requires previous reconnaissance before the attack can be launched. Since a reverse social engineering attack is more advanced and usually more intricate than other types of social engineering attacks, it is harder to detect. The first step of reconnaissance may be done passively at times (IE. Google or your companies website) but the first step will not be a reverse social engineering attack, so in the early stages, the attacker will be using another method which may not necessarily be a social engineering attack. At the next stage, the attacker will have access to something that is needed for your company to function and the attacker will then advertise that they can fix these

© SANS Institute 2008, Author retains full rights.

types of issues. The attacker can use business cards, phones, emails, or any type of media to advertise this, and while this is part of the attack, you should not necessarily go accusing everyone that advertises that they fix whatever issues they fix of attacking your company, however, if they claim to be with your company, I would ask around to see if there was a recently hired administrator. The final stage is the attacker will take down or cause a problem that they previously claimed that they fix and hope that someone will contact them asking them to fix that issue. If someone does contact them, the attacker will be in a better position to successfully launch their attack because the user is now at the mercy of the attacker. Even if they get a little suspicious, all the attacker has to do is say something like "Do you want this problem fixed or not?" which could force a user to comply with their demands. Staying alert of the situation however could prevent this. If someone comes advertising they fix this issue and all of a sudden this issue arises, I would be getting a little suspicious and asking questions and possibly getting the word out before any of my coworkers call them. Of course, at this stage, the attacker will already have compromised a part of your company with their first attack, so if someone discovers this type of attack at this stage, it will be imperative that they let someone know ASAP.

Detecting a reverse social engineering attack is again, the most difficult to attack, especially if they have good reconnaissance, but the most effective countermeasure is to remain alert at al times, and if there's an outage of anything, be sure to notify a verified

© SANS Institute 2008, Author retains full rights.

administrator or someone you know can deal with the issue. If your company doesn't have a verified administrator for such situations or you do not know the person to call in such situations, it is recommended that you find out as soon as you can or that your company find an administrator to handle such situations. This may be just what the attacker is counting on for a successful attack.

- Countermeasures for In-person persuasion attempts

Verification is the key here. Verify the identity of anyone who shouldn't be allowed inside your company on a normal basis. A typical social engineer may not attempt to do an in-person attack because if caught, they could be in serious trouble, but because of that they will probably be ready with a story and credentials. A social engineer's goal here is to fit in with the crowd. To look like someone who SHOULD be there. They may be disguised as a repair technician or any number of people who frequent companies and because they look like they belong there, your best defense will be asking someone who knows if they should be there. One recommendation is to have people who are expecting visitors to send out emails or notices around letting everyone know who to expect that day. This may not work though if there is an overwhelming amount of visitors to your company. If that is the case, your company may have a reception area or a security guard who can call around to see if someone is expecting a visitor. Another recommendation if your company has more than one door or exit that is used, (IE. A door to a smoking area or an exit to the parking lot) be sure that

© SANS Institute 2008, Author retains full rights.

NOONE lets anyone in through those doors that they do not know and that no one is "tailgating" into the building while no one is watching. A social engineer may be watching those doors and looking for opportunities to get inside. If you notice someone frequenting around the building that shouldn't be there, you may have a possible social engineer on your hand waiting for the right opportunity to get in.

6. Conclusion

No matter how much technology changes or the amount of money your company dumps into security measures, devices, and even protocols, it will still be most vulnerable to old fashioned persuasion. Procedures and guidelines should be in place specific to your companies function to minimize the threat of social engineering. There will never be an environment where there is a 0% chance of a social engineer attack and the second you think your company is safe and you let your guard down could be the second that a social engineer takes advantage of your company. A good strategy will constantly be reinforcing policies and countermeasures as well as occasionally conducting physical penetration tests against your company to see what areas need improvement as well as rewarding those employees who are consistently security conscious and taking precautions to minimize the risk of a successful attack. The best defense a person can take against these types of attacks is to be aware of

© SANS Institute 2008, Author retains full rights.

their surroundings. Constantly asking yourself questions like "What can someone do with this information?" or "Who is this person have and do they have a need to know this information?" A social engineer will be relying on someone who is not aware of their surroundings or someone who is not security conscious in the company. Everyone should want to be security conscious because not only does the company benefit from being aware, but that mentality will carry over into their personal lives as well, which will help prevent them becoming a victim of identity theft and a number of other crimes.

7. References

Mitnick, K. D. (2002). *The Art of Deception: Controlling the Human Element of Security.* New York, New York: Wiley Publishing.

Long, J. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* Rockland, MA: Syngress Publishing.

Graves, K. (2007). *CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50.* Indianapolis, Indiana: Sybex Publishing.

© SANS Institute 2008, Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**