**Social Engineering – Art of human hacking**

Have you heard of the e-mail from a Nigerian prince asking for help retrieving an inheritance in exchange for money? Or have you seen the movie The Sting and been amazed at how the two main characters can fool virtually anyone? You might have asked yourself if people really can pull off these sorts of schemes. Do people really fall for them? The clear answer is yes, but the real question is: why? Social Engineering is a whole category of knowledge and skills that can make us vulnerable to scammers. Most of the time, we don’t even know that it’s happening. Social Engineering is more than just an inherent skill of sweet talking and social adeptness; it’s a whole science that is used by scammers, as well as the very people who try to prevent scammers. In these blinks, we will take a close look at the foundations of Social Engineering, how it works and the techniques that it entails.

Have you ever been persuaded into buying something only to realize later on that you don’t need or want whatever you’ve bought? If so, you’re not alone. Most of us have been brought under the influence of some social engineering tactic at one point or another. Social engineering is a set of psychological tricks that exploit human vulnerabilities to influence a target’s actions. These tricks can manifest themselves as spoken language, body language and hidden suggestions. Governments, salespeople and law enforcement officers are deeply familiar with these tactics, but the fact is that we all use social engineering, even with our friends, family and coworkers. For example, when a kid says “I love you, Mommy. Can I have a puppy for my birthday?” they are using social engineering to influence their parent. Of course, social engineering isn’t only about short-term gain; it can actually be used to do great harm to people.

Scammers and con artists, for instance, use social engineering to manipulate their targets and compromise security systems. If you want to install malware onto a company’s server, you could go in guns blazing and fight your way to the server room. But that’s messy. A social engineer will instead do something like disguise themselves as an IT specialist and prepare a convincing story to get past security. Once inside, they’re free to do what they want and no one will be the wiser. As far as the security guard knows, the “IT person” was just doing their job. But no one wants to be conned like this. Luckily, we can protect ourselves with a solid understanding of how social engineering works. Security auditors, like the author, are hired to play the role of malicious social engineers to test a client’s security system by performing authorized penetration tests, or pentests for short, which are basically fake social engineering attacks. The client, of course, doesn’t know when, where or how this will happen.

Whether you’re a security auditor or a criminal social engineer, before you plan an attack, you need to know your target. The more you understand your target, the more you’ll know how to influence them, and the more effective your plan will be. Start by creating a profile of your target. A good place to start is on the internet: certain websites allow you to track a person’s e-mail address, phone number and even her IP address, while social media can also be a great resource. Be diligent! Even a minor detail can prove valuable. For example, the author’s mentor, Mati Aharoni, was once hired to do a pentest for a specific company. Aharoni discovered that one of the company’s high-ranking officials used his company e-mail on a stamp collectors’ forum. So, Aharoni created a website with a stamp-related address and embedded a program that made it possible to access the target’s computer. He then called the official, asked if he would be interested in buying his “deceased grandfather’s stamp collection” and offered to send him a link to the website. The target, caught completely unawares, happily accepted – and fell for the trap. As you can see, even the most seemingly trivial information can have a big payoff! You can also learn a lot about someone through simple observation of his daily life. It’s a good practice to follow your target through her daily routine. What places does she always visit? Does she smoke? If your target is a company, do employees use keys or magnetic cards to enter the building? Does the building have security cameras? Finally, while it is certainly not glamorous, you can nonetheless glean important information by looking through your target’s garbage. People throw out CDs, letters, invoices and all sorts of other things that contain important information. But be smart about it: take the bags somewhere else to avoid being caught!

Imagine you’re a detective about to go undercover. Would you use your real name, address and backstory? Of course not! You’d create a backstory and alias, and use everything you know to design a solid plan to go undercover. It all starts with a pretext, that is, a scenario that makes your target feel comfortable doing something they normally wouldn’t. This is why it’s so important to gather good information about your target in the beginning: the better your information about them, the more convincing the pretext will be. Let’s say your target is a CEO who regularly donates to a charity. This knowledge could be useful in creating your pretext. As a potential way to meet with the CEO, you could pretend to be a salesperson offering to donate a percentage of a purchase to the CEO’s preferred charity. After all, CEOs won’t see just anybody, and mentioning this charity improves your chances.

When crafting your identity, it’s important to draw inspiration based on your target’s interests in order to inspire their trust in you. The easiest way is to find a real common interest that you share with your target. If that’s not possible, you can mold your identity to match your real expertise level in your “shared interest.” For instance, if you want to convince a chemist to reveal a patented chemical formula but aren’t a scientist yourself, posing as a fellow chemist is risky. But you could be a “student” who admires their work. Accents and dialects are another good way to connect with people. These are not too difficult to learn with a keen ear and some good instructional audiotapes. Some accents can even make you instantly likeable, depending on your environment. In a training class offered by a sales organization, the author learned that 70 percent of Americans prefer to listen to someone with a British accent! But no matter what, remember that your pretext and identity should appear logical and natural.

People like to be liked, a fact social engineers know well. They also know that people who like you will do things to earn your affection. But how do you get complete strangers to like you immediately? Start by making the target feel like you have good chemistry and rapport. One way to do this is by making the conversation about the target. After all, everyone loves to talk about themselves! Be mindful of your body language. By matching their movements, you subtly demonstrate that the two of you have chemistry. For example, if they cross their arms, do the same. You can also build rapport by matching your appearance to theirs. If you’re talking to a company manager, for example, you’ll want to walk the walk and talk the talk: wear a suit and tie, and speak like they speak Once you’ve built a rapport, you can then use elicitation to influence targets to behave as you want them to because it makes sense or feels logical to them. To use elicitation effectively, it’s important to understand a few things about people: they want to be polite to strangers, they talk more when they’re praised and they respond kindly to someone who appears concerned about them. Social engineers use this knowledge to talk anyone into complying with their suggestions. If you know your target is a parent, for example, create a pretext that includes a child. You could tell a receptionist that you had a job interview scheduled, but that your daughter accidentally spilled coffee on your briefcase this morning and you didn’t have time to print out another CV. You could note that, judging from the picture on his desk, his kid must be about the same age as your daughter. Perhaps he could help you out and print another CV for you? That’s when you can hand him a USB stick with spyware in it.

Think of all the white lies you’ve ever told. Do you think people knew you were lying? Probably. But it’s not because they were listening carefully to the logic of your fib; rather, they probably read it on your face. Our faces tend to reveal our emotions involuntarily. These microexpressions flash by in less than a second, but are nonetheless unmistakable. Microexpressions are universal; people reveal their emotions in their faces in the same way, regardless of their cultural background. For example, a genuine smile triggers the muscles around the eyes called the orbicularis oculi, which, according to French neurologist Duchenne de Boulogne, can’t be moved voluntarily. While law enforcement agencies read microexpressions to detect deceit, social engineers use this information to manipulate their targets.

For example, one of the author’s colleagues, Tom, noticed that his target would smile when talking about something positive. Tom started clicking a pen every time his target talked about positive things until the target began associating the click with positive emotions. Eventually, Tom clicked the pen when his target mentioned something negative. This caused him to smile, and then feel embarrassed at having smiled at something negative. But noticeable emotions go well beyond smiles. The author identifies seven types of universal emotions, all of which have their own microexpressions: Anger makes the eyebrows slant down and together, and the lips stretch outward. Disgust wrinkles the nose and raises the upper lip. Contempt also wrinkles the nose, but raises only one side of the lip. Fear causes us to open our eyes wide, with eyebrows bunched and lips stretched outward. Surprise raises the eyebrows and drops the jaw. Sadness likewise drops the jaw, pulls the lips down and squints the eyes. Finally, happiness broadens the eyes, raises the cheeks and produces a smile. Reading your target’s microexpression can help you identify their emotions and give you the information you need to respond appropriately.

Con artists are well known for their ability to talk anyone into doing anything. Many chalk this up to a natural born talent for sweet talking, but there is an actual science behind it. In this blink, we’ll examine one such science: Neuro-linguistic programming. Neuro-linguistic programming, or NLP, is a mode of communication that focuses on the way people think and experience the world. Richard Bandler and John Grinder developed NLP in the 1970s in order to study the way language patterns affect behavior. NLP focuses on the concepts of state of mind, conscious/unconscious relationships and the filters we use when making sense of reality. Salespeople and company managers learn NLP to develop self-awareness and effective ways to communicate. For example, NLP training scripts can help a salesperson to get a customer talking about their goals and dreams. The salesperson, with this new information, can then position their product in the conversation as a means to fulfill those dreams. Social engineers use NLP to covertly insert commands into their speech without alerting the target. In NLP, this skill is called ultimate voice. One way to use ultimate voice is by emphasizing the words you want the target to focus on by using your tone of voice. For example, we normally end questions like “Don’t you agree?” with an upward tone. However, if you say “agree” with a downward tone instead, it sounds like a command. Another way is to hide commanding phrases in sentences structured like soft suggestions by emphasizing certain words and commanding the listener’s subconscious. For example, when you ask “So what do you want to eat for lunch today, steak or something else?” your emphasis on “you want to eat steak” will influence the listener’s decision. These are sophisticated psychological methods that require training and practice. But if you take the time to learn them, you can greatly influence people simply by talking to them in the right way.

Sometimes social engineers are confronted with a challenge that requires more than just sweet talk: locks. But no lock, be it physical or digital (in other words, password protection), is insurmountable. If you want to open up a physical lock to access personal files or other data, you’ll first need certain tools. A lock is made of uneven pin tumblers, which the key aligns in an even line. Once the tumblers are aligned, the key can turn and unlock the door. Lock picks do the same thing, except that you have to push each tumbler into position one by one. To accomplish this, you only need two tools: a tension wrench, which is just a flat piece of metal that keeps pressure on the bottom of the lock, and a pick. It’s easy: first, insert the tension wrench. Then, you use your pick, a long piece of metal with a curve at the end, to line up the tumblers. Once the tumblers are aligned, you’ll hear a click, and voilà! Passwords are a little different. Luckily for social engineers, most people’s passwords are very weak. How weak? Well, in 2009 a hacker known as Tonu copied a social media site using a web address that had recently been dropped. Out of the 734,000 people who logged into this fake site, 30,000 used their first name as their password, and 17,601 users used the password 123456. Of course, if your target’s password is something other than their first name, you’ll need to try something else. Passwords can be cracked using free software, like Common User Password Profiler, or CUPP. When the author conducts security training exercises, he asks a volunteer to type a password they think is secure into a computer. Using software like CUPP, he’s able to crack it in under two minutes. CUPP takes all the target’s personal information, like nicknames, birthdays and spouses’ names, and creates a file of probable passwords. Weak passwords can be cracked in a few days or even less.

Social engineers combine all these tactics and tools to manipulate their targets without them ever being the wiser. The best way to protect ourselves is to know their methods and how they work. If you don’t want to get duped, it’s important to educate yourself and your personnel about social engineering tactics. The more you know about elicitation, body language and so on, the better equipped you will be to recognize when someone is trying to use these tactics on you. Remember, any and all information can be valuable to an attacker. So be careful what you share with unauthorized people. Be especially aware of attackers posing as a distraught person asking for help. In one case, a social engineer was able to compromise an antivirus company by calling their customer service line and asking if the software was preventing him from accessing a website designed to compromise the company. The representative tried several times to explain to him that he simply wasn’t permitted to open the website in question, but the attacker pleaded that he go to the website to make sure anyway. Out of his desire to help, the representative ended up opening the web address and compromising the antivirus company. To avoid falling victim to social engineers, set up security protocols for all staff and follow them at all times. One way might be to develop a standard script that employees use to react to a suspicious person asking for information. It could be as simple as asking for their name and ID number and the name of the project they are inquiring about before answering any questions. If they can’t provide any of this information, then ask them to contact the company via e-mail and terminate the conversation. Of course, these are just ideas. You’ll have to develop your own system that is right for you and your company.