Monthly Newsletter

September 2016 | Social Engineering

In This Issue

Other Interesting Links

- Best Defenses
- Life Hacker
- YouTube
- Social-Engineer

Contact Us

Cyber Security website

Introduction

Social Engineering
The clever **manipulation** of the natural human tendency to trust!

Social Engineering is a non-technical psychological manipulation of a person (or people) designed to gather confidential information by breaking normal security procedures. It is used to gather information about the person and/or where they work. The information gathered is commonly used for identity theft, fraud, and/or to compromise computer systems.

A good Social Engineer can also be thought of as a good "con man" or interrogator. Social Engineers will research their victim(s) and decide what tactic will likely work best to get the information they desire. Traditional techniques appeal to individual vanity or greed; however the most successful attacks exploit the natural human tendency to be helpful. This is especially effective when targeting people in service related positions.

Social Engineering Techniques

The Washington Post reported in one of their March 2000 articles that the well-known hacker Kevin Mitnich said, "in more than half of his successful network exploits he gained information about the network, sometimes including access to the network, through social engineering." The weakest link in any security system is the human element.

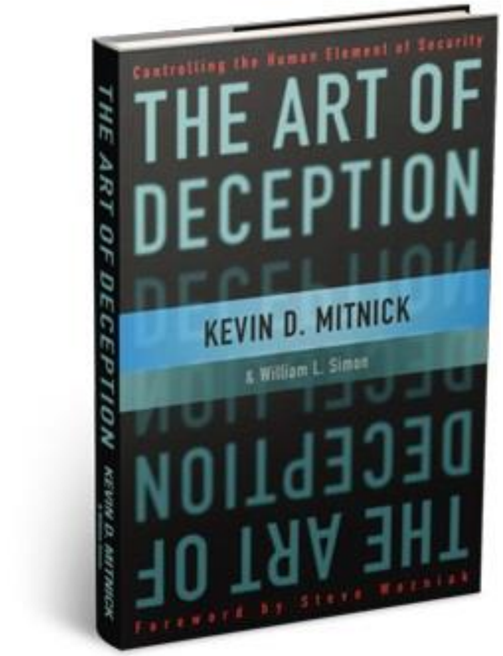
All social engineering techniques are based on attributes of the human decision-making process known as **cognitive biases**. The term cognitive bias refers to a systematic pattern of deviation from the norm or rationality in judgment, whereby inferences about other people and situations may be drawn in an illogical fashion. Individuals create their own "subjective social reality" from their perception of the input. In simpler terms, an attacker will devise a scheme that seems legitimate but in reality is designed to cause the victim to deviate from what they would normally do and what they know is the right procedure.

The most common type of social engineering happens over the phone, but is not the only type. Individuals posing as exterminators, fire marshals, technicians and janitors, delivery people, etc, are also forms of social engineering. Attackers will pose as these people because they are either overlooked or considered experts who should be left alone to do whatever it is they do. Exterminators, fire marshals, janitors, etc, are often let into areas without verifying their credentials, and often are left unsupervised while in those areas. And it isn't uncommon for a "technician" to be left unsupervised for hours at a time around computers. Thus, providing them the perfect opportunity to steal company secrets.

How is it done?

There are multiple examples of social engineering. Below are a few:

An individual walks into a building and posts an official-looking announcement on the company bulletin board saying the number for the help desk has changed. Employees see this and call the "new number". The person who answers asks for the callers ID and login password to "verify" the person. Since the employee is calling what they think is an official number for the company help desk, the employee provides the information even though they know the help desk should not be asking for their login password. This provides the attacker with valid information they can then use to contact the real helpdesk and have complete access to whatever the employee has access to.



A woman calls a credit card company. In the background there is a baby crying. She says that she is needing to get some information because her husband is out of town and they are trying to buy a house. If she can't provide the information immediately the deal will fall through. She has some basic information but seems flustered and can't remember everything. The whole time the person on the phone can hear a baby crying. The woman apologizes about the baby explaining that it has been like this since early this morning. The person on the other end of the phone can sympothize and wants to help the poor woman, so shortcuts are taken and procedures bypassed to help her out. Account information is provided to the woman as well as passwords changed and new contact information provided. Thus locking the legitimate user out of the account and giving the caller complete access.

An attacker contacts a target on a social media site (Facebook, LinkedIn, Twitter, Tumblr, Pinterest, etc.) and start a conversation. Slowly and gradually the attacker gains the trust of the victim and then uses what they have learned to get access to sensitive information like the victims passwords or bank account information.

There are numerous examples that can be provided, but the best way to truly understand is to watch it happening. This YouTube address will show you an example of how it is done (**https://www.youtube.com/watch?v=bjYhmX_OUQQ**). I suggest copying the link down and watching it at home if you aren't able to watch it on the TLE network.

How to protect against Social Engineering

There is no singular foolproof way to protect against Social Engineering. However, there are some things that can help.

1) Education. The more you know the safer you are. **Social-Engineer.org** provides a number of information resources on social engineering attacks. The two most effective attacks used are posing as an internal employee or posing as someone hired to perform an audit or take a survey.

2) Be aware of the information you're releasing. This applies to social media as well as in person or over the phone. Social media is often the first thing looked at when researching for a social engineering attack.

3) Determine which of your assets are most valuable to criminals. Knowing what you have access to will help you be on guard for attempts to get it from you.

4) Awareness training. Security awareness training is always a good thing. ☺

5) Keep your software up to date. Your work computers are managed and kept up to date. But are your personal computers up to date? Unpatched and out of date programs and anti-virus software makes you vulnerable. Also be wary of anyone asking you about what version of software you are running or if you have the ability to update your software.

Dumpster diving

- Digging through trash at corporations in search of sensitive data.

6) Security is everyone's business. We are all in the security business no matter what division you are in. Keeping our data, our employees and the citizens of Texas safe are part of our mission statement.

7) When asked for information, consider whether the person you're talking to deserves the information they're asking about. If you aren't sure, verify they are authorized to have the information before giving it to them. In most cases, someone you are talking to does not need to know what operating system you are using, what programs you have on your computer, or even what company handles trash collecting.

8) Watch for questions that don't fit the pretext. If a person asks a question that does not fit the persona they present, it should set off alarm bells. A sudden sense of pressure or urgency is often a sign they are trying to get unauthorized information.

9) If on the phone answering questions, consider putting the caller on hold for a minute. While this might not be the best customer service thing to do, it does break up the rhythm that a social engineer has going. Putting someone on hold also gives you time to collect your thoughts and ask your supervisor if this seems legitimate or not.

10) Stick to your guns. If you get the feeling that someone is fishing for information they shouldn't have, then you are probably correct.

Upcoming Cyber Projects

Online mandatory yearly cyber/CJIS awareness training is in the process of being pushed out.

- All employees listed in the HR database as working in an IT field have received the training information.
- All other employees should be seeing an email later today (1 Sept 2016) with instructions on how to take the training. You will have two (2) months to complete the training.

The online cyber/CJIS awareness training is a yearly requirement. Sometime after the beginning of the new year all accounts will be reset and you will be notified on when you have to have the training completed.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber**".

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.