What is Social Engineering?

Social engineering, as defined by Wikipedia in the context of security, is the art of manipulating people into performing actions or divulging confidential information.

While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

"Social engineering" as an act of psychological manipulation had previously been associated with the social sciences, but its usage has caught on among computer professionals.

Everyone in an organization is responsible for an organization’s data integrity. Human behavior is always the weakest link in a security program. A company can spend millions of dollars on all kinds of security equipment, but it only takes one person for a company’s security to be compromised.

Each of us is responsible for understanding and preventing Social Engineering Attacks.

How is Social Engineering accomplished?

Social engineering is accomplished through various methods including dumpster diving and persuasion. Methods of social engineering include:

- Telephone – Using telephones to contact individuals of a company to persuade them to divulge in confidential information or lead them to an internet site in the pretense of providing support. Many of these sites are designed to download malicious applications to your computer which can compromise your 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

- 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

- 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

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.

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. **Never give your password to anyone.**
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft (see Preventing and Responding to Identity Theft for more information).
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

How can I prevent Social Engineering?

There are a variety of best practices that each of us can follow to prevent a social engineering attack. These practices include:

- Disposal: Old hard drives should be adequately destroyed (physically) and optical media can also be shredded.

- Mobile Devices: Laptops, smartphones and other devices that access your personal information, email and social networking accounts should always be protected with secure passwords and codes.

- Be suspicious: Be suspicious of unsolicited phone calls or emails in which your personal information is being requested. Financial institutions will not call you for your account number or pin number or ask for personal information “out of the blue”. Similarly, a security company is very unlikely to call in order to warn you of problems with your computer.

Treat all calls as a scam, be suspicious and don’t compromise your PC or buy what they’re selling!