SOCIAL ENGINEERING ATTACK

Objectives

- Understand the principles of social engineering
- Define the goals of social engineering
- Recognize the signs of social engineering
- Identify ways to protect yourself from social engineering

What is Social Engineering

1. At its core it is manipulating a person into knowingly or unknowingly giving up information; essentially 'hacking' into a person to steal valuable information.

   - Psychological manipulation
   - Trickery or Deception for the purpose of information gathering

What is Social Engineering

2. It is a way for criminals to gain access to information systems. The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information

What is Social Engineering

3. Social engineering is one of the most effective routes to stealing confidential data from organizations, according to Siemens Enterprise Communications, based in Germany. In a recent Siemens test, 85 percent of office workers were duped by engineering.

"Most employees are utterly unaware that they are being manipulated," says Colin Greenlees, security and counter-fraud consultant at Siemens.

What are they looking for

- Obtaining simple information such as your pet's name, where you're from, the places you've visited; information that you'd give out freely to your friends.
  - Think of yourself as a walking computer, full of valuable information about yourself. You've got a name, address, and valuables. Now categorize those items like a business does. Personally identifiable data, financial information, cardholder data, health insurance data, credit reporting data, and so on…

What are they looking for

- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
  - ✓ What's the name of your first pet?
  - ✓ What is your maiden name?
  - ✓ When was your mother/father born?
  - ✓ Where were you born?

Do these sound familiar?

Tactics

1. Pretexting – Creating a fake scenario
2. Phishing – Send out bait to fool victims into giving away their information
3. Fake Websites – Molded to look like the real thing. Log in with real credentials that are now compromised
4. Fake Pop-up – Pops up in front of real web site to obtain user credentials

Protecting Yourself

A security aware culture can help employees identify and repel social engineering attacks

- Recognize inappropriate requests for information
- Take ownership for corporate security
- Understand risk and impact of security breeches
- Social engineering attacks are personal
- Password management
- Two factor authentication
- Physical security
- Understand what information you are putting on the Web for targeting at social network sites

Google **Twitter**

MySpace **Facebook**

Personal Blogs **LinkedIn**

Protecting Yourself

1. Network defenses to repel virus
   - Virus protection (McAfee, Norton, Symantec, etc…)
   - Email attachment scanning
   - Firewalls, etc…
2. Organizations must decide what information is sensitive
3. Security must be periodically tested
4. Contact your security office immediately if you have any concerns at work