Social Engineering

Learn ways to recognize and avoid social engineering manipulation techniques.

1. How Do Social Engineering Attacks Work?

Social engineering refers to methods and techniques used by scammers to trick you into doing something questionable, such as giving away your personal information or sending money. Social engineering has been around for centuries and has just adapted to the internet age.

The main aim of social engineering is to manipulate you. Here is how a social engineering attack works:

- The attacker identifies a victim and uncovers information about them
- They then decide what sort of social engineering technique to use
- The attacker engages the victim and uses different techniques to manipulate them
- The attacker convinces the victim to give away their information or money
- The attacker concludes the charade and disappears

2. What Are Some Common Social Engineering Techniques?

Social engineering attacks try to manipulate you. Here are some common tactics and techniques:

- **Baiting:** These attacks try to lure victims in with false promises of things like free downloads, free services, or prizes
- **Scareware:** This often takes the form of pop-up ads with alarming messages and tries to frighten you into giving away your information or data
- **Phishing Scams:** These very common forms of social engineering manipulate your emotions over text or email and try to convince you to click or download something, or send along information or money. Phishing scams often use urgency as a trigger but they can also try to scare you, play upon your sympathy, or entice you with a prize
- **Pretexting:** With this technique, an attacker might impersonate someone you trust or an authority figure in order to gain your trust and get you to give away your information

- **Spear phishing:** This type of phishing scam is targeted at one person or a small group of people and often appears to come from someone they know.

Note that social engineering can happen offline as well via spam phone calls or in-person. For example, criminals might dumpster dive to obtain your personal information from the trash or try to gain access to a building in order to steal data or technology.

3. What Are Signs of Social Engineering?

Be alert to the following:

- The request or message is unexpected
- The request is very urgent
- You feel like you're being pressured to do something quickly
- The offer seems too good to be true
- You notice odd spelling or grammar errors
- The message seems scary and threatening

Remember, social engineers are trying to manipulate you and to get you to act without pausing, reflecting, and thinking critically. Don't be pressured into doing something!

4. How Can You Avoid Social Engineering?

- Be alert to the techniques that these scammers use
- Investigate the request and don't reply right away or directly engage
- Consider your own emotional response - do you feel rushed or threatened?
- Practice data minimization and be mindful of what you put out on the Internet and make available to others
- Practice password hygiene by using multi-factor authentication and a password manager
- Don't open attachments or click on links from unknown sources
- Manage your account security settings and clean up your social media profiles to make sure there isn't private or sensitive information out there

- Keep your devices updated and install the latest security updates
- Destroy sensitive documents
- Keep your data backed up in case of a hack or a ransomware attack

5. Make a Plan

Consider things you can do to better secure your accounts and information and avoid falling for social engineering. Use this space to reflect: