Social Engineering

In This Module

- What is social engineering, and how does it work?
- What are signs of techniques of social engineering?
- How can you avoid and protect yourself against social engineering?

Social Engineering

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

Discussion

What are some manipulation techniques that scammers use?

Social Engineering Attacks

Here's playbook for a standard social engineering attack. An attacker will:

- Identify a victim and uncover information about them
- Decide what sort of social engineering technique to use
- Engage the victim, use different techniques to manipulate and fool them
- Convince the victim to give away their information or money
- Conclude the charade and disappear

Principles of Persuasion

Dr. Robert Cialdini has 7 Principles of Persuasion that appear in most social engineering efforts:

- **Reciprocity:** Someone gives you a gift and you want to reciprocate
- **Scarcity:** Scams with limited time offers and deals
- **Authority:** Scams related to your boss needing you to do something
- **Consistency:** Scams that appeal to your desire to keep your word
- **Liking:** Scams that appeal to positive feelings for a person or cause
- **Consensus:** Scams that appeal to your desire to follow the crowd

Social Engineering Targets

Social engineers can find potential victims by:

- Getting information on the dark web from data breaches
- Obtaining information from account hacks
- Gathering information about you from your online activities
- Sifting through physical mail and documents to find information
- Reviewing public records

Common Types of Social Engineering

- **Baiting:** These attacks lure victims in with false promises of things like free services or prizes
- **Scareware:** This often takes the form of pop-up ads with alarming messages
- **Pretexting:** An attacker might impersonate someone you trust or an authority figure in order to gain your trust

Common Types of Social Engineering

Phishing scams are very common forms of social engineering that manipulate your emotions over text or email and try to convince you to click or download something, or send along information or money.

Common Types of Social Engineering

- **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
- **Spam calls:** Spam callers use use various manipulative techniques, including baiting, pretexting, and phishing to fool you

Signs of Social Engineering

- 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

Social Engineering Manipulation

Remember, social engineering is trying to manipulate you. Don’t feel pressured into acting hastily or doing something without pausing to reflect and think.

Avoiding Social Engineering

- Don’t open attachments or click on links from unknown sources
- Investigate what you are being asked
- Don’t engage or respond directly
- Consider how the request makes you feel: Do you feel rushed, scared, or harassed?

Avoiding Social Engineering

- 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

Avoiding Social Engineering

- 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

Activity

What are some additional ways that you can avoid falling prey to social engineering?

Takeaways

- Social engineering aims to manipulate you into making poor decisions or into performing questionable actions
- Being aware of the techniques that are used, and the common forms social engineering can take, can help you be alert and aware
- Remember, managing your own data security can help you avoid becoming the target of a social engineering attack

Resources

Kaspersky's Guide to Avoiding Social Engineering Attacks (link)

"How to Spot—and Avoid—Dark Patterns on the Web" from *Wired* (link)

Digital Guardian's Guide to Social Engineering Attacks (link)

Questions?

NYC Digital Safety

Privacy & Security