Armaan Shamsaasef

Other Social Engineering Attacks

Other Social Engineering Attacks - SY0-701 - 2.2

Definition: Manipulating people into performing actions or divulging confidential information by exploiting human psychology.

1. Principles of Social Engineering

- Authority: People are more likely to comply with requests from someone perceived as an authority figure (e.g., a manager, IT support, police).
- Intimidation: Using threats or fear to pressure someone into acting quickly without thinking.
- Consensus/Social Proof: People are more likely to do something if they believe others are also doing it.
- Scarcity: Creating a false sense of urgency or limited availability (e.g., "This offer expires in one hour!").
- Familiarity/Liking: People are more trusting of those they like or feel a connection with.
- Trust: Exploiting an existing relationship or the human tendency to trust.
- Urgency: Forcing rapid action by presenting a time-sensitive problem, preventing the victim from thinking critically.

2. Specific Attack Types

A. Dumpster Diving

- Description: Retrieving sensitive information from discarded trash.
- Goal: Find documents containing passwords, network diagrams, customer lists, or other confidential data.
- Example: An attacker finds a discarded company memo with a list of internal usernames and departmental phone numbers, which they use for a subsequent spear-phishing campaign.

B. Shoulder Surfing

- Description: Directly observing someone's screen or keyboard to capture information.
- Goal: To steal passwords, PINs, or other sensitive data entered by the user.
- Example: Watching someone type their password at a coffee shop or looking at their screen on an airplane to see confidential documents.

C. Hoaxes

- Description: A false message designed to trick users into unnecessary actions, often spread by well-meaning people.
- Goal: To waste time and resources, create panic, or serve as a delivery mechanism for other attacks.
- Example: An email chain letter warning of a non-existent computer virus, instructing users to delete a critical system file, which then causes their computer to malfunction.

D. Typo Squatting / URL Hijacking

- Description: Registering domain names that are common misspellings of popular websites.
- Goal: To capture traffic from users who make a typo when entering a web address. These sites may host phishing pages, ads, or malware.
- Example: Registering `goolge.com` or `amaz0n.com` to trick users into visiting a malicious copycat site.

E. Invoice Scams

- Description: Sending a fake invoice for a product or service that was never rendered.
- Goal: To trick accounts payable departments into making a payment to the attacker's bank account.
- Example: A company receives a fake invoice from a non-existent "IT Services LLC" for "annual software licensing," hoping it will be paid without verification.

F. Credential Harvesting

- Description: The broad process of collecting usernames and passwords.
- Goal: To use or sell the stolen credentials for unauthorized access to systems.

- Example: Using a phishing email that links to a fake Microsoft 365 login page to steal corporate usernames and passwords.

G. Reconnaissance

- Description: The information-gathering phase that occurs *before* a social engineering attack.
- Goal: To learn details about the target (e.g., names, job titles, projects, vendors) to make the subsequent attack more convincing.
- Example: An attacker browses a company's "About Us" page and employee LinkedIn profiles to gather names and roles for a targeted spear-phishing email.

H. Influence Campaigns

- Description: A large-scale, organized effort to shape public opinion or manipulate behavior, often over social media.
- Goal: To sow discord, influence elections, or damage an organization's reputation.
- Example: Using a network of automated bots and fake accounts to spread disinformation about a political candidate or a company's products.

Summary

- Social engineering exploits human psychology (authority, urgency, trust) rather than technical vulnerabilities.
- Attacks can be physical (dumpster diving, shoulder surfing), digital (typo squatting, hoaxes), or psychological (influence campaigns).
- Reconnaissance is a critical first step that makes other attacks more effective.
- The goal is often to gain information (credentials, data) or financial gain (invoice scams).