# Social Engineering

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 5.6 - Given a scenario, you must be able to implement security awareness practices

- **Social Engineering**
  - *Social Engineering*
    - Manipulative strategy exploiting human psychology for unauthorized access to systems, data, or physical spaces
  - Motivational Triggers
    - Used by Social Engineers
      - Familiarity and Likability
      - Consensus and Social Proof
      - Authority and Intimidation
      - Scarcity and Urgency
  - Social Engineering Techniques
    - *Impersonation*
      - Pretending to be someone else
      - Includes brand impersonation, typo-squatting, and watering hole attacks
    - *Pretexting*
      - Creating a fabricated scenario to manipulate targets
      - Impersonating trusted figures to gain trust

- Types of Phishing Attacks
  - Phishing
  - Vishing
  - Smishing
  - Spear Phishing
  - Whaling
  - Business Email Compromise
- *Frauds and Scams*
  - Deceptive practices to deceive people into parting with money or valuable information
  - Identifying and training against frauds and scams
- *Influence Campaigns*
  - Spreading misinformation and disinformation, impacting politics, economics, etc.
- Other Social Engineering Attacks
  - Diversion Theft
  - Hoaxes
  - Shoulder Surfing
  - Dumpster Diving
  - Eavesdropping
  - Baiting
  - Piggybacking
  - Tailgating

- **Motivational Triggers**
    - Six main types of motivational triggers that social engineers use
        - Authority
            - Most people are willing to comply and do what you tell them to do if they believe it is coming from somebody who is in a position of authority to make that request
        - Urgency
            - Compelling sense of immediacy or time-sensitivity that drives individuals to act swiftly or prioritize certain actions
        - Social Proof
            - Psychological phenomenon where individuals look to the behaviors and actions of others to determine their own decisions or actions in similar situations
        - Scarcity
            - Psychological pressure people feel when they believe a product, opportunity, or resource is limited or in short supply
        - Likability
            - Most people want to interact with people they like, and social engineers realize this
            - Can be
                - Sexual attraction
                - Pretending to be a friend
                - Common interest
        - Fear
            - These types of attacks generally are focused on "if you don't do what I tell you, then this bad thing is going to happen to you”

- **Impersonation**
    - Four main forms of impersonation used by attackers
        - *Impersonation*
            - Attack where an adversary assumes the identity of another person to gain unauthorized access to resources or steal sensitive data
            - Requires the attacker to collect information about the organization so that they can more easily earn the trust of their targeted users
            - Attackers provide details to help make the lies and the impersonation more believable to a potential victim
            - Consequences
                - Unauthorized access
                - Disruption of services
                - Complete system takeover
            - To mitigate against these types of attacks, organizations must provide security awareness training to their employees on a regular basis so that they remain vigilant against future attacks
        - *Brand Impersonation*
            - More specific form of impersonation where an attacker pretends to represent a legitimate company or brand
            - Attackers use the brand's logos, language, and information to create deceptive communications or website
            - To protect against brand impersonation, organizations should do the following
                - Educate their users about these types of threats
                - Use secure email gateways to filter out phishing emails

        - Regularly monitor their brand's online presence to detect any fraudulent activities as soon as they occur
- *Typosquatting*
    - Also known as URL hijacking or cybersquatting
    - Form of cyber attack where an attacker will register a domain name that is similar to a popular website but contain some kind of common typographical errors
    - To combat typosquatting, organizations will often do the following
        - Register common misspellings of their own domain names
        - Use services that monitor for similar domain registrations
        - Conduct user security awareness training to educate users about the risks of typosquatting
- *Watering Hole Attacks*
    - Targeted form of cyber attack where attackers compromise a specific website or service that their target is known to use
    - The term is a metaphor for a naturally occurring phenomenon
        - In the world of cybersecurity, the "watering hole" the attacker chooses to utilize will usually be a trusted website or online service
    - To mitigate watering hole attacks, organizations should do the following
        - Keep their systems and software updated
        - Use threat intelligence services to stay informed about new threats
        - Employ advanced malware detection and prevention tools

- **Pretexting**
  - *Pretexting*
    - Gives some amount of information that seems true so that the victim will give more information
  - Mitigation involves training the employees not to fall for pretext and not to fill in the gaps for people when they are calling

- **Phishing Attacks**
  - Different Types of Phishing Attacks
    - *Phishing*
      - Sending fraudulent emails that appear to be from reputable sources with the aim of convincing individuals to reveal personal information, such as passwords and credit card numbers
    - *Spear Phishing*
      - More targeted form of phishing that is used by cybercriminals who are more tightly focused on a specific group of individuals or organizations
      - Has a higher success rate
    - *Whaling*
      - Form of spear phishing that targets high-profile individuals, like CEOs or CFOs
      - Attacker isn't trying to catch the little fish in an organization, but instead they want to catch one of the executives, board members, or higher level managers in the company since the rewards are potentially much greater
      - Often used as an initial step to compromise an executive's account for subsequent attacks within their organization

- *Business Email Compromise (BEC)*
  - Sophisticated type of phishing attack that usually targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious actions on behalf of the attacker
  - Taking over a legitimate business email accounts through social engineering or cyber intrusion techniques to conduct unauthorized fund transfers, redirect payments, or steal sensitive information
- *Vishing (Voice Phishing)*
  - Attacker tricks their victims into sharing personal or financial information over the phone
- *Smishing (SMS Phishing)*
  - Involves the use of text messages to trick individuals into providing their personal information

- **Preventing Phishing Attacks**
  - By implementing the right strategies and providing user security awareness training, the threat of a successful phishing campaign against your organization can be mitigated effectively
  - *Anti-phishing Campaign*
    - Essential user security awareness training tool that can be used to educate individuals about the risks of phishing and how to best identify potential phishing attempts
    - Should offer remedial training for users who fell victim to simulated phishing emails

- To help prevent phishing your organization should regularly conduct user security awareness training that contains coverage of the various phishing techniques
  - Phishing
  - Spear Phishing
  - Whaling
  - Business Email Compromise
  - Vishing
  - Smishing
  - Along with other relevant cyber threats and attacks that may affect your organization
- There are some commonly used key indicators that are associated with phishing attacks
  - Urgency
    - Phishing emails often create a sense of urgency by prompting the recipient to act immediately
  - Unusual Requests
    - If your receive an email requesting sensitive information, such as passwords or credit card numbers, you should treat these emails with a lot of suspicion
  - Mismatched URLs
    - When you are looking at an HTML-based email, the words you are reading are called the display text, but the underlying URL of the weblink could be set to anything you want
    - To check if the text-based link matches the underlying URL, you should always hover your mouse over the link in the email for a few seconds and this will reveal the actual URL that the link is connected to

        - Strange Email Addresses
            - If the real email address and the displayed email address don't match, then the email should be treated as suspicious and possibly part of a phishing campaign
        - Poor Spelling or Grammar
            - If an email has a lot of "broken English", poor grammar, or numerous spelling errors, it is likely to be part of a phishing campaign
    - Mitigation
        - Training
        - Report suspicious messages to protect your organization from potential phishing attacks
        - Analyze the threat
        - Inform all users about the threat
            - If the phishing email was opened, conduct a quick investigation and triage the user's system
        - An organization should revise its security measures for every success phishing attack

- **Frauds and Scams**
    - *Fraud*
        - Wrongful or criminal deception that is intended to result in financial or personal gain for the attacker
        - One of the most common types of fraud that you will see online is known as identity fraud or identity theft
            - *Identity Fraud and Identity Theft*
                - Involves the use of another person's personal information without

their authorization to commit a crime or to deceive or defraud that other person or some other third party

- Difference between identity fraud and identity theft
  - In identity fraud, the attacker takes the victim's credit card number and charges items to the card
  - In identity theft, the attacker tries to fully assume the identity of their victim

- *Scams*
  - Fraudulent or deceptive act or operation
  - Most common scam is called the invoice scam
    - *Invoice Scam*
      - In which a person is tricked into paying for a fake invoice for a product or service that they did not actually order

- **Influence Campaigns**
  - *Influence Campaigns*
    - Coordinated efforts to affect public perception or behavior towards a particular cause, individual, or group
    - Are a powerful tool for shaping public opinion and behavior
    - Foster misinformation and disinformation
  - *Misinformation*
    - False or inaccurate information shared without harmful intent
  - *Disinformation*
    - Involves the deliberate creation and sharing of false information with the intent to deceive or mislead
  - Remember, misinformation and disinformation can have serious consequences because

they can undermine public trust in institutions, fuel social divisions, and even influence the outcomes of elections

- **Other Social Engineering Attacks**
  - Some of the common other social engineering attacks
    - *Diversion Theft*
      - Involves manipulating a situation or creating a distraction to steal valuable items or information
    - *Hoaxes*
      - Malicious deception that is often spread through social media, email, or other communication channels
      - Often paired with phishing attacks and impersonation attacks
      - To prevent hoaxes people must fact check and use good critical thinking skills
    - *Shoulder Surfing*
      - Involves looking over someone's shoulder to gather personal information
      - Includes the use of high powered cameras or closed-circuit television cameras to steal information from a distance
      - To prevent shoulder surfing, users must be aware of their surroundings when providing any sensitive information
    - *Dumpster Diving*
      - Involves searching through trash to find valuable information
      - Commonly used to find discarded documents containing personal or corporate information
      - Use clean desk and clean desktop policies

- *Eavesdropping*
  - Involves the process of secretly listening to private conversations
  - perpetrator intercepts the communication of parties without their knowledge
  - Prevent this by encrypting data in transit
- *Baiting*
  - Involves leaving a malware-infected physical device, like a USB drive, in a place where it will be found by a victim, who will then hopefully use the device to unknowingly install malware on their organization's computer system
  - To prevent baiting, train users to not use devices they find
- *Piggybacking and Tailgating*
  - Involve an unauthorized person following an authorized person into a secure area
  - *Tailgating*
    - Attacker attempts to follow an employee through an access control vestibule or access control point without their knowledge
  - *Piggybacking*
    - Involves an attacker convincing an authorized employee to let them into the facility by getting the authorized employee to swipe their own access badge and allow the attacker inside the facility