Security Awareness

Objective 5.6: Given a scenario, you must be able to implement security awareness practices

- **Security Awareness**
  - *Security Awareness*
    - Knowledge and understanding of security threats and mitigation measures
    - Goal
      - Equip individuals to recognize and respond to threats for data protection
    - Focus
      - Common threats, potential risks, best practices for secure digital interactions
  - *Insider Threats*
    - Security risk from individuals within an organization
    - Source
      - Employees, former employees, contractors, or business partners
    - Risk
      - Exploiting inside information intentionally or unintentionally
  - *Password Management*
    - Practices and tools for creating, storing, and managing passwords
    - Goal
      - Ensure strong, unique passwords; securely stored; reduces unauthorized access risk

- Social Engineering Attacks
  - Techniques
    - Maintaining situational awareness, avoiding shoulder surfing, eavesdropping
  - Prevention
    - Avoiding unauthorized media, cables, recognizing phone scams, maintaining operational security
- Policies and Handbooks
  - *Policies*
    - Formal guidelines defining organization operations and decisions
  - *Handbooks*
    - Comprehensive guides providing information, serving as references
- Remote and Hybrid Work Environments
  - *Remote Work*
    - Performing job functions outside the office using technology
  - *Hybrid Work*
    - Combining in-office and remote work for flexibility
- Creating a Culture of Security
  - Organizational mindset prioritizing security in daily tasks and decision-making
  - Characteristics
    - Continuous education
    - Proactive risk mitigation
    - Collective responsibility

- **Recognizing Insider Threats**
    - Recognizing Insider Threats
        - *Insider Threats*
            - Involve risks posed by individuals within an organization
        - Threats can be intentional or unintentional, arising from various personal factors
        - Training employees to recognize anomalous behavior is essential in addressing insider threats
    - Behavior Indicators
        - Altered State or Substance Abuse
            - Employees arriving at work intoxicated or hungover may indicate personal issues
            - Impaired judgment may lead to unintentional data disclosure or misconduct
            - Potential for coercion into making poor security decisions
        - Emotional Distress
            - Signs of depression, giving away personal possessions, or emotional turmoil
            - Emotional distress may lead to non-compliance with security protocols
            - Vulnerability to exploitation by malicious parties
        - Lifestyle Incongruences
            - Employees demonstrating a lifestyle inconsistent with their finances
            - Investigate cases where an employee's spending doesn't align with income
            - Discreet investigations to rule out illicit activities, theft, or information selling

        - Financial Struggles
            - Employees under financial stress may express financial woes to coworkers
            - Financial pressures can make individuals susceptible to bribery or data selling
            - Organizations should have policies in place for handling such scenarios, like financial counseling or monitoring for unusual data access
    - Building a Robust Insider Threat Program
        - Establish an insider threat program to create a security culture
        - Encourage employees to report suspicious activities
        - Provide training to recognize warning signs
        - Implement policies that support mental health and financial well-being
        - Ensure fair and confidential investigation processes
        - Employ user activity monitoring tools to detect anomalous behavior while respecting employee privacy

- **Password Managers**
    - *Password Manager*
        - Specialized tool, plugin, or extension used with web browsers
        - Helps users securely store and manage various usernames and passwords for different websites
    - Password Reuse Risks
        - Reusing passwords across multiple websites is dangerous
        - Breaches of one website can expose reused passwords
        - Attackers use known credentials to compromise other sites
        - Most usernames are email addresses, further increasing risk

- Built-In vs. Third-Party Password Managers
  - Many web browsers offer built-in password functionality
  - Third-party password managers like Bitwarden, Dashlane, LastPass, or OnePass are often preferred for enhanced security
- Advantages of Password Managers
  - Securely store and manage multiple credentials
  - Prevent password reuse and enhance security
  - Simplify password management with a single master password
  - Encrypt and protect all stored passwords
  - Automatically fill in login details for easy access
  - Organize and manage numerous passwords efficiently

- **Avoiding Social Engineering**
  - *Social Engineering*
    - Involves deception to manipulate individuals into breaching security procedures
    - Attacks exploit human psychology and often appear innocent
    - Awareness and vigilance serve as the first line of defense against social engineering attacks
  - Maintaining Situational Awareness
    - *Situational Awareness*
      - Mindfulness about surroundings and actions
    - Essential to avoid social engineering attacks
    - Examples of social engineering threats
      - Shoulder surfing
      - Eavesdropping
    - Measures to counter threats

- Privacy screen protectors
- Secure discussions

- Piggybacking and Tailgating
  - Social engineers may try to enter secured premises by closely following authorized personnel
  - Use access control vestibules to restrict entry to one person at a time
  - Maintain situational awareness to prevent unauthorized access
- *Dumpster Diving*
  - Attackers sift through garbage for discarded information
  - Employees with situational awareness can spot such activities
  - Dispose of sensitive data securely to avoid being a victim of this attack
- *Operational Security (OPSEC)*
  - Protects critical information from being used by adversaries
  - Safeguard sensitive data, daily routines, and internal procedures
  - Discourage sharing seemingly innocuous details on social media or during personal interactions
- Technological Social Engineering Attacks
  - Baiting attacks use removable media devices (e.g., USB thumb drives) and charging cables
  - Picking up or connecting found devices can infect workstations or networks with malware
  - Carry your own charging cables and chargers to avoid untrusted ones
- Pressure Tactics
  - Social engineers may use a sense of urgency or fear to manipulate individuals
  - Urgent requests aim to bypass normal security protocols
  - People are more likely to make mistakes when rushed into action

- Proactive Culture of Security
  - Train employees regardless of their position in the company
  - Educate on recognizing phishing attempts, data privacy, and safe online behavior
  - Encourage employees to report suspicious activities
  - Conduct practical exercises, like simulated phishing attacks, to test and remediate employees' responses

- **Policy and Handbooks**
  - Policies and Handbooks
    - *Policy*
      - A system of principles and rules guiding decisions, ensuring compliance with legal and ethical standards
    - *Handbook*
      - A comprehensive guide providing detailed information on procedures, guidelines, and best practices
    - Policies and handbooks are living guidelines that shape behavior and decision-making in organizations
    - These documents vary between organizations based on industry, needs, and use cases
    - Importance of not just reading but understanding the policies and handbooks
  - Scope of Policies and Handbooks
    - Cover various aspects in an organization, e.g., data protection, remote work, technology use, conflicts of interest
    - Different handbooks for different aspects, e.g., Employee Handbook, Training Handbook, Compliance Handbook

- Data Destruction Policy Example
  - Some policies may define rules for data disposal, e.g., shredding
  - Color-coded paper for document classification
  - Shredding of sensitive documents to prevent data breaches
- Remote Work and Data Protection
  - Organizations may have strict guidelines regarding remote work
  - Policies cover physical files and digital files that leave the office
  - Restrictions on what can be taken home or worked on remotely
- Policy Guidance for Daily Responsibilities
  - Provide guidance on handling various situations, e.g., data breaches, reporting suspicious activity
  - Ensures employees know how to respond to specific scenarios
- Policy and Handbook Updates
  - Policies and handbooks should be reviewed at least annually
  - Updates to reflect changing cybersecurity landscape
  - Employee awareness of policy updates and significant changes is crucial
- Human Judgment and Culture of Security
  - Policies and handbooks may not cover every scenario
  - Employees should understand the "why" behind the policies to make judgment calls
  - Creating a culture of security involves reporting gaps and fostering a secure environment
- Importance of Employee Involvement
  - Encourage employees to bring up concerns and questions
  - Open communication with management and leadership teams
  - Collective responsibility in promoting a secure organization culture

- **Remote and Hybrid Work Environments**
  - *Remote Work*
    - Employees work outside the traditional office (e.g., from home, coffee shops, or while traveling)
  - *Hybrid Work*
    - Combines traditional office work with remote work opportunities
  - Security Challenges
    - Increased risk due to lack of physical security controls outside the office
    - Data transmitted over public and private networks can be exposed to malicious attackers
    - Home and public networks have weaker security controls
    - Potential for cyberattacks, eavesdropping, and data breaches
    - Increased risk of device loss or theft
  - Addressing Security Challenges
    - Establish comprehensive policies for remote work
    - Emphasize the use of secure connections like VPN for data access
    - Implement multi-factor authentication for added security
    - Provide cybersecurity training and awareness for employees
      - Encourage reporting of security incidents
    - Use company-issued devices with up-to-date security software
      - Define security measures for personally owned devices (BYOD)
    - Set up automated backups for data protection
    - Choose secure collaboration tools with end-to-end encryption and administrative controls
    - Maintain clear communication between cybersecurity team and remote

employees
    - Conduct regular security audits and feedback sessions

- **Creating a Culture of Security**
    - Importance of Security Culture
        - A culture of security is crucial for safeguarding an organization
        - Technical security solutions are ineffective if employees do not value security
    - Creating a Culture of Security
        - Involves integrating cybersecurity into the organization's ethos, behaviors, and decisions
        - Requirements
            - Organizational change management
            - Strategic planning
            - Execution
            - Monitoring
            - Reporting
        - Goal
            - Embed cybersecurity into every aspect of the organization to protect valuable information
    - Organizational Change Management
        - Recognizes the role of the human element in security
        - Emphasizes staff engagement and adherence to security policies and procedures
        - Begins with commitment from executive leadership
        - Communicates cybersecurity as a shared corporate responsibility
    - Development Phase
        - Involves developing specific and actionable security plans

- Allocates resources to support plans
- Create comprehensive policies
- Educate employees on threats,
- Establish guidelines for data handling
- Focuses on empowerment and employee confidence in recognizing and responding to threats

- Execution Phase
  - Ongoing process, not a one-time event
  - Includes rolling out policies, conducting training, and adapting to evolving security threats
  - Requires regular training updates, simulated cyberattacks, and consistent threat communication
- Reporting and Monitoring
  - Begin with initial monitoring after the rollout of a security program
  - Conduct recurring check-ins to maintain program integrity
  - Assessing employee compliance with security protocols
  - Identifying areas for improvement
  - Creating a culture of reporting suspicious activities
  - Establishing feedback loops to adapt based on insights from monitoring and reporting
- Benefits of Security Culture
  - Resilience against cyberattacks
  - Employee vigilance becomes inherent
  - Improved operations and trust-based reputation
  - Proactive security posture for future uncertainties