**Social Engineering Attacks**

Social engineering attacks trick people into giving away confidential information or performing actions that harm security. Social engineering manipulates human behaviour and trust.  
  
**Common Techniques**

1. **Pretexting**:
   * The attacker creates a fake story to get information. For example, pretending to be a company employee to ask for login details.
2. **Phishing**:
   * Fake emails or messages that look real try to get you to click on malicious links or share personal info. An email that seems to come from your bank asking you to verify your account.
3. **Spear Phishing**:
   * Its an attack where the message is personalized with specific details about the victim to make it more convincing.
4. **Baiting**:
   * Offering something appealing, like free software or prizes, to get the victim to download malware or give up sensitive information.
5. **Tailgating**:
   * Following someone into a secure area without proper authorization. For example, entering a building behind an employee to access restricted areas.

**Real-World Examples**

1. **Target Breach (2013)**:
   * Attackers used phishing to steal login credentials from a vendor, leading to a massive data breach at Target.
2. **Sony Pictures Hack (2014)**:
   * Spear phishing emails gained access to sensitive Sony data, causing major disruptions and leaks.
3. **Dropbox Phishing Scam (2016)**:
   * Fake emails tricked users into entering their Dropbox passwords on a fake site, exposing their files.

**How to Defend Against Social Engineering**

1. **Train Employees**:
   * Regularly educate employees about recognizing and avoiding social engineering attacks.
2. **Verify Requests**:
   * Always double-check requests for sensitive information by contacting the requester through a separate, known channel.
3. **Use Multi-Factor Authentication (MFA)**:
   * Add an extra layer of security by requiring additional verification steps beyond just passwords.
4. **Conduct Regular Security Audits**:
   * Regularly review security practices to find and fix potential vulnerabilities.
5. **Implement Strong Access Controls**:
   * Ensure physical security measures, such as access badges and security checks, are in place to prevent unauthorized entry.