SOCIAL ENGINEERING ATTACKS

Overview

Social engineering attacks trick people rather than exploiting technical flaws. Attackers manipulate trust, fear, or curiosity to gain sensitive information, access systems, or physical locations. These attacks rely on human behaviour, making them very effective.

Types of Social Engineering Attacks

1. **Phishing:** It is the most common social engineering attack where attackers impersonate trusted entities via email, messages, or fake websites to steal sensitive information like login credentials, credit card numbers, or personal data.

   How it works:

   - Attackers send convincing emails/messages that appear legitimate.
   - Victims click links or open attachments, entering confidential information.
   - Attackers use collected data for identity theft, financial fraud, or unauthorized access.

   Prevention: Use email filters, MFA, and train users to verify links. **Example:** Google & Facebook Scam (2013–2015) – fake invoices tricked companies into paying $100M.

2. **Vishing (Voice Phishing):** It uses phone calls instead of emails to trick victims into revealing sensitive data.

   How It Works

   - Attackers spoof phone numbers to appear official (bank/IT/hospital).
   - They create urgency: “Your account is blocked,” “Fraud detected.”
   - Victims are pressured into sharing OTPs, passwords, or financial info.
   - Attackers use the stolen data for fraud or account takeover.

   Prevention: Verify callers, avoid sharing info on unknown calls, and educate employees. **Example:** IRS Vishing Scam (USA) – victims paid or shared sensitive data after fake IRS calls.

3. **Smishing (SMS Phishing):** It involves fraudulent text messages designed to lure victims into clicking malicious links or revealing information.

How It Works

- Attackers send fake SMS alerts (bank updates, delivery failures, lottery wins).
- Victims click on malicious links or call fake support numbers.
- Credentials and data are stolen, or malware is installed.

Prevention: Avoid clicking unknown links, use anti-phishing tools, and verify messages.
Example: FedEx SMS Scam – fake "delivery failed" texts installed spyware.

4. **Pretexting:** It involves attackers creating a fabricated scenario or "pretext" to gain sensitive information or access. This could be posing as an employee, IT technician, or authority figure.

   How it works:

   - Attackers craft believable scenarios (e.g., "I'm from IT, I need your credentials to fix your account").
   - Victims provide passwords, personal details, or confidential information.
   - Attackers use the collected information to infiltrate systems or commit fraud.

   Prevention: Verify identities, train employees to question unusual requests.
   Example: American Express Pretexting (2007) – attackers obtained customer info by impersonation.

5. **Baiting:** It uses false promises or incentives to trick users into performing actions that compromise security. The "bait" is often physical (USB drives) or digital (free downloads).

   How it works:

   - Attackers leave infected USB drives or offer free software/music.
   - Victims insert the USB or download files, unknowingly executing malware.
   - Attackers gain access to systems, steal data, or install malicious software.

   Prevention: Avoid unknown devices/files and scan all media before use.
   Example: USB Baiting in Government Agencies – malware spread via dropped USB drives.

6. **Tailgating (Piggybacking):** It occurs when an unauthorized person physically follows an authorized employee into a restricted area without proper authentication.

   How It Works

   - Attackers wait near secure entrances.
   - When an employee opens the door, the attacker follows closely behind.

- The employee assumes the attacker is legitimate and holds the door open.
- The attacker gains physical access to offices, servers, or sensitive files.

Prevention: Use access controls, educate staff, and monitor entrances. **Example:** Facebook Data Center (2018) – intruder tried tailgating, security stopped it.

7. **Quid Pro Quo Attack:** In this attack, the attacker promises a benefit (free service, reward, or technical support) in exchange for sensitive information or access.

   How It Works

   - Attackers impersonate support staff (IT, telecom, bank).
   - They call or email employees offering "help" or "benefits."
   - Victims are asked to disclose credentials, reset passwords, or install software.
   - The attacker gains access or infects systems.

   Prevention: Verify requests, avoid sharing info for rewards, train staff. **Example:** University Tech Support Scam – attackers gained access by offering fake IT help.

8. **Shoulder Surfing:** It is when attackers observe someone's screen or keyboard to steal information (PINs, passwords, OTPs, card details).

   How It Works

   - Attackers watch victims typing in public places (ATMs, cafés, offices).
   - They memorize passwords, PINs, or sensitive details.
   - This information is later used for fraud or unauthorized access.

   Prevention: Shield screens, use strong passwords, and be aware of surroundings. **Example:** ATM Fraud – attackers stole PINs by watching customers.

9. **Watering Hole Attack:** This infects websites commonly visited by a target group. When victims visit the site, malware is automatically delivered.

   How It Works

   - Attackers identify popular websites used by employees of a company.
   - They compromise the site and plant hidden malware.
   - When employees visit, devices get infected.
   - Attackers later use the access to breach corporate networks.

   Prevention: Keep software updated, use security tools, and avoid suspicious sites. **Example:** U.S. Department of Labor (2012) – zero-day malware infected visitors.

10. **Dumpster Diving:** Attackers search through discarded documents, notes, or storage devices to find sensitive information.

    How It Works

    - Attackers check trash bins, shredded paper bags, or dumpsters.
    - They recover passwords, financial data, network diagrams, or access cards.
    - Information is used to perform follow-up attacks (phishing, pretexting, identity theft).

    Prevention: Shred documents, secure disposal, and limit physical data exposure.
    Example: UK Bank Incident – customer data found in trash led to fines.

Impacts of Social Engineering Attacks

1. Data Theft – Sensitive information is stolen.
2. Financial Loss – Money lost due to fraud or ransom.
3. Reputation Damage – Trust of customers and partners is affected.
4. Unauthorized Access – Systems or accounts are compromised.
5. Operational Disruption – Services may be slowed or halted.
6. Identity Theft: Attackers misuse stolen personal information for fraud.

Mitigation & Prevention Strategies

1. **Employee Training**
    - Regular awareness programs on phishing, vishing, baiting, etc.
    - Teach employees how to verify emails, messages, and phone calls.
2. **Strong Authentication**
    - Use MFA (Multi-Factor Authentication) everywhere.
    - Enforce strong, unique passwords and regular password updates.
3. **Verification of Requests**
    - Confirm sensitive requests through official channels.
    - Never share passwords or OTPs via calls, SMS, or emails.
4. **Email & Network Security Tools**
    - Enable spam filters, anti-phishing protection, and safe browsing features.

- Use endpoint security, firewalls, EDR, and intrusion detection.

5. **Policy Enforcement**
   - Strict rules on sharing credentials, accessing sensitive data, and connecting external devices (USB).
   - Enforce clean desk policy and secure disposal of documents.
6. **Simulated Social Engineering Tests**
   - Conduct mock phishing and vishing tests to measure employee awareness.
   - Provide feedback and training to improve weak areas.
7. **Physical Security Controls**
   - Use access cards, biometric scanners, and security guards.
   - Prevent tailgating with turnstiles and surveillance cameras.
8. **Secure Disposal of Information**
   - Shred sensitive papers.
   - Properly wipe storage devices before disposal.

Conclusion

Social engineering works because it targets people, not systems. Organizations can reduce the risk by training employees, enforcing strong policies, and using technical safeguards. Real incidents show how damaging these attacks can be, but proactive prevention greatly lowers the threat.