TASK-5: RESEARCH REPORT: SOCIAL ENGINEERING ATTACKS

1. INTRODUCTION

Social engineering attacks take advantage of human behavior rather than system vulnerabilities. Instead of breaking software, attackers manipulate trust, curiosity, fear, and routine. These are the real beginning points of most large-scale breaches: malware infections, data theft, and financial fraud. It is important to understand major techniques, real-world incidents, and defenses to avoid such attacks.

2. TYPES OF SOCIAL ENGINEERING ATTACKS

2.1 Phishing

A broad attack where, through fake emails or messages, victims are lured into clicking malicious links, downloading malware, or sharing credentials.

Key variants:

- Spear-phishing: Highly targeted and personalized.
- Whaling: Targets executives with high-ranking positions.
- Smishing: SMS-based attacks with malicious links.
- Vishing: Calls in the guise of banks, IT, and government.
- Clone phishing: An existing legitimate email is cloned and replaced with malicious content.
- Credential harvesting pages: Spoofed login pages masquerading as services such as Microsoft 365 or Gmail.

2.2 Pretexting

Attackers make up a story that will surreptitiously get the target to comply with their wishes. They might act as if they are from HR and need information about employees, from a bank checking on account information, or from IT support saying they will need to take control of the target machine in order to "fix" an issue.

Example pretexts:

- “We detected suspicious activity on your account…”
- “This is IT support—your password is expiring.”
- “I'm calling from finance, we need vendor details urgently.”

2.3 Baiting

This employs curiosity or temptation to entice the victim.

Examples:

- USB drives labeled "Confidential Payroll" left in parking lots
- Free downloads with games, music, or software that have malware.
- Fake QR codes on public surfaces redirect users to malicious sites.

2.4 Quid Pro Quo

An attacker provides some sort of service in return for access or data.

Common scenario:

- Someone, pretending to be from technical support, offers assistance and requests the victim to execute a "diagnostic tool" that is really malware.

2.5 Tailgating / Piggybacking

Tailgating: A physical attack in which unauthorized individuals follow authorized employees through secure doors.

Examples:

- Pretending to carry heavy boxes and asking someone to “hold the door.”
- Wearing fake visitor badges.

2.6 Watering Hole Attacks

The attackers infect websites frequented by a particular group. When the target accesses the site, the malware silently delivers itself.

2.7 Impersonation Attacks

Attackers impersonate coworkers, managers, delivery staff, or suppliers with spoofed email addresses, spoofed caller ID, or a polished social profile.

Advanced forms:

- Deepfake voice calls that trick employees into approving transfers.
- Fake LinkedIn profiles used to approach employees for information.

2.8 Business Email Compromise (BEC)

A highly damaging attack in which criminals impersonate executives or vendors to request financial transfers.

Techniques:

- Spoofing executive email domains.
- Hacking a vendor's real email and sending fraudulent invoices.
- Pretending to be the CEO with urgent requests.

2.9 Dumpster Diving

Attackers search through discarded documents, IDs, and storage devices in order to gain sensitive information that helps future attacks.

2.10 Shoulder Surfing

Looking over a victim’s shoulder to capture passwords or screen information in public places, for example, airports or cafes.

3. CASE STUDIES

Case Study 1: RSA Spear-Phishing Breach

Attackers were able to breach RSA through a targeted e-mail with a malicious Excel file attached and steal data related to their authentication products.

Impact: Global remediation, financial loss, and weakened customer trust.

Case Study 2: High-Value BEC Incident

Attackers spoofed a company's CEO, requesting an urgent wire transfer. The finance team complied.

Impact: Multi-million-dollar loss, subsequent litigation, and additional internal controls.

Case Study 3: Watering Hole Attack on NGO Researchers

Hackers infected websites that are commonly used by research staff.

Impact: Silent data theft, tapping of communications, and long-term espionage.

Case Study 4: USB Baiting in a Government Office

Employees plugged found USB sticks into their workstations.

Impact: The malware spreads throughout the internal networks, necessitating shutdowns to clean up.

Case Study 5: Deepfake Voice Scam

Attackers used AI-generated audio to impersonate a company executive to ask an employee to transfer funds.

Impact: Exposure of weaknesses in identity verification and fraudulent transfers.

4. PREVENTING SOCIAL ENGINEERING ATTACKS

4.1 Technical Defenses

- Multi-factor authentication (MFA), preferably hardware-based.
- Email filtering with malware scanning and URL protection.
- Reduce spoofed emails by implementing SPF, DKIM, and DMARC.
- Disable auto-run for USB devices.
- Use endpoint detection and response tools.
- Regular system patching and updating.

4.2 Organizational Policies

- Verification procedures for all financial transactions.
- Companywide data handling rules: not sending data via email or by phone.
- Vendor management checks to ensure third-party security.
- Clear policies regarding guests and visitors' access.

4.3 Physical Security Controls

- Provide secure badge access to buildings.
- Anti-tailgating turnstiles or guards Lockable shredding bins for sensitive documents.
- Surveillance cameras that deter physical intrusions.

4.4 Employee Training

- Regular awareness sessions about social engineering tactics.
- Simulated phishing testing to assess readiness.

- Train employees to validate suspicious requests with a phone call.
- Encourage and foster a "no blame" approach to reporting suspicious activities.

5. CONCLUSION

Social engineering attacks are still the easiest and most effective way to break into organizations because they target people, not machines. The best defense against social engineering involves a combination of strong technical defenses, clear policies, physical security, and regularly updated training. Human awareness is the most powerful defense.