Social Engineering Attacks Report

🎯 Introduction

Social engineering attacks exploit human psychology rather than technical vulnerabilities. Attackers manipulate individuals into revealing confidential information, clicking malicious links, or granting unauthorized access. These attacks are among the most effective methods used by cybercriminals due to the human element involved.

🕵️ 1. Phishing

➤ How It Works

Phishing involves tricking users into believing they're interacting with a legitimate entity (like a bank or trusted company). Common tactics include:

- Emails with fake login links

- Text messages (smishing)

- Voicemail messages (vishing)

➤ Real-World Case Study

“Google & Facebook Scam (2013–2015)”

A Lithuanian man defrauded both companies of over “$100 million” by sending fake invoices while pretending to be a real vendor.

➤ Impact

- Credential theft

- Financial loss

- Malware infections (e.g., ransomware)

➤ Prevention

- Enable “two-factor authentication (2FA)”

- Verify URLs before clicking

- Train employees to spot phishing emails

- Use “anti-phishing software”

🎭 2. Pretexting

➤ How It Works

Pretexting involves an attacker creating a fabricated scenario to gain a victim’s trust and extract sensitive data. Often used in combination with phishing.

Examples:

- Pretending to be IT support asking for login details

- Claiming to be from HR requesting personal information

➤ Real-World Case Study

HP & Deloitte Pretexting Scandal (2006)

HP hired investigators who used pretexting to obtain phone records of board members and journalists, leading to a high-profile privacy breach.

➤ Impact

- Identity theft

- Access to confidential data

- Legal consequences

➤ Prevention

- Verify identities before sharing sensitive info

- Train staff on pretexting scenarios

- Implement strict internal communication protocols

🎁 3. Baiting

➤ How It Works

Baiting uses physical or digital "bait" to trick victims into taking an action. Common forms:

- Infected USB drives labeled “Confidential” left in public places

- Free downloads that install malware

➤ Real-World Case Study

Stuxnet USB Infection (2010)

Stuxnet worm reportedly entered Iran’s nuclear facility through an infected USB drive planted strategically — a classic baiting technique.

➤ Impact

- Malware/ransomware infection

- Data breaches

- System compromise

➤ Prevention

- Disable auto-run on USB devices

- Educate employees about the risk of unknown drives

- Use endpoint protection tools

🔐 General Recommendations to Prevent Social Engineering

- Regular cybersecurity awareness training

- “Simulated phishing campaigns” to test readiness

- “Strict access control policies”

- “Encourage reporting of suspicious activity”

- “Don’t overshare on social media”(can reveal useful info to attackers)

☑ Conclusion

Social engineering attacks continue to succeed because they exploit human behavior, not just technical flaws. Organizations must focus on “people, processes, and training” alongside technical defenses to build true cybersecurity resilience.

References

- [CISA: Social Engineering Awareness](https://www.cisa.gov/news-events/news/social-engineering-awareness)

- [Phishing.org](https://www.phishing.org/)

- [Verizon Data Breach Report](https://www.verizon.com/business/resources/reports/dbir/)

- [Stuxnet Explained - Wired](https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)