Research Report on Social Engineering Attacks

Introduction

Social engineering is a form of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. Attackers use deception to trick individuals into revealing confidential information, granting access, or performing certain actions. This report explores common types of social engineering attacks, real-world examples, their impacts, and how to prevent them.

---

1. Phishing

Overview

Phishing is one of the most prevalent social engineering techniques. It involves sending fraudulent emails, messages, or websites that appear legitimate, aiming to steal sensitive data such as login credentials, credit card numbers, or personal information.

How It Works

Attackers impersonate trusted entities (like banks or government agencies) and send emails urging users to click malicious links or download attachments.

Case Study

In 2020, **Twitter suffered a major phishing attack** where attackers tricked employees into providing login credentials. This allowed hackers to access high-profile accounts (Elon Musk, Barack Obama, etc.) and run a Bitcoin scam.

Impact

- Compromise of sensitive data
- Financial fraud
- Loss of brand trust

Prevention

- Conduct regular phishing awareness training
- Use email filters and anti-phishing tools

Enable Multi-Factor Authentication (MFA)

Avoid clicking suspicious links or downloading unknown attachments

2. Pretexting

Overview

Pretexting involves creating a fabricated scenario (pretext) to obtain information or access. The attacker often impersonates someone in authority or with a legitimate need for the information.

How It Works

The attacker builds trust by pretending to be a colleague, IT support, or a police officer and asks the target to share confidential data or grant system access.

Case Study

In a notable case, an attacker **impersonated an IT administrator** of a UK-based bank. Through a phone call, he convinced a new employee to reveal network login credentials, which were then used to access internal systems.

Impact

Unauthorized access to networks and databases

Exposure of private or classified data

Prevention

Verify identities before sharing any sensitive information

Implement strict authentication procedures

Educate employees about the signs of pretexting attempts

---

3. Baiting

Overview

Baiting involves luring victims with promises of rewards (free music, movie downloads, or USB drives) that contain malware or lead to compromised websites.

How It Works

Attackers leave infected devices (e.g., USB drives) in public places or offer online "freebies" that, when accessed, install malware on the victim's device.

Case Study

In 2016, a **university IT team ran a test** by dropping USB drives around campus. Nearly half of the found drives were plugged into university computers, revealing how effective baiting could be.

Impact

- Malware installation
- Ransomware attacks
- Data breach or loss of control over systems

Prevention

- Train users to never plug unknown USBs into device
- Disable auto-run features on computers
- Use endpoint protection software
- Promote cybersecurity hygiene

Conclusion

Social engineering attacks like phishing, pretexting, and baiting exploit human trust rather than technical flaws. These attacks are increasing in frequency and sophistication, making employee awareness and organizational policy crucial for defense. Training, verification protocols, and technical safeguards must work together to prevent these manipulative tactics.

Recommendations

Regular security awareness training for all employees

Strong identity verification processes

Implementation of security policies for email, USB use, and communication

Use of MFA, endpoint protection, and intrusion detection systems

Simulated attack exercises to test and improve user awareness

---

References

Social Engineering Basics – CISE

Twitter Hack 2020 – BBC News

Pretexting and Phishing – Norton

USB Drop Experiment – University of Illinois