ST. KITTS BRANCH
Financial Services Regulatory Commission

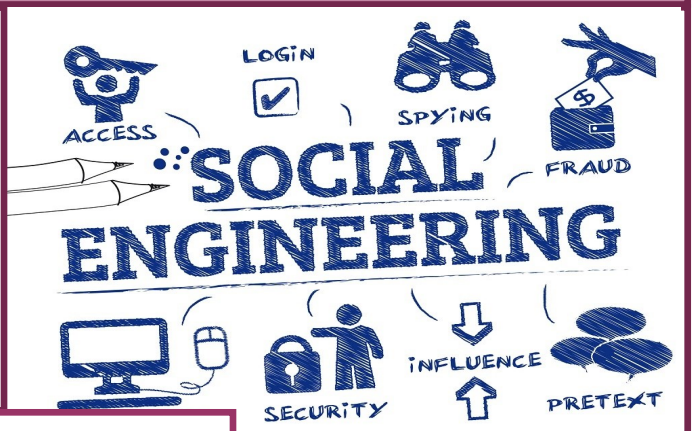
NewsLetter

February 2025
Issue No. 128

The Many Faces of Social Engineering

What is Social Engineering

Social engineering is a manipulation technique that exploits human error to gain access to private information or valuables. In cyber-crime, these "*human hacking*" scams tend to lure unsuspecting users into exposing data, spreading malware infections or giving access to restricted systems. Attacks can happen online or in-person. Scams based on social engineering are centered around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behaviour. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.



How to Prevent Social Engineering Attacks

Social Engineering attacks manipulate individuals into divulging confidential information or performing actions that compromise security. Here are key strategies to prevent such attacks:

Employee Training & Awareness - Educate employees about common social engineering tactics such as phishing, pretexting, baiting and tailgating. Regularly conduct cybersecurity awareness training and include topics on emerging trends and threats.

Verify Identities - Always verify the identity of individuals requesting sensitive information or access, whether via email, phone or in person. Use Multi-Factor Authentication (MFA) to confirm identities.

Strong Password Policies - Implement and enforce strong, unique passwords. Encourage the use of password managers and require frequent password updates (e.g. quarterly).

Beware of Phishing Attempts - Train employees to recognize suspicious emails, links or attachments. Encourage them to report any dubious communications.

Restrict Access & Implement Least Privilege - Limit access to sensitive data based on job roles. Employees should only have access to the information necessary for their duties.

Use Secure Communication Channels - Avoid sharing sensitive information over unsecured channels such as email or phone calls unless properly encrypted and verified.

Regular Security Audits & Simulations - Conduct penetration testing and simulated social engineering attacks to evaluate employee readiness and identify vulnerabilities.

Encourage Security Culture - Foster a workplace culture where employees feel comfortable reporting suspicious activities without fear of reprimand.

By implementing these measures, organizations can significantly reduce the risk of falling victim to social engineering attacks.

15 Types of Social Engineering

- Phishing
- Spear Phishing
- Vishing (Voice Phishing)
- Smishing (SMS Phishing)
- Pretexting
- Baiting
- Quid Pro Quo
- Tailgating (Piggybacking)
- Dumpster Diving
- Watering Hole Attack
- Business Email Compromise (BEC)
- Honey Trap
- Rogue Security Software
- Social Media Exploitation
- Impersonation

The Five Stages of a Social Engineering Attack Cycle

The five (5) stages of the social engineering attack cycle are:

1. **Reconnaissance** - The attacker gathers information about the target through research, social media, company websites or direct observation. The goal is to identify vulnerabilities and entry points.
2. **Engagement (Pretexting)** - The attacker establishes trust by crafting a convincing pretext (fake scenario). They may impersonate a trusted entity (e.g., IT support, bank representatives) to manipulate the target into sharing sensitive information.
3. **Exploitation (Attack Execution)** - The attacker exploits the target by using psychological manipulation to gain access. This could involve phishing emails, baiting, tailgating or other deceptive tactics.
4. **Execution (Control & Access)** - Once inside the system or network, the attacker gains control by installing malware, stealing credentials or accessing confidential data.
5. **Disengagement & Cover-up** - The attacker exits the system without raising suspicion. He/She may erase traces of his/her presence to avoid detection and possibly prepare for future attacks.

Case Study

Overview

In July 2020, one of the most high-profile social engineering attacks occurred when hackers gained access to Twitter's internal systems and used them to hijack several high-profile accounts including those of Barack Obama, Elon Musk, Bill Gates and Apple. The attackers used these accounts to promote a Bitcoin scam, tricking users into sending cryptocurrency with the false promise of doubling their money.

Attack Method

The hackers used vishing (voice phishing) to manipulate Twitter employees into granting them access to internal systems. They impersonated IT staff and convinced employees to reset credentials, allowing the attackers to bypass security measures and take over prominent accounts.

Impact

The financial loss was over US$118,000.00 in Bitcoin which was stolen within hours. Twitter faced severe backlash and brand damage for its security vulnerabilities. The regulatory scrutiny of the attack led investigations and policy changes within Twitter.

Lessons Learned

The Importance of Multi-Factor Authentication (MFA): A stronger authentication could have prevented unauthorized access.

Employee Training: Regular training on social engineering tactics to help employees recognize and resist manipulation.

Internal Security Policies: Companies must implement strict controls for accessing critical systems and sharing of information.

Other Cases of Social Engineering

1. The Sony Pictures Hack (2014) where phishing led to a massive data breach.
2. In 2016, a hacker tricked a Snapchat Human Resource employee into disclosing payroll information by posing as the CEO.

References

- Newman, L. (2020). "Inside the Twitter Hack." *Wired*. Retrieved from Wired.com
- Mitnick, K. (2003). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.