RCM&D

A UNISON RISK ADVISORS Company

SOCIAL ENGINEERING EXPLAINED
ATTACK METHODS & MITIGATION TECHNIQUES

Some of the most notable tools in a cybercriminal's toolbox are social engineering schemes, which rely on deception and playing on a victim's emotions to extort money and personal information.

Social Engineering: The Schemes

Business Email Compromise (BEC):

Occurs when cybercriminals hack into or create fake company email accounts. With these legitimate or fake accounts, hackers then request things like urgent fund transfers, defer payments to a new account, set up fake employee records or send out spam links and attachments to company employees. Since these messages look as if they are coming within the organization, many employees may honor the fraudulent requests without validation.

Vendor Spoofing Scheme:

Hackers impersonate a vendor, supplier or other third-party partner to infiltrate a business. Much like BEC, hackers will either create fraudulent mailing addresses or hack into legitimate ones to accomplish this. The attacker may make simple requests to victims, such as asking to update banking details.

Fake Presidents Fraud:

Also known as a Senior Executive Scheme, this attack involves hackers identifying themselves as the company owner or C-level director to sidestep standard security protocols. They will target another employee or fellow executive to make an immediate transfer, often phrasing requests as "funding a recent acquisition" or simply "for tax purposes." They may even have a fake attorney call victims to verbally verify the transaction.

Phishing:

The most common and oldest social engineering scheme is undoubtedly phishing. This attack involves criminals tricking victims into divulging personal information such as passwords and account numbers. Phishing attacks may include links or attached files that, when clicked, may give a hacker access to an organization's entire network. In addition to traditional phishing schemes, there are several sub forms, which include:

- **Spear Phishing:** Addresses a specific individual by name, often targeting key employees who have access to accounting logins and other details.
- **Whaling:** Targets high-ranking company executives who have access to corporate finances and confidential information.
- **Credential Phishing:** Tricks victims by using a fake website designed to look like a real account login page. From there, hackers can collect passwords and login details.

Mitigation Techniques

Preparing your workforce for social engineering schemes is critical to navigating today's turbulent cyber market. The following list from McGowan are effective methods:

- **Train Employees to Recognize Threats:** Since social engineering schemes deal directly with employee emotions and behaviors, proper training should be top priority. Regular anti-fraud and awareness training is key to building awareness.
- **Establish and Enforce Security Protocols:** Never let employees stray from the path of your standard business procedures pertaining to transferring funds or updating billing details. If your policy requires employees to validate transfers and payment requests either by phone or in person, this should be ensured. Methods such as multi-factor authentication (MFA) or callback verification should be strongly considered. In some cases, carriers require MFA and callback verification for coverage.
- **Limit Account Access and Security Clearances:** Limit the number of people granted wire transfer authority and financial access. Require supervisor sign-offs for any internal transfer requests or billing updates.
- **Keep Your Guard Up:** Ensure employees never feel rushed by urgent undertones or through intimidation to provide sensitive information or to make money transfers. Emotion is one of the keys to a social engineering scheme.
- **Deploy Cybersecurity Software:** Utilize adequate cybersecurity software. Work with your IT department to ensure all cybersecurity technology is working and up-to-date.
- **Test Your Defenses:** A third-party audit and penetration-testing program can help you evaluate your preventive techniques to uncover any vulnerabilities.

Questions?

The RCM&D Cyber Practice stands ready to help you defend your business from social engineering schemes and attacks. We have access to industry-standard tools, such as BitSight cybersecurity scanning, to help you ensure your business is protected.