Social Engineering

Bank of America Merrill Lynch

The human firewall is under attack.

It’s often stated that an organization’s greatest threat and best defense regarding fraud and cybersecurity is their human capital. As fraud techniques continue to evolve, social engineering is becoming the most effective means of gaining access to secure systems to obtain sensitive information, defraud organizations and conduct cyber espionage. Social engineering works by manipulating human behavioral traits and, as such, there are limited techniques to guard against it. Education is the key defense to help thwart social engineering attacks. This document is intended to provide background on the practice of social engineering and provide the audience with steps to help mitigate its threat.

Social engineering’s impact:

Information security is essential for any organization and most organizations have robust security protocol in place. As fraud techniques continue to evolve, bad actors are leveraging social engineering techniques to defraud individuals and organizations. Eighty-four percent of hackers leverage social engineering in cyber-attacks and 50% change their attack methodologies with every new target[1]. Targeted business email compromise (BEC) is the medium of choice for fraudsters. From early 2013 until May 2018, twelve billion dollars has been lost to BEC comprise attacks.[2]

What is social engineering and why are fraudsters using it?

Social engineering is an attack method that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain. Fraudsters use social engineering techniques to conceal their true identities, motives and present themselves as a trusted individual or information source. The goal is to influence, manipulate or trick users into giving up privileged information or access within an organization.[3]

Social engineering behavioral vulnerabilities:

Fraudsters use phishing emails, pretext calling and emergency queries all designed to appear normal with the goal of getting employees to take action. The following three behavioral vulnerabilities pose a high risk for social engineering fraud. [4]

- **We are helpful by nature:** A request for help is one of the most successful social engineering techniques that fraudsters use. This attack will typically take place either in person or over the phone. The fraudster will engage an employee at an organization either as an employee, customer or vendor. Typically, they show a need for assistance, always with a bit of urgency, and on the surface appears harmless to the organization.
- **We are curious by nature:** We are supposed to ask questions, try new things, read and stay abreast of the news. Fraudsters know that we are curious and use this against us when engaging in a social engineering attack. They create emails and social networking posts to entice employees to click on links or respond to emails.
- **We are efficient at multitasking:** We live in an “always-on” world; employees typically multitask while on the phone or in a meeting. Fraudsters rely on employees missing key details while multitasking. A key attack is a malicious email delivered at the start of the business day or social media spam posting times mirroring peak usage times.

[1] https://www.esecurityplanet.com/hackers/fully-84-percent-of-hackers-leverage-social-engineering-in-attacks.html

[2] https://www.ic3.gov/media/2018/180712.aspx

[3] https://www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat

[4] https://securityintelligence.com/three-reasons-social-engineering-still-threatens-companies/

General disclaimer for Bank of America Merrill Lynch. AR# AR8PYBYQ

How to help guard against social engineering threats

Organizations spend countless hours and financial resources securing critical IT infrastructure. Whether it's through network security, firewalls, security appliances or encryption, the human element remains vulnerable to attack. With proper education and due diligencem employees can help keep their organization's data and IT infrastructure secure.

Social engineering defense best practices:[5]

- ***Education***: The most effective strategy to guard against social engineering fraud is employee education and training. Employees should be educated on the types of attacks most commonly seen and how to effectively guard against it.
- ***Make cybersecurity training personal and relatable***: When training and implementing a cybersecurity policy organizations should make the training personal and actionable. Employees should be able leverage their organizations cybersecurity program to help safeguard them at home.
- ***Be aware of your social media profile***: Social media users should be aware of what they are posting on the internet. Most social media users are unaware of how much information is available about them on the internet. When using social media, use extra caution when posting personally identifiable information, including but not limited to job title, address, maiden name or employment history.
- ***Social media policy***: Organizations should also consider implementing a strong social media policy. The social media policy should have clear guidelines in place to respond to numerous situations. Be sure this policy protects your organizations data assets, products and intellectual property.
- ***Determine which assets are most valuable to criminals***: Organizations should determine what assets are most valuable to criminals. Many times organizations will place more protection around physical assets or assets that have intrinsic value to the organization. Criminals will many times target an organizations critical infrastructure, client data or other confidential proprietary information.
- ***Always be sure your organizations applications and software are up to date***: Hackers will use social engineering techniques to determine whether or not your organization is running updated software. Unpatched software can expose your organization to malware and ransomware.
- ***Use caution when disclosing information***: Whenever you are in a conversation with someone you don't know, before you answer a question they ask, make sure they have a need to know that information. Since it's a human tendency to instinctively try to be helpful to others when asked, social engineers will leverage that instinct to their advantage. Client or customer facing employees need to be helpful with restraint.
- ***If something doesn't feel right, escalate or end the conversation:*** Human intuition is the ability to understand something immediately, without the need for conscious reasoning. This human intuition is very important when guarding against social engineering threats. If something doesn't feel right, stop your conversation, escalate to a manager and (most importantly) do not disclose confidential information.
- ***Physical security***: Tailgating or "piggybacking" attacks occur when someone lacks the proper authority to be in a particular area but follows an employee that has the proper authorization into a restricted area. Most organizations have strict protocol in place for who can be in restricted areas. However, criminals have been known to utilize the natural human response to gain access to areas where proprietary information can be compromised.[6]

How organizations can protect against social engineering

The key to preventing a social engineering attack lies in the training and trust of employees. Security is no longer just a problem for IT departments. All employees must do their part to be sure their organizations remain secure against Social Engineering threats.

- Organizations should implement regularly occurring security awareness training for the entire company.
- Organizations should create, implement and enforce a social media policy for their organization.
- Always be sure your organization is administering network privileges with a "least access" necessary mindset.

For more information about social engineering, visit our Fraud Education site through CashPro Assistant at https://cashproonline.bankofamerica.com/cpocms/sites/CashProUniversity/Landing/Fraud/page.htm

[5] https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

[6] https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

General disclaimer for Bank of America Merrill Lynch. AR# AR8PYBYQ