Fusco Orsini & ASSOCIATES INSURANCE SERVICES

Common Social Engineering Tactics to Watch For

Social engineering refers to a cyberattack method in which a cybercriminal preys on key human behaviors (e.g., trust of authority, fear of conflict and promise of rewards) to obtain unwarranted access to targets' technology, systems, funds or data. These attacks can be deployed through various tactics, such as digital impersonation, deceitful messages or malicious software (known as malware). Social engineering attacks have become a significant threat to businesses of all sizes and sectors; after all, anyone can be targeted in these incidents—including entry-level workers, managers and CEOs. With this in mind, it's crucial for businesses to be aware of frequently utilized social engineering methods and adopt effective cybersecurity measures to help mitigate these incidents. This article outlines common social engineering tactics to watch for and offers associated prevention and response tips.

Common Social Engineering Techniques

In a social engineering attack, a cybercriminal implements a number of manipulative tactics to lure their target into performing actions that they normally wouldn't. Some common social engineering methods include the following:

- **Phishing**—This technique involves cybercriminals leveraging fraudulent emails to trick recipients into providing sensitive information, clicking malicious links or opening harmful attachments. In order to make their emails appear genuine, cybercriminals will often impersonate trusted sources (e.g., a co-worker or well-known organization) and feign a sense of urgency to rush targets into acting. In addition to traditional phishing, cybercriminals may also attempt to manipulate targets over text messages or phone calls (known as smishing and vishing, respectively).
- **Spear phishing**—A spear-phishing scheme typically focuses on specific individuals or companies and uses personalized information to convince targets to share their data. In these instances, cybercriminals will research targets' online behaviors, such as where they shop or what they share on social media, to collect personal details that make their schemes seem more legitimate.
- **Business email compromise (BEC)**—Such a technique refers to cybercriminals posing as business leaders or partners (e.g., executives, senior-level employees, vendors or suppliers), often for financial gain. Cybercriminals generally deploy BEC scams via email by creating fake accounts for business leaders or partners and using deceiving messages to trick targets into transferring money, divulging financial data or changing banking details.
- **Baiting and quid pro quo**—Through this strategy, cybercriminals make false promises to persuade targets to share data or download malware. These false promises may appear in the form of fraudulent pop-up advertisements or deceitful online promotions. For example, a cybercriminal may use a false advertisement for a free movie download to trick their target into installing a virus on their device. Similar to baiting, quid pro quo incidents involve cybercriminals promising to provide something valuable to their targets (e.g., an e-commerce coupon code or discounted security software) but only in exchange for the targets' sensitive information (e.g., contact details, bank account numbers or login credentials).
- **Pretexting**—This technique consists of cybercriminals impersonating a co-worker, community leader or authority figure (e.g., a police officer, government employee, banker or tax official) and asking targets to provide sensitive information to confirm their identities or help complete critical tasks and assignments. Some of the most common types of data stolen amid pretexting incidents include employees' contact details and Social Security numbers, company bank records and workplace security information.
- **Tailgating**—Through this tactic, cybercriminals physically sneak into workplaces by following closely behind employees or other credentialed individuals (e.g., custodians or building maintenance workers) without their knowledge. That is, after these authorized individuals leverage their key fobs or identification badges to pass through locked doors or security checkpoints, the cybercriminals will also slide inside before the locks can reengage. From there, the cybercriminals may leverage their on-site access to steal essential company records, infect important technology with viruses or malware and compromise security systems to allow continued workplace infiltration.
- **Scareware**—This method entails cybercriminals utilizing various scare tactics to frighten and manipulate targets into paying ransoms, often through seemingly legitimate prompts (e.g., fraudulent virus infection alerts urging targets to purchase security software for their devices or deceptive messages claiming to be from law enforcement that accuse targets of committing crimes and demand payment for any associated fines). Scareware may either initially contain malware or eventually coerce targets into downloading malware.

Tips to Mitigate Social Engineering Attacks

Businesses can consider these steps to help prevent and respond to social engineering attacks:

- **Provide training.** Businesses should educate employees on social engineering and how it could affect them. Additionally, employees should be required to participate in routine cybersecurity training on social engineering attack

detection and prevention. This training should instruct employees to do the following:

- Maintain a healthy sense of skepticism across communication channels by watching for social engineering tactics in emails, texts and calls (e.g., lack of personalization, generic phrasing and urgent requests).
- Refrain from interacting with emails, texts or calls from unknown or suspicious senders.
- Avoid clicking links or downloading applications provided within emails or texts.
- Never share sensitive information online, via text or over the phone.
- Utilize trusted contact methods (e.g., calling a company's official phone number) to verify the validity of any suspicious requests.
- Report any suspicious emails, texts or calls to the appropriate parties, such as a supervisor or the IT department.

- **Implement access controls.** By allowing employees access to only the information they need to complete their job duties, businesses can reduce the risk of cybercriminals compromising excess data or securing unsolicited funds amid social engineering incidents. To further protect their information, businesses should consider leveraging encryption services and establishing secure locations for backing up critical data.
- **Utilize proper security software.** Businesses should make sure all workplace technology is equipped with adequate security software. In some cases, this software can halt cybercriminals in their tracks, stopping fraudulent messages from reaching recipients' devices and rendering harmful links or malicious applications ineffective. In particular, workplace technology should possess antivirus programs, spam detection systems, email filters, firewalls, message-blocking tools and multifactor authentication capabilities. This security software should be updated as needed through patch management systems to ensure its effectiveness.
- **Ensure safe financial transactions.** Having secure financial procedures can help limit the risk of any money being lost during social engineering attacks. As such, businesses should instruct employees who handle financial operations to carefully analyze fund transfer requests and similar payment demands to ensure their validity. When possible, these requests should be discussed in person before moving forward, especially if they involve alternative payment procedures or changes in banking details. Businesses may also want to consider utilizing several verification methods and implementing the "two-person rule" to confirm payment requests, in which two authorized individuals must review and approve transactions before they can go through.
- **Adopt a cyber incident response plan.** In the event that a social engineering attack is suspected or detected, it's essential for businesses to have dedicated cyber incident response plans in place that outline steps to ensure timely remediation and keep damages to a minimum. These response plans should address a variety of possible attack scenarios and be communicated to all applicable parties. Both the Cybersecurity & Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) have resources available to help businesses create such plans.
- **Conduct tabletop exercises and penetration testing.** It's not enough for businesses to simply create cyber incident response plans. Rather, they should routinely assess these plans for ongoing security gaps and make changes as needed to ensure maximum protection amid social engineering attacks. Common assessment techniques include the following:
  - **Penetration testing**—Such testing consists of an IT professional mimicking the actions of a cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and is able to withstand attack efforts. This testing usually targets a specific type of workplace technology and may leverage various attack vectors.
  - **Tabletop exercises**—A tabletop exercise is an activity that allows an organization to simulate a realistic cyberattack scenario (e.g., a phishing simulation) for the purpose of testing its incident response plan's efficiency. In other words, this exercise serves as a cyberattack drill, giving participants the opportunity to practice responding to an attack.
- **Consult trusted experts and professionals.** Businesses don't have to navigate and address their social engineering exposures alone. Instead, they can seek assistance and supplement their existing resources with guidance from a wide range of trusted external parties, including insurance professionals, legal counsel, cybersecurity firms, law enforcement and government agencies (e.g., CISA and NIST).
- **Purchase sufficient coverage.** It's critical for businesses to purchase adequate insurance to secure ample financial protection against potential losses that may arise from social engineering attacks. Businesses should consult trusted insurance professionals to discuss their specific coverage needs.

Conclusion

Social engineering is a common and widespread cyberthreat that has the potential to wreak havoc on businesses across industry lines. Fortunately, organizations that ensure a solid understanding of key social engineering methods and leverage proper prevention and response measures can help minimize these incidents and their related losses. Contact us today for more risk management guidance and insurance solutions.