VISIT MAGAZINE WEBSITE

How Criminals Use Social Engineering to Target Your Company

Understand the three stages of a social engineering attack so you can build your company's defense strategy.

Cybercriminals use a variety of schemes to find vulnerabilities they can leverage to attack companies, but one of the weakest links is easier to exploit than the others: your employees.

Through social engineering—the art of manipulating people—cybercriminals study their victims, play on emotions and build trust. Attacks often create a sense of urgency or appeal toward reward, guilt or sympathy to gain access to a company's network.

"Criminals invest time and resources, such as scouring public websites and social media accounts, to study intended fraud victims," said Alec Grant, Head of Client Fraud Prevention for Commercial Banking. "Like a game of chess, these opponents gather pieces of information on victims before launching a covert attack against their defenses."

continued on next page >

The Three Stages of a Social Engineering Attack

A social engineering attack happens over three stages. The best way to protect your business from becoming a victim is to understand how attacks happen so you can implement protocols for protection. You can use the attacker's playbook to strengthen your own defense strategy.

1 Preparation

Criminals research victim by gathering public information on websites and social media. They use creative methods, such as quizzes to entice victims into providing personal information. Asking questions about cars, pets, and former schools might not seem obvious, but they provide answers to questions used to reset forgotten online account passwords.

2 Execution

The criminal uses a convincing pretext to engage the victim, build trust and gain cooperation—sometimes as simple as giving verbal information in a face-to-face conversation or getting the victim to click a file or link. Once the connection is successful, criminals can install malware into the computer system.

3 Exit

Criminals will try to conceal what's happening until they can make a proper getaway. An attack can last a few minutes, or it can progress slowly, gradually infiltrating a network before launching a ransomware attack or a payments fraud scheme. You may not realize the attack has occurred until it's too late.

Assessing Risk and Implementing Controls

With this playbook in hand, your organization can design and implement controls to prevent and detect an attack. Consider developing a social engineering prevention program to study each phase of a social engineering attack, assess your risks and build or strengthen security controls.

ASSESS RISK: **A target that's harder to scope out is a target that's harder to exploit. What information is publicly shared about your company or executives on social media, websites or in vendor profiles?**

IMPLEMENT CONTROLS:

- **Work to remove information** that can potentially be used against you in an attack.
- **Develop and enforce** a corporate social media policy to prevent disclosures about personal information, like specific job descriptions.
- **Restrict access** to websites that risk information sharing. Consider using a third-party vendor to find and remove look-alike website domains that may impersonate your company.

ASSESS RISK: **Vigilant employees are tougher to trick. How would your employees perform in a simulated test of your cybersecurity policies?**

IMPLEMENT CONTROLS:

- **Use unannounced phishing tests** to measure what proportion of employee "victims" reported receiving a suspicious email versus employees who clicked on a suspicious link.
- **Develop a continuous employee education program.** Create awareness among your staff on how to spot social engineering attacks and follow established internal policies and procedures to help protect your company.
- **Add technical controls** to flag external emails with a warning banner to make it easy for employees to report any suspicious emails.

continued on next page >

As your program matures, continuously monitor that it has the proper resources to maintain your defense protocols. Attackers are always innovating, so it's important that your plan is dynamic and ready to implement new defensive strategies.

You never know when a social engineering attack will occur. But designing a culture of preparedness now will improve your organization's resiliency and recovery efforts if you are impacted.

What Does a Social Engineering Attack Look Like?

There are several ways criminals launch social engineering attacks. Here are a few schemes to watch for:

PHISHING

Fraudulent emails that encourage you to unwittingly open harmful links or files.

SMS PHISHING (SMISHING)

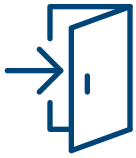
Text messages or instant messages with malicious links or files.

BUSINESS EMAIL COMPROMISE

A personalized email attack impersonating a trusted vendor or executive, often containing fraudulent payment and banking instructions.

VOICE PHISHING (VISHING)

A phone call designed to get you to share sensitive information.



TAILGATING

Also called "piggybacking." In this in-person attack, criminals seek physical access to secure areas where they can cause harm to networks.

Key Takeaways

- Know the different attack vectors criminals use.
- Look at your organization from an outsider's perspective to identify vulnerabilities or gaps that can be exploited.
- Conduct regular cybersecurity training and educate your staff on how to remain vigilant to suspicious emails, phone calls or text links.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Summer 2021.

Explore the full issue