Social engineering tactics

Social engineering attacks are a popular choice among threat actors. That’s because it’s often easier to trick people into providing them with access, information, or money than it is to exploit a software or network vulnerability.

As you might recall, **social engineering** is a manipulation technique that exploits human error to gain private information, access, or valuables. It's an umbrella term that can apply to a broad range of attacks. Each technique is designed to capitalize on the trusting nature of people and their willingness to help. In this reading, you will learn about specific social engineering tactics to watch out for. You’ll also learn ways that organizations counter these threats.

Social engineering risks

> Un pirate informatique se faisant passer pour une personne connue de sa cible.

Social engineering is a form of deception that takes advantage of the way people think. It preys on people’s natural feelings of curiosity, generosity, and excitement. Threat actors turn those feelings against their targets by affecting their better judgment. Social engineering attacks can be incredibly harmful because of how easy they can be to accomplish.

One of the highest-profile social engineering attacks that occurred in recent years was the *Twitter Hack of 2020*. During that incident, a group of hackers made phone calls to Twitter employees pretending to be from the IT department. Using this basic scam, the group managed to gain access to the organization’s network and internal tools. This allowed them to take over the accounts of high-profile users, including politicians, celebrities, and entrepreneurs.

Attacks like this are just one example of the chaos threat actors can create using basic social engineering techniques. These attacks present serious risks because they don’t require sophisticated computer skills to perform. Defending against them requires a multi-layered approach that combines technological controls with user awareness.

Signs of an attack

Oftentimes, people are unable to tell that an attack is happening until it's too late. Social engineering is such a dangerous threat because it typically allows attackers to bypass technological defences that are in their way. Although these threats are difficult to prevent, recognizing the signs of social engineering is a key to reducing the likelihood of a successful attack.

These are common types of social engineering to watch out for:

- **Baiting** is a social engineering tactic that tempts people into compromising their security. A common example is USB baiting that relies on someone finding an infected USB drive and plugging it into their device.
- **Phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. It is one of the most common forms of social engineering, typically performed via email.
- **Quid pro quo** is a type of baiting used to trick someone into believing that they'll be rewarded in return for sharing access, information, or money. For example, an attacker might impersonate a loan officer at a bank and call customers offering them a lower interest rate on their credit card. They'll tell the customers that they simply need to provide their account details to claim the deal.
- **Tailgating** is a social engineering tactic in which unauthorized people follow an authorized person into a restricted area. This technique is also sometimes referred to as piggybacking.
- **Watering hole** is a type of attack when a threat actor compromises a website frequently visited by a specific group of users. Oftentimes, these watering hole sites are infected with malicious software. An example is the *Holy Water attack of 2020* that infected various religious, charity, and volunteer websites.

Attackers might use any of these techniques to gain unauthorized access to an organization. Everyone is vulnerable to them, from entry-level employees to senior executives. However, you can reduce the risks of social engineering attacks at any business by teaching others what to expect.

Encouraging caution

Spreading awareness usually starts with comprehensive security training. When it comes to social engineering, there are three main areas to focus on when teaching others:

- **Stay alert** of suspicious communications and unknown people, especially when it comes to email. For example, look out for spelling errors and double-check the sender's name and email address.
- **Be cautious** about sharing information, especially over social media. Threat actors often search these platforms for any information they can use to their advantage.
- **Control curiosity** when something seems too good to be true. This can include wanting to click on attachments or links in emails and advertisements.

Pro tip: Implementing technologies like firewalls, multi-factor authentication (MFA), block lists, email filtering, and others helps layers the defenses should someone make a mistake.

Ideally, security training extends beyond employees. Educating customers about social engineering threats is also a key to mitigating these threats. And security analysts play an important part in

promoting safe practices. For example, a big part of an analyst's job is testing systems and documenting best practices for others at an organization to follow.

Key takeaways

People’s willingness to help one another and their trusting nature is what makes social engineering such an appealing tactic for criminals. It just takes one act of kindness or a momentary lapse in judgment for an attack to work. Criminals go to great lengths to make their attacks difficult to detect. They rely on a variety of manipulation techniques to trick their targets into granting them access. For that reason, implementing effective controls and recognizing the signs of an attack go a long way towards preventing threats.

Resources for more information

Here are two additional resources to review that will help you continue developing your understanding of social engineering trends and security practices:

- OUCH! is a free monthly newsletter from the SANS Institute that reports on social engineering trends and other security topics.
- Scamwatch is a resource for news and tools for recognizing, avoiding, and reporting social engineering scams.

Revision #1
Created 26 August 2023 09:10:01 by naruzkurai
Updated 26 August 2023 09:10:22 by naruzkurai