This Type of Cyber Attack Preys on Your Weakness. Here's How to Avoid Being a Victim.

Opinions expressed by Entrepreneur contributors are their own.

You may not realize it, but social engineering attacks are the most common form of cyber attack out there. And, do you know why they are so popular?

For starters, to carry out a cyber attack, social engineering is incredibly effective. You can gain access to systems and data simply by tricking the owner into giving up their login credentials or other sensitive information. Social engineering attacks are difficult to detect because they rely on human interaction. Yes, there have been so many successful attacks using this method, but it's interesting to know that it can be controlled. In this article, I'll be exposing you to different forms of social engineering attacks and how you can protect yourself from them.

Related: **How Small Businesses Can Shield Themselves Against Cyberattack**

What is social engineering?

Social engineering is the art of gaining unauthorized access to a network or sensitive information by exploiting human behavior or psychology. Social engineering is a popular component used as an initial access vector to gain access to a network.

Social engineering is carried out mostly via email – phishing. One example of such an attack is the 2016 FACC hit. According to this report, the CEO and CFO of FACC got fired as a result of the whaling incident that cost the company $47 million. An email, claiming to be from the CEO, asked an employee to transfer funds to support an acquisition. After the cybercriminal was long gone with the funds, it was discovered that both the email and the deal were fake. This describes how dangerous social engineering is – as it relies on human error and not some sort of software or operating systems.

In recent years, there has been an increase in sophisticated social engineering attacks plaguing organizations. Examples of sophisticated social engineering attacks are reverse tunneling and URL shorteners, which are used by cybercriminals to launch virtually undetectable phishing campaigns.

While cyber attackers often use social engineering tactics to try and get their targets to reveal sensitive information such as passwords and financial data, it is very important you know that this method of attack is so effective and has a high success rate because people are often the weakest link in an organization's security. Hackers can use social engineering to bypass technical security measures, such as firewalls and antivirus software, by exploiting the trust and willingness of individuals to help others or follow instructions. More so, social engineering attacks are often relatively low cost, as they don't require the attacker to invest in expensive tools or infrastructure.

Additionally, social engineers are very calculative, clever and manipulative. Most cybercriminals employ social engineering to gain initial access to a network because it's easier to manipulate and fool people than break into a secure system. Here are the four major types of social engineering to watch out for:

Phishing: Phishing attacks are the most widely used form of

social engineering you need to watch out for. It involves acquiring personal and sensitive information about an individual or an organization via email by disguising itself as a trustworthy entity in electronic communication.

Pretexting: Pretexting is also another type of tricky social engineering technique to watch out for. In this kind of attack, the threat actor creates a false scenario where the victim feels compelled to comply. The attacker typically acts as someone in executive rank to intimidate and persuade the victim to follow their order.

Vishing: Vishing is another type of social engineering attack technique that has a high rate of success. It is important to watch out for this kind of attack that is done over voice communication. Typically, the visher pretends to be from a legitimate company and tries to urge you to share your sensitive information, like the example highlighted earlier.

Baiting: Baiting is another form of social engineering that exploits human weakness. The attacker puts up something enticing or compelling to lure the victim into a social engineering trap. For example, you might get “Congratulations, you are a lucky winner of an iPhone 14. Click on this link to claim it.” “Download this premium Adobe Photoshop software for $69. Offer expires in two hours.”

As an active internet user, you might have come across this or not; well, it’s advisable to pass without clicking because it’s most likely a trap!

Related: Hackers Aren’t The Only Unseen Enemy Behind Cyber Attacks – Your Board’s Ignorance Could Be To Blame, Too. Here’s What You Can Do About It.

Social engineering attacks are

successful because they exploit human vulnerabilities

In this digital age where so much of our personal information is out there for the taking, it is easy for cyber attackers to gain our trust and get what they want. Moreover, it is not just clicking on phishing emails that can leave you open to an attack. It can be as simple as answering a phone call from someone who is pretending to be from your bank or tech support.

Social engineering attacks are incredibly easy to execute. All it takes is a little bit of knowledge about how people work and some basic hacking skills. Then with it, a skilled hacker can easily get information from innocent victims, information that can be used to gain access to networks or steal identities.

However, that does not mean you are powerless against them. Well, here are key tips that can help you recognize and prevent social engineering attacks from happening to you.

Common telltale signs that indicate you're under the web of social engineering attackers:

1. When you keep receiving unusual emails and phone calls from unknown sources especially when they contain attachments and links to click on.
2. When an unknown person keeps requesting your sensitive and personal information such as name, address, DOB, credit card numbers and so on.
3. When an unknown person creates a sense of urgency and pressure just to get you to act swiftly without proper thoughts or analysis on matters related to work or

personal accounts. And many more.

How can you protect yourself from social engineering attacks?

- Firstly, be aware of the dangers of social engineering attacks. These attacks are becoming more and more common, so it is crucial to be vigilant.
- Be suspicious of unsolicited emails, calls or texts and never give out your personal information unless you are sure who you are dealing with. For example, if you receive an email from someone you do not know asking for sensitive information, do not respond. If you are not sure whether an email is legitimate or not, do not hesitate to reach out to the sender to verify its authenticity.
- Only enter your information on trusted websites and make sure the URL starts with “HTTPS.”
- Make sure the security software of your computer is up-to-date.
- Use two-factor authentication, which is an extra layer of security that requires something you know (like a password) and something you have (like a physical security key or mobile app).
- Make sure your passwords are strong and unique. Do not use the same password for multiple accounts, and ensure that your passwords are a mix of letters, numbers, and symbols.
- Keep your personal information private. Do not share your passwords or login credentials with anyone, and be careful about the information you post online. Keep your personal information private!

Social engineering attacks thrive in exploiting the human factor. People are often the weakest link in cybersecurity, and attackers know how to take advantage of that using social

engineering.

Remember that this is one of the most common ways cyber attackers gain access to your systems. That means they use deception to gain your trust and then extract information from you, like your passwords or login credentials.

Now you have learned what you can do to keep yourself safe, remember that cyber attackers are experts at getting people to click on links and open attachments. Therefore, be vigilant when you are browsing the web and emailing.

To fortify yourself against social engineering attacks, you have to stay up-to-date on the latest security threats. How do you do that? Do that by subscribing to a cybersecurity newsletter and reading blog posts on cybersecurity, such as this one, to stay informed.

https://www.entrepreneur.com/science-technology/this-type-of-cyber-attack-preys-on-your-weakness-heres/438839