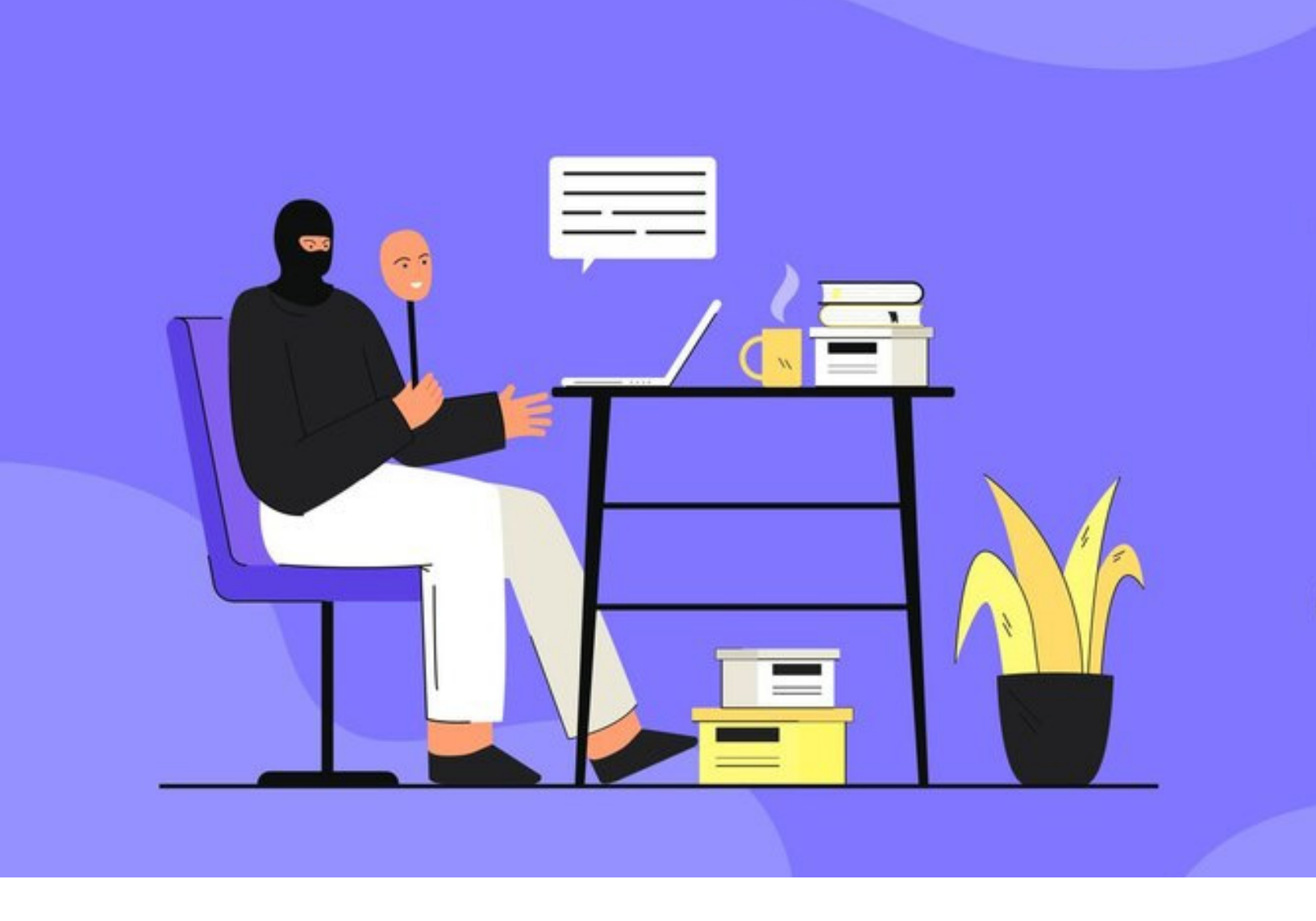


What is a Social Engineering Attack and How to Protect Yourself

Cybersecurity professionals continue to defend businesses and networks from different types of threats. Cyber-attacks target thousands of businesses and private users every day. The primary motive of the attack is money, but it may also include the theft of personal information.

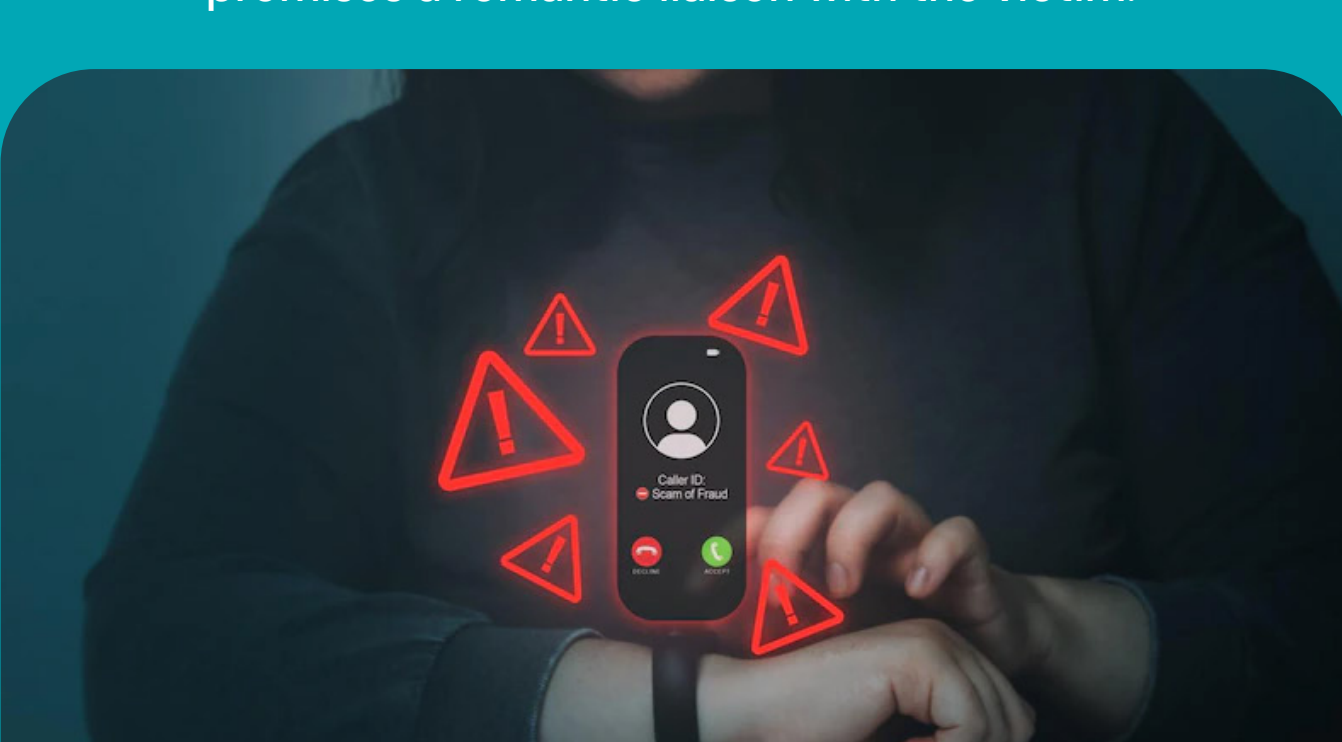
Introduction to Social Engineering

Social engineering is the use of psychological manipulation to trick unsuspecting users into giving away information or downloading infected code for malicious purposes. The fact that social engineering relies on human error rather than flaws in software and operating systems makes it particularly dangerous. Legitimate user failures are significantly less predictable than malware-based intrusions, making them more difficult to spot and stop.

The end goal of most social engineering attacks is to gain access to sensitive information or breach an account.

Social Engineering Attack Techniques and Types

Social engineering attacks take many forms, whether it's a fake call from someone claiming to be the CEO of a company, a bank asking for financial information, or even a catfish that promises a romantic liaison with the victim.



Phishing

Phishing attacks occur when a social engineer masquerades as a trusted entity or a person of authority in the hopes of extracting confidential information from the victim. It is relatively easy for attackers to spoof emails and trick users into thinking that the message came from a trustworthy source.

Spear Phishing

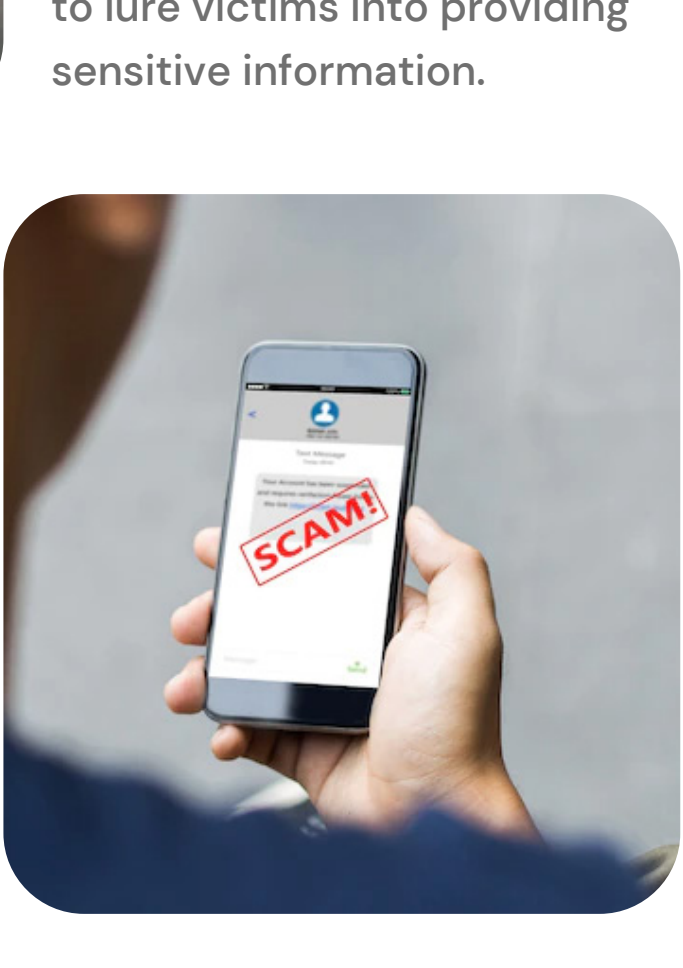
Spear phishing is a subset of phishing attacks and is directed toward a specific individual or business. It often includes information that may catch the target's attention, such as current events and financial information.

Vishing

The term vishing is a portmanteau of voice and phishing. The perpetrator initiates voice communication with the victim (usually over the phone) because it is a more effective means of gaining trust to lure victims into providing sensitive information.

Smishing

Smishing attacks involve the use of messages sent using SMS (short message service). These messages use convincing text to trick would-be victims into clicking on a link or sending sensitive information.

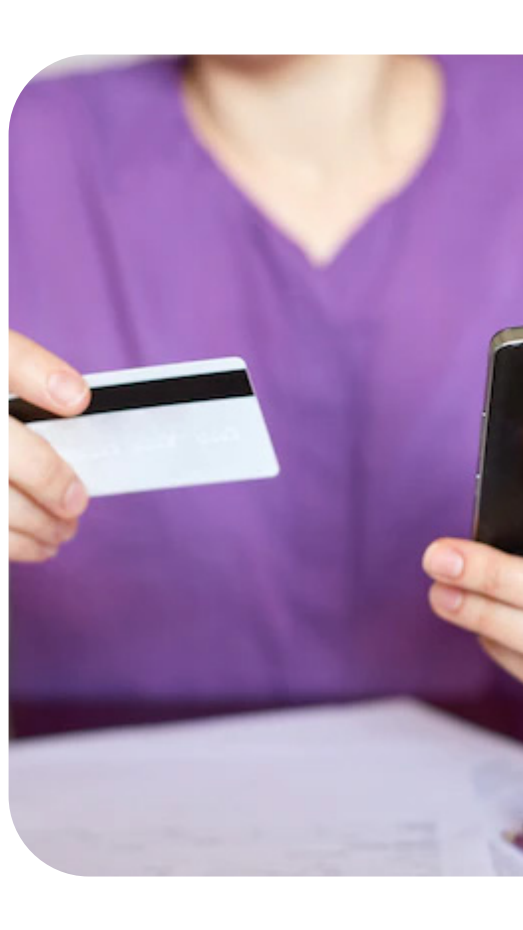


Whaling

A whaling attack, also known as CEO fraud, is when a cybercriminal claims to be a senior member of an organization or someone with authority. While phishing scams don't have a set target, whaling attacks are very specific to the person.

Baiting

Baiting relies on the victim's curiosity or greed. It will lure victims with a false promise or reward to steal their identity and infect their systems.

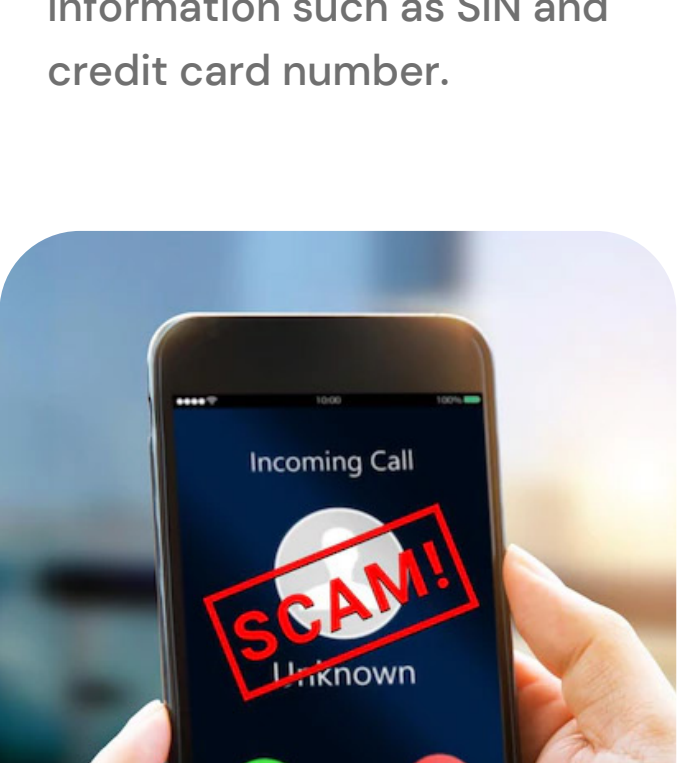


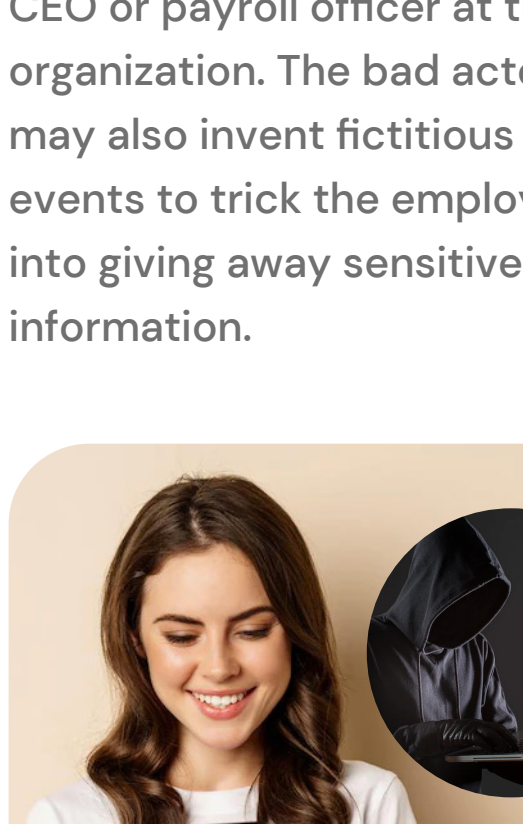
Scareware

Scareware is a common phishing attack that hackers use to warn their victims of a non-existing threat. The most popular scareware is an email or call that claims to be from the Canada Revenue Agency (CRA) and requests personal information such as SIN and credit card number.

Pretexting

A pretext is very similar to whaling attacks, in that, the malicious actor calls an employee and claims to be the CEO or payroll officer at the organization. The bad actor may also invent fictitious events to trick the employee into giving away sensitive information.



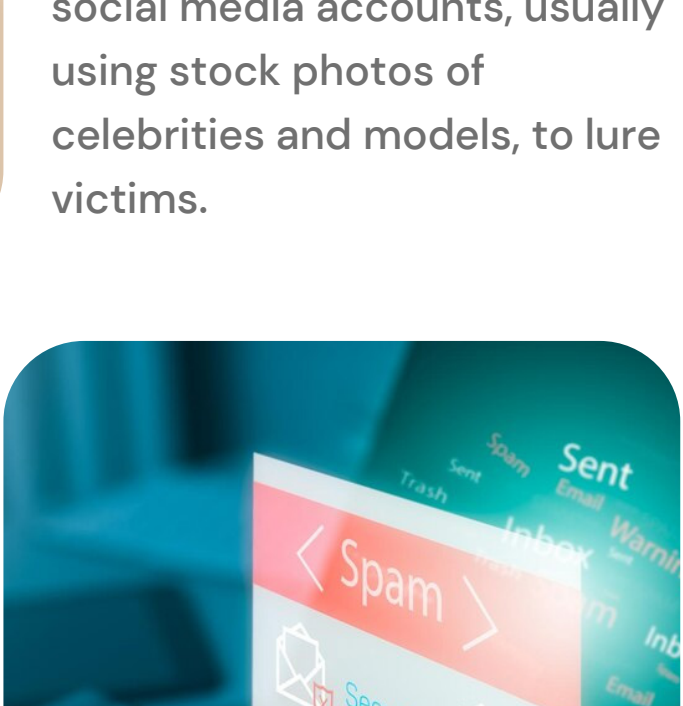


Honey Trap

A honey trap usually involves the promise of a relationship with the victim, usually of an intimate nature, in order to extract information or resources. The most common honey trap is the use of fake social media accounts, usually using stock photos of celebrities and models, to lure victims.

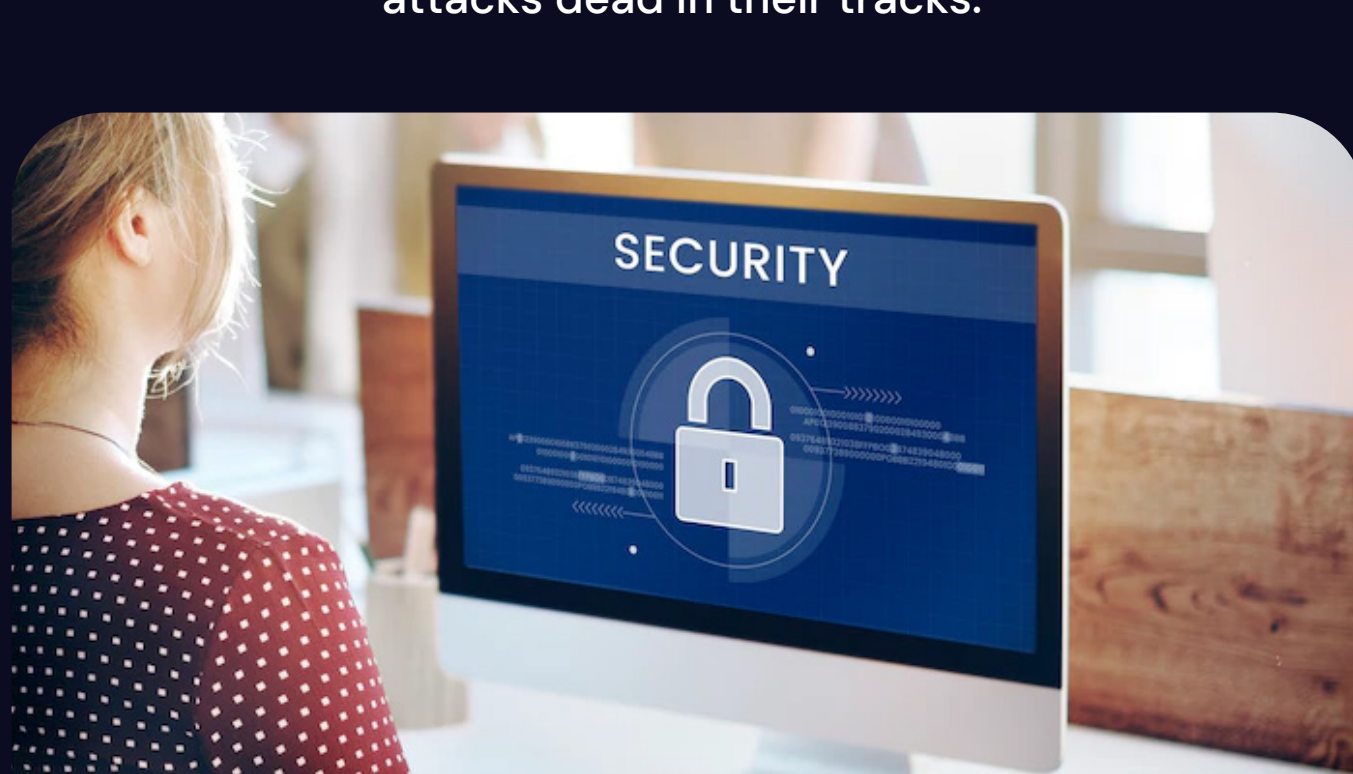
Email Spamming

Email spamming is when the cybercriminal sends annoying and often dangerous emails, usually in bulk, to several users. At best, these emails may be harmless and only advertise products or services. At worst, they may attempt to steal information.



How to Avoid Social Engineering Attacks

This section explores how you can stop social engineering attacks dead in their tracks.



Evaluate the Source of the Information

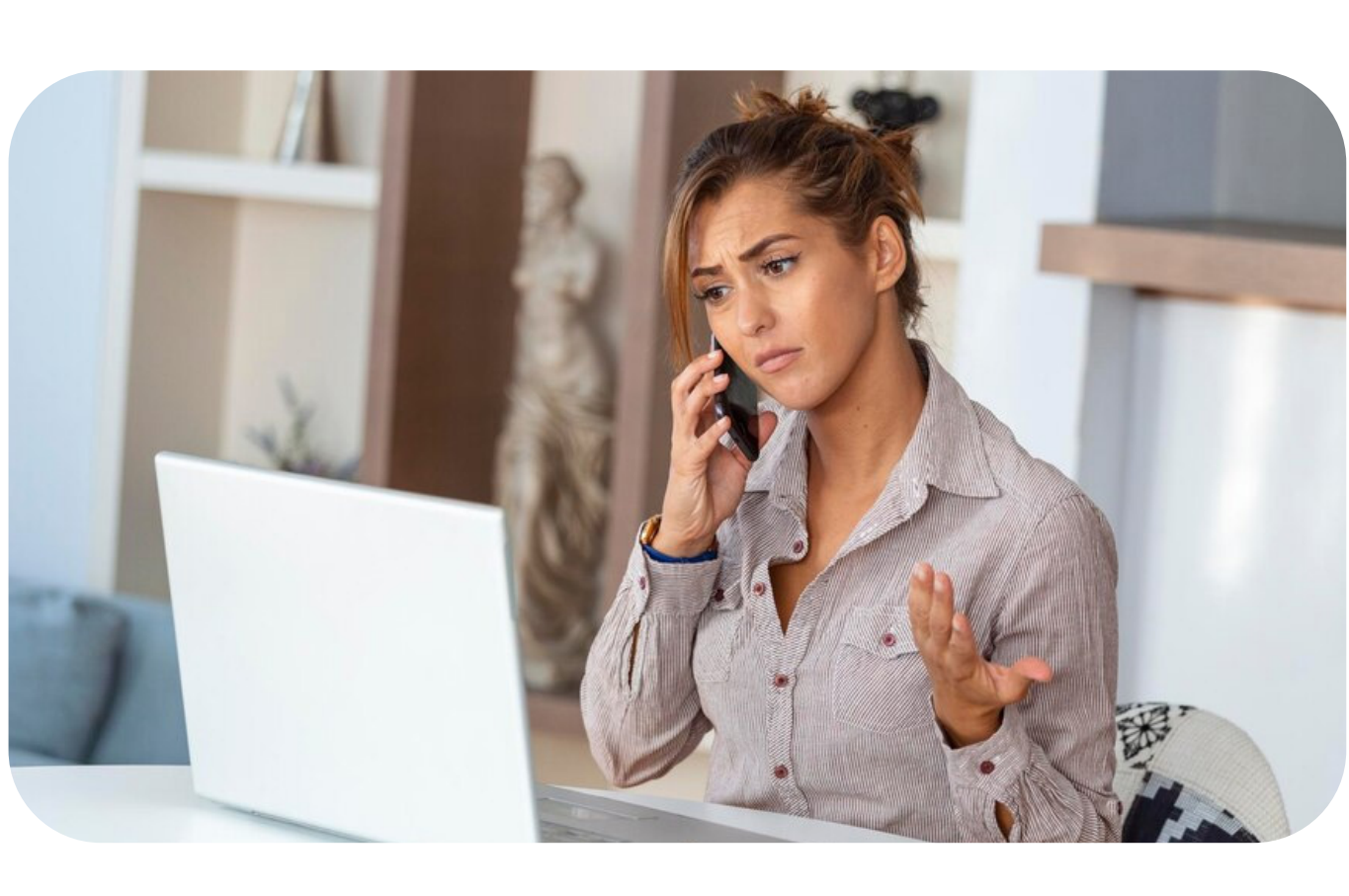
Whether you get a phone call from someone claiming you won a free 4-night cruise or an email from your CEO asking for sensitive information - you should start assessing the origins of the communication.

In the case of email, inspect the email header and cross-reference it against legitimate emails from the same sender. Look for grammar errors and spelling mistakes - a legitimate organization, especially a financial firm, have an entire team of qualified experts whose sole task is communications.

Also, the email contains links or attachments which allows you to provide sensitive information or download malicious file into your system. Always make sure to avoid these emails to eliminate the risks.

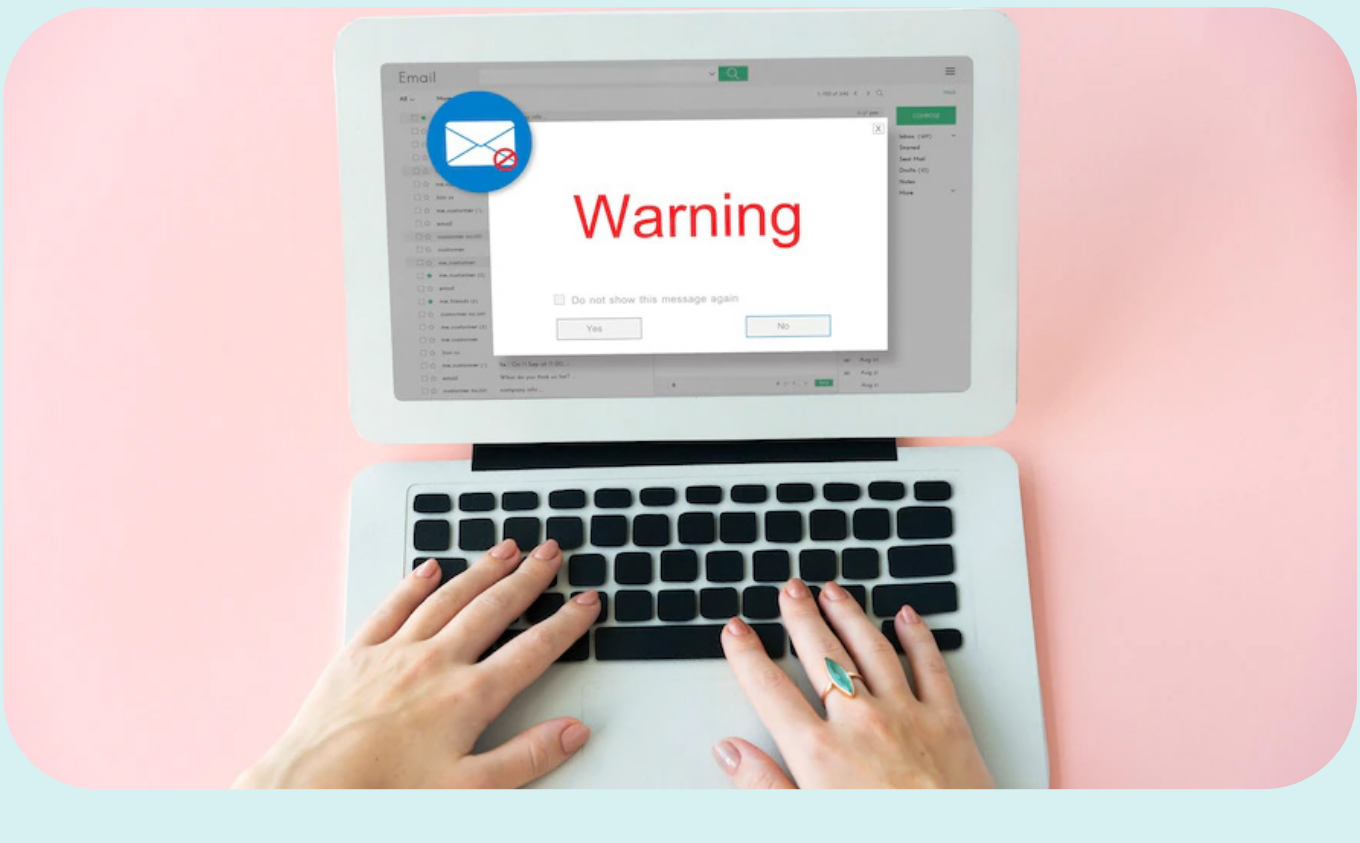
Cross-reference all Facts that they Know

Start asking a few questions for information you would expect them to have. For example, a bank would know your full name, address, details of transactions, and other information. Your CEO would know specific details pertaining to your employment. If the source doesn't have obvious information on you, then they are very likely to be fake.



Use Email Gateways and Filters

Email gateways are increasingly popular among users and businesses alike. They scan all communications for URLs, signs of malicious content, and obvious signs of social engineering attacks. Emails that fail the test are either quarantined or rejected.

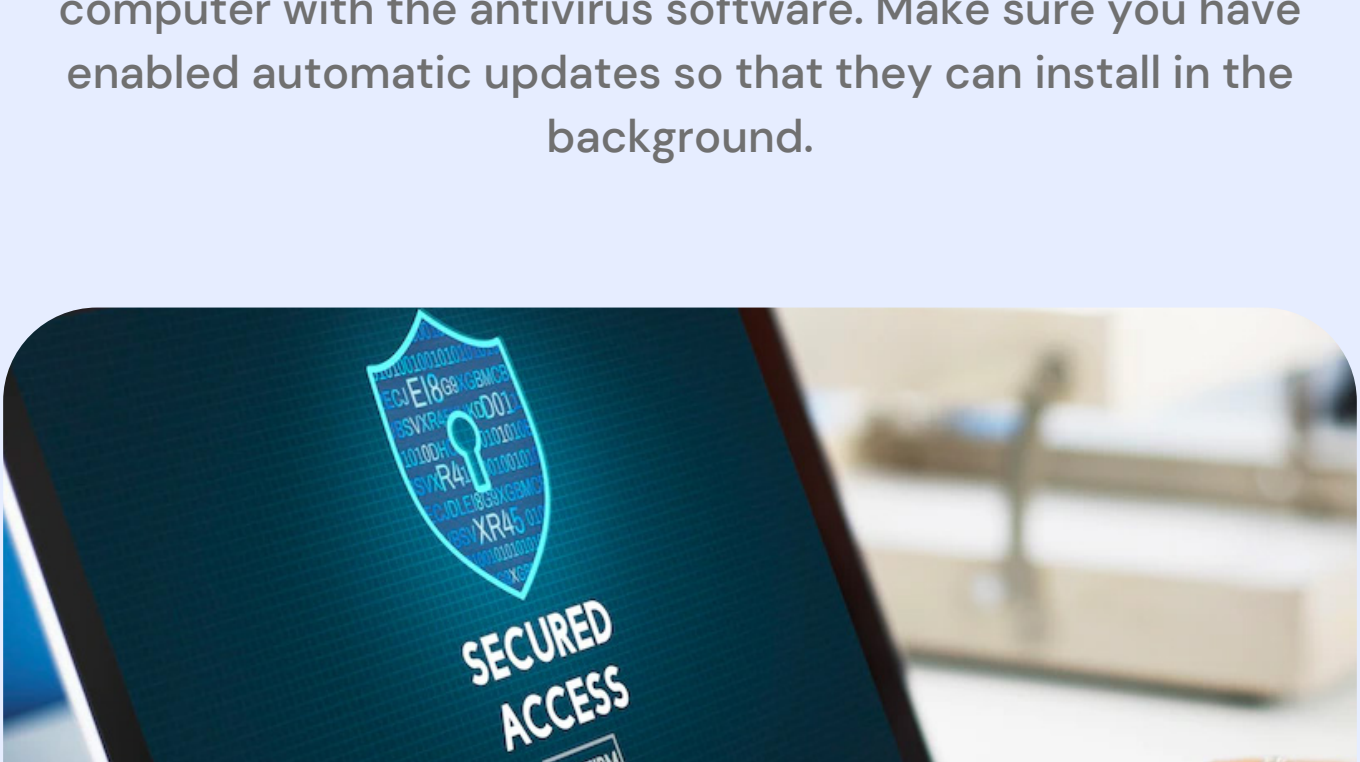


Secure Your Device

It is just as important to secure your devices to prevent social engineering attacks. The basic principles of protecting your device are the same, whether it's an enterprise system, a personal computer, or a smartphone.

Use Antivirus Software

This piece of advice cannot be stressed enough: your antivirus is your first and last line of defence. Run regular scans on your computer with the antivirus software. Make sure you have enabled automatic updates so that they can install in the background.



Enable Multi-Factor Authentication

MFA applies a second layer of security that requires another piece of identification to confirm that you are who you say you are.

These days, the most common MFA is a fingerprint scan, or a code generated via an authenticator app. Businesses operating in more sensitive industries may go beyond 2FA to include even more elements for authentication that include:

01 Only Visit Websites with SSL Certification

An SSL certificate is relatively affordable and hardly costs $10 for a year - depending on the level of security you're going for.

02 Never Share the Same Password for Different Accounts

In the event a hacker gets access to the password for your social media account, you don't want them to use the stolen credentials to break into your other accounts too.

Think About Your Digital Footprint

An effective safeguard against social engineering attacks is to carefully manage your digital footprint and take ownership of all data that belongs to you or your organization. Assess your social media accounts to see if you have accidentally given up too much information.

For example, many banks use your mother's name for security questions. Did you inadvertently give up this information on social media? If so, you may be vulnerable! We recommend using a private setting on all your social media accounts to prevent bad-faith actors from accessing your personal information.

Wrapping Up

Cybercriminals are getting smarter by the day and leveraging zero-day attacks that exploit vulnerabilities in outdated software. Threats like this are popping up every other day.

It is up to the end-user to take cyber security more seriously. For more information on the steps, you can take to protect your systems and network, get in touch with our experts here.

Get In Touch With Microsys