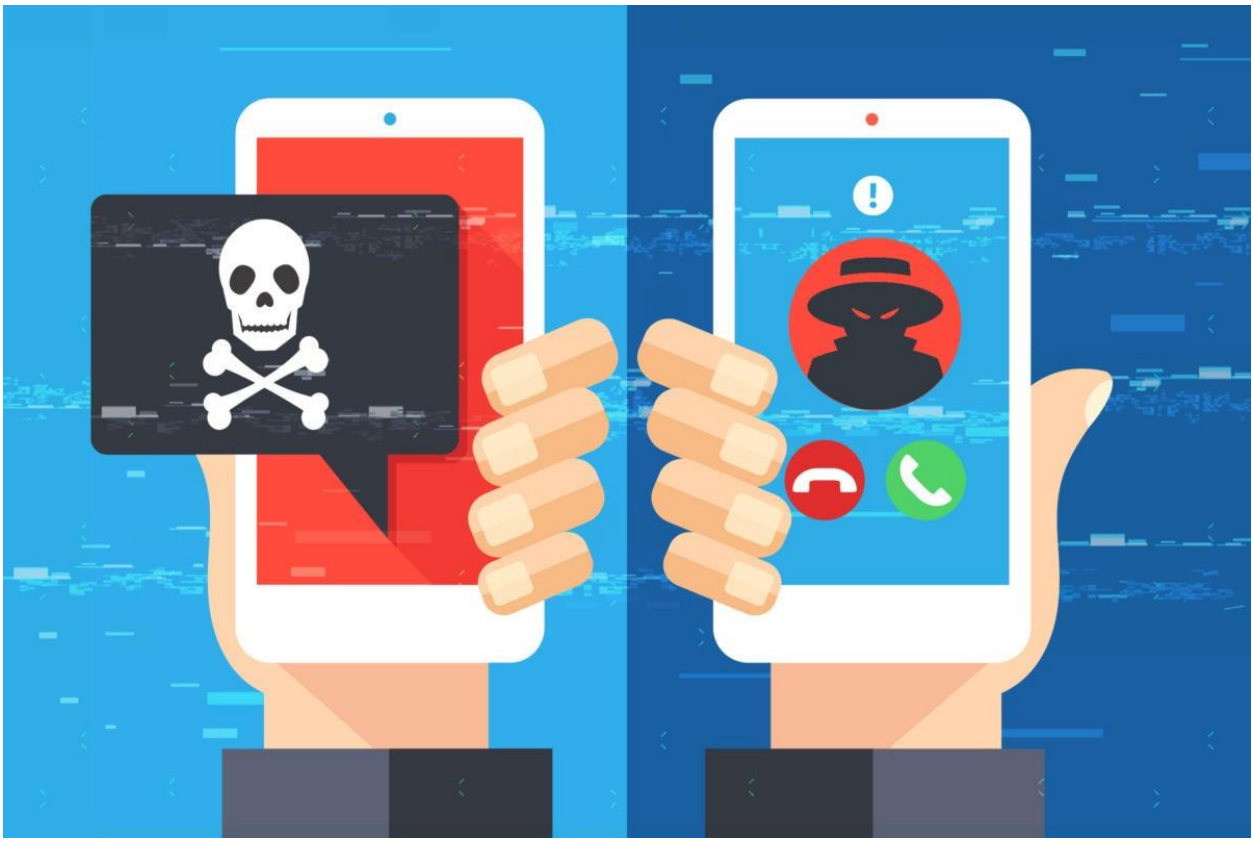
VISHING

Phone Call Attacks and Scams

OVERVIEW



When you think of a cyber-criminal you probably think of an evil mastermind sitting behind a computer, launching sophisticated attacks over the internet. While some of today's cyber criminals do use advanced technologies, many simply use the phone to trick their victims. There are two big advantages to using a phone: Unlike other attacks, there are fewer security technologies that can detect and stop a phone call attack; also, it is much easier for criminals to convey emotion and build trust over the phone, which makes it easier to trick their victims.

Recently, many of these attacks are happening over apps like WhatsApp, so be on the alert.

Let's learn how to spot and stop these attacks.

HOW DO PHONE CALL ATTACKS WORK?

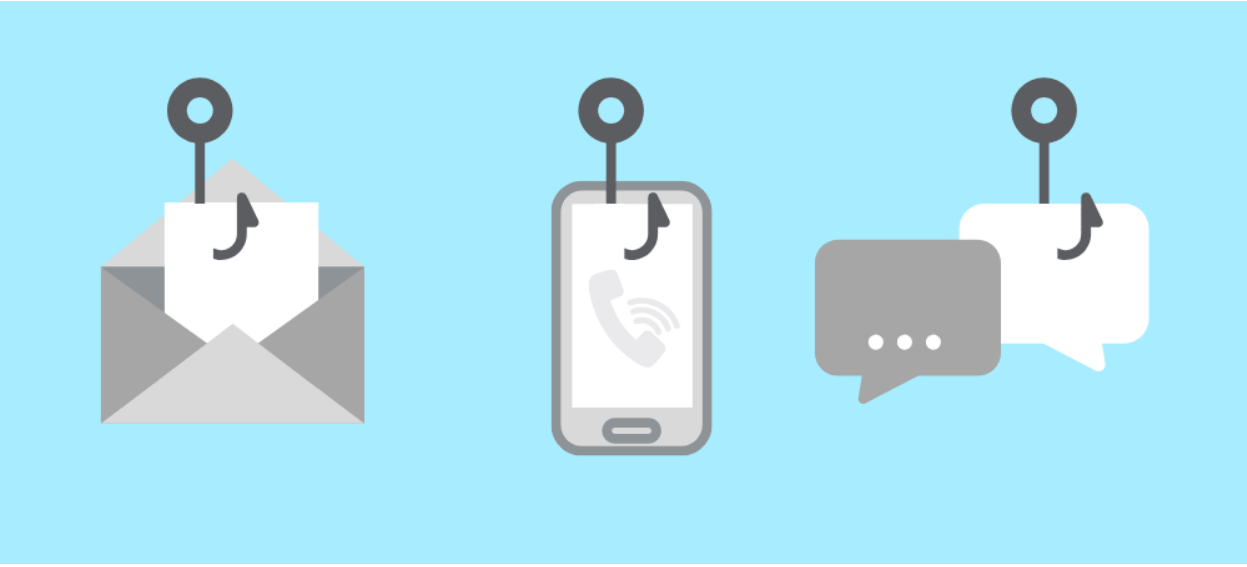
First, understand that these criminals are usually after your **money**, **information**, or **access to your computer** (or all three). They do this by tricking you into doing something you should not do, a technique called "**social engineering**." Cyber criminals often create situations that feel very urgent and realistic on the call.

Some of the most common examples include:

- The caller pretends they are from the government and informs you that you have unpaid taxes. They explain that if you don't pay your taxes right away you will go to jail, then pressure you to pay your taxes with your credit card over the phone. This is a scam. The government will send official tax notifications only by regular mail.

- The caller pretends to be from a company such as Amazon, Apple, or Microsoft Tech Support and explains that your computer is infected. Once they convince you that your computer is infected, they pressure you into buying their software or giving them remote access to your computer.

- An automated voicemail informs you that your bank account or credit card has been cancelled, and you have to call a number back to reactivate it. When you call, you get an automated system that asks you to confirm your identity as well as all sorts of private questions. This is really not your bank. They are simply recording all your information for identity fraud.



SOCIAL ENGINEERING

Social engineering is a psychological attack where an attacker tricks you into doing something you should not do through various manipulation techniques. Think of scammers or con artists; it is the same idea. However, today's technology makes it much easier for any attacker from anywhere in the world, to pretend to be anything or anyone they want, and target anyone around the world, including you. Let's take a look at two real-world examples:

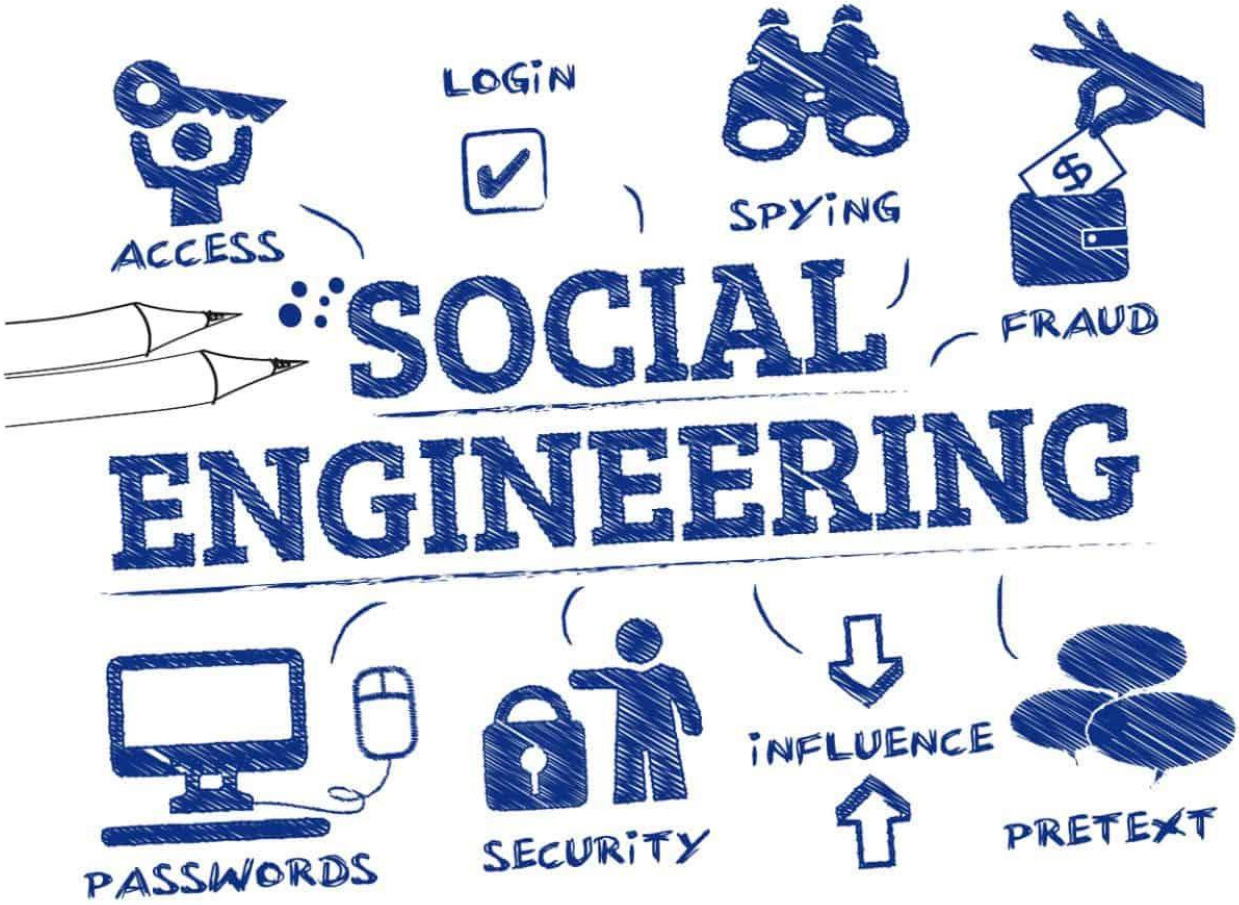
You receive a phone call from someone claiming to be from the government informing you that your taxes are overdue and that if you do not pay them right away you will be fined or arrested. They then pressure you to pay over the phone with a credit card, gift card, or wire transfer warning you that if you don't pay you could go to jail. The caller is not really from the government, but an attacker attempting to trick you into giving them money.

Another example is an email attack called phishing. This is when attackers create an email that attempts to trick you into taking an action, such as opening an infected email attachment, clicking on a malicious link, or giving up sensitive

information. Sometimes phishing emails are generic and easy to spot, such as pretending to come from a bank. Other times phishing emails can be highly customized and targeted as attackers research their targets first, such as a phishing email pretending to come from your boss or colleague.

Keep in mind, social engineering attacks like these are not limited to phone calls or email; they can happen in any form including text message, over social media, or even in person. The key is to know what clues to look out for.

SPOTTING CLUES



The most common clues include:

- A tremendous sense of urgency or crisis.
- Pressure to bypass or ignore security policies or procedures.
- Requests for sensitive information they should not have access to or should already know, such as your account numbers.
- An email or message from a friend or co-worker that you know, but the message does not sound like them - perhaps the wording is odd or the signature is not right.
- An email that appears to be from a co-worker or legitimate company, but the email is sent using a personal email address such as @gmail.com.
- Playing on your curiosity or something too good to be true.

PROTECTING YOURSELF

The greatest defence you have against a phone call attack is **yourself**. Keep these things in mind:

- Anytime anyone calls you and creates a tremendous sense of urgency or pressure, be extremely suspicious. They are attempting to rush you into making a mistake. Even if the phone call seems OK at first, if it starts to feel strange, you can stop and say “no” at any time.
- Be especially wary of callers who insist that you purchase gift cards or prepaid debit cards.
- Never trust Caller ID. Bad guys will often spoof the number, so it looks like it is coming from a legitimate organization or has the same area code as your phone number.
- Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how they can infect your computer.
- Unless you placed the call, never give the other party information that they should already have. For example, if the bank called you, they shouldn’t be asking for your account number.
- If you believe a phone call is an attack, simply hang up. If you want to confirm that the phone call was legitimate, go to the organization’s website

(such as your bank) and call the customer support phone number directly yourself. That way, you really know you are talking to the real organization.

- If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way you can review unknown calls on your own time. Even better, on many phones you can enable this by default with the “Do Not Disturb” feature.

CONCLUSION

Scams and attacks over the phone are on the rise. If you suspect someone is trying to trick or fool you, do not communicate with the person anymore. Remember, common sense is ideal. **YOU** are the best defence at detecting and stopping them.