Don't Take the Bait: Phishing, Fake Messages and the Human Hacker

Some of the most successful cyberattacks don't begin with a brilliant hacker defeating a computer's security system. They begin with an ordinary person receiving an email, text message or telephone call and believing what it says.

This is **social engineering**: manipulating people rather than machines. The criminal takes advantage of perfectly normal human reactions such as curiosity, fear, trust, sympathy and the desire to solve a problem quickly. Instead of breaking through your computer's defenses, the attacker tries to persuade you to open the door.

Phishing: An Old Trick That Still Works

Phishing usually begins with a message pretending to come from an organization or person you trust. Your bank may supposedly warn that your account has been compromised. A retailer may announce that an expensive purchase was charged to your account. A delivery company may claim that your package cannot be delivered. The IRS, Social Security Administration, Microsoft, Apple or another familiar name may appear in the message.

The message typically asks you to take some immediate action. Click this link. Open this attachment. Call this number. Confirm your password. Pay a small fee. The criminal hopes you'll react before you have time to think.

Suppose an email apparently from your bank announces that suspicious activity has been detected. It conveniently provides a button marked **VERIFY YOUR ACCOUNT**. Clicking it takes you to a website that looks remarkably like your bank's real website. You enter your username and password, but instead of logging into your bank, you've just given your credentials to a criminal.

Watch Out for the Urgency Button

One of the easiest ways to recognize social engineering is to look for **manufactured urgency**. Criminals don't want you to have time to investigate their story.

Messages such as *Your account will be closed today*, *Payment required immediately*, *Your computer has been infected*, or *Your package will be returned unless you respond* are designed to make you act first and think later.

Fear isn't the only tool. Curiosity works, too. An unexpected message might say, *Is this you in this photograph?* Another might promise a prize, refund or unbelievable bargain. A criminal impersonating a friend might simply write, *You've got to see this!* followed by a malicious link.

The wording changes, but the objective is the same: **get you to do something before you stop to question it.**

Spear Phishing Gets Personal

Ordinary phishing messages may be sent to thousands or millions of people. **Spear phishing** is more carefully aimed at a particular individual.

The attacker may know your name, employer, occupation, friends or interests. Much of this information isn't difficult to find. Social media, professional websites and other public sources can provide enough personal detail to make a fraudulent message sound convincing.

An employee might receive an email apparently from a supervisor asking for an important document. A business office might receive what looks like a legitimate invoice. A family member might receive a message that appears to come from a relative requesting emergency assistance.

Personal details make these messages more believable, but they don't make them genuine.

Artificial Intelligence Raises the Stakes

Artificial intelligence has given scammers another powerful tool. Poor grammar and awkward wording once provided useful clues that an email might be fraudulent. Today, AI can produce polished messages in excellent English, imitate different writing styles and help criminals create convincing correspondence on a massive scale.

Even voices and images can be imitated. A telephone caller may sound remarkably like someone you know, and a photograph or video is no longer absolute proof that an event actually occurred.

This doesn't mean we have to distrust everything we see and hear. It means that an unusual request involving **money, passwords, account access or sensitive personal information deserves independent verification**, regardless of how convincing the message appears.

Don't Use the Door the Stranger Provides

One of the simplest defenses against phishing is to avoid using the contact information supplied in a suspicious message.

If your bank supposedly warns about your account, don't click the email link. Open the bank's app yourself or enter the bank's known address in your browser. If a retailer reports a problem with an order, go directly to the retailer's website and check your account. If someone claiming to be a family member asks for emergency money, call that person using a telephone number you already know.

The principle is simple: **verify through a second, independent route.** Don't let the person making the claim also dictate how you verify it.

Never Hand Over the Keys

Legitimate organizations generally don't send unsolicited messages asking you to reveal passwords, authentication codes or other security credentials. A one-time verification code deserves particular protection. If a criminal already has your password, that temporary code may be the final key needed to enter your account.

Never give an unexpected caller or message sender remote control of your computer, either. A common scam begins with someone claiming to be from Microsoft, Apple, your Internet provider or another technology company. The caller says your computer has a serious problem and offers to fix it remotely. Once granted access, the supposed technician can become the very security problem he claimed to be fixing.

Your Best Defense Is Between Your Ears

Modern computers have firewalls, malware protection, spam filters and increasingly sophisticated security systems. All of them help, but none can completely protect a user who is persuaded to ignore the warnings and voluntarily provide access.

Fortunately, the human element works both ways. The criminal depends upon your cooperation, and you can refuse to provide it.

Whenever an unexpected message creates urgency, asks for money, requests personal information or tells you to click a link, give yourself permission to do absolutely nothing for a moment. Read it again. Check the sender. Contact the supposed source independently. Ask someone else if you're uncertain.

Cybercriminals want speed. **You have the advantage whenever you slow things down.**

Phishing is called phishing because criminals throw out bait and wait for somebody to bite. You don't have to catch the hacker. Just don't take the bait.