Imagine opening your inbox to find a message that looks exactly like it's from your bank—same logo, same tone, even the same signature line. Without a second thought, you click the link to "verify your account." In that single moment, you may have handed a cybercriminal the keys to your personal information. This is phishing: a digital con game designed to trick you into trusting what you shouldn't. And it's getting smarter by the day.

One of the biggest threats we all face is phishing, and it's important to recognize the many forms it can take and how they work before they catch you off guard. The type of phishing you've probably seen the most is email phishing. This is when scammers send emails that look like they're from a real company or person, hoping you'll hand over personal details like bank info or work logins. Instead of asking outright, they'll often trick you into clicking a link—maybe to 'claim a prize' or to 'reset your password'—so it feels convincing. Other forms of phishing you may have experienced are Smishing and Vishing.

Smishing is a type phishing where a scammer sends a text messaging appearing to be from a legitimate source, such as your bank, an online store, or a shipping company requesting that you take some action. More recently for Southern Californians, this came in the form of a text message appearing to be a text from FasTrack requesting you pay missed tolls, or you will incur additional penalties. While the vector, text messages, is different, the goal is the same-trick you into willingly providing your personal information. Vishing is when a scammer tries to trick you over the phone into giving away personal information. They might pretend to be from technical support, the IRS, or your bank. Again, the goal is the same, to trick you into giving away your personal information.

To protect yourself from email phishing, smishing (text scams), and vishing (voice scams), always pause and think before responding. Check the sender's details carefully, avoid clicking on unexpected links, and never share personal information with unverified sources. Check out the image below to see what a phishing email looks like—and how to spot the warning signs:

If something feels off, contact the company directly using a trusted number or website—not the one in the message. Staying cautious and verifying first is the best defense.