Email attacks, commonly referred to as phishing, have become one of the primary attack methods in the cyber thief’s playbook. These attacks try to trick you into taking an action that allows them to steal personal information and money. Here are some additional points and a few simple tips to help keep you from taking the bait and falling victim to these attacks.

WHAT’S IN A PHISH

✓ Malicious links or attachments. The attacker’s goal is for you to open an infected attachment – say a PDF or Microsoft Office document – or to click on a link to a malicious website, either of which can install a virus on your computer. If successful, it can give the attacker complete control of your system and allow them to steal your identity and your money.

✓ Requests for confidential information. When they’re not trying to infect your computer, the bad guys are trying to collect information from you with the same purpose in mind: to steal your money or identity. Phishing emails may contain links to imposter websites that look authentic in order to obtain your user ID and password or other personal information.

PROTECTING YOURSELF

✓ When in doubt, throw it out. Bad links in emails, tweets, posts and online advertising are popular avenues used by cybercriminals to compromise computers. If it looks suspicious, even if you know the person sending it, it’s best to just hit delete.

✓ Dear Customer. Did the email use a generic salutation such as ‘Dear Customer’ or nothing at all? Your bank and other service providers know who you are and will typically personalize their emails with your name and the last few digits of your account number. Be wary of emails that seem overly general and could be addressed to anyone.

✓ Think before you act. Did the unknown sender ask for your bank account number or have an urgent call to action. They are almost always a scam. As are those with offers too good to be true – did you really think you’ve won the European lottery?

✓ Be suspicious of attachments. If you don’t know the sender, or receive something from a friend that looks suspicious, don’t open the attachment. Opening infected attachments can install malware on your computer, which can steal your personal information and your money. If it is from a friend, you can always pick up the phone and give them a quick call to make sure that they actually sent it.

✓ Don’t click on links from emails or texts. Your best bet is to enter the website’s address manually or select it from your ‘Favorites’ or list of bookmarked sites.

✓ Bad grammar. You don’t need to call in the grammar police, but if you receive something with lots of spelling mistakes or improperly worded sentences, it’s a good indication of a phish. Legitimate businesses go out of their way to proofread all of their email.

✓ Hover over website links. If you hover your mouse over a website link, you will see the website you’re about to visit. You can do the same thing with smartphones or tablets by holding your finger on the link for a second or two. If the link in your email is different from what you see when you hover over it, things aren’t on the up and up. Instead, type the website directly into your browser.
FIND A PHISH?

✓ Looks suspicious? If you think you’ve received a phishing email, just delete it. There’s no need to report it.

ONLINE SAFETY TIPS

✓ Make passwords long and strong. Use a mix of capital and lowercase letters, numbers and symbols to create a secure password that is difficult to guess.

✓ Unique account, unique password. Using different passwords for each important account helps thwart cyber thieves and helps keep you safe.

✓ Keep a clean machine. Regularly check your computer for viruses and malicious software with a trusted and reputable antivirus program – and make sure it’s up-to-date. Watch out for fake antivirus programs that may try to trick you into downloading them by using scary looking popup windows that say your computer is infected.

✓ Automate software updates. Always update your operating system, web browsers and software as soon as new versions are available. You can make this easier by turning on automatic updates, which will download and install the updates as they become available. This is one of the best defenses against viruses, malware and other online threats.

✓ Enable a firewall. Firewalls prevent unauthorized people from ‘breaking through’ your computer. They are built into most operating systems, security software and routers.

✓ Admin user account only to complete a specific task. Using a standard user account for daily activities helps protect your computer from viruses and malware by limiting changes that affect the entire system. Save the administrator account for those times when you do need to install new hardware, programs or software updates.

✓ Consider the information you post on social media sites. More than just family or friends may see or use it. This information often serves as answers to website authentication questions.