In an effort to further enhance your cyber defenses, we want to highlight a couple of prominent attacks that everyone should be aware of – phishing and tech support scams. These are active threats you or someone you know have likely been exposed to recently.

"**Phishing**" is the most common type of cyber attack that affects both normal everyday people and businesses like yours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details. In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.

"**Tech Support Scams**" are when someone comes across an issue and is prompted to call a number for support. It could be a pop-up message while browsing the internet, or even something you searched for and thought you were reaching out to a reputable company. The malicious (and fake) "repair tech" is given access to your system, where they can gain entry into the network, including stored passwords, email activity, and banking details. These attacks have recently become more sophisticated in that they can blank the user's screen after being given remote access. Once connected, they may try to log into various sites like Amazon, eBay, banks, or gift card sites and purchase things without your knowledge.

They may even try to collect payment information from you or ask you to complete a webform with sensitive details.

Although we maintain controls to help protect your networks and computers from cyber threats, increasing awareness is a critical component in combating these costly attacks.

If you do happen to find yourself in a situation with a pop-up, or someone you suspect logged into your computer with deceitful intentions, please power down your computer immediately and reach out to us so we can help you assess.

What You Can Do

To avoid these schemes, we suggest the following practices:

- Do not click on links or attachments from senders that you do not recognize.
- Be cautious when clicking links in emails that you do recognize and closely examine the address before clicking (hover your mouse over the link before clicking to see where it will go). Many scammers can craft emails that have logos and appear legitimate, but the link address that shows will usually look abnormal.
- Do not provide sensitive personal information (like usernames, passwords, social security numbers, or bank/credit cards) over email.
- Watch for email senders that use suspicious or misleading domain names. Closely inspect the “From” address for typos.
- Inspect website addresses carefully to make sure they’re legitimate and not imposter sites before trying to login.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

Thanks again for helping to keep yourselves, your data, and your company safe from these cyber threats.