SPOOFING AND "PHISHING" SCAMS

HOW THE SCAMS WORK:

SPOOFING – Spoofing is when someone disguises an email address, sender name, phone number, or website URL to convince you that you are interacting with a trusted source. Examples include receiving an email which looks like it is from your bank, a company with whom you have done business, or even from someone in your family; however, it actually is not. Or you receive a phone call with an area code showing it to be from another state or Washington D.C.; however, that is not from where the scammer is calling. Scammers count on being able to manipulate you into believing these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information.

"PHISHING" – Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving scammers information to which they should not have access. For example, you may receive an email which appears to be from a legitimate business asking you to update or verify your personal information by replying to the email or visiting a website. The email may be convincing enough to get you to take the requested action, or the URL might look like one you have used in the past. However, when you click on the link, you are sent to a spoofed website which looks like the real thing, such as your bank or credit card website. You will then be asked to enter sensitive information like passwords, PINs, dates of birth, social security numbers, etc... These fake websites are used solely to steal your personal and private information.

Phishing has evolved and now has several variations which use similar techniques:

- VISHING scams happen over the phone or VoIP (Voice Over Internet Protocol) calls.
- SMISHING scams happen through SMS (Text) messages.
- PHARMING scams happen when malicious code is installed on your computer to redirect you to fake websites.

WHAT CAN BE DONE TO AVOID BEING VICTIMIZED?

- Carefully examine the email address, URL, and/or spelling used in any correspondence. Scammers can change an email header and display name to look as though it is from a company you trust and hide the actual email address from which it was sent.

- Be careful what you download. Never open an email attachment from someone you do not know and be wary of email attachments forwarded to you.

- Do NOT click on anything in an unsolicited email or text message. Look up the company's phone number on your own (do NOT use the one a potential scammer is providing) and call the company to ask if the request is legitimate.

- Remember that companies will NOT contact you to ask for your username and/or password.

- Set up two-factor (or multi-factor) authentication on any account which allows it.

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, family members, and your birthday, you can give a scammer all the information they need to guess your passwords or answer your security questions.

NEVER give out your personal information to a person who is calling YOU!!!