#BeCyberSmart: PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

HOW CRIMINALS LURE YOU IN

The following messages are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

SIMPLE TIPS TO SECURE IT.

- **Play hard to get with strangers.** If you're unsure who an email is from – even if the details appear accurate – do not respond, and do not click on any links or attachments found in that email. Be cautious of genetic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.
- **Think before you act.** If you receive a suspicious email that appears to be from someone you know or from an organization, reach out to that person directly on a separate secure platform or via customer service to verify the communication.
- **Protect your personal information.** If people contacting you have key details from your life – your job title, multiple email addresses, full name, and more that you may have published online somewhere – they can attempt a direct spear-phishing attack on you. Cybercriminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.
- **Be wary of hyperlinks.** Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.
- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. Enable MFA by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token – a small physical device that can hook onto your key ring.
- **Shake up your password protocol.** Use longest password or passphrase permissible. Get creative and customize your standard password for different sites. Use password managers to generate and remember different, complex passwords for each of your accounts.
- **Install and update anti-virus software.** Make sure all of your computers, internet of things devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.