Phishing is a way for cyber-criminals to access secure or confidential information simply by making a fraudulent request for it. These scams rely on the tendency for most people to be trusting and cooperative when faced with what seems to be a legitimate request. This type of manipulation is referred to as social engineering, and it can be done via email, phone call, text message, social media message, or even in person.

Phishing scams can take many forms, but all have a common goal—gaining access to information that can be used to do harm or defraud a person or company. They are often urgent requests to click on a link, fill out a form, or otherwise provide sensitive data. Use good judgement and think before acting.

**EXAMPLES OF PHISHING THREATS:**
- An email message appears to come from your IT support team or the security team at a well-known website. The urgent email states that your account has been compromised and will be disabled unless you provide your password or PIN immediately.
- A phone call from someone claiming to be a client, vendor, former employee or other connected person, requesting an account number or access code that they “lost”.
- A social media message from a “friend” telling you to check out the attached job posting, but that requires you to re-enter your password to the site before you can read it.
- Someone appears at your desk claiming to be conducting a security audit, and asks you to enter your password to verify you have access to various accounts and systems.
- You receive a text message asking you to call in and reset your account information for the shipping company you use.

**HOW TO IDENTIFY A PHISHING ATTEMPT AND NOT FALL VICTIM:**
- Many email phishing scams use urgent language and even threats that accounts may be disabled. They often contain misspelled words, bad grammar or other flaws. Any request to provide passwords or other sensitive information should be viewed with skepticism.
- Always verify the identity of anyone requesting information. Ask for a call-back number and/or a supervisor’s number to verify authenticity. When in doubt, contact IT support.
- Verify the authenticity of any website that asks you to provide sensitive or confidential information. Look closely at the website address (URL) and verify that it’s a secure link.
- Notify IT support if you encounter any phishing scam, especially if you feel you may have been tricked into providing information.