

**To:** All Staff

**From:** Dale Wallace  
IT Manager

**Date:** Tuesday April 29, 2025

**Subject:** **Important Cyber Security Tip: What is Phishing and Spear Phishing?**

---

Phishing is an attempt to steal personal information using a fraudulent email asking for information such as username, password, social security number, or birth date.

The email generally looks authentic and appears to come from another reputable organization. The message contained in the email often includes a link to an official looking website and asks the reader to log in with their credentials.

Spear Phishing goes a step further by targeting you specifically. The cyber-criminal researches information about you that they have obtained from a public forum (e.g. LinkedIn or Facebook, etc.), and uses it to customize an email to you. This way, you are more likely to fall victim.

### **Why is Phishing such an issue?**

Phishing can result in losses to both you and the Organization. On a personal level, phishing can steal your identity resulting in financial theft and damage to your reputation. In most cases, accounts are used to generate massive amounts of SPAM.

## **How can I spot a phish?**

Phishing messages also tend to have general characteristics that should alert you, including:

- Sense of Urgency - the message conveys a reason why you need to act quickly.
- Forged Link - a link may have the name of a known organization, but not belong to them.
- Requests for Personal Information - the message will attempt to trick you into providing personal information by appearing to be authentic.
- Generic Greetings or Signatures - the messages are generally sent to hundreds of people at a time which makes them somewhat generic. Spear Phishing is an exception.
- Errors, Typos, and Inaccurate Names - the messages often include grammatical errors, misspelled words, or other inaccuracies.

## **Best Practices to avoid becoming a victim of Phishing!**

- Never give your username and password to anyone for any reason. I.T. personnel will never ask you for your password, in person, on the phone, or via email.
- Never respond, or click on links in email messages that say you have exceeded your email quota or that your account will be deleted.
- Never provide personal information to an email from a generic title, such as, Department Manager or System Administrator instead of from a specific person.
- Always roll your cursor over a link to see whether the URL matches the text that appears in the email. If it doesn't, do not click the link.
- Only enter personal information at websites where the URL begins with "https" rather than "http"; the 's' indicates secure.
- Verify an email in question by reviewing its full domain name.
  - Delete a phishing attempt by clicking the SPAM option.