Safe Email Guidelines

What Is Safe Email Practice?

- Don't open email attachments unless you know what they are.
- Don't open, forward or reply to spam or suspicious emails; delete them

Be aware of the following signs of scam email.

- Not addressed to you by name
- Asks for personal or financial information
- Asks you for password
- Asks you to forward it to lots of other people

❖ Don't click on website addresses in emails unless you know what you are opening.

❖ Do use antivirus and anti-malware tools and update them regularly.

❖ Don't open an email unless you know who the sender/source is.

❖ Please report email security concerns to the IT Help Desk.

How Do I Recognize Phishing?

Phishing is a type of email or instant message scam designed to steal your identity.

- Phishing is the act of attempting to fraudulently acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as trustworthy entity in electronic communication using email or instant message.

- Please look for the [Potential Spam] symbol when opening emails, only open if you know the sender is a trusted source.

How Can I Safeguard Against Phishing?

- Don't reply to email or pop-up messages that ask for personal or financial information.
- Don't click on links in email or instant message.
- Don't cut and paste link from questionable message into your Web browser.
- Use antivirus and anti-malware software and update them regularly.
- Don't email personal or financial information
- If you do not know the sender DO NOT open the email

If you have any questions, please contact the IT Help Desk @ 603-899-4214