Practice Safe Emailing

While email is an extremely useful tool, it is important to remember that opening malicious email attachments or clicking on unknown web addresses in emails can infect your computer. Malicious people will try to get you to open harmful email or reveal private information and passwords.

What are some risks of email?

Phishing Scams: Email that appears to be from someone in authority, IT, or a trusted business attempting to trick you into revealing your password or other personal information - often in order to fix a problem or verify an account.

- A reputable company will never ask you to send your password through email. Neither will IT.

"Click on this link" emails: Deceptive emails trying to trick you into clicking on a harmful link - possibly to compromise your computer, possibly to steal information or passwords, or trick you out of money. Even legitimate-looking URLs can lead to malicious web pages.

Attachments: Attachments can contain malicious programs.

Example: Beware of fake e-cards or job openings - Email pretending that an attachment (usually a .zip file) is an electronic greeting card or job opening from "a friend." The attachment contains a harmful program that could infect your computer.

Generic Spam: Unsolicited bulk email, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.

Privacy: Never assume that email or attachments are private or confidential. Some sure signs of a "scam" email:

- It asks you for a password
- It asks you for personal or financial information, or for money
- It is not addressed to you by name
- It asks you to forward it to lots of other people

** Delete spam and suspicious emails. ** Don't open, forward, or reply to them.

Avoiding Harmful Attachments

Don't open email attachments unless you REALLY know what you're opening:

- If it's suspicious, don't open it!
- What is suspicious?
    - Not work-related
    - The email containing the attachment was not addressed to you, specifically, by name
    - Incorrect or suspicious filename
    - Unexpected attachments
    - Attachments with suspicious or unknown file extensions (e.g.: *.zip, *.exe, *.vbs, *.bin, *.com, *.pif, or *.zzx)
    - Unusual topic lines; "Your car?"; "Oh!" ; "Nice Pic!"; "Family Update!"; "Very Funny!"

Avoiding Malicious Links

Don't click on links in email unless you REALLY know where you're going.

- If an email is unsolicited or even slightly suspicious, look up the website yourself and go there on your own instead of clicking on a link in the email. This includes:
- Links in what appear to be bulk emails - especially if they aren't addressed to you by name
- Security alerts - Example: Don't use a "Microsoft software security update" link in unsolicited email. Go to the Microsoft security web page directly on your own.
- Emails telling you to follow a link in order to verify or fix a problem with your account.
- Cryptic or shortened URLs (e.g. Tiny URLs) - these are particularly risky because you can't easily tell where they are supposed to go
- Bargains and "great offers," or links to claim an award/reward
- Links to pictures or videos from people you don't personally know

Additional "Best Practices" for Email

- Avoid sending large attachments.
- Avoid sending proprietary file formats (e.g. Word or Excel documents). Send PDFs instead when possible.
- Use the "Bcc:" (blind carbon copy) line for large numbers of recipients. This protects the email addresses of the recipients by hiding them and makes your email easier to read.