Protect Your Computer from Phishing, Viruses & Ransomeware

Watch for these warning signs in emails you receive...

Always check the FROM line of the email

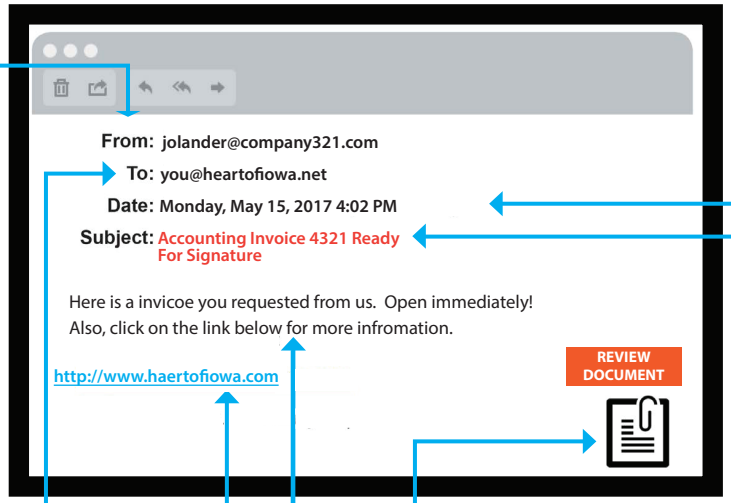
- Is the email from someone you usually communicate with? Do you recognize the sender's email address? If you do not recognize DO NOT OPEN.
- Do you recognize the domain name? Watch for suspicious domains like (mircorsoft-support.com)
- Look for misspellings with domain names.
- Do you have a business relationship with the email sender? Or had any communications by email in the past with the sender? If you have not, DO NOT OPEN.
- Watch for emails that contains an embedded hyperlink. Often times there may be more that one hyperlink. Do not click on any hyperlinks unless you know the email is legitimate.
- Also, beware of emails that include attachments. Did the sender tell you that they would be emailing you an attachment? Does it seem unusual for them to be doing so?

Check the TO line of the email for unusual or other addresses

- Carefully look to see if the email was sent to other people or if you were "cc"'d. Do you know or recognize any of the peoples names or email addresses?

Does the email contain one or more HYPERLINKS?

- ALWAYS hover over any hyperlink that is in the content of the email message. Simply hover over the hyperlink with your mouse and check the link-to address. Does it look suspicious or is it from a different website? DO NOT CLICK on any hyperlinks that display different websites or any thing that looks unusual or suspicious.
- Watch for hyperlinks that contain misspellings of commonly know websites. (Example- www.arnazon.com- which should be www.amazon.com)
- Never click on a hyperlink in an email that is completely blank other than the hyperlink. These links usually tend to be very long in nature.



Check DATE & TIME that email was sent

- Be sure to check the date and time that the email was sent. Was it sent during normal business hours? Or perhaps it was sent in the middle of the night or very early morning hours.

Always check the SUBJECT line- is it relevant?

- Watch for subject lines that are relevant to the message content. Messages with subject lines that do not match or are irrelevant to content of the message should be considered suspicious.
- Does the message appear to be a reply to a message that you never sent to anyone? If so, simply delete the message.

Watch for ATTACHMENTS! Were you expecting it? Is it a safe file type?

- Do not open attachments included with any email if you were not expectingit from anyone or any that seem suspicious to you. if the attachment does not seem relevant to the emaill message content delete it.
- There are many dangerous file types that now appear on line. Look closely at the file format extension (Example- .pdf, .jpg, .gif, .png, etc.) The ONLY safe file type that is safe to open is a .txt file format. DO NOT OPEN any email attachment that end with: .com, .bat, .scr, .exe or any file type you do not recognize!

Carefully look at the CONTENT of the email. Watch for anything that seems odd, compromising, etc.

- If the email is telling you that you must click on a link or open an attachment so that you don't experience a negative consequence - DON'T CLICK ON ANY LINK(S) OR OPEN ANY ATTACHMENT(S)!
- Watch for spelling errors and/or bad grammar in the content of the email.
- Be cautious of emails that seem to good to be true- because they usually are! For instance, if the sender asks you to click on a link or open a file for money, or to reveal something about yourself or someone you know DO NOT CLICK ON LINK(S) OR OPEN ATTACHMENT(S)!
- Never click on or open anything that you feel suspicious of or have a bad feeling about.