Phishing & Scam Emails

☐ I have read and understand.

Name: _____

Date: _____

Oops! It looks like you got tricked by a phishing or scam email.

It is important to understand that <u>there is no ONE way to tell</u> if an email is legitimate, however, there are many ways to know if the email is a phishing attempt or scam.

There are several ways to tell if an email is a phishing attempt or scam:

1. **Check the content of the email:**
    a. Emails threatening to close your account.
    b. Emails urging you to sign in or verify your account.
    c. Emails urging you to update or change your password that is about to expire.
    d. Emails about shipments or packages.
    e. Emails about getting a refund for a service or product.
    f. Emails threatening that you will be charged or that you were already charged.
    g. Emails with links to follow. It is generally advised to NOT click ANY links in emails.
    h. Emails requesting you to confirm your account details to UNLOCK your account.
    i. Emails urging you to "take action" before a certain date or time (usually within 24-48 hours).
    j. Emails from Microsoft, Google / Gmail, Norton, McAfee, etc. are most commonly sent by scammers.

2. **Check the email sender's EMAIL ADDRESS (not just the name):**
    a. Check the EMAIL address of the SENDER. <u>IT IS A SCAM</u> if it's from a random email address (@hotmail.com, @gmail.com, @outlook.com, etc.).
    b. Just because an email address LOOKS legitimate, does not mean that the email is from that sender or safe.
    c. <u>So, if an email address looks correct, DO NOT TRUST IT, it still could be a scam.</u>

3. **Do you even have "that" service or product?**
    a. Many people are tricked into opening email and following links for services that they don't even have. People who get scammed often say: *"I got an email from McAfee about a bill / charge, but I don't have McAfee. So, I opened the email to make sure they didn't have my credit card info and that they weren't going to charge me".* <u>DO NOT FALL FOR THIS. This is exactly how the scammers want you to respond.</u>

4. **Links in emails:**
    a. Most phishing and scam emails have phone numbers to call or links to click (some just want you to reply via email to them).
    b. On the computer you can use your mouse to <u>HOVER OVER THE LINK</u> then the **FULL and ACTUAL** link address will appear (usually in the bottom left-hand corner of the screen).
    c. If the link address looks fake (ex: microsoft-email.com/sign-in/) then you know the email is a scam.

Remember: Use this info to know that the email is a scam (none of this will tell you that the email is legitimate or safe).

There are tons of new types of phishing and scam emails that are being created. It is usually better to be cautious and assume that it's a scam first, then ask for help if you are not 100% certain.

None of the large companies like Microsoft will ever "lock you out of your account", or "charge you" if you don't follow the email directions within 24-48 hours. NONE OF THEM USE TIME LIMITS LIKE THAT.

If you have an email that you really think is legitimate, but you are still unsure, just CALL ME.

Derek Rowley – (253) 564-7777 – Computer Repair & Tutorials - Updated: 5 November 2023