EMAIL PHISHING RED FLAG INDICATORS

Below is a condensed list of 'red-flag' indicators that can help you determine if an email is suspicious. The more red flags an email raises, the more suspicious the email is, the more care and attention should be given, and the more likely the email should be reported and deleted.

(Note: Almost every email has a few red flags. Most of the time an email isn't malicious. But sometimes it is and that's why we need to pay attention.)

- You've never received an email from this sender before.
- The email was unsolicited, unwanted, or not relevant to you or your work.
- The wording of the email is not grammatically consistent with the communications you'd expect to receive.
- The email is addressed generically ('Dear Sir' or 'Madam,' 'To Whom it May Concern,' 'Sales,' etc.)
- The email has a call to action ('Click this link,' 'Send me this information,' 'Download this attachment,' etc.).
- The email requests money, stating that the sender has confidential or compromising information — such as' photos or videos that will be released to your contacts' unless the sender gets paid.
- The email expresses urgency, prompting you to respond 'right away,' 'by the end of the hour,' 'day, 'etc.
- This is the first time you've seen this email, but it states that it's a 'final notice.'
- The email states that the sender is 'extremely busy' ('in a meeting,' etc.) and that you must do something ' urgently,' outside your normal duties.
- The sender cannot be contacted.
- The email prompts you to contact the sender via alternative means ('Reply to this [non-standard] email address,' 'Call me at this [non-standard] number, if you have questions,' etc.)
- You don't recognize the sender.
- You don't recognize the sender's email address.
- You don't recognize the sender's domain.
- The sender's domain or links within the body of the message end in an obscure top-level domain (such as .ch, .xyz, or .site).
- The email was sent outside of business hours.
- You don't recognize the sender's email signature.
- You don't recognize the sender's phone number.
- The website listed by the sender is different from the company's official website.
- The physical address listed is different from the company's official address.
- The physical address has suddenly changed when you proceed to ship materials.
- The payment method has suddenly changed when you proceed to pay the invoice.
- The email has a suspicious 'Unsubscribe' link.
- Contact was made via a free email service, such as a yahoo.com, gmail.com, hotmail.com. cableone.net, etc.
- You're not certain where a link goes.
- An attachment prompts you to 'Enable Macros' or 'Disable Antivirus.'
- The email states that your account or system is 'at risk' and requests you to 'download an extension,' 'allow notifications,' or 'install an antivirus update' via a link or attachment, etc.