Staying Vigilant About Malicious Email Messages

IDENTIFYING MALICIOUS EMAILS

CHECK

Check that the sender's email address has a valid username and domain name. A suspicious email could look safe like: "John Doe" <John Doe@gmail.com> You may know John Doe from work, but if you look at his email address it's not actually from your organization.

VERIFY

Verify that you know the sender of an email and that its tone is consistent with the sender.

GRAMMAR

Look for grammatical errors or typos in the body of the message. Companies want to maintain a high degree of professionalism and generally do not send out emails that contain these types of errors.

TONE

Consider the tone of the email or what is being offered. If the email is threatening or sounds too good to be true, then it is probably a phishing email.

REQUEST

Pay attention to what is being requested. Most companies do not ask for sensitive or personal information in an email.

HANDLING MALICIOUS EMAILS

HANDLE WITH CARE

When in doubt, avoid opening suspicious emails and contact the sender by another means (e.g. phone call) to confirm they contacted you.

DO NOT CLICK/BUY

Do not click on links, attachments or QR codes provided in emails. If you are being asked to log in to an account for an unsolicited reason, do not click the link. Do not purchase gift cards or other items.

REPORT

If you accidentally clicked on a link it is imperative that you report to the IT department immediately.

REMOVE

On the ribbon of your outlook desktop app, or by clicking the ... beside the message in the mobile app, click on the report message button. If you feel as though there is a more serious nature to the email report it to your IT department.

https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100