Email Security Guide

think CSC

THINK BEFORE YOU CLICK

Who is the email from?

- Do you know the sender?
- Is the email typical of what you would receive from this person?
- If email from someone outside of your organization, is the request in line with your relationship?

WARNING: When you hover over the sender's email address, does the actual sender email match what it says? If it does not match the company domain or the name in the header, proceed with extreme caution.

Who is the email to?

- Was the email sent to multiple people within your organization who would typically be cc'd on the same messages?

WARNING: Watch for misspellings of your name and for people cc'd on the email who would not typically be included. Be extremely wary of emails sent to large numbers of people.

Subject line:

- Does the subject line match the contents of the email?
- Is the language of the email appropriate and accurate?

WARNING: If the subject line implies urgency, makes you panic or feel like something is wrong, or demands you to take action immediately, proceed with extreme caution.

Date:

- Was the email sent at an odd hour compared to when you received it?

WARNING: Many hackers are in other countries, so if the datestamp on a email does not match the actual time it arrived in your inbox, be cautious.

Hyperlinks:

- Is there a hyperlink included in the email?
- When you hover over (do not click) the link, does it go to a different website?
- Does the link look almost like the legitimate website link but differ slightly?

WARNING: A common phishing tactic is to emulate a legitimate website to trick you into clicking the link. When in doubt, do NOT click on the link.

Attachments:

- Is there an attachment with the email?
- Was the attachment unexpected?
- Do you typically receive attachments from this sender?

WARNING: Attachments are a common method for introducing malware, and any type of attachment can infect your network. Be extremely cautious about opening attachments. Reach out to the sender by composing a new email (do not reply, as this could simply go to the hijacked email) to confirm that recent communication was sent by them.

If the email is suspicious in any way, do not click any links. Do not open any attachments. DELETE THE EMAIL.