DON'T GET **HOOKED!**

Before you click

be on the lookout for the tell-tale signs of a phishing email. Following these basics can help protect you, CCRCE and our stakeholders.

BE CAUTIOUS

Always be careful when using email. Follow precautions **before** clicking links or opening attachments.

SPELLING ERRORS

Many **phishing** emails contain strange phrasing, typos and poor grammar. Attackers will hastily send emails to numerous people, hoping to "cast a wide net" and trick an unsuspecting victim.

URGENT ACTION

Watch out for calls to action with a **deadline** or a suggested consequence meant to cause panic. Attackers use time-sensitive and threatening language to increase the chance of clicking.

VERIFY LINKS

Phishing emails may contain a link that **appears** to be legitimate. Double-check by hovering your mouse over the link to see the actual URL.

"FROM:" ADDRESS

An email's *"From:"* address can be **forged**. Attackers may slip a small typo into the address to make it look like it's from a legitimate source, like a senior administrator, a bank or a retailer.

PERSONAL INFORMATION

Emails asking for personal information are always suspect. **Never** provide usernames, passwords or confidential information of any kind.

Chignecto Central
Regional Centre for Education

Click the Report as SPAM button, this will remove the message from your inbox to be evaluated by the IT Department.