DON'T GET **HACKED!**

Protect yourself from email fraud!

Every day, the Chignecto Central Regional Centre for Education (CCRCE) blocks thousands of fraudulent messages before they ever reach your inbox. Unfortunately, it's impossible to catch them all. That's why it's important to **always be vigilant** when using CCRCE email. Here are a few of the most common types of email fraud:

Spam

Also known as junk email, spam is designed to **trick you** into thinking their message is worth reading. *Example: Great value medical store!*

Scam

Scams are intentional **deceptions** made for gain. *Example: You won $1M! Click to claim your reward.*

Hoax

These are warnings about a **non-existent** threat. *Example: Your CCRCE account will be deactivated in 24 hours unless you confirm your email address and password.*

Phishing

Phishing emails try to entice you into disclosing **personal information**, such as your username, password and/or banking information. *Example: Your account is compromised, please log in here and change your password to receive your deposit.*

Spear Phishing

These are emails **targeted** at individuals who would typically know the name of the person being imitated. *Example: a staff member receives an email from a sender pretending to be a co-worker with a request to purchase gift cards or something else of value.*

Spoofing

In these emails, the sender's address has been **altered** to hide its true origin, a technique used by virus and spam authors to make their emails look legitimate. The email looks as though it is from one address but hovering over it reveals a different address.

Scareware

These messages are intended to extort money from you in order to prevent the sender from releasing images of you or distributing your banking information. The sender requests that you **click to install** software as your computer is infected with a virus.

How can you protect yourself from email fraud?

- Do not respond to any emails that ask for personal information such as login IDs or passwords. Please note: CCRCE will **never** ask you for your password.
- Do not share personal information, download/open attachments, or click on any links in emails if you are not certain they are genuine.
- Hover your mouse over links or email addresses to see if the address looks legitimate.
- Instead of clicking on links, open a new browser and manually type in the address.

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