Strait
Regional Centre for Education

Don't Get Hacked: Think Before You Click

protect yourself from email fraud

Every day, the Strait Regional Centre for Education (SRCE) 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 for you to always be vigilant when using SRCE email.

Here are a few of the most common types of email fraud:

1. Spam

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

2. Scam

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

3. Hoax

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

4. Phishing

Phishing emails try to entice you into disclosing personal information, such as your username, password and/or banking information. Phishing emails contain strange phrasing, typos and poor grammar. Attackers will hastily send emails to many people, hoping to cast a wide net and trick an unsuspecting victim. Example: *Your account is compromised, please log in here and change your password to receive your deposit.*

5. 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.

6. 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.

7. 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 and the SRCE from email fraud?

Be Cautious: Do not share personal information, download/open attachments, or click on any links in emails if you are not certain they are genuine.

Personal Information: Do not respond to any emails that ask for personal information such as login IDs or passwords. These emails are always suspect.

Verify Links: Emails may contain a link that appears legitimate. 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.

Urgent Action: Watch out for a call 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.

Trust your instincts: If it feels wrong, it likely should be avoided. If you receive one of these types of emails, please DO NOT click on anything in the email, immediately delete it and report it to the SRCE IT Staff at *spam.reporting@srce.ca* along with your immediate supervisor.