Don't get HOOKED

Before you click, be on the lookout for the tell-tale signs of a phishing email. Following these basic steps can help protect you, AVRCE and our stakeholders.

1 BE CAUTIOUS

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

2 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.

3 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.

4 VERIFY LINKS

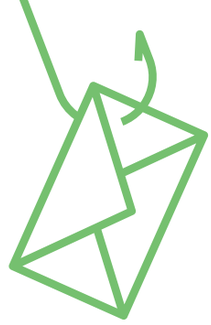
Phishing emails may contain a link that appears to be legitimate. Double-check by hovering your mouse over the link to see the actual URL.

5 "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.

6 PERSONAL INFORMATION

Emails asking for personal information are always suspect. Follow the previous steps before providing usernames, passwords or confidential information of any kind.



Annapolis Valley
Regional Centre for Education

Information Technology Division

902.538.4674
techsupport@avrce.ca
http://it.avrce.ca/