Phishing and email safety

"Phishing" is an online safety concern that involves fake emails (or spam) written to appear as if they have been sent by a genuine organization (for example, a bank) with the intent of luring the recipient into revealing sensitive and confidential information such as usernames, passwords, account credentials, personal identifying numbers (PIN) or credit card details. Typically, phishing attacks will direct the recipient to a web page to get the user's personal information.

Phishing can lead to financial losses, identity theft or viruses on your computer.

Reporting phishing attacks

If you've received a phishing email, take these steps to protect yourself and others:

1. Contact the company that was being impersonated to learn if they are alerting others of phishing scams and inform them of the incident. Report the incident to the Canadian Anti-Fraud Centre (Toll Free at 1-888-495-8501) and to the Anti-Phishing Working Group (APWG).

If you did not provide personal information to the scam, delete the email. If you did provide person information, take these subsequent steps:

1. Contact your bank or credit card company if any of your financial information was used.
2. File a complaint with the Calgary Police Service by calling 403-266-1234 and obtain a police case number.
3. Give your police case number to your bank and credit card company to place on file.
4. Provide the police case number to either of the two credit bureau companies, Equifax or TransUnion in Canada.
5. Report the phishing to the groups above if you haven't done so already.
6. Run an anti-virus scan on your computer.
7. Check your e-commerce accounts - for example, Paypal, Ebay and Amazon.
8. Tell your friends and family to be wary of suspicious emails from you.
9. Change your passwords.

How do I prevent phishing attacks

- Use your best judgment when on the internet. Listen to your intuition. Stop and think before sending personal information to anyone over the Internet or phone.
- Delete email messages that ask for personal or financial information.
- Remember that, no matter how real the email looks, no legitimate company will ask for personal information through email. If in doubt, find the phone number of the company from their official website - don't trust any phone numbers provided in the email.
- Be suspicious of emails with spelling mistakes, grammatical errors or inconsistencies.

- Be wary of emails that begin with "Dear valued customer" or use words to evoke a sense of urgency or emotion.
- Review online safety as well as email scams and safety for more information on protecting yourself online

How to tell if you're a victim of a phishing attack

The following are possible signs that your computer may have been compromised by phishing or a virus:

- Your computer runs more slowly than normal or behaves strangely. For example, it makes unexpected sounds, has lots of error messages or shows changes in files or folders.
- It 'freezes' frequently, run slowly or completely stops responding.
- Computer applications do not work properly.
- Disk drives may be inaccessible or start unexpectedly.
- There are unusual or unexpected error messages, images, distorted menus and dialog boxes.
- Your contacts may tell you that they have received e-mail messages from your address and you haven’t sent them anything.
- Your personal firewall may advise you that an application has tried to connect to the Internet although it is not a program that you are running.