Email Phishing Scams

Have you ever received an email from a bank or government agency with an enticing tag line that is so tempting to open? It may have an intriguing FREE offer or be asking you to URGENTLY update or confirm your personal information. The email may look official but it might have some slight irregularities such as: color, spelling/grammar mistakes and/or logo/design flaws.

Within the email you will be instructed to open a link or an attachment but BE AWARE by following the email prompts or responding you may be unknowingly providing scammers with your personal and/or financial information. That link that appeared legitimate was a FAKE!

Common Email Phishing Scams:

- Unemployment scams: You may have recently lost your job and received an email directing you to the unemployment website or new job opportunities. You may be prompted to provide your personal details.
- Donation scams: Emails that appear to be from well-known charities or foundations that instruct you to make a donation to receive your FREE item.
- Health Care scam: This official appearing email alerts that you have been exposed to COVID-19 and guides you to confirm your personal health care and credit card information in order to receive your prescription.

Protect Yourself from Email Phishing Scams:

- **DO NOT** open any emails or attachments from unknown or suspicious addresses.
- **DO NOT** use phone numbers or email links that were provided in the email. Research company contact information independently.
- **DO NOT** reply to the email.
- **DO NOT** give out your personal or financial information.
- Confirm invoices with the issuing company directly (such as Netflix, BC Hydro, Apple, etc.) *Remember if you aren't receiving services from a company, you won't have an invoice!*
- No government agency or bank will threaten to arrest you.
- No government agencies will request payment in Bitcoin, iTunes cards, gift cards or interact e-transfers.

When to Contact the Police

If you are a victim of fraud in which you have incurred a financial loss and/or given out your personal information call your local police to report the incident. Record details of your interaction with the fraudster including phone numbers, email addresses and communication with the scammer. Photographs or screenshots of the online conversation are helpful. If you have **not** been a victim of a fraud but have information related to scams, please report this to the Canadian Anti-Fraud Centre at **1 888-495-8501.**

Helpful Links

https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-eng.htm

https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/phshng-smshng-en.aspx

https://cba.ca/email-fraud-phishing

https://www.canada.ca/en/public-safety-canada/campaigns/covid19.html