FYI

Online Shopping

Overview

More people are shopping online than ever before. While making online purchases from the comfort of your home, cyber-criminals are using online stores and transactions to attempt to gain access to your personal and financial information. It is important to know how to protect yourself when making a purchase online.

For more information about this FYI, contact OCIOInfoProtection@gov.nl.ca.

Best Practices

Review and adhere to the Directive - Acceptable Use of the Government Network and/or Information Technology Assets.

Review and adhere to Treasury Board Secretariat's Equipment Resource Usage Policy.

Never use your government-issued email address for personal use. Have a dedicated, personal email account specifically for online shopping.

Use a secure Wi-Fi network. Do not connect to untrusted / open Wi-Fi networks (e.g., networks that do not require authentication).

Manually type URLs in the browser's address bar, rather than clicking on email links, to ensure you are going to a legitimate site and not a malicious site. Typos or errors in the URL are common when cyber-criminals create spoofed websites of popular brands. Though they might seem similar, websites like 'nika.com' or 'go0gle.ca' are not what they seem to be.

Look for “Secure” or a padlock icon in the browser’s address bar, which denotes the website’s data is secured. Do not make purchases from sites that do not have these distinctions.

Only provide confidential information requested on a website when you have verified the website’s authenticity and the website address begins with ‘https’; the ‘s’ stands for secure. Refer to FYI – Safe Web Browsing.

Do not use the same security questions and passwords for your government employee activities and personal activities.

Enable two-factor authentication (2FA) where possible. This requests a one-time code along with your password when you need to log in to your account. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when using online services.

Ensure the answers to an online site’s security questions (e.g., what is your mother’s maiden name) cannot be found on your social media platforms. Refer to FYI – Staying Safe on Social Media.

Use a credit card instead of a debit card; a debit card is like using cash. Allocate a credit card, with a lower limit, that is solely used for online shopping.

Do not use ‘Remember Me’ features on websites and mobile applications for your passwords or credit card information; always type in this information.

Review the content of the website. Oddly priced items (e.g., $1,500 headphones on sale for $150), typos in text, blurry images and logos could be signs of a fraudulent site. Refer to FYI – Phishing Don’t Get Hooked.

Legitimate stores should have their privacy and return policies clearly displayed on their online sites.

Trusted e-commerce sites will provide shipping details in the body of the email versus directing you to another site.

Steps to take if you suspect fraud or identity theft

Document all your steps from the time you suspect you have been compromised.

Change all your passwords.

Notify your bank or financial institution.

Place fraud alert flags on your accounts and check your credit report.

If you have identity theft coverage, notify your insurance company.

Monitor your emails, mail, calls, bank and credit card statements; be extra cautious.

Supporting Materials

Acceptable Use of the Government Network and/or Information Technology Assets Directive
https://www.gov.nl.ca/exec/ocio/im/employees/asset-use/

Equipment and Resource Usage Policy
https://www.gov.nl.ca/exec/tbs/working-with-us/equipment-and-resources/

FYI – Safe Web Browsing
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-fyi-information-protection-safeweb-browsing.pdf

FYI – Staying Safe on Social Media
https://www.gov.nl.ca/exec/ocio/files/FYI-Staying-Safe-on-Social-Media.pdf

FYI - Phishing – Don't Get Hooked
https://www.gov.nl.ca/exec/ocio/files/im-employees-pdf-phishing.pdf

Government of Canada - How to report fraud and scams in Canada
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04339.html

Version History

Date (yyyy mm dd)	Reference
2022-10-01	Version 1.0