FYI

Staying Safe on Social Media

Overview

Social Media platforms are an integral part of an individual or an organization's online presence. Whether it is Facebook, X (formerly known as Twitter), Instagram, Snapchat, YouTube or LinkedIn, Social Media platforms allow us to stay connected.

However, in the digital world, not everyone is your friend. These platforms also provide another venue for cyber-criminals to use phishing schemes to trick you into providing personal and confidential information.

As such, it is important to know how to manage the security and privacy settings on your social media accounts to safeguard your personal or organizational information and to make this information harder for a cyber-criminal to obtain.

For more information, contact the Cyber Security Office at: cso@gov.nl.ca.

Best Practices

The following Best Practices identify what you can do to help protect your personal or organizational information when using Social Media platforms:

Terms of Services:

Know the Social Media platform's terms of service (i.e., terms of use). Anything you post or upload might become the property of the platform.

Privacy:

Most Social Media platforms have strong privacy options. Enable these options when possible (e.g., consider whether a site really needs to be able to track your location?).

In addition, privacy options can be confusing and change frequently. Make it a habit to review them regularly and confirm they are working as expected.

Each of the major social media platforms provides guidance on privacy:

Facebook: Basic Privacy Settings and Tools

X: How to Protect and Unprotect your Posts

Instagram: Privacy Settings and Information

Snapchat: Privacy Settings

YouTube: Privacy and Safety

LinkedIn: Account and Privacy Settings Overview

Profile:

Your government email address should not be used to register for personal use of Social Media platforms (e.g., Facebook, X, LinkedIn, Hotmail, Yahoo, Google, etc.). If you have used your government email account for personal use on these platforms, unlink or deactivate your account using the following guidance:

Facebook: Add or remove your accounts from an Accounts Center

X: How to Deactivate your Account

Instagram: How to Add or Remove your Accounts from Accounts Center

Snapchat: How to Change and Verify My Email Address on Snapchat

YouTube: Change the Email Address for your Account

LinkedIn: Remove an Email Address from Your LinkedIn Account

There may be circumstances whereby there is a need to protect your identity when using Social Media platforms. Consider using an alias versus your real name. Do not associate a picture of yourself to the profile, as it negates the intent of using an alias. Colleagues, family and friends would need to be informed accordingly.

Securing Your Social Media Account

Passphrase: A passphrase is a password made up of multiple words, making it easy for you to type and remember, but difficult for a cyber-criminal to guess. Secure your social media account with a long, unique passphrase. Refer to Password Management Standard and Guideline.

Lock Down Your Account: Enable multi-factor authentication (MFA) on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is very simple to do and is one of the most powerful ways to secure your account. MFA provides a way of 'double checking' that you really are the person you are claiming to be when you are using online services, such as social media, banking or email. Even if a cyber-criminal knows your password, they will not be able to access any of your accounts that are protected using MFA.

Each of the major social media platforms provide guidance on enabling MFA:

Facebook: What is Two-Factor Authentication and how does it work

X: How to Use Two-Factor Authentication

Instagram: Securing your Instagram Account with Two-Factor Authentication

Snapchat: Set Up Two-Factor Authentication

YouTube: Turn on 2-Step Verification

LinkedIn: Turn Two-Step Verification On and Off

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

Posting:

Be cautious and think before posting including any travel plans. Consider the message and the information before posting.

Anything you post will most likely become public at some point. Do not forget that what you put out on social media does not actually ever get deleted — sure, you can delete it, but it is still out there, accessible by someone.

Deleting Posts:

Although content is never truly deleted, it is good practice to review posted content and delete posts you no longer want visible. The use of 'memories' is a good way to remember to review and delete past posts.

Each of the major social media platforms provide guidance on deleting posts:

Facebook: How to Remove Facebook Posts

X: How to Delete a Post

Instagram: Editing and Deleting Your Posts

Snapchat: How to Delete a Snap in Chat

YouTube: How to Delete YouTube Posts

LinkedIn: Edit or Delete Posts or Comments on LinkedIn Groups

Scams:

Just like in email, a cyber-criminal will attempt to trick or fool you using social media messages. They may try to trick you out of your password or credit card. They may post fun, nostalgic, seemingly innocent questions (e.g., name a song that takes you back to high school, your stage name is your middle name plus your dog's name, etc.) that are actually phishing schemes. Be careful what links you click and what information you provide. If a friend sends you what appears to be another friend request, an odd message or one that does not sound like them, it could be a cyber-criminal pretending to be your friend.

Use the website 'Have I've Been Pwnd' to search across multiple data breaches to see if your email address or phone number may have been compromised. If your email address is identified as being 'pwned', change your password on all of your accounts, especially if you use the same password across multiple accounts and/or websites.

Report suspected compromise of your account to the social media provider:

Facebook: Report Compromised Account

X: Help with My Compromised Account

Instagram: Hacked Instagram Account

Snapchat: My Account is Compromised

YouTube: Fix a Hacked YouTube Account

LinkedIn: Report a Compromised Account

Fake News and Misinformation:

One of the biggest issues facing Social Media platforms is their role in the distribution of fake news. Cyber propaganda is not new, but 24/7 social media platforms allow opportunistic cyber-criminals to manipulate public perception quickly and efficiently.

Verify if a story is credible:

- Verify the story on other reputable media outlets.
- Check the sources of the article and look at the links carefully; make sure that they are from legitimate sites.
- Research the author, the time and place of publishing.
- Check if the commenters on the story are real people or just computer-generated comments - are the posts verbatim from another person? Is it detailed or just a generic message? Facebook has a service that that you can use to check the source of posts and comments. You can access it here: Facebook.

- Read news from a broader range of titles; sometimes similar publications share stories so check outside of your normal sources.
- Visit a fact-checking website. Do your own detective work and feel more confident in being able to identify fact vs. fiction. Websites like FactCheck.org, International Fact-Checking Network (IFCN), Politifact.com/, or Snopes.com are great resources.

Supporting Materials

GNL's Social Media Policy and Guidelines
https://www.gov.nl.ca/wp-content/uploads/social_media_guidelines.pdf

OCIO's Cyber Security Awareness Campaign
https://www.gov.nl.ca/exec/ocio/security/cybersecurity/

Password Management Standard
https://www.gov.nl.ca/exec/ocio/files/Standard-Password-Management.pdf

Password Management Guideline
https://www.gov.nl.ca/exec/ocio/files/Guideline-Password-Management.pdf

FYI – Information Protection – Phishing – Don't Get Hooked
https://www.ocio.gov.nl.ca/ocio/im/employees/pdf/Phishing.pdf

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

Version History

Date (yyyy mm dd)	Reference
2019-08-26	Version 1.0
2021-10-01	Version 2.0
2022-10-01	Version 3.0
2023-10-01	Version 4.0