## Wi-Fi

Avoid conducting government business through public Wi-Fi networks.

Disable auto-connect features and always log out of your accounts on your mobile device.

Ensure websites you visit are encrypted (showing https://).

Never use your government-issued mobile device as a Wi-Fi Hot Spot.

## Passwords

Your password must be known only to you, and should be sufficiently complex that it cannot be easily guessed (e.g., avoid using spouse's name, favorite sports team, birthdays, etc.).

## Call OCIO IT Service Desk

Immediately report compromised passwords, lost or stolen devices.

When in doubt, call! We are here to help you maintain cyber security.

Cyber Security Awareness Month is an internationally recognized campaign held each October to emphasize the importance of cyber security.

The OCIO is focused on helping all employees be more secure and know the simple steps to protect themselves and government as a whole.

For more information about Cyber Security Awareness, visit the OCIO's website at gov.nl.ca/ocio

Newfoundland Labrador

**Stay vigilant.**
**Visit gov.nl.ca/ocio**

# ARE YOU RISKING A CYBER ATTACK

# CYBER SECURITY @ WORK

Cyber security and information protection is everyone's responsibility. Cyber Security means protecting your information and devices from external (internet based) and internal threats. Even small actions can make a huge difference in keeping you safe online. As the volume of cyberattacks continues to increase, it is more important than ever to know how to protect yourself and government in a digital world.

## Software

Only authorized software can be installed on a government device.

Download software and applications from trusted sources.

Always check the permissions the application requires.

Check for updates on your smartphone.

Remove unused apps on your mobile device.

## Always On, Always Connected

Leave your work computer powered on at the end of the day to ensure the OCIO has the opportunity to apply critical security updates.

When Operating System updates are available for your mobile device, install them! These updates often contain security updates, and without them your device can be vulnerable.

## Lock Your Device

Every time you leave it unattended to prevent unauthorized access.

## Government Records

Do not save secret, confidential or sensitive government information on a local computer drive, mobile device or in cloud storage.

Do not forward government information to your (or other's) personal or non-government email account.

## Portable Storage Devices

Only store confidential government information on encrypted USB flash drives.

Do not use USB drives given to you or purchased from unknown or unapproved sources.

## Physical Security

Protect your smartphone, tablet, laptop or USB Drive. These compact devices are particularly vulnerable to theft, accidental loss, or damage.

Do not leave devices unattended in unlocked cars, offices, or open cubicles, and always store devices in a secure/ locked location when traveling.