Privacy at Work

- Only visit legitimate and trusted websites while using business computers or working with business information.
- Before providing your personal information to anyone, verify that they are a trusted source (e.g., a bank would not send out personal inquiries by email, so a call to the bank might be advised).
- If someone is seeking your personal information, ask why the information is required. If the answer is not satisfactory, do not provide it.
- Be careful where, and with whom, you discuss confidential information.
- Never remove or disable any security safeguards put into place on business networks and devices (such as anti-virus software).
- Don't write your password down (if you do, hide it).

- Review, understand and comply with your employer's mobile device usage policy.
- Secure your devices. Passwords should be complex (see our Best Password Practices).
- Install only IT approved apps and software.
- If other apps are installed, review app privacy settings and/or check with IT.
- Install all IT recommended updates without delay.
- Links:
  - https://www.nytimes.com/wirecutter/guides/iphone-privacy-tips/
  - https://www.nytimes.com/wirecutter/guides/privacy-tips-for-android-phone/

- Review, understand and comply with your employer's computer usage policy.
- Use and install only recommended and approved software.
- Connect only to approved and secure internet connections – avoid Wi-Fi hotspots.
- Avoid visiting non-work websites.
- Be aware of phishing techniques in use. Report to your IT Department anything you receive that seems suspicious and any unexpected activity on your devices. Check all link destinations even in seemingly innocuous messages.
- Never share your login credentials, including passwords, with anyone.

- Review, understand and comply with your employer's work from home policy.
- Avoid using personal devices for work, and work devices for personal use.
- Router/Home Network – change admin password – change Wi-Fi password:
  - https://staysafeonline.org/online-safety-privacy-basics/securing-your-home-network
- Avoid storing files locally on your devices; store files on a network drive so they can be backed up.
- Lock your devices when not in use or if you step away, even for a short time.
- Log out completely if you are away from a device for an extended period of time.
- Secure all documents when not in use, in a locked file cabinet.
- If traveling with equipment or files, they must be locked and never left unattended.

OIPC
Office of the Information & Privacy Commissioner
Nova Scotia
Box 181
Halifax, NS B3J 2M4

Phone: (902) 424-4684
No Charge-Dial: 1-866-243-1564
Fax: (902) 424-8303

oipcns@novascotia.ca
https://oipc.novascotia.ca/