



Nova Scotia/Nunavut Command
The Royal Canadian Legion

61 Gloria McCluskey Avenue
Dartmouth, Nova Scotia B3B 2Z3

Tel: 902-429-4090
Fax: 902-429-7481

ns.legion.ca

All Branch Mail Out #56

Date: May 20, 2026

To: NS/NU Branches
NS/NU Executive Council
NS/NU Zone Commanders
NS/NU Past Presidents
NS/NU Command Staff

From: Comrade George Della Valle
President
Nova Scotia/Nunavut Command, RCL

Subject: Strengthening Cybersecurity Practices Across
All Branches

Message:

Following the recent phishing email that was sent to several branch contacts, I want to take this opportunity to reinforce some simple but important cybersecurity practices for all Legion members who use email or electronic devices for branch communication. This message is not directed at any individual or branch. Cybersecurity threats are increasing everywhere, and even experienced computer users can be affected. A few small precautions can greatly reduce the risk of future incidents.

I am asking all branch executives, secretaries, and committee members to review the following steps:

- 1.** Use strong, unique passwords. Avoid using the same password for multiple accounts. A strong password includes a mix of letters, numbers, and symbols.
- 2.** Enable two-factor authentication (2FA). This adds an extra layer of protection to your email account. Most email providers offer this feature.
- 3.** Avoid using public Wi-Fi for Legion business Public networks (hotels, airports, cafés) are not secure. If you must use them, please ensure you are connected through a secure method such as a VPN.
- 4.** Keep your computer and antivirus software up to date Updates often include important security fixes. Please ensure your devices install updates regularly.
- 5.** Do not open unexpected attachments or links If an email seems unusual, even if it appears to come from someone you know, verify it before clicking anything.
- 6.** Store branch contact lists securely Contact lists should be kept in password-protected files and not stored on shared or public devices.
- 7.** Report suspicious emails immediately If you receive a message that seems unusual or concerning, please notify your branch president or secretary so it can be reported and addressed quickly. These steps are simple, but they make a significant difference in protecting our members and our organization.

Cybersecurity is a shared responsibility, and I appreciate everyone's cooperation in keeping our communications safe.

Thank you for your attention and continued service.