ᒪᓕᒐᓕᕆᔨᒃᑯᑦ ᑲᑐᔾᔨᖃᑎᒌᖕᒋᑦ ᓄᓇᕗᒥ
NUNAVUMI MALIGALIUQTIT
LAW SOCIETY OF NUNAVUT
BARREAU DU NUNAVUT

NOTICE TO THE PROFESSION

TO: Members of the Law Society of Nunavut and Students-at-Law

DATE: October 13, 2025

SUBJECT: Cyber Security

Legal professionals are prime targets for cybercriminals due to the sensitive and valuable nature of the data they manage.

In light of increasing cybersecurity threats and recent breaches affecting legal professionals and organizations worldwide, the Law Society of Nunavut issues this Notice to remind all Members of their duty of confidentiality and technological competence. Members have ethical and professional obligations to safeguard client information and maintain the confidentiality, integrity, and availability of their systems and data.

There has been reports that members of the Law Societies of Nunavut and of the Northwest Territories are experiencing cyberattacks including impersonations of websites, emails and mail. Letters are being sent to individuals in the United States, fraudulently under the name of a member. All cyber security attacks, including If you become aware of your name being used in a fraudulent manner, must be reported to the RCMP.

If members of the Nunavut bar are insured by the **Canadian Lawyers Insurance Association**, the reporting requirements can be found here.

CLIA offers Advice of Fake Websites and Understanding and Combating Social Engineering.

Recommended Cybersecurity Best Practices

To mitigate the risk of cyber incidents, members are urged to implement the following best practices:

1. Access Control & Authentication

- Use strong, unique passwords and enable Multi-Factor Authentication (MFA) on all accounts.
- Limit access to sensitive data based on roles and responsibilities.

2. Data Protection

- Encrypt sensitive data both in transit and at rest.
- Regularly back up data using secure, offline or cloud-based solutions.

3. Software & System Updates

- Keep all operating systems, applications, and firmware up to date.
- Enable automatic updates where possible.
-

4. Email & Communication Security

- Be vigilant for phishing attempts and suspicious attachments or links.
- Use encrypted email services or secure client portals when sharing confidential information.

5. Staff Training & Awareness

- Review the security Tidbits from the e-News and other sources; sign-up for upcoming continuing legal education events hosted by the Law Society of Nunavut.
- Encourage a culture of security and proactive reporting of suspicious activity.

6. Backups

- Conduct regular weekly backups of data, stored offsite.
- Ensure to test backups or utilize a system to confirm successful completion of the backups.

Additional Resources

The following resources can be utilized for more training and tips to protect your data.

General Cyber Security Information

- Clia Cyber Security Training
- Password Security
- Data Security

Working Remotely – How to Stay Secure

- Guidance on Public Wifi
- Cyber Security at home and in the office
- Securing your device with Multi-Factor Authentication

Data Protection

- Tips for backing up your information
- Updating Software – Why it's important
- How updates protect your device