# Cybercrime is faster, smarter, and more organized than ever.

Ransomware remains the #1 cyber threat in Canada.
Over 30 new ransomware groups emerged last year alone —
many of them supercharged by AI-powered attacks.

*Source: Deloitte*

# Stay safe online with these essential tips

In today's interconnected world, cybersecurity is more important than ever. Protecting your personal and financial information from cyber threats is crucial.

Check out these tips to enhance your online security.

## 1 Use strong, unique passwords and passphrases

◇ **Create complex passwords:** Use a combination of letters, numbers, and special characters.

◇ **Avoid reusing passwords:** To reduce risk, use a unique password for each account. Reusing passwords raises the chance of a breach.

◇ **Consider a password manager:** Securely store and manage your passwords with ease.

◇ **Use passphrases where possible:** Passphrases are memorable sequences of mixed words, with or without spaces.

## 2 Enable two-factor authentication (2FA)

◇ **Add an extra layer of security:** 2FA requires a second form of verification, such as a text message or authentication app.

◇ **Protect your accounts:** Even if someone gets your password, 2FA can prevent unauthorized access.

## 3 Be cautious with public Wi-Fi

◇ **Avoid accessing sensitive information:** Public Wi-Fi, especially in busy places like airports, is often insecure and can expose your data to hackers.

◇ **Use a VPN:** A Virtual Private Network encrypts your internet connection, adding a layer of security.

## 4 Backup your data

◇ **Regular backups:** Keep copies of important files on an external hard drive or cloud storage.

◇ **Automate backups:** Set up automatic backups to ensure your data is always protected.

## 5 Beware of phishing scams

◇ **Verify senders:** Be wary of suspicious emails — attackers may use domains that mimic real ones, like @postoffice-updates.com.

◇ **Don't click on unverified links:** Check link URLs before clicking, and avoid links in text messages.

◇ **Report phishing attempts:** Notify your email provider or relevant authorities about suspicious emails.

## 6 Secure your social media accounts

◇ **Adjust your privacy settings:** Limit who can see your posts and personal information.

◇ **Be mindful of what you share:** Avoid posting sensitive information like your address or phone number.

◇ **Regularly review account activity:** Check for any unauthorized access or unusual activity.

## 7 Educate yourself and your family

◇ **Stay safe online:** Look out for the right resources to stay safe online.

◇ **Always check it twice:** If an email or SMS seems too good to be true, it likely is.

◇ **Learn together:** Make learning about cybersecurity a fun family exercise.