

YOUR CYBER SAFETY ROAD TRIP

A simple guide to staying safe
online in an **AI-powered** world.

Practical tips, real-life examples, and
simple steps to help you protect
yourself, your loved ones, and
what matters most.



PROTECT
Your Information



PREVENT
Scams & Fraud



STAY PREPARED
In an AI-powered
digital world



SPOT
SCAMS



PROTECT
YOUR ACCOUNTS



UNDERSTAND
AI RISKS



KEEP YOURSELF
& OTHERS SAFE



BE READY
FOR WHAT'S NEXT



SAME PEOPLE. SAME ROAD.
A SAFER CANADA.

LET'S GET STARTED.
YOUR CYBER SAFETY JOURNEY
BEGINS NOW.



1

WELCOME TO THE JOURNEY

HOW CYBER READY ARE YOU?

The online world is part of everyday life—from banking and shopping to staying connected with family and using AI tools. This quick check will help you see where you're doing well and where you can strengthen, so you can stay safer online.

A SAFER
CANADA
STARTS WITH
SAFER PEOPLE.



THE REALITY: Canadians are increasingly targeted by online scams, fraud, and AI-driven threats.

Source: Canadian Anti-Fraud Centre, 2024

QUICK SELF-ASSESSMENT

Where do you stand on your cyber safety journey?
Check the box that best describes you **today**.

AREAS TO CONSIDER	NOT YET I need to work on this.	IN PROGRESS I'm working on it.	YES I'm confident.
I use strong, unique passwords and multi-factor authentication (MFA).	☐	☐	☐
I can spot suspicious emails, texts and phone calls.	☐	☐	☐
I think carefully before sharing personal information online.	☐	☐	☐
I understand the risks of AI tools and know how to use them safely.	☐	☐	☐
I keep my devices and apps updated.	☐	☐	☐



**EVERY JOURNEY STARTS
WITH A CLEAR VIEW.**

Use this assessment as your starting point. You'll revisit it at the end of the guide to see how far you've come!



YOUR ROADMAP TO CYBER SAFETY

This guide takes you on a step-by-step journey through the key areas every Canadian should know to stay safe online. Each stop gives you practical tips, real-life examples, and simple actions you can take right away.

 **EACH STOP BUILDS CONFIDENCE.
EACH MILE MAKES YOU SAFER.
LET'S HIT THE ROAD.**



	STOP 1	PROTECT YOUR ACCOUNTS Build strong passwords, use multi-factor authentication, and secure your digital identity.	PAGES 3-4
	STOP 2	SPOT THE SCAM Recognize common scams, fraud tactics, and red flags before you act.	PAGES 5-6
	STOP 3	UNDERSTAND AI RISKS Learn how AI is changing scams and what to watch for.	PAGES 7-8
	STOP 4	SOCIAL MEDIA & PRIVACY Protect your personal information and think before you share.	PAGES 9-10
	STOP 5	RESPOND & RECOVER What to do if something happens and how to get back on track.	PAGES 11-12



YOUR PROGRESS TRACKER

Check off each stop as you go. Every step you complete brings you closer to a safer you online.

-   **PROTECT YOUR ACCOUNTS** ☐
-   **SPOT THE SCAM** ☐
-   **UNDERSTAND AI RISKS** ☐
-   **SOCIAL MEDIA & PRIVACY** ☐
-   **RESPOND & RECOVER** ☐

 **FINISH STRONG.
STAY SAFE.**

Revisit this guide anytime to keep building your cyber safety knowledge and stay one step ahead.



STOP
1

PROTECT YOUR ACCOUNTS

PASSWORD PARKWAY LOCK DOWN YOUR ACCOUNTS

Your online accounts hold your personal information, finances, photos and more. Strong, unique passwords, a password manager and multi-factor authentication (MFA) make it much harder for cyber criminals to get in.



1



STRONG, UNIQUE PASSWORDS

Use long, unique passwords for every important account.

- ✓ At least 12–16 characters
- ✓ Use a mix of letters, numbers and symbols
- ✓ Don't reuse passwords across accounts

REAL LIFE EXAMPLE



If a cyber criminal gets your password from one website, they'll try it on your email, bank and other accounts.

KEY TAKEAWAYS



USE STRONG, UNIQUE PASSWORDS
A different password for every important account.



TRY A PASSWORD MANAGER

Keeps your passwords secure and easy to use.



TURN ON MFA

Adds an extra layer of protection.

2



PASSWORD MANAGER

A password manager securely stores your passwords so you don't have to remember them all.

- ✓ Creates strong, unique passwords for you
- ✓ Keeps them encrypted and secure
- ✓ Makes it easy to sign in safely

REAL LIFE EXAMPLE



Instead of using the same password everywhere or writing them down, a password manager keeps track of them for you — safely and securely.

3



MULTI-FACTOR AUTHENTICATION (MFA)

MFA adds another check beyond your password, making it much harder for someone to access your account.

- ✓ Use MFA wherever possible
- ✓ Common methods include a code (text or app), a security key, or a biometric (fingerprint/face ID)
- ✓ It only takes a few extra seconds and can stop attackers.

REAL LIFE EXAMPLE



Even if someone gets your password, they still need your phone or security key to get in. This extra step protects you from most account takeovers.



QUICK TIPS

- ✓ Change default passwords on new devices.
- ✓ Avoid using personal info (e.g., your name or birthday).
- ✓ Use MFA on email, banking, social media and work accounts.
- ✓ Review your accounts regularly and remove ones you no longer use.



ACCOUNT CHECKPOINT PROTECT YOUR DIGITAL IDENTITY

Your accounts are more than just passwords. Keeping your recovery methods up to date, checking your logged-in devices, and using account alerts can help you stay in control and spot suspicious activity early.



01 RECOVERY METHODS

MAKE SURE YOU CAN GET BACK IN.

If you ever get locked out of an account, recovery methods help you prove it's you.

- ✓ Add a backup email or phone number
- ✓ Keep recovery information up to date
- ✓ Use secure and trusted contacts

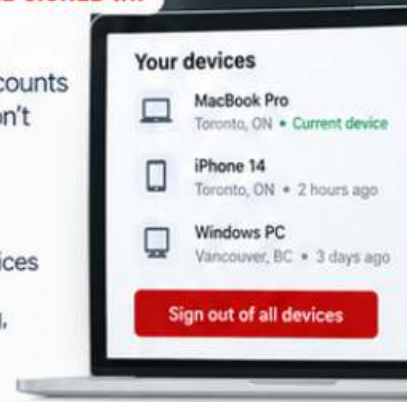


02 CHECK LOGGED-IN DEVICES

KNOW WHERE YOU'RE SIGNED IN.

Regularly review the devices that have access to your accounts and remove anything you don't recognize.

- ✓ Check active sessions
- ✓ Sign out of unknown devices
- ✓ Do this for email, banking, social media and more



03 ACCOUNT ALERTS

GET NOTIFIED ABOUT IMPORTANT ACTIVITY.

Turn on alerts so you're notified about new logins, password changes or suspicious activity.

- ✓ Enable login alerts
- ✓ Get notified about security changes
- ✓ Act quickly if you see something unusual



04 BASIC SECURITY SETTINGS

TAKE A FEW MINUTES TO REVIEW.

Review your account settings and make sure they're as secure as possible.

- ✓ Review privacy settings
- ✓ Limit what you share
- ✓ Turn on extra security features where available



PRO TIP

Take 10 minutes today to check your recovery options, review your logged-in devices, and turn on account alerts. A few quick steps can save you a lot of trouble later.



KEY TAKEAWAY

Keep control of your accounts. Keep yourself ahead.

SCAM DETOUR

STOP BEFORE YOU ACT

Scams can show up in many ways — emails, text messages, phone calls, fake websites and people pretending to be someone you trust. Know what to look for so you can stop, think and avoid becoming a target.



SUSPICIOUS EMAILS

Action Required: Verify Your Account

Dear user,
Your account has been suspended. Click the link below to verify your information.

[Verify Account](#)

! Don't click on unexpected links or attachments.

SUSPICIOUS TEXTS

10:24
+1 (437) 555-0123
Text Message
Today 10:24 AM

Your package is delayed.
Please confirm your shipping address here:
<http://canadapost-trck.ca>

! Be cautious of unexpected messages, especially those asking for personal information.

SUSPICIOUS CALLS

Incoming Call
+1 (800) 555-0199

! Don't give out personal or financial information over the phone.

IMPERSONATION SCAMS

<https://payroll-update.com>

YourCompany

Log in to view your payroll details

Email
Password

[Log In](#)

! Look for fake websites and people pretending to be someone you trust (e.g., your employer, bank or a known brand).

STOP. CHECK. ACT.



STOP

Take a moment before you click, reply or share.



CHECK

Look for signs it could be a scam (e.g., urgent language, unknown sender).



ACT

If it seems suspicious, report it and delete it.



KEY TAKEAWAY

IF SOMETHING FEELS OFF, IT PROBABLY IS.

Stop. Think. Verify.
Stay safe online.

MONEY CROSSING BEFORE YOU PAY

Scammers often create a sense of urgency and try to get you to send money quickly. Take a moment to pause and check — once money is sent, it's often hard to get back.



E-TRANSFERS

Don't send money to someone you don't know or weren't expecting.

GIFT CARDS

No legitimate business or government will ask you to pay with gift cards.

CRYPTO

Be cautious if someone asks you to send cryptocurrency — it's hard to recover.

FAKE PURCHASES

If a deal seems too good to be true, it probably is. Watch for fake online stores.

URGENT REQUESTS

Scammers often pretend to be a friend, family member or colleague and create urgency.

BEFORE YOU PAY, ASK YOURSELF:

- STOP**
Am I being rushed or pressured?
- CHECK**
Is this person or business legitimate?
- VERIFY**
Can I confirm this request through a trusted source?

KEY TAKEAWAY
Don't send money, share gift cards or pay with crypto unless you're absolutely sure it's legitimate.

AI CHANGES THE SCAM

Scammers are using AI to create more convincing messages, voices, videos and fake identities. It's getting harder to tell what's real — know what to look for.



SAME FACES.
NEW TRICKS.

VOICE CLONES

! Sounds real, but it's not.

DEEPPAKES

! Looks real, but it's fake.

AI-WRITTEN MESSAGES

! Well written, but still a scam.

FAKE IDENTITIES

! Real people, fake profiles.

SPOT THE SIGNS:



PAUSE

Take a moment before you respond.



CHECK

Look for signs it might be AI-generated or fake.



VERIFY

Confirm through a trusted channel (e.g., call the person directly).



KEY TAKEAWAY

AI makes scams more convincing, but you can still spot them. Pause, check and verify.

REALITY CHECK

CAN YOU VERIFY IT?

AI makes it easier to create convincing messages, voices, videos and fake identities. Instead of relying on whether something “looks real,” take a moment to verify the person, source or claim.

1

THE PERSON



Even if it looks and sounds real, confirm it's actually them.

2

THE SOURCE



Check the sender, website or contact the organization directly.

3

THE CLAIM



Look for trusted sources and check the context before sharing.

QUICK TIPS:



PAUSE

Take a moment before you respond.



CHECK

Verify the person, source or claim through a trusted channel.



CONFIRM

Only proceed when you're sure it's real.



KEY TAKEAWAY

Just because it looks real doesn't mean it is. Verify the person, source or claim instead of relying on how real it seems.

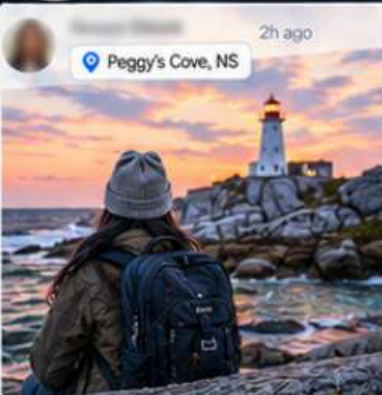
YOUR FEED KNOWS MORE THAN YOU THINK

What you post can reveal more than you intend — from your location and routines to personal details. Adjust your privacy settings, watch for suspicious messages, and think before sharing.



YOUR LOCATION

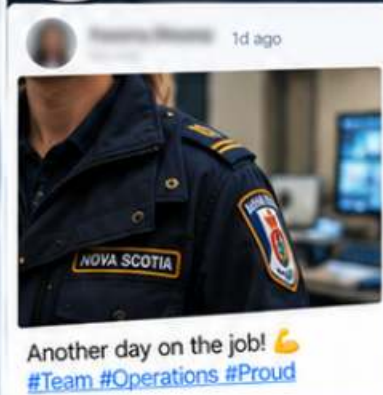
Tells them where you are.



Posting your location in real time can show where you are — at home, work or away.

YOUR WORK

Tells them where you work.



Photos in uniform, badge or office spaces can reveal your workplace.

YOUR NETWORK

Tells them who you know.



Tagged photos can reveal your friends, family and associates.

YOUR PERSONAL DETAILS

Tells them key information.



Posts like "26 today!" can reveal your exact birthday and year — useful for guessing your passwords.

QUICK TIPS:



PAUSE

Think before you post.



ADJUST

Review your privacy settings regularly.



BE CAUTIOUS

Watch for suspicious messages, friend requests and fake accounts.



KEY TAKEAWAY

Your online activity can reveal more than you think. Share mindfully, protect your privacy, and be cautious of unexpected messages.

PRIVACY PIT STOP

THINK BEFORE YOU SHARE

Your personal information is valuable. From what you share online to the apps you use and the AI tools you try, every detail can add up. Be mindful of what you share, who can see it, and what access you give.

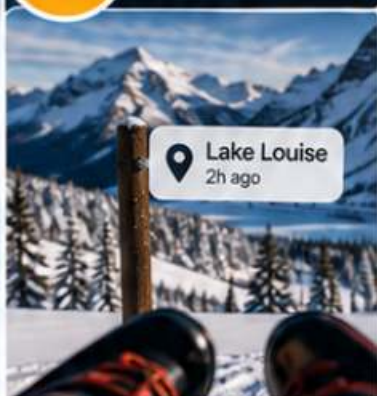


PERSONAL INFORMATION



Details like your full name, birthday, home address or travel plans can be used by attackers.

LOCATION SHARING



Sharing your location in real time can show where you are — at home, work or away.

APP PERMISSIONS



Only give permissions to apps you trust and review them regularly. Turn off access you don't need.

AI TOOLS



Avoid sharing sensitive information with AI tools, such as personal details, work data or confidential files.

QUICK TIPS:

PAUSE

Think before you share.

REVIEW

Check your privacy settings and app permissions regularly.

PROTECT

Keep personal and sensitive information off public platforms and out of AI tools.

KEY TAKEAWAY

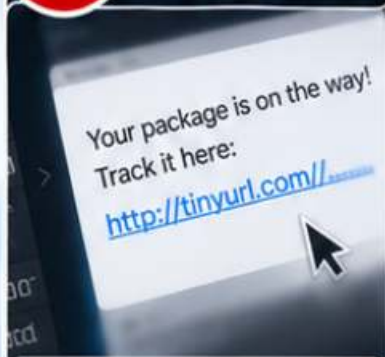
Your personal information has value. Share carefully, manage your privacy settings, review app permissions, and be cautious with what you give to AI tools.

SOMETHING HAPPENED. NOW WHAT?

Whether you clicked a suspicious link, sent money, shared a code, lost an account or are being impersonated, it's important to act quickly. Knowing what to do can help limit the damage and get you back on track.



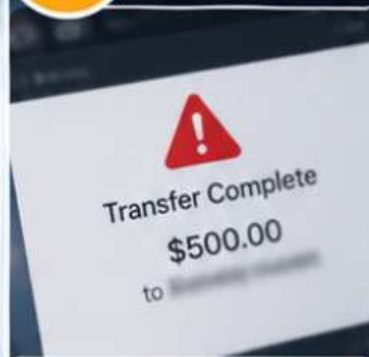
CLICKED A SUSPICIOUS LINK



Disconnect if needed, run a scan, change your passwords and watch for unusual activity.



SENT MONEY



Contact your bank immediately, report the fraud and keep records of the transaction.



SHARED A CODE



Change your passwords right away, turn on multi-factor authentication and monitor your accounts.



LOST AN ACCOUNT OR BEING IMPERSONATED



Recover your account using official channels, enable stronger security and let your contacts know.

QUICK TIPS:



PAUSE

Take a moment and assess the situation.



ACT

Follow the right steps and contact your bank, platform or IT support.



MONITOR

Keep an eye on your accounts for any unusual activity.



KEY TAKEAWAY

Acting quickly can reduce damage and help you recover. Know the steps to take and keep your accounts secure.

12

FINAL CHECKPOINT

READY
SET
CYBER

YOU'RE READY!

BE SMART. BE SAFE. BE READY.

You've completed the road map. Now it's time to put it into action and keep the momentum going. A safer, more confident digital life is within reach — and it starts with you.

YOUR NEXT STEPS



1 REVIEW YOUR HABITS

Take a few minutes to check your online habits and make sure they're up to date.



2 KEEP THE CONVERSATION GOING

Talk about online safety with your family, friends and community.



3 PRACTICE AND IMPROVE

Use what you've learned, keep exploring resources, and build new habits.



4 LEAD BY EXAMPLE

Show others that online safety matters — at home, work, school and in your community.



A SAFER, MORE CONFIDENT CANADA STARTS TODAY.

By making small changes and staying informed, we can all reduce risk, recover faster, and build a safer, more resilient Canada — together.



PEOPLE

Are aware, informed, and empowered.



COMMUNITIES

Are safer, stronger, and more connected.



CANADA

Is more resilient and ready for what's next.

 **READYSETCYBER**

BE SMART. BE SAFE. BE **READY.**

Same Road. 
A Safer Canada.

