



Connected Canadians  
Canadiens Branchés

# Digital Safety Tools: Building Your Personal Cyber Security Toolkit

## Create Strong Passwords

Your password is the first line of defense. Never reuse the same password across sites.

WEAK – Easy to Crack	STRONG – Hard to Crack
✗ password123	✓ At least 12 characters long
✗ John1952	✓ Mix letters, numbers & symbols
✗ Fluffydog!	✓ No names, dates, or pet names
✗ qwerty	✓ Use a passphrase (4 random words)
✗ 123456	✓ Unique password for every site

💡 Try [bitwarden.com/password-strength](https://bitwarden.com/password-strength) to test your password. A passphrase like "railcar shamrock routine crate" would take centuries to crack!

You can also use [useapassphrase.com](https://useapassphrase.com) to generate a passphrase or test your password's strength.

## Use a Password Manager

Think about your keychain. You have a key for your front door, your car, maybe your mailbox, maybe a storage locker. You do not memorize which key is which, you just grab the right one when you need it.

A password manager is exactly the same thing, but for your online accounts. It stores every password securely. You only need to remember one thing, your master password, and it handles the rest.

🌐 [www.connectedcanadians.ca](https://www.connectedcanadians.ca)

📍 78 George St #204,  
Ottawa, ON K1N 5W1

📞 (613) 699-7896

✉ [info@connectedcanadians.ca](mailto:info@connectedcanadians.ca)



Connected Canadians  
Canadiens Branchés

## Here is how it works:

- 1 You create ONE strong master password
- 2 The app generates a unique password for every site
- 3 It auto-fills your login whenever you visit that site
- 4 If one site is hacked – no other account is at risk

Some popular password managers are: Bitwarden, Google Password Manager, and Apple Passwords.

⚠ Write your master password down and keep it somewhere safe at home. There is no recovery if you forget it.

## Check If Your Data Was Leaked

Visit [haveibeenpwned.com](https://haveibeenpwned.com) and enter your email address to see if it has appeared in a known data breach.

Result Types	
✓ Good News: "No pwnage found!" You're in the clear.	⚠ Action Needed: "Oh no – pwned!" Change those passwords immediately.

💡 Sign up for free email alerts at [haveibeenpwned.com](https://haveibeenpwned.com) so you know immediately if your data is compromised in future breaches.

🌐 [www.connectedcanadians.ca](http://www.connectedcanadians.ca)

📍 78 George St #204,  
Ottawa, ON K1N 5W1

📞 (613) 699-7896

✉ [info@connectedcanadians.ca](mailto:info@connectedcanadians.ca)



Connected Canadians  
Canadiens Branchés

## Spot Scams & Phishing

Scammers rely on **panic**. The moment you feel rushed, threatened, or confused is exactly when you need to slow down.

Use this three-step rule every time:

- **STOP.** Do not click, pay, or give any information. Hang up or close the browser. Scammers create fake deadlines (“Act in the next 10 minutes!”) to stop you from thinking clearly.
- **BREATHE.** Ask yourself: Did I initiate this contact? Are they asking for something unusual like gift cards, a wire transfer, remote access to my computer? Would I be embarrassed to tell a family member? If anything feels off, trust your gut. It is almost always right.
- **CALL BACK.** Hang up and call the organization back using a number you find yourself, from their official website or the back of your bank card. Never use a number the caller provides. If it was a real agency, they will be there when you call back. If it was a scam, the number will not match.

No real government agency, bank, tech company, or utility will ever demand payment by gift card, cryptocurrency, or Interac e-Transfer, **ever**.

This payment method is the single biggest sign of a scam. **Once an e-Transfer or gift card number is sent, the money cannot be recovered.**

Four Red Flags	Top Canadian Scams
<b>Urgency / Threats</b> "Pay now or be arrested"	<b>CRA Fake Calls</b> Verify: 1-800-959-8281
<b>Gift Cards or e-Transfer</b> No gov't or bank ever demands these	<b>Grandparent Scam</b> Call the grandchild directly
<b>Asks You to Click a Link</b> Go to the website directly - never click!	<b>Tech Support Scam</b> Microsoft never calls you
<b>Too Good to Be True</b> You can't win a prize you never entered!	<b>Romance / e-Transfer</b> No fraud protection once sent

[www.connectedcanadians.ca](http://www.connectedcanadians.ca)

78 George St #204,  
Ottawa, ON K1N 5W1

(613) 699-7896

[info@connectedcanadians.ca](mailto:info@connectedcanadians.ca)



Connected Canadians  
Canadiens Branchés

## Enable Two-Factor Authentication (2FA)

**Two-Factor Authentication (2FA)** is an extra security step that helps protect your accounts, like email or online banking.

Normally, you sign in with **one thing: your password**.

With 2FA, you need **two things** to prove it's really you.

A helpful way to remember it is:

1. **Something you know**

This is your **password or PIN**. Only you should know it.

2. **Something you have**

This is usually **your phone or a special code sent to you**. For example, after entering your password, your bank might text you a **6-digit code** that you type in to finish signing in.

So even if someone guesses your password, they **still can't get into your account without your phone**.

You can think of it like **an ATM card and a PIN**:


- The **card** is something you have
- The **PIN** is something you know

You need **both** to access your money.


### **Why it helps:**

It makes it much harder for scammers or hackers to access your accounts.

 [www.connectedcanadians.ca](http://www.connectedcanadians.ca)

 78 George St #204,  
Ottawa, ON K1N 5W1

 (613) 699-7896

 [info@connectedcanadians.ca](mailto:info@connectedcanadians.ca)

## Secure Your Devices

### Step 1 - Check your screen lock

Open your Settings and make sure you have a PIN or biometric lock set up, such as a fingerprint or Face ID.

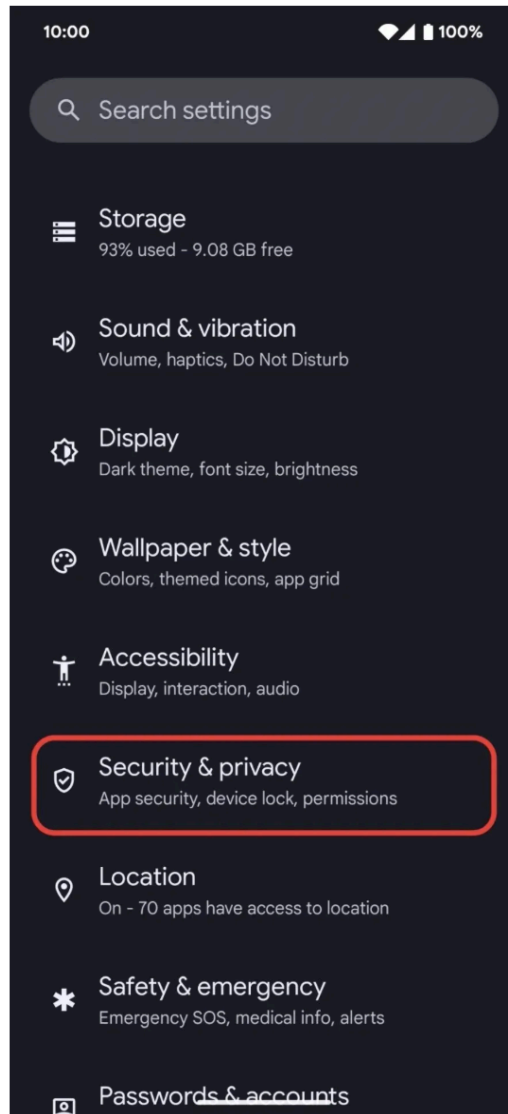
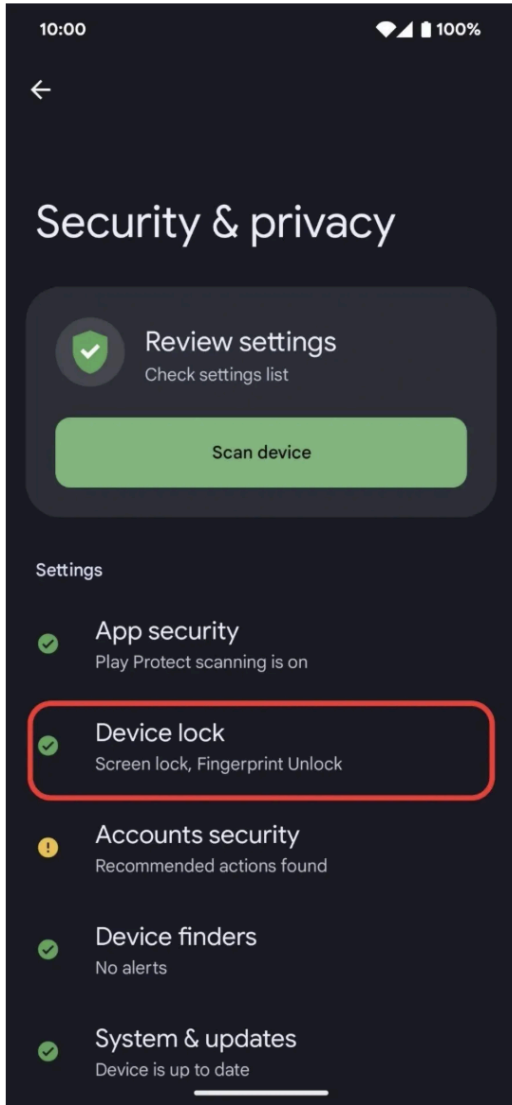
iPhone: Settings → Face ID & Passcode





Connected Canadians  
Canadiens Branchés

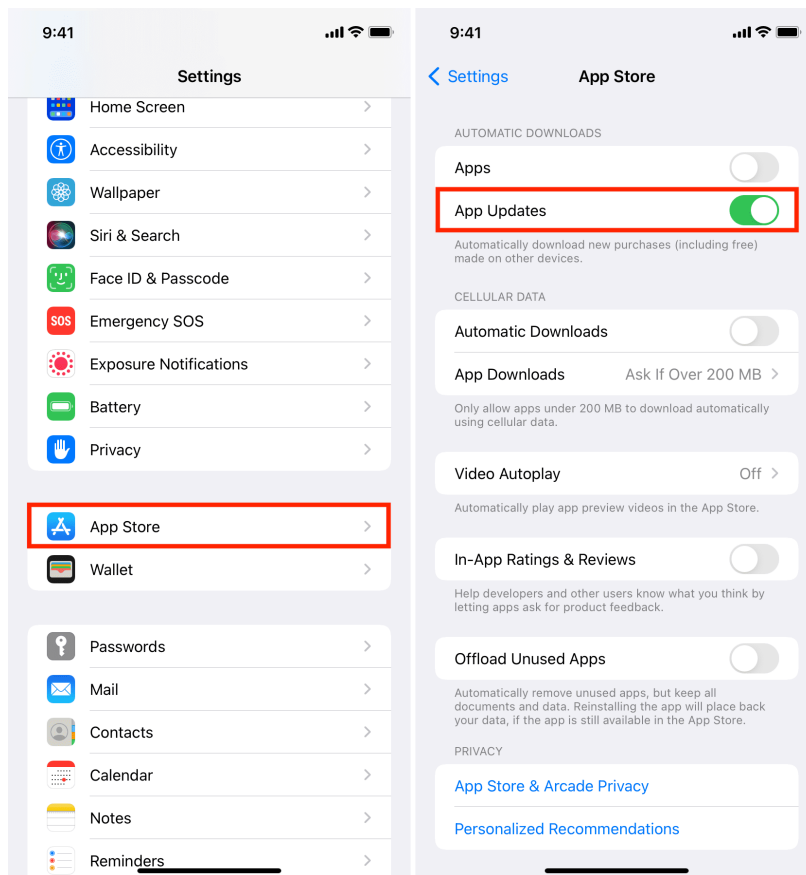
## Android: Settings → Security → Screen Lock



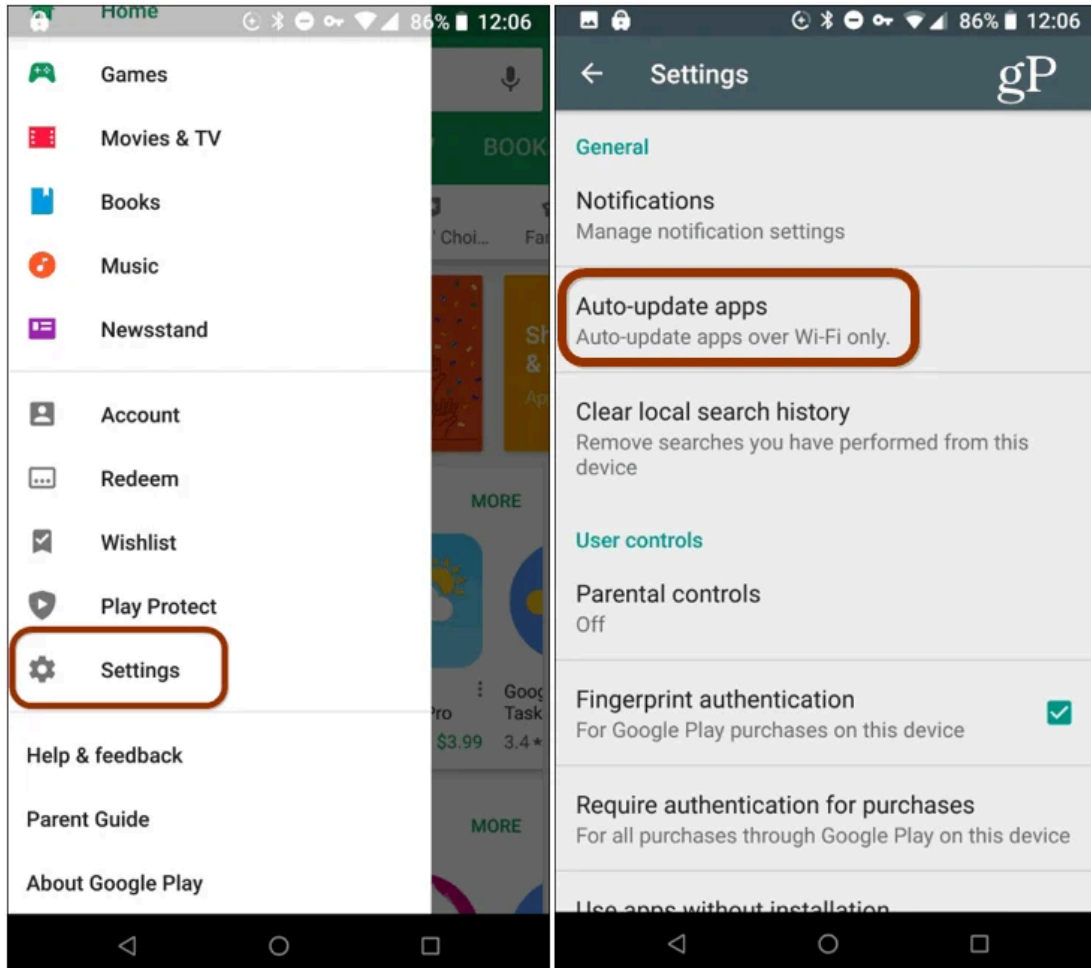
## Step 2 - Turn on app updates

Turning this on helps make sure your apps stay up to date with the latest security fixes without you having to remember to update them manually.

iPhone: Settings → App Store → App Updates ON



## Android: Play Store → Settings → Auto-update apps

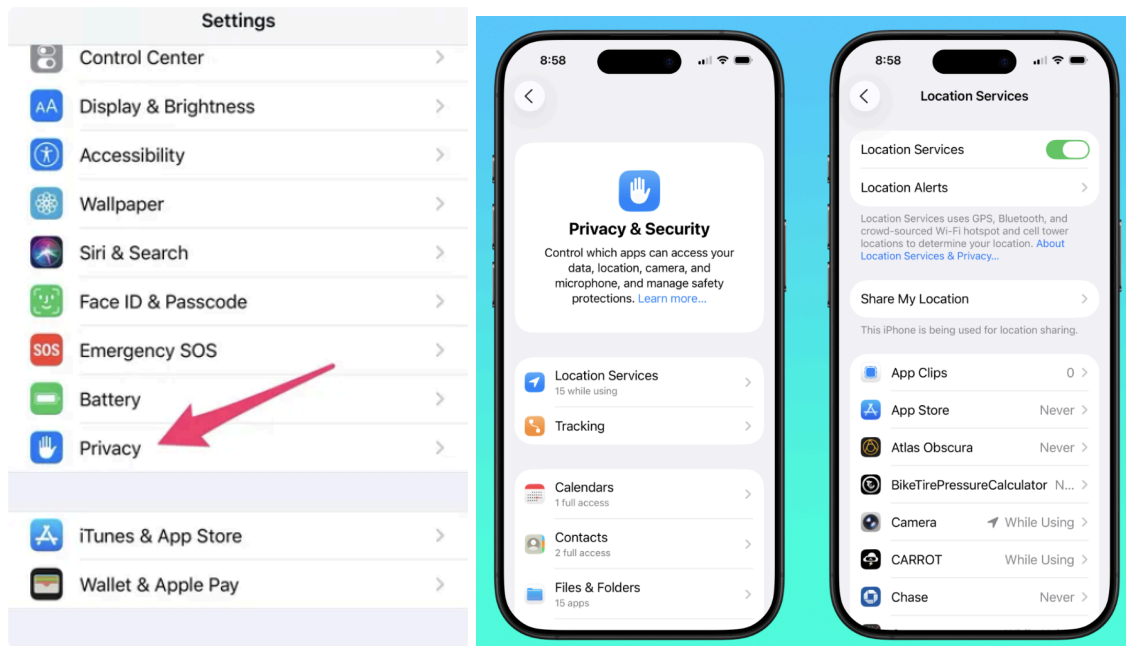


### Step 3 - Review app access

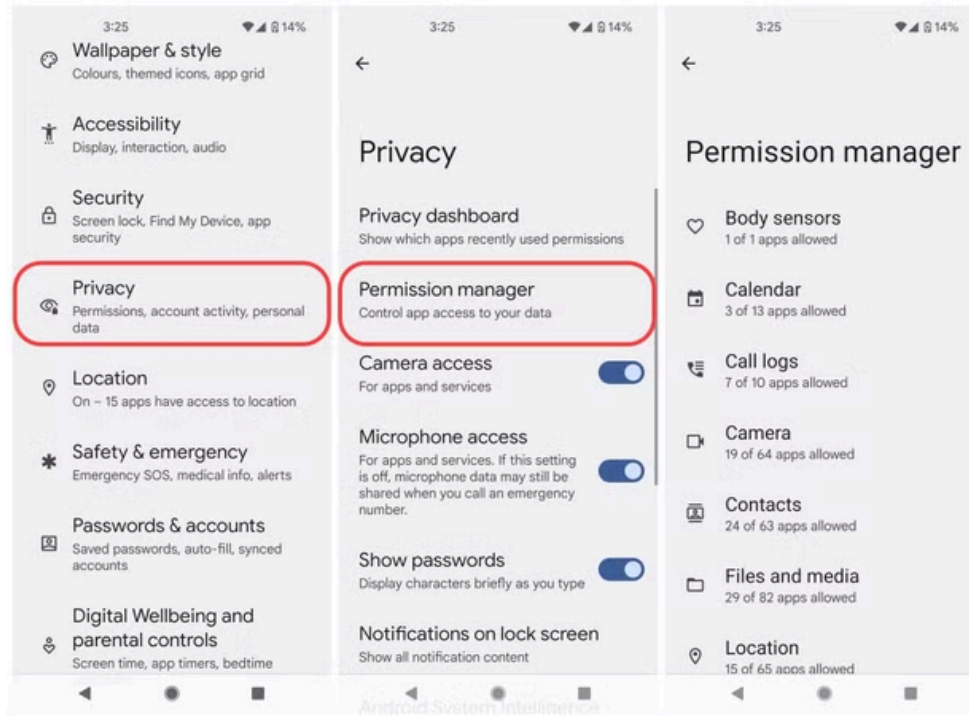
Look through the list and ask yourself, does every app that has your location actually need it? Maps, yes. A flashlight app? No. Remove access from anything you do not recognize.

While you are there, look at who has access to your microphone and camera. Anything unexpected should be turned off.

iPhone: Settings → Privacy → Location Services



## Android: Settings → Privacy → Permission Manager



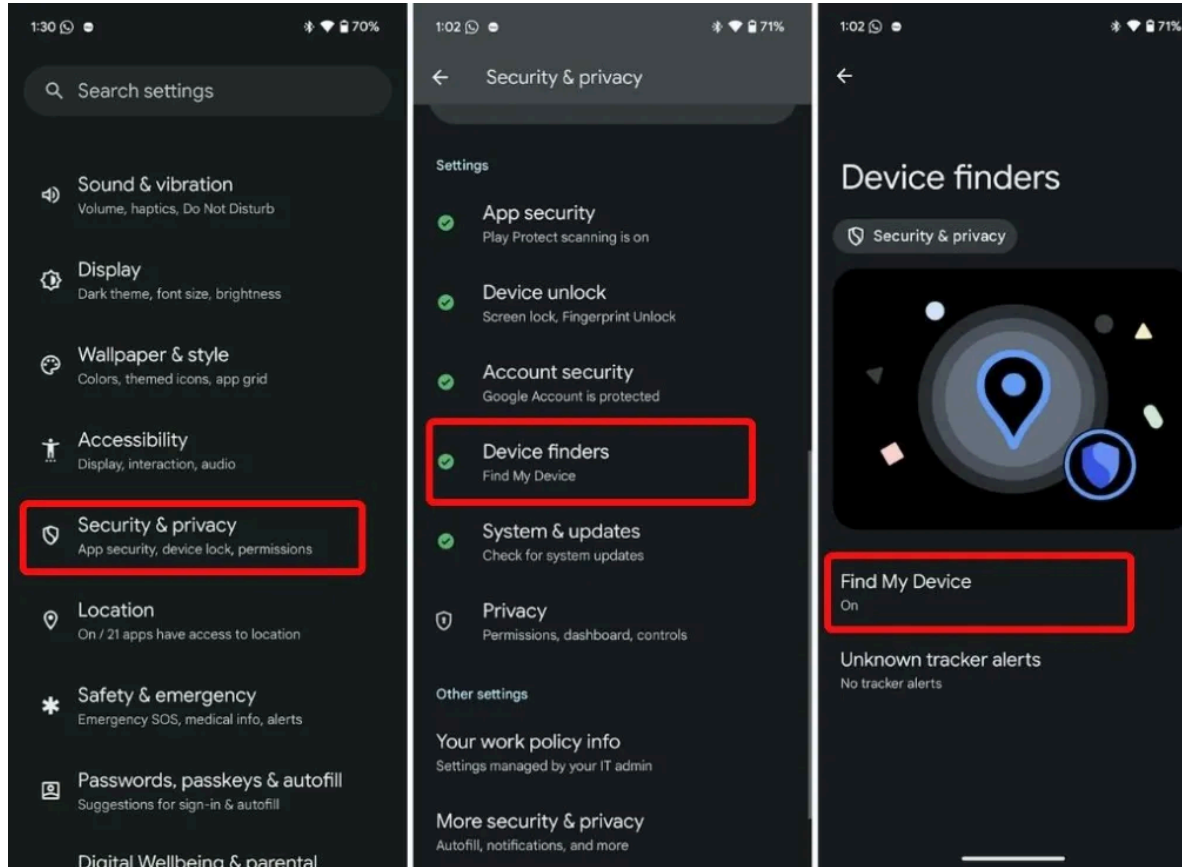
## Step 4 - Turn on Find My Device

Turning on Find My Device lets you locate, lock, or erase your device if it's lost or stolen, helping protect both the device and the personal information on it.

iPhone: Settings → Privacy → Location Services



## Android: Settings → Security → Find My Device



## Browse Safely

### The Padlock

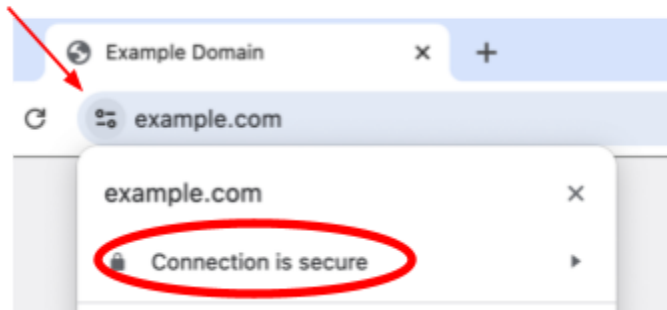
Look for a  padlock before entering passwords or card numbers

No padlock = do not enter your info

Note: A padlock does NOT guarantee the site is real.

Always check the web address spelling.

Click here

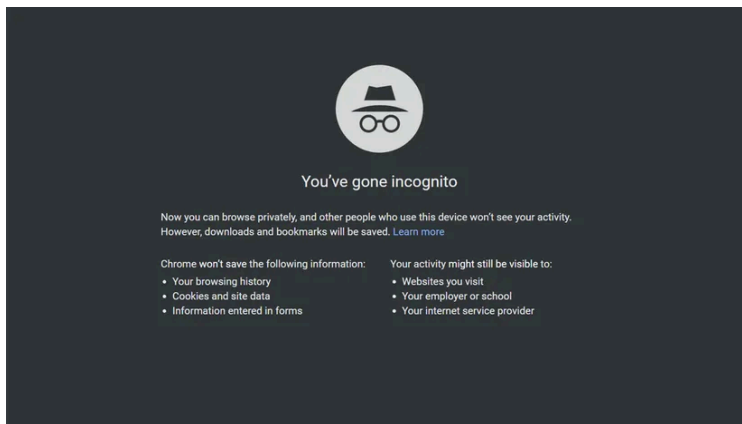


### Private / Incognito Mode

Clears your history and logins when you close the window.

Use on shared or public computers. It doesn't hide you from your internet provider.

Press Ctrl+Shift+N (Windows) or Cmd+Shift+N (Mac).





Connected Canadians  
Canadiens Branchés

## Browse Safely

- **Set Up Bank Alerts:** Ask your bank to text you whenever money moves. You'll know about fraud in seconds.
- **Interac e-Transfer Warning:** e-Transfer has NO fraud protection. Once sent, it's gone. Never send to someone you haven't met in person.
- **Free Fraud Alert:** Call Equifax Canada and TransUnion Canada to place a free fraud alert. Lenders must take extra steps before opening accounts in your name.
- **Use Credit, Not Debit Online:** Credit cards have stronger fraud protection. If fraud happens, the bank fights for you. With debit, your cash is gone while they investigate.

## Back Up Your Data – The 3-2-1 Rule

A virus, theft, or dropped phone can erase everything. A backup is your safety net. The **3-2-1 backup rule** is a simple way to protect your data from loss.


It means:

- keeping **3 copies of your data** (the original plus two backups),
- stored on **2 different types of storage** (for example, your computer and an external hard drive),
- with **1 copy stored off-site** (such as in cloud storage).

This way, if one device fails, is stolen, or infected by malware, you still have other copies safely available.

If you have questions or would like support with any of the topics discussed here, please reach out to Connected Canadians through our website: [www.connectedcanadians.ca](http://www.connectedcanadians.ca) . Our helpful volunteers are ready to assist you and ensure you feel confident and supported in your digital journey.

 [www.connectedcanadians.ca](http://www.connectedcanadians.ca)

 78 George St #204,  
Ottawa, ON K1N 5W1

 (613) 699-7896

 [info@connectedcanadians.ca](mailto:info@connectedcanadians.ca)