Staying Safe in a Digital World

Your safety superpower



PAUSE
Take a breath. Pressure is a reason to slow down.

CHECK
Contact the person or organization through a number or app you already trust.

ASK
It’s okay to check with a tech-knowledgeable youth or friend.



You do not need to be a technology expert.

A few good habits can help protect your money, accounts and peace of mind.

Inside: suspicious messages • passwords • Facebook and shopping • phone and AI scams • getting help

Spot the scam!

Phishing is a fake message designed to steal information or money.

FICTIONAL TEXT MESSAGE

“Your parcel is on hold. Pay $1.95 within 2 hours:
parcel-help.example.com
Example only. Do not visit the address.

Digital Detective: what looks suspicious?

Circle the clues in the message. Then check these seven warning signs:

1. Pressure or threats to act quickly.
2. Requests for passwords, codes or banking details.
3. An unexpected prize or amazing bargain.
4. A message you were not expecting.
5. A sender address or link that does not match.
6. An unexpected attachment.
7. Odd wording or an unusual appearance.

Answer: urgency + payment + unfamiliar link

Do not reply, click or pay. Open the delivery company’s official app or website yourself.

Perfect spelling is not proof. Scammers can copy logos and write convincing messages.

Passwords without the panic

Give every account its own password.

Use a different, long password for each account. Try a passphrase of several unrelated words. Avoid names, birthdays and common sayings.

A password manager = a digital safe



It creates and stores unique passwords. Protect it with a long, unique main password and multi-factor authentication.

Add a second lock

Two-factor authentication (2FA) adds another check, such as an authenticator app. Turn it on for important accounts. Never share login codes with someone who contacts you.



Prefer paper for now?

Fill in a paper organizer with your passwords privately at home. Store it securely, use a separate notebook that you keep private and safe. Do not share it in a group session.

Detective challenge

If Poppy uses the same password for email and shopping. What could happen?

Answer: If one account is breached, someone could try that password on the other.

Facebook: friend or fraud?

A familiar photo does not always mean a familiar person.

FICTIONAL MESSENGER MESSAGE

“Hi! I need $200 urgently. Please keep this between us. Send it now!”

Check another way. Call your friend using the number you already have. Their account may have been copied or taken over.

Limit what strangers can see. Review your audience, friend list and personal details in Facebook’s Privacy Checkup. Enable login alerts and 2FA in account security settings.

Skip revealing quizzes. Avoid posts asking for your birthday, first pet, childhood street or other personal details.

SHOP WITH YOUR DETECTIVE HAT ON



Check sellers independently. Check google reviews or general reviews. Be wary of extreme discounts and requests for gift cards, cryptocurrency or deposits. A padlock or “https” alone does not prove a shop is honest.



Calls, AI and getting help

A familiar voice or image can be faked, especially now with AI. Take time to check.

FICTIONAL FAMILY EMERGENCY 

“Grandma, it’s me! Send money now. Don’t tell anyone.”

Hang up and verify. Call your loved one on their usual number. Caller ID and voices can be copied.

Bank call? Use the number on your card. Never move money into a so-called “safe account”.

Computer warning? Do not call a pop-up number or let unexpected callers control your device.

Already clicked, paid or shared information?

1. Stop contact and payments. If you allowed remote access, disconnect from the internet and get trusted technical help.

2. Call your bank or card provider immediately using its official number.

3. From a trusted different device, change affected passwords, enable 2FA and review sign-ins.

4. Save messages and receipts. Report to local police and the Canadian Anti-Fraud Centre. If identity details were stolen, contact Equifax and TransUnion.

Canadian Anti-Fraud Centre: 1-888-495-8501
reportcyberandfraud.canada.ca
Immediate danger? Call **911**.

Your final safety reminder

Pause. Check. Ask. You do not have to figure it out alone.



Before you click, pay or share: stop and check through a number or app you already trust. Ask a tech-knowledgeable friend if you are unsure.

Keep learning! 

Your digital safety & resource guide

1. Get Cyber Safe - Government of Canada
https://www.getcybersafe.gc.ca/en

2. Seven red flags of phishing
https://www.getcybersafe.gc.ca/en/resources/ 7-red-flags-phishing

3. Password managers
https://www.getcybersafe.gc.ca/en/secure-your-accounts/ password-managers

4. Your offline password organizer
https://www.getcybersafe.gc.ca/en/resources/ your-offline-password-organizer

5. Canadian Anti-Fraud Centre https://antifraudcentre-centreantifraude.ca/index-eng.htm

6. Internet safety for seniors - Elder Care Alliance
https://eldercarealliance.org/blog/internet-safety-for-seniors/

7. The Imitation Game (Ishir's suggested movie)

8. Toren Darby's 2026 Scam Safety http://threats.toren.dev

9. Facebook Privacy Checkup (sign-in required)
https://www.facebook.com/privacy/checkup/

PAUSE · CHECK · ASK
When unsure, ask a tech-knowledgeable friend.

Thank you to our wonderful volunteers and participants for being our models.