Staying Safe Online in Canada: A Newcomer's Guide

Cyber safety tips for individuals, families, and students

English Version

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

Settlement.Org Welcome to Ontario

Introduction

Moving to a new country comes with many changes, and the internet can be a great tool for helping newcomers settle into Canada. But navigating this process without caution can also expose you to online risks.

This guide is designed to help you understand online risks. You will gain practical tips to help you stay safe when using the internet, learn what to watch out for, how to protect your personal information, and learn what to do if you think you are a victim of an online scam or fraud.

The Catalyst developed this guide in partnership with OCASI - Ontario Council of Agencies Serving Immigrants and Rogers to help newcomers stay safe online.

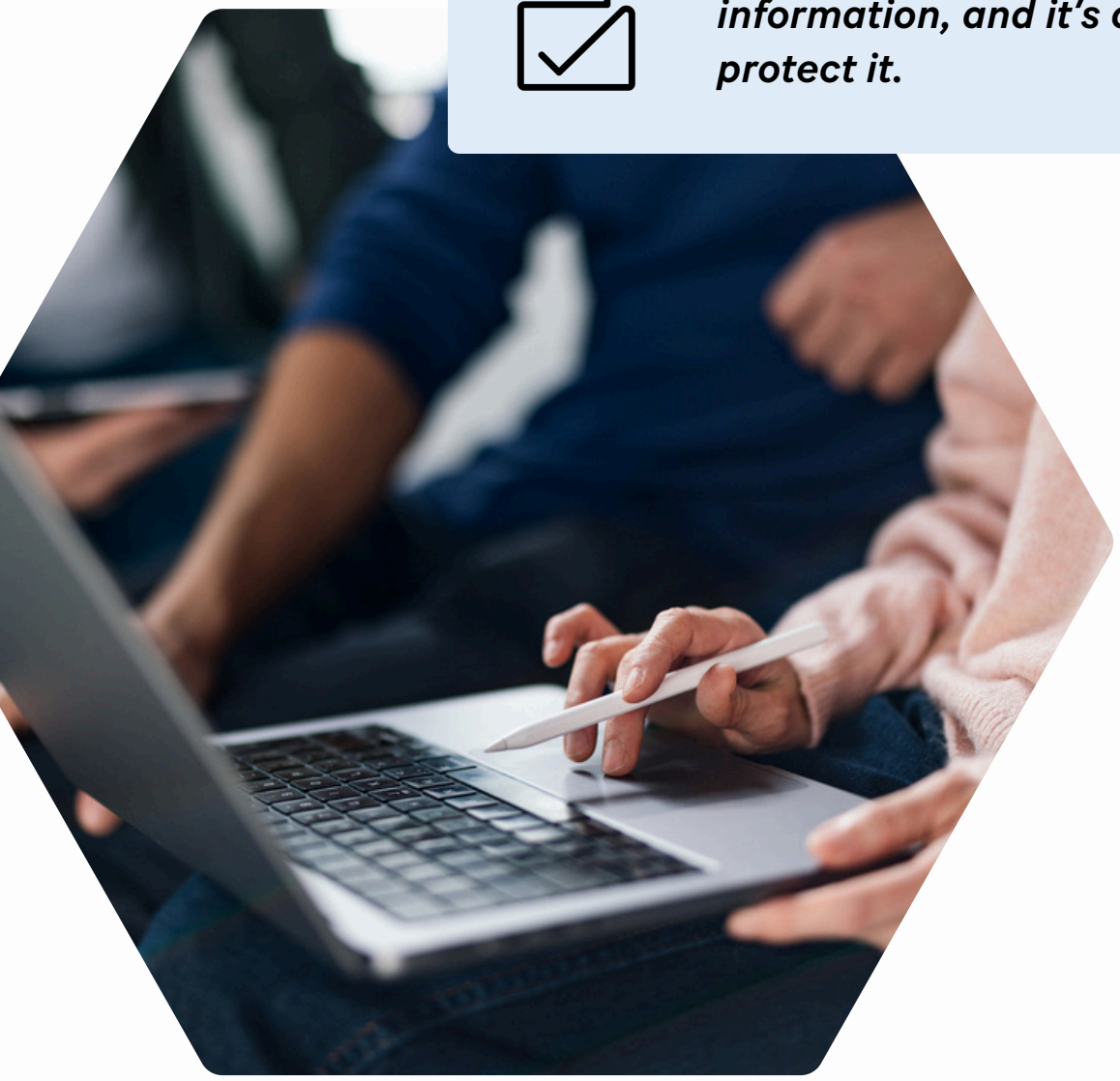
What risks should you be aware of online?

Being online is part of modern everyday life, and it's important to understand what could put your personal information and safety at risk, such as:

- Disclosure of your personal and health data
- The release or misuse of your financial information
- The misuse or manipulation of images you share
- Harassment

Cybercriminals may also attempt to scam, exploit, or bully you online.

You have personal and sensitive information, and it's critical to protect it.



Knowing what you can trust online

The best way to help protect yourself from online scams or fraud is to recognize suspicious activity, like calls or messages from unknown sources. Before clicking a link or sharing information, ask yourself these questions:

- Is it something you expect?
- Do you know the sender, and do they seem legitimate?
- Are they requesting personal or other sensitive information?
- Are they using fear, threats, urgency, or coercion to get you to do something or to obtain information?

These are just some of the indicators that suggest you should be cautious. Taking a moment to double-check can help keep you safe.

If you are uncertain, don't reply.

Ways to verify

- Search for an official page or phone number through another source to verify if the sender is legitimate.
  - Some government agencies like the Canada Revenue Agency have pages dedicated to verifying whether or not they called you.
- If you are sent a link or attachment, hover over it
  - Note: this only works on a computer and not on a phone. Does the URL or name make sense? If you're uncertain, don't click — check with a legitimate source.
- Watch out for impersonators who pretend to be your family to get information from you.
  - Consider having family members memorize a shared, secret "safe word" to help you identify whether it is really them.
- The key action is to PAUSE and VERIFY before responding or engaging any further.

How to stay safer online

Beyond safe habits, using the right tools and settings is an important part of staying secure online. Here are some steps you can take:

1. Secure your accounts:

- Use strong passwords or passphrases.
- Enable multi-factor authentication (a secondary device, code, or biometric).
- Review your social media privacy settings.
- Sign up with your bank to receive fraud alerts.

2. Secure your connections:

- Secure your home Wi-Fi by changing the default password to a strong password.
- Turn off Bluetooth when not in use.
- If you need to use public Wi-Fi, do so through a virtual private network (VPN).

3. Secure your devices:

- Set strong passwords, passcodes, passphrases, or personal identification numbers (PINs) on all your devices.
- Install and use credible security software on all devices.
- Keep software up-to-date and delete unused applications and software.
- Keep physical control of your devices and avoid sharing them with people you don't know.
- Back up your critical data and software.

Visit www.getcybersafe.ca to learn more about some of the actions recommended by the Government of Canada you can take to stay safe online.

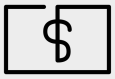
How to respond if you think you've been a victim of online fraud

If you believe that you have been the victim of a scam, online fraud, or another cybercrime, you should:

1. Take extra precautions based on the situation, such as changing your passwords, running security scans, or checking your financial statements for unusual transactions.
2. Contact your bank or credit card company if you think your accounts or cards may be at risk.
3. For serious incidents, call your local police non-emergency number.
4. Report fraud or scams to the Canadian Anti-Fraud Centre: https://antifraudcentre-centreantifraude.ca/index-eng.htm

Examples of incidents you should report to your local police, financial institutions and the Canadian Anti-fraud Centre:

Identity theft:
someone has stolen your personal information and used it to open credit cards or take out loans in your name. Contact your local police and your financial institutions.



Financial fraud:
you know or suspect unauthorized money has been stolen from your bank account. Contact your local police, your financial institutions and the Canadian Anti-fraud Centre.

Phishing and social engineering:
you've been tricked into giving someone access to your accounts.

Online harassment and cyberbullying:
you've received threatening messages or have had your private information published online.

How students can stay safe online

Students are prime targets for cybercriminals and scammers. These scams attract students with quick offers of enhancing grades, offering low-cost student loans, or free exam papers to help you succeed. But if an offer seems too good to be true, that is a sign that it could be a scam.

Your student number, records, and financial information are valuable to cybercriminals. Be cautious about sharing this information with anyone outside of your school. If you think your information has been exposed without your authorization, report it to your school's Security Office or other officials — it is likely you're not the only one affected.

Helping family members stay safe online

Kids can face serious risks online, including being tricked or pressured by strangers, cyberbullied, stalked, or asked to share personal images.

These situations can be upsetting and harmful, so it's important to talk openly with your child about how to stay safe online. Remind them not to share personal information, photos, or videos with people they don't know, and to tell you if something they come across online makes them feel uncomfortable

Additional Resources

In addition to reviewing your child's online security settings and reporting suspected threats to law enforcement, you should also consider reporting any incidents involving the online exploitation of children to cybertip.ca.

If your child needs someone else to talk to about what they are experiencing online, you can encourage them to contact resources that can help.

- Kids Help Phone – Canada's only 24/7 e-mental health service offering free, multilingual and confidential support. Text CONNECT to 686868 or visit kidshelpphone.ca.
- Good2Talk – a free and confidential support service for post-secondary students in Ontario and Nova Scotia that is available in over 100 languages. Visit Good2Talk.ca.

Conclusion

The internet offers many benefits, but cybercriminals are always looking for opportunities to exploit people online. You have the power to protect yourself and your loved ones by asking questions and practicing safe online habits.

This guide shares examples and tips to help you stay safe and secure online. For more resources, visit our online guides for newcomers, students, and families.

Access more resources
cybersecurecatalyst.ca/cyber-resources-for-educators-schools

Terms You Should Know

Here are some common words and phrases used in this guide. This glossary gives short, clear definitions to help you follow along and stay safe online:

Scam:
A fake offer or message designed to trick you into giving away something valuable, like money or personal information.

Threats:
When someone says or does something that makes you feel unsafe, it is often to scare you into doing what they want.

Coercion:
When someone pressures or forces you to do something you don't want to do.

URL (Uniform Resource Locator):
The web address you type into a browser to visit a website. For example: getcybersafe.ca

Impersonators:
People pretending to be someone else (like a friend, family member, or company) to gain your trust.

Safe Word:
A secret word or phrase you and someone you trust agree to use, so that you can confirm it's really them.

Multi-Factor Authentication (MFA):
A security step that asks you for more than just a password, like a code sent to your phone or a fingerprint scan.

Bluetooth:
A wireless technology that lets devices (like headphones or speakers) connect without cables.

Passphrase:
A type of password made of several words, numbers, or symbols put together, which makes it harder to guess.

- Example: Newcomer$afety!Guide2025

PIN (Personal Identification Number):
A short number code, often 4–6 digits, used to unlock accounts or devices (like a phone).

Security software:
Software or applications installed on devices that help protect you from viruses and malicious software.

Phishing and Social Engineering:
Tactics used by criminals to try to fool you into giving away personal information, often through phone calls, fake emails, texts, or websites.

Cyberbullying:
When someone uses the internet to harass, threaten, or embarrass another person.

Strong Password:
A strong password is long and unique, using a mix of letters, numbers, and symbols. It avoids personal details so it's hard for anyone to guess or crack.

Personal Information:
Personal information is any detail that identifies you, such as your name, address, phone number, or school. Cyber criminals can use it to steal your identity or commit fraud.

Health information:
Health information includes your medical history, doctor visits, or insurance details. It's private and valuable to cybercriminals who might use it for fraud.

Cybersecurity for all

Connect with us

cybersecurecatalyst.ca

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

Settlement.Org Welcome to Ontario