Newcomers to Canada:

Scams and Fraud Awareness

KnowledgeShare.KnowledgeFlow.org

SCAM RED FLAGS

KnowledgeShare.KnowledgeFlow.org

These are 4 signs that someone is trying to scam you.

A Sense of Fear, Urgency, or Secrecy

Example: "You must do this right now or else you will be in big trouble! And do not tell anyone."

Scammers will try to create **panic** to convince you to follow their instructions.

Requiring Payment

Example: "You need to pay $1,000 in fines immediately."

Scammers often try to get **payment** in any form. Electronic transfers, gift cards, or placing charges to your account.

A Sense of Authority

Example: "Hello, this is Agent Watson. There is a warrant out for your arrest."

Scammers sometimes impersonate authority figures to **intimidate** you.

Using Your Personal Information

Example: "Is this Ms. Podalski? Address 427 Spadina Avenue?"

Scammers may use personal information about you to seem more **legitimate**.

Immigration Extortion

Scammers may try to scam you by saying that you have not completed certain immigration documents.

They may tell you to pay the fees immediately or risk:

- Loss of citizenship
- Loss of passport
- Deportation
- Loss of SIN

Remember:

No one will ever block or deactivate your Social Insurance Number (SIN).

Citizenship Scams

Scams may also come in the form of promising fast Canadian citizenship or visas for a "special fee".

Only immigration officers in Canada and at Canadian embassies can decide to issue a visa.

Immigration officers will never:

- ask for payment into a personal bank account
- ask you to transfer payments through a private money transfer service
- threaten you

Job Scams

Never share your SIN or banking information when applying to jobs.

Be very suspicious if you are promised a well-paying job without an interview or experience.

Scammers may ask you to pay for special training or materials upfront.

KnowledgeShare.KnowledgeFlow.org

Law Enforcement Scams

Scammers may contact you claiming to be an officer from:

- **Royal Canadian Mounted Police**
- **Interpol**
- **Europol**

They may claim that criminal charges are being held against you or that a warrant is out for your arrest.

They will try to demand payment to avoid your arrest.

Remember:

Scammers will claim to be a law enforcement officer to intimidate and scare you.

Canadian officers will never call or email to tell you that you are under arrest and will never demand payment.

Officers will also never ask for payment over the phone or through electronic money transfer.

KnowledgeShare.KnowledgeFlow.org

Email Scams

Email scams can come in various forms.
Here are some signs to look out for.

Impersonated Email Address

Example: amazonaccount@gmail.com

These email addresses make you believe they are coming from a trusted organization.

Don't let brand recognition trick you. Always stay cautious.

Prizes and Exclusive Offers

Prizes and "exclusive offers" are often a way to get your address and other personal information.

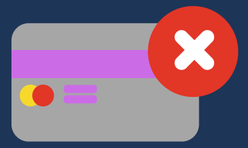
Scammers will ask you to send payment for fees like importing or shipping costs for a prize that does not exist.

Attachments

Attachments can include malware, which is designed to gain access to and/or damage a device's contents.

Attachments of all types (PDFs, JPG, PNG) can contain malware.

Failed Payment or Invoice



Scammers may send you emails with invoices or failed payment notices for a popular service or subscription.

These messages will often ask you to enter your financial information to dispute the charge.

Phone Call Scams

KnowledgeShare.KnowledgeFlow.org

Scammers will use a trick called Caller ID Spoofing to make it look like a legitimate number or organization is calling you.

You cannot trust the number of your Caller ID anymore, no matter which device you have.

Recently, scammers have been calling people pretending to be a relative in an emergency.

The scammer will say that the relative needs money immediately for a bail payment or car crash repairs.

Never send money or prepaid cards to anyone you do not know or trust.

Scammers often ask for these forms of payment because they are difficult to trace.

Legitimate organizations and businesses will never ask for payment in the form of gift cards or electronic money transfer to a personal account.

Research charities before giving a donation. Scammers may be pretending to be a charity or organization to take your money.

How To Avoid Scams

KnowledgeShare.KnowledgeFlow.org

1

Delete messages and emails from accounts that you do not recognize.

2

Do not trust your Caller ID to verify someone's identity or organization.

When receiving calls from a bank or other financial institution, it is always best to hang up and call the phone number on your card, invoice or statement.

3

Do not open or reply to messages with attachments from unverified senders.

4

Use unique passwords for each account. If scammers get your password, they will use it to gain access to your other accounts.

Use a password manager to create and store your passwords securely.

5

Never give out personal information. This includes your Social Insurance Number, bank account numbers, and credit card information.

6

Use 2-Factor Authentication (2FA) for all important accounts.

2FA is an extra layer of security, requiring users to verify their identity by entering their password AND a one-time code (sent by phone, text, email, or authenticator app).

KnowledgeShare.KnowledgeFlow.org

Reporting Scams

If you are targeted by scammers, be sure to contact:

- **Your Local Police**

If money is taken from you, you can file a police report. Save any evidence of the scam you have.

- **Your Bank**

If you think you have been scammed, contact your bank immediately. They can often recover lost funds.

- **The Canadian Anti-Fraud Centre**

The CAFC tracks ongoing scams and alerts the public to prevent more financial loss.

- **Equifax and TransUnion**

It's important to alert the credit bureaus of fraud because scammers can affect your credit score.

Support Services

211 Ontario

211 Ontario is a free and confidential service that connects people to social and community supports.

211ontario.ca 2-1-1

Get Cyber Safe

Get Cyber Safe is a national public awareness campaign about cybersecurity and how to protect yourself online.

www.getcybersafe.gc.ca

Free Newcomer Services

Find newcomer community support in your area. Get support with job searches, language classes, residence searching, and more.

ircc.canada.ca

KnowledgeShare.KnowledgeFlow.org

Learn More About Cybersafety

KnowledgeFlow.org

We are making the world #UnHackable by fighting predatory online behavior, protecting **privacy** and disrupting cybercrime.

Our mission is to ensure that all Canadians have access to expert cybersafety **instruction and resources** regardless of their location or financial status.

The Cybersafety Academy

Available for FREE public registration, individuals of all ages can become **#UnHackable!**

Complete **courses** on device protection, personal information protection, spotting scams and cyber fraud, and more!

Our Resources

We have many resources available in multiple languages. Learn about protecting your privacy online, recognizing popular scams, and protecting your devices.

Our tip sheets and visuals can be used by parents, teachers and community groups in their **cybersafety education** programming.

Find us on social media

facebook.KnowledgeFlow.org

youtube.KnowledgeFlow.org

twitter.KnowledgeFlow.org

instagram.KnowledgeFlow.org

linkedin.KnowledgeFlow.org

www.KnowledgeFlow.org