SCAM
RESOURCE

Thousands of Canadians have lost millions of dollars each year after being tricked into providing their personal information.[1] This type of trickery is called a 'scam'. The definition of a 'scam' is an illegal trick, with the goal of getting money, or personal information that can then be used to get a person's money or identity.[2] Scams are real and can target anyone. Often, fraudsters will target individuals online, over the phone, by mail and even in person. If you have been the target of a scam the best thing to do is report it to the appropriate authorities, regardless of the amount. This resource outlines some of the most common scams that are currently being used, the agencies fraudsters often pose as and what you can do to be aware and better protect yourself.

[1] Canadian Anti-Fraud Centre. (2020). from https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
[2] Merriam-Webster Dictionary. (2020). 'Scam' from https://www.merriam-webster.com/dictionary/scam

TYPES OF GENERAL SCAMS

Identity Theft

1. **What is identity theft?**

   When someone takes and uses your personal information without your permission.
   The personal information they may take can include: [3]

   - Name
   - Address
   - Date of Birth
   - Social Insurance Number
   - Bank Accounts
   - Credit Card Number

2. **What can be done with my information?**

   Identity thieves may use your information to:

   - Apply for credit cards, bank loans, and other types of credit
   - Take money from your bank account and shop with your credit card numbers
   - Apply for government benefits, obtain passports, rent an apartment, or buy furniture or other goods with a store loan[4]

3. **How do scammers get the information?**

   Identity thieves may go through your trash bins or steal mail looking for personal information.
   OR, they may use online techniques such as hacking, viruses or phishing scams to look for your personal information.[5]

4. **Tips to protect yourself:**

   - Never give your sensitive personal information over the phone, via text, email or internet
   - Be cautious with public computers, WI-FI hotspots
   - Avoid giving out personal information on social media along with your picture, as it can be used to commit fraud
   - Always keep your PIN private when using your card and never lose sight of your card
   - Shred and destroy documents with your personal information[6]

[3] Canadian Anti-Fraud Centre. (2020). 'Don't give out personal information' from https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm#a3
[4] Government of Ontario. (2012-2020). 'Types of ID Fraud' from https://www.ontario.ca/page/how-avoid-or-recover-identity-theft
[5] Competition Bureau Canada. (2018). 'Little Black Book of Scams- 2nd Ed'- Identity Theft, p.8 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf
[6] Competition Bureau Canada. (2018).'Little Black Book of Scams- 2nd Ed'- Identity Theft, p.8 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf

Phishing Emails & Text[7]

1. **What is Phishing?**

   It is when you get an unsolicited email or text that claims to be from a legitimate organization, like a bank, business or government agency.

2. **How do they get your information?**

   You are asked to provide or verify (either by email or clicking on a web link) your personal or financial information, such as your credit card number, passwords and social insurance number.

3. **Tips to protect yourself:**

   - Ignore communication for unknown organizations
   - Delete suspicious communication from unknown contacts
   - Do not reply to spam messages and do not open any attachments or follow any links
   - To verify a hyperlink, hover your mouse over the link, without clicking on it
   - Do not use the phone numbers or email address provided in the message, go to the actual website to find the contact information

[7] Competition Bureau Canada. (2018). 'Little Black Book of Scams – 2nd Ed'- Phishing and Smishing Scams, p.13 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf

Emergency Scams[8]

1. **What is an emergency scam?**

   They are fraudsters calling to say that a family member (usually a grandchild) is in trouble and they need money immediately.
   The "trouble" could be getting locked up in jail, involved in a car accident, or trouble returning home from another country.

2. **How do they get your information?**

   The caller will ask you questions, getting you to reveal personal information. They may also ask you to keep this a secret as the family member is embarrassed.
   Sometimes there will be two fraudsters on the phone, one posing as the family member and the other as a police officer or lawyer.

3. **Tips to protect yourself?**

   - Take your time and ask questions about the story. The fraudsters are wanting you to panic and offer to help
   - Call other family members who may know where the caller family member is
   - Ask the caller questions that only a real family member would know and be able to answer
   - Never send money to anyone you do not know or trust
   - Never give the caller any personal information

[8] Competition Bureau Canada. (2018). 'Little Black Book of Scams – 2nd Ed'- Emergency Scams, p.16 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf

Tax Scams[9]

1. **What is it?**

   You get a text or an email from the Canada Revenue Agency (CRA) claiming you are entitled to an extra refund or that you owe money to CRA and any delay will result in them calling the police.

2. **How do they get your information?**

   The caller, email or text will ask you to collect your refund or pay an overdue amount through Interac e-transfer.
   OR, they may also ask you to send them payment via prepaid visa or gift cards. Often, the caller will become aggressive, threatening and threaten to call or send the police.

3. **Tips to protect yourself:**

   - The CRA will never ask you for your financial information in their emails
   - They will also never provide financial information in an email.
   - The CRA's accepted payment methods are: online banking, debit card or pre-authorized debit
   - Always double check with the CRA directly either by checking online via "My Account"
   - or by calling 1-800-959-8281

[9] Competition Bureau Canada. (2018). 'Little Black Book of Scams – 2nd Ed'- Tax Scams, p.14 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf

TOP AGENCIES THAT FRAUDSTERS ARE POSING AS

Immigration, Refugees and Citizenship Canada (IRCC)

1. **What is the Scam:**

   A scammer calls you at home and claims to be with Immigration, Refugees and Citizenship Canada (formerly Citizenship and Immigration Canada). They tell you that you've failed to complete or register certain immigration documents. They insist you need to pay the fees immediately or risk:

- Deportation
- loss of passport
- loss of citizenship[10]

2. **Who to contact:**

   As scammers often give a fake name and agent number to appear legitimate. If you think the caller is a scammer:

- hang up
- Or, If you have started a conversation then ask for the name and number of the agent and then HANG UP,
- call the Immigration, Refugee and Citizenship Canada center to confirm the agent's identity
- If you have a lawyer assisting you with your Immigration file, call them to advise
- call your local police if you lost money.[11]

   1-888-242-2100 (IRCC)

[10] Canadian Anti-Fraud Centre. (2020). 'Immigration Extortion' from https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm#a7

[11] Immigration, Refugees and Citizenship Canada. (2020). 'What kind of frauds should newcomers to Canada watch out for?' from https://www.canada.ca/content/dam/ircc/migration/ircc/english/pdf/fraud_newcomers.pdf

Royal Canadian Mounted Police (RCMP)

1. **What is the Scam:**

   Scammers are posing as RCMP officers will make contact either through email or phone that the person owes a large amount of income tax and that an arrest warrant has been issued in their name.

   OR There is a Notice to Appear in Court:

   An individual will receive an email claiming to be from the RCMP and that there is notice for them to appear in court.
   The email contains an attachment that may contain a virus, malware and/or spyware.[12]

2. **Who to Contact:**

   If you have sent money or items, contact your local RCMP detachment or local police department.

Ontario Provincial Police (OPP):

1. **What is the Scam:**

   Scammers are using caller Id that shows as "Ontario Provincial Police" and once the call is answered the person is told there is legal action against the caller.
   They are then told they must speak to an officer immediately and if they do not, they are trying to avoid appearances before the 'judge or jury'.
   Then person is asked for their Social Insurance Numbers, and other personal information.[13]

2. **Who to Contact:**

   1-888-310-1122 (OPP)

[12] Pam Douglas. (April 8, 2019). Brampton Guardian. "Fake phone calls not from the RCMP, police warn." From https://www.bramptonguardian.com/news-story/9263952-fake-phone-calls-not-from-the-rcmp-police-warn/
[13] Mira Miller. blogTO. "Police say phone scam callers now have OPP as call display." From https://www.blogto.com/tech/2019/11/police-say-phone-scam-callers-now-have-opp-call-display/

Collection Agencies [14]

1. **What is the Scam:**

   A scammer calls to demand payment for a non-existent debt.
   They use high-pressure tactics to get you to pay immediately.
   To avoid collection agency scams, request a written notice through regular mail.

2. **Who to Contact:**
   Check to see if the collection agency is registered with the appropriate provincial agency.
   You can also contact Equifax Canada and TransUnion to make sure someone hasn't stolen your identity.

   Equifax Canada: 1-800-465-7166

   TransUnion Canada: 1-866-525-0262

[14] Canadian Anti-Fraud Centre. (2020). 'Collection Agency' from https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/agency-agence-eng.htm

COVID-19 RELATED SCAMS

Be cautious as Fraudsters are either texting, emailing or calling and posing as the following:

Loan and Financial Service Companies:

1. **What is the Scam:**

   Fraudsters are posing as companies that are offering loans, debt consolidation and other financial services.[15]

2. **Who to Contact:**

   The Financial Consumer Agency of Canada has specific information regarding Government financial help and what to do if you are facing financial hardship

   https://www.canada.ca/en/financial-consumer-agency/services/covid-19-managing-financial-health.html

Public Health Agency of Canada:

1. **What is the Scam:**

   Fraudster posing as the Agency and saying that the person has tested positive for COVID-19 and ask you to confirm your health card number and credit card.[16]

2. **Who to Contact:**

   If you are currently awaiting the results of your test, you can check your lab results directly after signing into the secure site found at:

   https://covid-19.ontario.ca/

   OR

   If you have questions or want more information about COVID-19:

   https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html

COVID-19 Information Service Line:

[15] Canadian Anti-Fraud Centre. (2020). 'Covid-19 Fraud (Reported Scams)' from https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

[16] Canadian Anti-Fraud Centre. (2020). 'Covid-19 Fraud (Reported Scams)' from https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

1. **What is the Scam:**

   Fraudsters calling and posing as the Information Service and requesting personal information.[17]

2. **Who to Contact:**

   Call the Information Service line directly if you are unsure: **1-833-784-4397**

Local and provincial hydro/electrical power companies:

1. **What is the Scam:**

   Fraudsters are posing as the companies and threatening to disconnect the service for non-payment or late payment.[18]

2. **Who to Contact:**

   Contact your provider directly to confirm the information.

Canadian Red Cross:

1. **What is the Scam:**

   Fraudsters are texting or emailing claiming to be the Red Cross offering every household a box of free face masks (or other medical products) with a website link.
   When you click the link, you are directed to a website that offers facemasks for a delivery fee or a donation and then asks users for their address, email, phone number and credit card information.[19]

2. **Who to Contact:**

   Your local Red Cross branch:

   https://www.redcross.ca/in-your-community/ontario/ontario-find-a-branch

[17] Canadian Anti-Fraud Centre. (2020).'Covid-19 Fraud (Reported Scams)' from https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm
[18] Canadian Anti-Fraud Centre. (2020). 'Hydro' from https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm#a6
[19] Canadian Red Cross. (2020). 'Red Cross Fraud and Misinformation' from https://www.redcross.ca/how-we-help/current-emergency-responses/covid-19-%E2%80%93-novel-coronavirus/fraud-and-misinformation

WHAT TO DO IF YOU HAVE BEEN SCAMMED[20]

Step 1: Gather all information about the fraud. This includes documents, receipts, copies of emails and/or text messages.

Step 2: Report the incident to your local police. This ensures that they are aware of which scams are targeting their residents and businesses. Keep a log of all your calls and record all file or occurrence numbers.

Step 3: Contact the Canadian Anti-Fraud Centre - **1-888-495-8501**

Step 4: Report the incident to the financial institution where the money was sent (e.g., money service business such as Western Union or MoneyGram, bank or credit union, credit card company or internet payment service provider).

Step 5: If the fraud took place online through Facebook, eBay, a classified ad such as Kijiji or a dating website, be sure to report the incident directly to the website. These details can be found under "report abuse" or "report an ad."

Step 6: Victims of identity fraud should place flags on all their accounts and report to both credit bureaus, Equifax (1-800-267-2384) and TransUnion (1-866-525-0262).

[20] Canadian Anti-Fraud Centre. (2020). 'What To Do If You Are Victim of Fraud' from https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm

TIPS TO PROTECT YOURSELF

1. **Don't give out personal information**

   Beware of unsolicited calls where the caller asks you for personal information, such as:

   - Your name
   - Your address
   - Your birthdate
   - Your Social Insurance Number (SIN)
   - Your credit card or banking information

   If you didn't initiate the call, you don't know who you're talking to. [21]

2. **Beware of upfront fees**

   Many scams request you to pay fees in advance of receiving goods, services, or a prize. It's illegal for a company to ask you to pay a fee upfront before they'll give you a loan.
   There are no prize fees or taxes in Canada. If you won it, it's free.[22]

3. **Protect your computer**

   Watch out for urgent-looking messages that pop up while you're browsing online.
   Don't click on them or call the number they provide.
   No legitimate company will call and claim your computer is infected with a virus.
   Some websites, such as music, game, movie, and adult sites, may try to install viruses or malware without your knowledge. Watch out for emails with spelling and formatting errors and be wary of clicking on any attachments or links. They may contain viruses or spyware.
   Make sure you have anti-virus software installed and keep your operating system up to date.
   Never give anyone remote access to your computer. If you are having problems with your system, bring it to a local technician.[23]

4. **Beware of Phishing Scams**

   Scammers will use emails pretending to be government agencies, banks or other businesses or organizations you may know. Once you click on the link you are led to a fraudulent scheme. Protect yourself by:

---

[21] Canadian Anti-Fraud Centre. (2020). 'Protect Yourself From Scams and Frauds' from https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm
[22] Canadian Anti-Fraud Centre. (2020). 'Protect Yourself From Scams and Frauds' from https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm
[23] Canadian Anti-Fraud Centre. (2020). 'Protect Yourself From Scams and Frauds' from https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm

- Think before you click a link or download an attachment. If you're unsure, don't click or download.

- Don't respond to any requests for sensitive information, even if it's supposedly to update payment information with an account.
- Use well-known websites, such as the CDC or WHO, to stay up-to-date on coronavirus information.

- Hover over the sender's email address to verify whether or not it's a legitimate domain from a familiar organization.

- Remember that legitimate organizations won't ask you to update account information or send personal data via email."[24]

5. Beware of fake Immigration websites

Scammers create fake websites and online ads that offer "cheap" immigration services or even may "guarantee" high paying jobs. Many of the websites will look like official government sites.
Beware if they are asking you to pay for application access fees or deposits before the application is even started.[25]

6. Be careful who you share images with

Carefully consider who you're sharing explicit videos and photographs with. Don't perform any explicit acts online.
Disable your webcam or any other camera connected to the internet when you aren't using it. Hackers can get remote access and record you.[26]

7. Look for spelling mistakes

Be wary of emails, messages or websites that have misspelled common words; grammar errors that make it difficult to read or expressions that are used incorrectly. Carefully examine email and web addresses to see if there are mistakes.[27]

---

[24] Competition Bureau Canada. (2018). 'The Little Black Book of Scams- 2nd Ed' - Phishing and smishing scams: Tips to protect yourself, p.13 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf
[25] Immigration, Refugees and Citizenship Canada. (2020). 'Fake Websites and other Internet Scams' from https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html
[26] Canadian Anti-Fraud Centre. (2020). 'Protect Yourself From Scams and Frauds' from https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm
[27] Competition Bureau Canada. (2018). 'The Little Black Book of Scams- 2nd Ed'- Red Flags: Things to Watch for (spelling mistakes), p.19 from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf

SCAM SCENARIOS

Scenario 1: Telephone Scam

Amy receives a call from a number she does not recognize. The caller identifies himself as a **CRA** employee, Bob, and that Amy has an **outstanding debt**. Bob tells Amy that he needs her to confirm her **personal information**, including her date of birth, credit card and bank account to sort out the debt with a repayment plan.

Amy does not remember owing the CRA any money. When Amy starts asking Bob questions, he becomes **angry** and warns Amy that if she does not cooperate there will be consequences. Bob then tells Amy the CRA will **lay criminal charges** or have her **put in jail** if she does give him the information he is requesting.

What should Amy do?

1) She should **not** provide any information to Bob. As she is unsure, she should hang-up and contact **CRA directly at 1-800-959-8281** to confirm if there is an outstanding debt.

2) Amy should then call and report the call to the **RCMP Anti-Fraud Centre by calling 1-888-495-8501.**

3) Remember the CRA **will not** ask for information such as credit card, health card or passport. Nor will the CRA threaten to lay criminal charges or have someone put in jail.

4) **Never** use the caller ID number that showed up or use it to confirm the identity of the caller, as it can be altered by fraudsters. [28]

[28] Immigration, Refugees and Citizenship Canada. (2020). 'Internet, Email, and Telephone Scams' from https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html

Scenario 2: Text Phishing Scam[29]

Mira receives a text message from a number she **does not recognize**. When she opens the text it reads that in light of COVID-19 and the WHO recommendation for people to wear masks, the Red Cross is offering every household a box of **free** facemasks. After the information there is a link. Mira **clicks on the link** and is brought to a website with the Red Cross banner. The site **asks for** her name, address, date of birth and for a $5 donation to help support their work and cover delivery costs of the masks.

Mira is excited as she has been trying to find facemasks but they have been sold out everywhere. She believes a $5 donation is not a large price if she is able to get a box of facemasks and also support the Red Cross. The website wants the donation by **credit card only**.

What should Mira do?

1) Mira should **not** have clicked on the link from an unknown number as they are often fraudulent websites created to steal your personal information or can carry harmful viruses.

2) As Mira has clicked on the link, she **should not** provide any information. The Red Cross is not providing free masks. She should **contact her local Red Cross Branch directly** if she is unsure.

3) Remember **do not** provide your personal and financial information so easily. Carefully look at the website, if it is one you are unsure of do not provide any information and **delete** the message. If it is from an organization you recognize, type in the web address yourself to ensure it is authentic.

[29] Canadian Red Cross. (2020). 'Red Cross Fraud and Misinformation' from https://www.redcross.ca/how-we-help/current-emergency-responses/covid-19-%E2%80%93-novel-coronavirus/fraud-and-misinformation

Scenario 3: Identity Theft

Bo receives a credit card statement in the mail from a company **she does not** recognize. When she opens the statement, she realizes the credit card is in her name but she has **never owned** a credit card with this company.

What should Bo do?

1) Contact the credit card issuer **right away** and advise them that she never applied for this card and discuss the situation with them.

2) Contact the **local police department** and file a report about the fraud.

3) As it appears Bo's identity was stolen, someone had applied for a credit card in her name, she should **contact both of Canada's credit reporting agencies**: Equifax Canada and TransUnion Canada, and obtain a copy of her credit report.

4) It may be necessary for Bo to contact other organizations and government agencies to know if her personal information was stolen and used to commit fraud.[30]

[30] Financial Consumer Agency of Canada. (2019). 'What to do if you're a victim of credit card fraud' from https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html

REFERENCES

Websites

1. Canadian Anti-Fraud Centre. (2020). < https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>

2. Canadian Anti-Fraud Centre. (2020). *Collection Agency* <https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/agency-agence-eng.htm>

3. Canadian Anti-Fraud Centre. (2020). *Covid-19 Fraud (Reported Scams)* <https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm>

4. Canadian Anti-Fraud Centre. (2020). *Don't Give Out Personal Information* <https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm#a3>

5. Canadian Anti-Fraud Centre. (2020). *Hydro* <https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm#a6>

6. Canadian Anti-Fraud Centre. (2020). *Immigration Extortion* <https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm#a7>

7. Canadian Anti-Fraud Centre. (2020). *Protect Yourself From Scams and Frauds* <https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm>

8. Canadian Anti-Fraud Centre. (2020). What To Do If You Are Victim of Fraud <https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm >

9. Canadian Red Cross. (2020). *Red Cross Fraud and Misinformation*. <https://www.redcross.ca/how-we-help/current-emergency-responses/covid-19-%E2%80%93-novel-coronavirus/fraud-and-misinformation>

10. Competition Bureau Canada. (2018). *The Little Black Book of Scams- 2nd Ed*. <https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/CB-lBBS2-EN.pdf/$file/CB-lBBS2-EN.pdf>

11. Financial Consumer Agency of Canada. (2019). *What To Do If You're A Victim Of Credit Card Fraud*. <https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html>

12. Government of Ontario. (2012-2020). *Types of ID Fraud*. < https://www.ontario.ca/page/how-avoid-or-recover-identity-theft>

13. Immigration, Refugees and Citizenship Canada. (2020). *Internet, Email, and Telephone Scams*. <https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html>

14. Immigration, Refugees and Citizenship Canada. (2020). *Fake Websites and other Internet Scams.* <https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html>

15. Immigration, Refugees and Citizenship Canada. (2020). *What kind of frauds should newcomers to Canada watch out for?* <https://www.canada.ca/content/dam/ircc/migration/ircc/english/pdf/fraud_newcomers.pdf>

16. Merriam-Webster Dictionary. (2020). *Scam.* <https://www.merriam-webster.com/dictionary/scam>

17. Mira Miller. blogTO. *Police say phone scam callers now have OPP as call display*. <https://www.blogto.com/tech/2019/11/police-say-phone-scam-callers-now-have-opp-call-display/>

18. Pam Douglas. (April 8, 2019). Brampton Guardian. *Fake phone calls not from the RCMP, police warn.* <https://www.bramptonguardian.com/news-story/9263952-fake-phone-calls-not-from-the-rcmp-police-warn/>

ADDITIONAL RESOURCES

CRA - Contains posters in: Arabic, Farsi, Tagalog, Chinese (simplified and traditional) for service providers about: email, credit card, phone calls, caller id, digital services fraud associated with CRA.

https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html

IRCC – Posters of top scams

https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/newcomers.html

Canada Anti-Fraud Centre

https://www.antifraudcentre-centreantifraude.ca/index-eng.htm