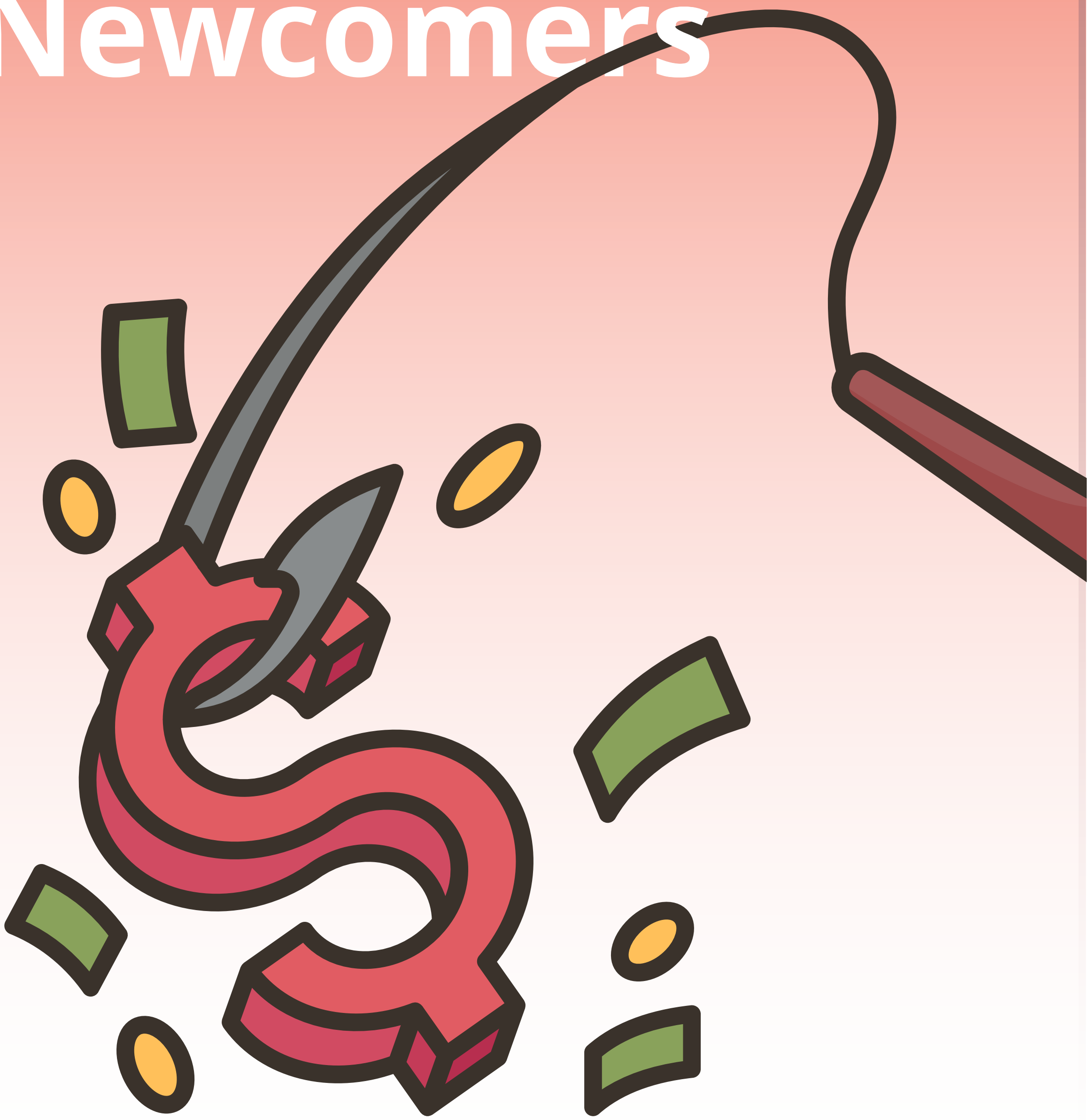
Common Scams & Frauds Affecting Newcomers



AMSSA®
Strengthening Diversity In BC

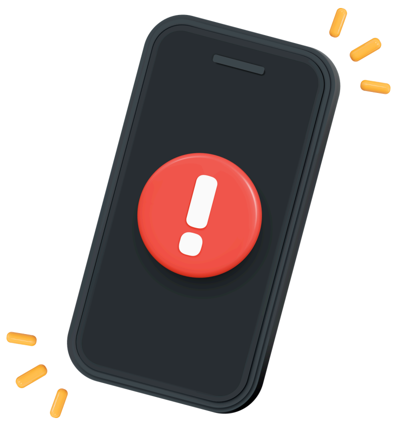
About this guide

Anyone can become a victim of a scam or fraud, regardless of age, education level, income, language ability, or immigration status. However, newcomers can be particularly vulnerable. After arrival, newcomers are often seeking immigration information and assistance, employment, and financial services.

During this transition, they might be unfamiliar with Canadian government processes and institutions, as well as with their rights in Canada. These factors might make them vulnerable to being targeted through fear-based tactics.

Table of contents

Scams



Scams are schemes designed to trick individuals into voluntarily giving money or personal information. Scammers often use psychological manipulation and false promises to convince victims to act.

Whether by phone call or through digital messages (phishing), scams usually follow a common structure.

Be aware of and help clients recognize a scam through these red flags:

Unexpected Communication

Unsolicited calls, messages, or emails, especially through social media.

Urgent or Threatening Language

Messages that create panic and pressure acting quickly.

Requests for Sensitive Information

Requests to update personal information or demands for financial details.

Anything Too Good to Be True

Unexpected rewards or benefits.

Information Mismatches

Websites or email addresses with spelling or grammar mistakes, characters slightly rearranged.

Scams

The following table describes four of the most common scams newcomers face.

Scam Theme	Support your clients by informing them
Immigration Status Scams Someone pretending to be a government official and claiming there is an issue with an immigration application.	Government officials will never: • Threaten to deport over outstanding fees. • Rush into paying fees right away • Make promises or offer special deals For more information, refer to the IRCC fraud prevention website.
CRA (Tax) and Government Benefit Scams Someone pretending to be a Canada Revenue Agency (CRA) agent and claiming there is an issue with a tax payment or offering a financial benefit.	The CRA will never: • Threaten to arrest • Demand immediate payment through unusual payment platforms or currencies • Charge a fee to speak with an agent • Ask for personal or financial information in a voicemail or email • Send messages about benefits or tax credits with links asking to click them. For more information, refer to the CRA scams and fraud information website. If a newcomer is a victim of suspicious activity on their CRA account, you can support them to report it to the CRA here.

Scams

Scam Theme	Support your clients by informing them
Employment and Recruitment Scams Someone claiming to be a Canadian employer or recruiter makes a job offer but asks clients to pay a fee upfront.	Legitimate Canadian employers do not: • Charge fees for job offers or a Labour Market Impact Assessment (LMIA). • Ask for SIN, bank details, or sensitive information before any interview. These practices are illegal in Canada. Prevention measures include: • Verify the company's official website and call their official phone number. • Verify if a Canadian Job offer is real here. • Identify employers who have been found non-compliant with the Temporary Foreign Worker Program or International Mobility Program here.
Cellphone Provider Impersonation Scams Someone pretending to be a mobile phone provider (e.g., Rogers, Bell, TELUS) and claiming there is an issue with their account / or giving a special offer.	Mobile providers will never: • Ask for password or full account credentials by phone, email, or text message. • Request authentication codes sent to your device. • Contact to offer exclusive deals in exchange for sensitive information.

Fraud

Fraud is a broader term that refers to illegal or unauthorized acts of deception intended to gain financial or personal benefits. Fraud typically involves unauthorized access to personal information without the victim's knowledge or consent.

Fraud Scheme	Support your clients by informing them
Unlicensed consultants People who present themselves as immigration consultants, but who are not licensed. They may not have the same training and education, and are not held to the same ethical standards.	• If they hire a consultant, they must be licensed by the College of Immigration and Citizenship Consultants. • IRCC will not accept applications submitted by unlicensed consultants. • Check if a consultant is licensed and look for license revocations, suspensions & restrictions here. • They can report unauthorized practitioners here. • If they have their documents stolen, or suspect someone is fraudulently using them, they must contact IRCC Client Support Centre.

Fraud

Fraud Scheme	Support your clients by informing them
Fraudulent job offers, or employers having unsafe and unfair working conditions Individuals or organizations who misrepresent working conditions to obtain money or personal information. Some recruiters may promise guaranteed immigration outcomes in exchange for fees. Others may expose workers to exploitative, unsafe, or illegal working conditions.	Employers can't: • Charge workers for job offers, recruitment services, or guaranteed work permits. • Keep their passport, work permit, or other identity documents. • Threaten deportation or immigration consequences. • Require them to work in unsafe conditions. • Refuse to pay wages owed for work performed. Workers are protected under employment standards legislation and workplace safety laws. Newcomers can report unsafe work and workplace health and safety concerns here. They can report unpaid wages, illegal recruitment practices, and employment standards violations to the BC Employment Standards Branch. Learn more on when to fill a complaint here.
Identity theft Criminals use stolen personal information to impersonate another person. Identity theft is often used to commit additional crimes, such as accessing bank accounts, opening credit cards, obtaining loans, applying for government benefits, or using someone else's identity documents.	They should never: • Send copies of identity documents to unverified individuals or organizations. • Share passwords or security codes. • Provide personal information through unsolicited phone calls, emails, or text messages.

Ways to support a client who has been a victim

01 Show compassion and empathy

02 Understand the client's situation

03 Educate clients to prevent future scams and fraud

04 Support the client to report the incident

05 Encourage clients to contact affected institutions

01 Show compassion and empathy

Let clients know that scams and fraud can happen to anyone, anywhere, at any time. Encourage them to acknowledge any feelings and practice self-care.

02 Understand the client's situation

Understand the client's situation and encourage them to collect and organize all information related to the incident, including:

- Details about what happened
- Supporting evidence. Advise clients not to delete any messages, emails, or other evidence related to the incident
- Information that might reveal a suspect’s identity (if available)

03 Educate clients to prevent future scams and fraud

Newcomers should be advised to limit the personal information that they post publicly online, as well as videos, audio clips, and images of themselves. Personal information can be used by scammers to learn more about victims’ personal lives, while videos, audio, and photos can be used by scammers to impersonate victims’ identities or those of their family and friends through AI tools.

Settlement workers should emphasize the importance of waiting before acting on a possible scam post or message. Newcomers should avoid sharing personal/financial information with strangers unless their identity is confirmed. If a newcomer is unsure of the message, they should research the official website of the organization that the message claims to come from. There they can confirm if official email addresses, names, and phone numbers align with the message’s source.

5 Steps to support a client who has been a victim

04 Support the client to report the incident

Information earlier in this guide provides information on where to report incidents in specific situations. It is also encouraged to support the client to report the incident to both:

Their local police	The National Cybercrime Coordination Centre and the Canadian Anti-Fraud Centre
Particularly if: • Money was lost • Personal information was compromised • Identity theft is suspected • Threats or intimidation occurred Let clients know that a police report may be required by banks or other organizations during their investigation or recovery process. Emergency Situations: If a scam or fraud involves immediate danger or a crime in progress, call 911 for urgent police assistance. Non-Emergency Situations: For scams and frauds that are not life-threatening, clients can contact their Municipal police department or RCMP detachment. Online reporting is available for minor impact scams and frauds through the RCMP Online Crime Reporting website.	Use their Online Reporting System or report by phone at 1-888-495-8501. They collect information on all types of fraud and can provide guidance on the next steps. Witnesses can report as well. It is important to report even if no harm was done, or the client decides not to do it. Reporting helps law enforcement; information could link several crimes together and/or help progress or complete an investigation. Reports can be done anonymously.

5 Steps to support a client who has been a victim

05 Encourage clients to contact affected institutions

Encourage clients to contact any institution whose information may have been compromised to reduce the risk of further financial loss or identity theft.

Financial institutions	Government institutions
If they shared financial information, passwords, or transferred money, they should contact their bank immediately. Financial institutions may be able to: • Freeze or secure affected accounts • Stop or reverse certain transactions • Monitor accounts for suspicious activity	If government-issued documents or personal information were shared, lost, or stolen, clients should contact the appropriate organization as soon as possible. Depending on the situation, this may include: • Canada Revenue Agency (CRA) if tax-related information was compromised. • Immigration, Refugees and Citizenship Canada (IRCC) if immigration documents, permits, passports, or application information may have been misused. • Service Canada at 1-866-274-6627 if the newcomer suspects or knows that their Social Insurance Number is being used by anyone else.

If personal information has been compromised, encourage clients to:

- Place a fraud alert on their credit file. A fraud alert can help prevent criminals from opening credit accounts or obtaining loans using stolen personal information. Contact Canada's two national credit bureaus: Equifax Canada and TransUnion Canada.
- Request a free copy of their credit report. This is a way to monitor unauthorized accounts or suspicious activity. Order a free credit report through the Financial Consumer Agency of Canada.

Additional Resources and Supports that settlement workers can share with clients

- VictimLinkBC: Call 1-800-563-0808 if a client is experiencing significant emotional distress following a scam or fraud. This free and confidential service is available 24/7 and provides crisis support, information, and referrals to victims of crime.

- WelcomeBC - Fraud Awareness: This website provides an overview of many types of immigration fraud and how to report it.

- A Fraud Prevention Toolkit for Newcomers: Developed by the Canadian Bankers Association and Get Cyber Safe, this resource helps newcomers recognize common scams, protect personal information, and develop safe online and banking practices.

Funded by / Financé par:

Affiliation of Multicultural Societies and Service Agencies of British Columbia
Metrotower II, Suite 2308, 4720 Kingsway, Burnaby, British Columbia, V5H 4N2
1 888 355-5560 | 604 718-2780 | amssa@amssa.org | www.amssa.org