Scams that target newcomers

When you are new to Canada, you may not be used to how companies or the government does business.

Below are some common scams aimed at newcomers to Canada. Read them so you know what to do if you are targeted.

1. People posing as staff from Immigration, Refugees and Citizenship Canada (IRCC)

What happens: A person poses as a government official on the telephone. They call people and try to scare them by saying they have done something wrong (like not filing proper paperwork), and that they owe fees. They may say the person can lose their immigration status or be deported if they do not pay right away. These people may even threaten someone's family or home. They say the police are coming to arrest them.

Things to remember

Immigration, Refugees and Citizenship Canada (IRCC) will **never**:

- contact you over the telephone to collect fees or fines,
- be aggressive or threaten to arrest or deport you,
- threaten to harm you or a member of your family, or damage your home or property,
- ask for personal information over the phone (except to verify information you already gave them),
- ask for financial information over the phone,
- try to rush you into paying right away,
- ask you to pay fees using prepaid credit cards, Western Union, Money Gram, gift cards, or any other similar services, or
- send police to arrest you for unpaid fees.

If you get a suspicious immigration call, you should:

- Ask for the name of the person calling and then hang up.
- Call the call centre **1-888-242-2100** to confirm that the call was real.
- If the call wasn't real, report it to the **Canadian Anti-Fraud Centre. 1-888-495-8501**
- If you have lost money to a scam artist, report it to your local police.

If you get a suspicious call about taxes, you should:

- Hang up, then confirm if the call was real by calling the Canada Revenue Agency at 1-800-959-8281.
- If the call wasn't real, report it to the **Canadian Anti-Fraud Centre. 1-888-495-8501**
- If you have lost money to a scam artist, report it to your local police.

Note: If you use caller ID, an agency's phone number may appear real, but it is not. Some scam artists use technology to fake the number, so this is not always proof that a caller is legitimate.

2. Fake emails

What happens: You may get an email trying to convince you to invest money or to give personal information or passwords related to your banking accounts.

What to do: Delete it. Legitimate investors don't send bulk emails to people they do not know.

Watch out for emails from a stranger that direct you to a website that asks for personal information. Never give out personal information unless you know who you are giving it to, and that the website is secure.

If you get this kind of email, don't click on any links or give any information about yourself. If you have any doubts about where the email came from, make sure to check the identity of the sender.

3. Fake computer virus

What happens: You may get a phone call or email saying that your computer has been infected with a virus. The caller or sender will offer to remove the virus from your computer. The person will try to get your computer passwords and other private information.

What to do: Never give access to your computer to someone you didn't contact for help. You should only have your computer fixed at a professional shop, or install anti-virus software bought from a trusted store.

4. Fake prizes

What happens: If you get a phone or text message that says you won something, but you did not enter a contest, it is probably a scam.

What to do: If you get a text message from a stranger, and it directs you to a form that asks you to enter any personal information, delete the text. Do not enter any information.

If the text tells you to text "STOP" or "NO" so you don't get more texts, delete it. **Do not reply**. Scam artists do this to confirm they have a real phone number.

Forward the texts to 7726 (SPAM on most keypads). This will let your phone provider block future texts from those numbers. If you think your text message is real, check that the link it is sending you to is the correct website.