GENERAL INFORMATION

RED FLAGS :

- Sense of urgency (no time to think)
- Who initiated communication
- Protect your Personal Information
- Are you paying money?
- Why are you being contacted?

TELEPHONE / TEXT MESSAGE

Did you ask for someone to contact you? If you did not ask for someone to call or text message you, this should be the first red flag. Phone numbers can be dialed randomly.

Does it sound like an automated message? Most phone related scams are automated and sent to thousands of people at a time.

What information do they really know about you? Names and phone numbers are very easy to find online with very little effort. Fraudsters will try to remain vague to catch more people.

Do not click on any links in Text Messages. There are a number of scams involving fake website links that are sent through Text Messages. If you want to check your banking information, open a browser and find the legitimate website for your bank.

What are the standard practices for official communications? The police will never ask you for a processing fee, CRA will notify you via regular mail for outstanding balances, etc.

What are they asking for? Reputable businesses will not ask to be paid in gift cards, this is a tactic used by fraudsters to avoid tracking of the money changing hands.

Do not trust any information provided by suspected fraudsters, especially call back numbers. Offer to call them back on an official number, and search for the correct number yourself. You can find correct numbers online or in a phone book.

Optional services, like Air Duct Cleaning, may be poor quality or overpriced.

DOOR TO DOOR

Ask for identification. You can request identification from any suspected Fraudsters.

Do not allow uninvited services inside. One known scam involved obtaining the rental details for Hot Water Tanks, which they could then transfer the contract to a higher cost company.

You can call the police if you feel threatened or unsafe. Sometimes Fraudsters may threaten to call police as a trick to scare you into submitting to their request.

What information do they really know about you? Remember that they already have your address because they are at your door, but do they know your name or other personal information?

WEBSITES / INTERNET

Look for the Security Lock. Secure websites will show a padlock, or sometimes a shield, icon. Even if you see the secure icon, you are not guaranteed to be safe! (See next step)

What is the full address you are visiting? Website addresses follow similar rules to postal addresses. "123 Elm St." could exist in many different cities, or even countries. Start at the end - trust your Country name the most, then City name, then finally your address.

This would be like your specific address – "123 Elm St."	This would be like your city name – "Ottawa"	This would be like your country name – "Canada"
www.	**mybankwebsite**	**.com**

Do not trust pop-up ads. If you are interested in a product from an advertisement, you can always open a new window and search for the item using a Search Engine (Google, Bing).

Does this site look unusual? Keep an eye out for big changes to a website you are familiar with. There could be a virus or malware on the computer that changes the websites you visit.

Do not use public computers for banking. Software can track your login details for websites you visit, so be wary of the owner of the computer you are using.

Do not use free public Wi-Fi that does not contain a password. Wi-Fi traffic is encrypted only when there is a password to connect to it.

EMAIL

Was the email marked as spam or sent to the junk folder? Most email providers will already have some protection in place to mark suspicious emails to protect you.

Do not click any links inside suspicious emails. Links can redirect to malicious websites. EXAMPLE If you want to check your banking information, open a browser and navigate to the website either through your bookmarks or find the correct website with a Search Engine.

What is the address from the sender / Do you know the sender? Make sure it is from a trusted source.

Were you expecting this email? Many services will send a link to reset your password if you forgot your password. If you did not request a password reset, do not click the link.

Have others received emails from your account? If you have friends or family asking why you sent them spam email, you need to change the password for your email.