Scam alert – fraudsters pose as Canada Revenue Agency

Nearly every day, the Calgary Police Service receives reports of scammers posing as agents of the Canada Revenue Agency (CRA) or Immigration Canada (IC). Unfortunately, scammers have obtained thousands of dollars from several unsuspecting victims. So how does the scam work and how can you protect yourself?

The CRA scam, and many similar ones, usually follows the same pattern. Victims are contacted via phone by people pretending to be a CRA or IC employee. The fraudsters claim that the victim owes back taxes and that they need to pay money to correct the issue, or they will be arrested or deported. Sometimes, the scammers have valid personal information about victims and their families, such as names and birthdays, to try to legitimize the fraudulent claim.

The scammers can become very aggressive and may begin to threaten victims. Victims are then told to send money through a wire service or to purchase prepaid credit cards or gift cards. Once the money is gone, it is nearly impossible to trace.

You can help protect yourself from phone and email scams by following these tips:

- Do not feel pressure to respond to a request until you have a chance to verify the story.
- Never transfer money, or give out credit card or other financial information, until you can verify the person's identity and the story, and determine whether it is legitimate.
- The CRA will not ask for payment via prepaid credit cards or wire transfer.
- Some scammers are using a technique called spoofing where the caller ID looks like the call is legitimately coming from the CRA or IC. Hang up and look up published numbers for the agency in the phone book or online and call them directly to confirm the legitimacy of the caller's story before you take any action. Do not call numbers provided to you by the person who called you.
- Don't believe what you see. Business logos, websites and email addresses can easily be duplicated to look legitimate.
- Watch for poor grammar and spelling.
- Hover your mouse over links to check their true destination. If the URL doesn't match the link, or seems suspicious, don't click on it.
- Be wary of unexpected emails that contain links or attachments from unknown senders.
- Update your computer's anti-virus software.
- Ignore calls for immediate action or messages that create a sense of urgency.
- Beware of phishing emails posing as the Canada Revenue Agency (CRA) requesting personal information, or links within an email re-directing to a

fraudulent website that appears to represent the Canada Revenue Agency (CRA). The CRA does not email Canadians and request personal information.

- Never provide personal information such as SIN, bank account information or credit card numbers.