# Police warn residents of increase in CRA-themed scams throughout tax season

Written By Brian Lockhart

As Canadians begin preparing their 2026 income tax returns, the Ontario Provincial Police are reminding the public to stay vigilant against Canada Revenue Agency impersonation scams.

This includes phishing emails and text messages designed to steal personal and financial information.

According to the Canada Revenue Agency, scammers frequently impersonate CRA employees and may contact victims by phone, email, text message, or through fake websites that appear official.

The CRA confirms that it will never send refunds by e-transfer for text message, request personal or financial information by email or voicemail, or pressure you to click links to receive benefits or avoid penalties.

The Canadian Anti-Fraud Centre continues to receive high volumes of reports involving tax-related fraud. It notes that fraudsters increasingly use phishing messages, spoofed caller ID numbers, and official-looking CRA branding to trick victims into sharing sensitive information.

The CAFC stresses that it does not contact individuals to request money or personal information, and encourages all Canadians to report suspicious activity.

There are several common tactics used in CRA scams.

Residents should be cautious if they receive:

Emails or text messages with links urging you to ?claim your refund,' ?update your tax account,' or avoid account suspension.' Scammers often use threats or promises of refunds to pressure victims into clicking fraudulent links.

Phone calls demanding immediate payment or threatening arrest, deportation, or legal action are used to intimidate victims. The CRA states it will never threaten arrest or use aggressive language.

Fake websites imitating CRA long pages, often using unusual domain endings or extra characters, are used to dupe victims. Official CRA sites always start with canada.ca or end in .gc.ca.

You may be dealing with a scam if someone sends you a link and asks you to click it, or requests personal details such as your SIN, banking information, or passport number.

Be aware if someone asks for payment by cryptocurrency, gift cards, or e-transfer. CAA does not accept these transactions.

If you are unsure if you are being scammed, hang up, delete the message, and contact CRA yourself.

If you believe you have been targeted by a CRA-related scam, whether or not you shared personal information, you are urged to report the matter.

Reporting helps law enforcement identify patterns and prevent further victimization.