CANADIAN ANTI-FRAUD CENTRE BULLETIN

Fraudsters Impersonating the CAFC 2025-05-29

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre (CAFC) is warning the public about fraudsters impersonating the CAFC. Fraudsters are using CAFC employee names, spoofing the CAFC's phone number and email addresses to mislead victims while promising to assist with investigations and/or recover lost funds.

Below are common scam variations where fraudsters claim to be from the CAFC:

Bank Investigator:
Victims are contacted by someone claiming to be from their financial institution, Amazon or law enforcement, including the CAFC. The fraudster says there's suspicious activity on the victim's bank account or credit card and they want to help the victim get their money back or assist with the investigation.

Tech Support Frauds:
Victims may receive unsolicited calls or pop-up messages claiming there's a problem with their computer or device. Fraudsters may direct the victim to grant remote access or pay for "necessary" services.

In some cases, fraudsters will claim to be the CAFC and advise victims that if they don't cooperate with them, they can be arrested due to fraudulent activity being detected from their device.

Recovery Frauds:
Fraudsters often impersonate the CAFC or law enforcement to build trust and deceive individuals. They often claim to be assisting with an ongoing investigation to recover lost funds and may reach out by phone, email or create fake websites, social media profiles or advertisements that appear on legitimate search engines or social media platforms.

The CAFC will **NEVER:**

- Ask for personal information such as your Social Insurance Number (SIN), bank account details, or driver's license
- Demand payment under any circumstances
- Ask for a code sent via email or text message (Multi-Factor Authentication Code)
- Ask you to transfer money to another account for fund recovery
- Promise to recover lost funds
- Request remote access to your computer
- Request login credentials for your accounts
- Appear in social media advertisements

How to protect yourself:

- If you receive a phone call or email claiming to be from the CAFC, ask for the caller's information and contact the CAFC directly by making the outgoing phone call to 1-888-495-8501 or contact your local police.
- Don't share codes received via text message or email with unknown callers as these can grant access to your accounts.
- Never provide remote access to your devices.
- Never be afraid to hang up the phone
- Never allow an unknown person to gain remote access to your computer/device
- Always have your computer/device serviced by a reputable local business
- Never pay an advance fee to obtain a refund
- Learn more tips and tricks for protecting yourself

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police and to the CAFC's online or by phone at 1-888-495-8501.