

COMMON FRAUD TACTICS
& HOW TO RESPOND



Impersonating a Trusted Source

Fraudsters can pretend to be your bank, government agencies, law enforcement, businesses, or someone you know. They may contact you by phone, text, email, social media or appear in sponsored ads on the internet.

Response: Verify their identity by contacting the organization using official contact information.



Fake Offers

Fraudsters may offer fake employment opportunities, services, or products that do not exist. These include fraudulent remote job offers, counterfeit goods, telecommunications services, device upgrades, or technical support. They may request personal information, an upfront payment, or remote access to your device.

Response: End the communication. Research the product, service or company. Do not provide remote access, until you're certain you're connected with a trusted source.



Door-to-Door Sales

Someone might come to your home offering urgent repairs, inspections, or special deals on services such as roofing, paving, or energy products. They may also claim that you're guaranteed grants to cover a large portion of the costs.

Response: Don't rush! Request and confirm identification. Request documentation in writing to review. Research the company and all offers.



Fake Sense of Urgency or Emergency

Fraudsters create a sense that you must immediately act causing you to feel panicked. They may claim that your accounts are at-risk, your services are going to be disconnected, a loved one is in need and immediate action is required.

Response: **Slow down.** Verify the details provided by contacting any associated businesses or people through trusted contact methods.



Requests for Money or Personal Information

Fraudsters will ask for sensitive information. Don't share your password or multifactor authentication code with anyone. Be cautious sharing banking information, gift cards, cryptocurrency, or e-transfers.

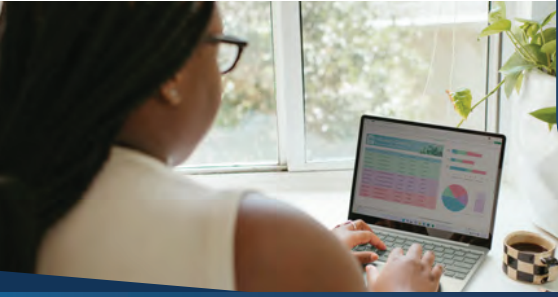
Response: You should never feel rushed into sharing sensitive information. Confirm the recipient is legitimate before sending money.

RECOGNIZE, REJECT, AND REPORT IT!

antifraudcentre.ca

CANADIAN ANTI-FRAUD CENTRE

1-888-495-8501



PREVENT FRAUD
VERIFY BEFORE YOU TRUST IT!

Fraudsters rely on trust and urgency.

Take a moment to confirm who you're dealing with before sharing information, sending money, or taking action.

Red flags!

- If it seems too good to be true, it is!
- Don't be afraid to say no
- Do your research
- Don't give out personal information
- Protect your online accounts. Use strong passwords!
- Recognize spoofing. Fraudsters can alter the call display to show any phone number or name that they want

Protect Yourself

- Guaranteed money, prizes or high investment returns with little or no risk
- Pressure to act immediately or threats of losing money, prizes or access to accounts
- Requests for upfront payments, fees, taxes, or "processing costs" to release money.
- Requests for payments via gift cards or cryptocurrency
- An "investigator" who asks you to hand over, cut up or surrender your credit credit/debit card
- Rapid emotional bonding or romantic declarations followed by requests for money or help

RECOGNIZE, REJECT, AND REPORT IT!

antifraudcentre.ca
CANADIAN ANTI-FRAUD CENTRE
1-888-495-8501