Canadian Senior Scam Protection Guide

A Quick Reference Guide for Canadian Seniors

Bill & Marilyn Gould

W. H. Gould Publishing

Contents

CANADIAN SENIOR SCAM PROTECTION GUIDE

A Comprehensive Guide to Recognizing and Avoiding Email, SMS, Telephone, and Postal Scams
Updated for 2026
For Canadian Seniors
Published by Canadian Senior Moment
CanadianSeniorMoment.ca

Introduction

Scammers increasingly target Canadian seniors through email, text messages, phone calls, and traditional mail. This guide provides comprehensive information about common scams, how to recognize them, and what to do if you encounter one.

This booklet is organized by scam delivery method (email, SMS, phone, mail) for quick reference. Each section describes common scams, warning signs, and protective actions you can take.

Remember: If something feels wrong, it probably is. When in doubt, hang up, delete, or throw it away.

Chapter 1

Section 1: Email Scams

1.1 CRA (Canada Revenue Agency) Email Scams

How It Works:

Scammers send emails claiming to be from the CRA, stating you owe taxes, are entitled to a refund, or need to verify your information.

The email includes links to fake CRA websites or requests immediate payment.

Warning Signs:

- Email address doesn't end in @cra-arc.gc.ca or @canada.ca
- Urgent language demanding immediate action
- Requests payment via gift cards, cryptocurrency, or wire transfer
- Threatens arrest, deportation, or license suspension
- Poor grammar or spelling errors

What To Do:

- Delete the email immediately - do NOT click any links
- The CRA NEVER uses email to request personal information
- If concerned, call CRA directly at 1-800-959-8281
- Report to Canadian Anti-Fraud Centre: 1-888-495-8501

1.2 Banking/Financial Institution Scams

How It Works:

Emails claiming to be from your bank, credit union, or credit card company, stating there's suspicious activity, account needs verification, or security update required. Links lead to fake banking websites designed to steal your credentials.

Warning Signs:

- Generic greetings like 'Dear Customer' instead of your name
- Suspicious sender email address (check carefully - may look similar but be slightly different)
- Urgent deadline to 'verify' or 'update' your account
- Links that don't match your bank's actual website address

What To Do:

- NEVER click links in banking emails
- Go directly to your bank's website by typing the address yourself
- Call your bank using the number on your bank card or statement
- Report suspicious emails to your bank's fraud department

1.3 Prize/Lottery Scams

How It Works:

Emails claiming you've won a lottery, sweepstakes, or prize (often from another country). Requires you to pay fees, taxes, or provide banking information to claim your 'winnings.'

Warning Signs:

- You didn't enter any contest or lottery
- Requires upfront payment to receive prize

- Requests banking information or personal details
- Claims to be from foreign lotteries (illegal in Canada)

What To Do:

- Delete immediately - legitimate prizes never require payment
- NEVER send money or provide banking details
- Report to Canadian Anti-Fraud Centre

1.4 Grandparent/Family Emergency Scams (Email Version)

How It Works:

Email claims to be from a grandchild, family member, or their friend, urgently needing money due to emergency (arrested abroad, medical emergency, car accident). Requests wire transfer or gift cards.

Warning Signs:

- Urgent request for money
- Asks you to keep it secret from other family members
- Email address doesn't match family member's usual email
- Writing style doesn't sound like your family member

What To Do:

- STOP and verify - call your family member directly using a known phone number

- Contact other family members to confirm
- NEVER send money without verification
- If scam confirmed, report to police and Anti-Fraud Centre

1.5 Romance/Dating Scams

How It Works:

Scammer creates fake profile on dating sites or social media, develops online relationship, then creates emergency requiring money (medical bills, business opportunity, travel to meet you).

Warning Signs:

- Professes love very quickly
- Makes excuses to avoid meeting in person
- Claims to be overseas (military, oil rig, business)
- Asks for money, gift cards, or financial help
- Photos look professional or model-like

What To Do:

- NEVER send money to someone you've only met online
- Use reverse image search to check if photos are stolen
- Discuss with trusted friend or family member
- Report to dating site, police, and Anti-Fraud Centre

Chapter 2

Section 2: SMS/Text Message Scams

2.1 Package Delivery Scams

How It Works:

Text claims to be from Canada Post, FedEx, UPS, or other courier, stating a package couldn't be delivered or requires additional payment. Link leads to fake website requesting personal/payment information.

Warning Signs:

- You weren't expecting a package
- Sender is a random phone number, not official company number
- Urgency to click link and 'confirm delivery'
- Link address looks suspicious (not canadapost.ca or official domain)

What To Do:

- Delete the text - do NOT click the link
- Contact the delivery company directly using their official website
- Legitimate delivery notices come through official tracking systems
- Report suspicious texts to your mobile carrier

2.2 Service Canada/Government Benefit Scams

How It Works:

Text claims to be from Service Canada, CRA, or government benefits department, stating your benefits are suspended, SIN compromised, or action required. Link requests personal information.

Warning Signs:

- Government rarely communicates important issues via text
- Threatens to suspend CPP, OAS, or GIS payments

- Requests SIN, banking info, or personal details
- Creates sense of panic or urgency

What To Do:

- Delete immediately
- Call Service Canada directly: 1-800-622-6232
- Log into My Service Canada Account directly (type address yourself)
- Report to Anti-Fraud Centre

2.3 Bank Alert Scams

How It Works:

Text appears to be from your bank warning of suspicious activity, locked account, or required verification. May include a phone number to call or link to click.

Warning Signs:

- Sender number doesn't match your bank's official short code
- Urgent action required
- Asks you to call a number not on your bank card
- Generic language not specific to your actual accounts

What To Do:

- DO NOT call the number in the text

- Call your bank using the number on your bank card
- Check your account online or via your bank's official app
- Forward suspicious texts to your bank's fraud department

2.4 Prize/Gift Card Scams

How It Works:

Text claims you've won a gift card from Tim Hortons, Walmart, or other retailer. Requires clicking link and providing personal information or completing surveys.

Warning Signs:

- You didn't enter any contest
- Link leads to site that doesn't match retailer's official domain
- Requests excessive personal information
- Too good to be true (large gift card amount)

What To Do:

- Delete the text
- Legitimate contests notify winners through official channels
- NEVER provide personal information via text message links

Chapter 3

Section 3: Telephone Scams

3.1 CRA Phone Scams

How It Works:

Caller claims to be from CRA, states you owe taxes or face arrest, demands immediate payment via gift cards, cryptocurrency, or wire transfer. May use threatening language or claim police are on the way.

Warning Signs:

- Aggressive, threatening tone
- Demands immediate payment
- Requests gift cards or cryptocurrency
- Threatens arrest, deportation, or license suspension
- Uses fake or spoofed caller ID showing 'CRA' or government number

What To Do:

- Hang up immediately - do NOT engage
- CRA NEVER threatens arrest or demands immediate payment
- CRA NEVER accepts gift cards or cryptocurrency
- If concerned about taxes, call CRA directly: 1-800-959-8281
- Report to Anti-Fraud Centre: 1-888-495-8501

3.2 Tech Support Scams

How It Works:

Caller claims to be from Microsoft, Apple, Norton, or other tech company, stating your computer has viruses or security issues. Requests remote access to 'fix' problems, then charges fees or installs malware.

Warning Signs:

- Unsolicited call about computer problems

- Requests remote access to your computer
- Heavy accent claiming to be from major tech company
- Creates urgency about security threats

What To Do:

- Hang up - legitimate companies don't make unsolicited tech support calls
- NEVER give remote access to unsolicited callers
- If you already gave access, disconnect from internet and call local tech support
- Report to Anti-Fraud Centre

3.3 Grandparent Scam (Phone Version)

How It Works:

Scammer calls pretending to be your grandchild in distress (arrested, in accident, stranded abroad), begs you not to tell parents, needs money urgently. May pass phone to 'lawyer' or 'police officer.'

Warning Signs:

- Caller claims to be grandchild but voice sounds off
- Begs you to keep it secret from parents
- Needs money immediately via wire transfer or gift cards
- Story sounds dramatic or implausible

What To Do:

- STOP - ask questions only your real grandchild would know
- Hang up and call your grandchild directly using known number
- Contact other family members to verify
- NEVER send money without verification
- If scammed, report immediately to police and Anti-Fraud Centre

3.4 Utility/Service Disconnection Scams

How It Works:

Caller claims to be from hydro, gas, phone, or internet company, states your account is overdue, service will be disconnected within hours unless immediate payment made.

Warning Signs:

- Threatens immediate service disconnection
- Demands payment via gift cards or wire transfer
- You haven't received any bills or disconnection notices by mail
- Aggressive or intimidating tone

What To Do:

- Hang up
- Call your utility company using number on your bill

- Legitimate companies provide written notice before disconnection
- Report to Anti-Fraud Centre

3.5 Robo-calls/Automated Scams

How It Works:

Automated message claims to be from government agency, stating SIN compromised, warrant for arrest, or legal action pending. Instructs you to press button to speak with agent.

Warning Signs:

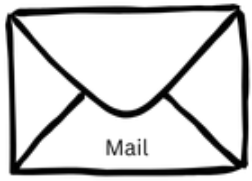
- Automated message (government doesn't use robo-calls)
- Threats of arrest or legal action
- Claims SIN is suspended or compromised
- Asks you to press button or call back

What To Do:

- Hang up immediately - do NOT press any buttons
- SIN cannot be 'suspended' - it's permanent
- Block the number if possible
- Report to Anti-Fraud Centre

Chapter 4

Section 4: Postal/Mail Scams



4.1 Foreign Lottery Scams

How It Works:

Letter claims you've won foreign lottery (often from Spain, Netherlands, or other country), includes official-looking documents and cheque. Requires payment of fees or taxes to claim prize.

Warning Signs:

- You didn't enter any lottery

- Claims to be from foreign country
- Includes cheque that you're instructed to deposit and send back portion
- Requests payment of 'taxes' or 'fees' to release winnings
- Participating in foreign lotteries is illegal in Canada

What To Do:

- Throw away immediately
- DO NOT deposit any cheques - they will bounce and you'll be responsible
- NEVER send money to claim prizes
- Report to Anti-Fraud Centre

4.2 Fake Cheque/Overpayment Scams

How It Works:

You receive cheque (often for item you're selling or work-from-home job). Cheque is for more than agreed amount. Sender asks you to deposit cheque and wire back the overpayment. Cheque bounces days later, you're liable.

Warning Signs:

- Cheque amount exceeds the agreed price
- Sender requests you wire back difference
- Cheque is from different person/company than expected

- Urgency to deposit and send money quickly

What To Do:

- DO NOT deposit the cheque
- NEVER wire money back to anyone
- If you deposited it, contact your bank immediately
- Report to local police and Anti-Fraud Centre

4.3 Inheritance/Beneficiary Scams

How It Works:

Letter claims you're beneficiary of estate or inheritance from distant relative or stranger with same last name. Requires payment of fees, taxes, or legal costs to release funds.

Warning Signs:

- Claims of inheritance from unknown person
- Requires upfront payment of fees
- Official-looking documents from foreign country
- Large sum of money (millions)

What To Do:

- Throw away - legitimate inheritances don't work this way
- Real estates contact legitimate beneficiaries through lawyers
- NEVER send money to claim inheritance

- Report to Anti-Fraud Centre

4.4 Charity Scams

How It Works:

Letter requests donation to fake charity, often using name similar to legitimate organization or exploiting recent disaster. May include emotional stories and photos.

Warning Signs:

- Charity name you don't recognize or sounds similar to known charity
- Pressures for immediate donation
- Requests cash, gift cards, or wire transfer
- No charitable registration number provided

What To Do:

- Research charity before donating
- Check CRA's registered charities list online
- Donate directly through charity's official website
- Report suspicious charities to CRA and Anti-Fraud Centre

4.5 Medical/Health Product Scams

How It Works:

Mailed advertisements for miracle cures, medical devices, or supplements making unrealistic health claims. Products are often worthless or dangerous.

Warning Signs:

- Claims to cure serious diseases
- 'Miracle cure' or 'scientific breakthrough' language
- Before/after photos or testimonials that seem fake
- Not approved by Health Canada
- Pressure to buy immediately with 'limited time' offers

What To Do:

- Throw away - if it sounds too good to be true, it is
- Consult your doctor before trying any health products
- Check Health Canada's database of approved products
- Report to Health Canada and Anti-Fraud Centre

Chapter 5

Section 5: General Scam Recognition Tips

5.1 Red Flags Present in Most Scams

- **Urgency or pressure to act immediately**
- **Requests for payment via gift cards, cryptocurrency, or wire transfer**
- **Too good to be true promises (large sums of money, miracle cures)**

- **Requests for personal information (SIN, banking details, passwords)**
- **Threats of arrest, legal action, or service suspension**
- **Asks you to keep it secret**
- **Poor grammar or spelling in written communications**
- **Sender/caller information doesn't match official sources**
- **Emotional manipulation (fear, excitement, sympathy)**

5.2 Questions to Ask Yourself

1. Was I expecting this contact?
2. Does this person/organization have a legitimate reason to contact me?
3. Can I verify this through official channels?
4. Why are they rushing me?
5. Would a legitimate organization use this payment method?
6. Does this make sense?
7. What would happen if I just ignored this?

5.3 Protecting Yourself

- **Never give personal information to unsolicited contacts**

Chapter 6

Section 6: What To Do If You've Been Scammed

6.1 Immediate Actions

1. **Stop all contact with the scammer immediately**

2. **If you sent money:**

- Contact your bank/credit card company immediately
- If via wire transfer, contact company (Western Union, MoneyGram) for possible recall

- If via cryptocurrency, contact the exchange platform

1. **If you gave personal information:**

- Change all passwords immediately
- Contact your banks and credit card companies
- Place fraud alert on credit report (Equifax: 1-800-465-7166, TransUnion: 1-800-663-9980)
- Monitor accounts closely for suspicious activity

1. **If you gave remote computer access:**

- Disconnect from internet immediately
- Run antivirus/anti-malware scan
- Change all passwords from a different device
- Consider professional computer cleanup

6.2 Reporting the Scam

It's important to report scams even if you didn't lose money. Your report helps authorities track scammers and warn others.

- **Canadian Anti-Fraud Centre**
- Phone: 1-888-495-8501
- Online: antifraudcentre-centreantifraude.ca

- Email: info@antifraudcentre.ca
- **Local Police**
- File a report with your local police department
- **Credit Bureaus (if identity theft)**
- Equifax: 1-800-465-7166 / equifax.ca
- TransUnion: 1-800-663-9980 / transunion.ca
- **Service Canada (if SIN compromised)**
- Phone: 1-800-206-7218
- **Canada Revenue Agency (for CRA scams)**
- Phone: 1-800-959-8281

6.3 Emotional Support

Being scammed can feel embarrassing, but it's not your fault. Scammers are professionals who manipulate people for a living. Many intelligent, careful people fall victim to scams.

- Don't blame yourself - scammers are skilled manipulators
- Talk to family, friends, or counselor if you're struggling
- Learn from the experience to protect yourself going forward
- Consider joining a seniors' support group

Chapter 7

Section 7: Important Canadian Resources

Provincial Consumer Protection Offices:

- British Columbia: 1-888-564-9963
- Alberta: 1-877-427-4088
- Saskatchewan: 1-877-880-5550
- Manitoba: 1-204-945-3800
- Ontario: 1-800-889-9768

- Quebec: 1-888-672-2556
- New Brunswick: 1-888-762-8600
- Nova Scotia: 1-902-424-5200
- Prince Edward Island: 1-902-368-4580
- Newfoundland & Labrador: 1-877-932-4636

Remember: When in Doubt, Don't!

It's always better to verify than to become a victim.

Share this guide with friends and family to help protect them too.

For more helpful information for Canadian seniors, visit:

CanadianSeniorMoment.ca