THE SENIORS SCAM PREVENTION GUIDE

HOW TO RECOGNIZE AVOID AND RESPOND TO FRAUD

A practical Canadian guide for older adults and their families

Mark Manuel

REALTOR® | SRES®

Seniors Real Estate Solutions

seniorsrealestate.net

WELCOME

A note from Mark

Scammers are skilled at creating urgency, fear, excitement or trust. Being targeted is not a sign of weakness or poor judgment. It can happen to anyone. The best protection is a simple routine that gives you time to verify before you act.

This guide explains that routine in plain language. Keep it nearby, share it with family and use the checklists whenever a call, message, visitor or offer feels unusual.

The most important lesson is simple: stop, end the contact and verify independently. A legitimate organization will allow you time to check.

Mark Manuel, REALTOR® SRES®

Seniors Real Estate Solutions

Important

This guide is educational and is not legal, financial, banking or cybersecurity advice. Contact the appropriate institution or professional for help with your situation.

QUICK NAVIGATION

Contents

YOUR STRONGEST DEFENCE

The pause and verify habit

Scams succeed when a person is pushed to act before thinking. Use this five-step routine every time money, personal information, passwords or computer access are requested.

1 STOP	Do not send money, click a link, read out a code or allow access to your device.
2 END CONTACT	Hang up, close the message or ask the visitor to leave. You do not need to be polite to a suspicious stranger.
3 CHECK	Call a trusted family member or friend. A second person often notices pressure or inconsistencies.
4 VERIFY	Find the organization’s number yourself from a bank card, statement or official website. Never use the number or link supplied by the caller.
5 REPORT	Tell your bank and the appropriate authorities. Reporting quickly may limit losses and helps protect others.

Create a family safe word

Choose a private word or short phrase that family members can use during a real emergency. Do not post it online. If a caller claims to be a relative, ask for the safe word and then call the relative using a number you already know.

A useful sentence to practise

“I never make financial decisions during an unexpected call or visit. I will contact the organization myself.”

RECOGNIZE THE PRESSURE

Warning signs that appear in many scams

- You must act immediately, keep the matter secret or stay on the phone.
- You are threatened with arrest, deportation, account closure, service disconnection or loss of benefits.
- You are promised a prize, inheritance, investment return or refund, but must pay first.
- Payment is requested by gift card, cryptocurrency, wire transfer, cash courier or e-transfer to an unfamiliar person.
- Someone asks for your password, PIN, card security code or a one-time verification code.
- A caller wants remote access to your computer or phone.
- The story changes when you ask questions, or the caller becomes angry or overly emotional.
- The message contains an unexpected link or attachment, even if it appears to come from someone you know.
- The offer sounds unusually profitable, urgent or exclusive.
- You are told not to speak with your bank, family, police or lawyer.

Trust the uncomfortable feeling

You do not need proof that something is a scam before ending the conversation. If it feels rushed, secretive or confusing, stop and verify.

THE NUMBER CAN BE FAKE

Phone calls and caller ID spoofing

Caller ID can be altered to show a local number, your bank, a government office or even your own telephone number. A familiar display is not proof of identity.

Safe phone habits

- Let unknown numbers go to voicemail. A genuine caller can leave a message.
- Never provide personal or banking information during an unexpected call.
- Do not press a number to be removed from a suspicious call list.
- If a caller claims to represent your bank, credit card company, police, CRA or Service Canada, hang up and call the published number yourself.
- If practical, wait several minutes or use another phone before calling back.
- Ask your telephone provider about call-control or spam-filtering features.
- Register on Canada’s National Do Not Call List. It reduces legitimate telemarketing calls but cannot block every scam.

Remember

Police and government agencies will not demand that you pay a penalty using gift cards, cryptocurrency or a cash courier.

VERIFY THE STORY

Emergency and grandparent scams

A caller may pretend to be a grandchild, child, police officer, lawyer or hospital worker. The story may involve an accident, arrest or medical emergency. Modern scammers may use personal details from social media or imitate a voice.

What to do

- Do not say the relative’s name first. Ask the caller to identify themselves.
- Ask a question only the real relative would know, or request the family safe word.
- Hang up and call the relative directly. If they do not answer, call another family member.
- Never send bail money, legal fees or emergency cash until the story is independently confirmed.
- Do not hand cash to a courier who comes to your home.
- If someone may be in immediate danger, call 911 yourself.

Secrecy is the trap

A scammer may claim that a court order or embarrassment requires secrecy. A real emergency is exactly when trusted family should be involved.

DO NOT FOLLOW THE MESSAGE

Email text and social media scams

Phishing messages imitate banks, delivery companies, streaming services, government agencies and people you know. They try to make you click, sign in or pay.

Before you click

- Check the full sender address, not just the displayed name.
- Be suspicious of unexpected refunds, invoices, password warnings and delivery problems.
- Do not open unexpected attachments, including documents that ask you to enable editing or sign in.
- Do not use a link in an unexpected message. Open the organization's official app or type its known website address yourself.
- If a friend asks for money through social media, contact them another way.
- Forward suspicious text messages to 7726 (SPAM) if your mobile provider supports it, then delete them.
- Block and report impersonation accounts through the platform.

Fake websites

Look carefully at the web address. Misspellings, extra words and unfamiliar endings can signal an imitation. A padlock symbol only means the connection is encrypted; it does not prove the business is honest.

REDUCE THE DAMAGE

Passwords accounts and devices

A few practical changes can prevent one stolen password from opening several accounts.

Use unique passwords	Never reuse your email or banking password. A password manager can create and store strong passwords.
Choose passphrases	Use several unrelated words that are easy for you to remember but hard to guess. Avoid names, birthdays and addresses.
Turn on MFA	Multi-factor authentication adds a second check such as an app prompt, code, fingerprint or security key.
Update automatically	Keep phones, tablets, computers, browsers and security software current.
Lock every device	Use a PIN, password, fingerprint or face recognition and set the screen to lock automatically.
Back up files	Keep copies of important photos and documents in a reputable cloud service or disconnected drive.

Protect your email first

Your email account can be used to reset many other passwords. Give it a unique password and MFA, and review the recovery phone number and email address.

NEVER SURRENDER CONTROL

Tech support and remote access scams

A pop-up, phone call or message may claim that your device is infected, your account was hacked or a charge must be cancelled. The scammer then asks you to install remote-control software.

Do not

- Call a number shown in a frightening pop-up.
- Install software at the request of an unexpected caller.
- Share your screen while banking or entering a password.
- Move money to a so-called safe account.
- Believe that a refund requires access to your computer or bank account.

If access was granted

Disconnect the device from the internet, contact your financial institutions from a different trusted device, change important passwords, remove unfamiliar software and obtain help from a reputable local technician. Report any loss immediately.

PROTECT THE TRANSACTION

Banking payment and investment fraud

Banks may contact customers about suspicious activity, but a bank employee should not ask for your full password, PIN or a one-time code to stop fraud.

Payment warning signs

- Gift cards, cryptocurrency and cash couriers are favourite scam payments because recovery is difficult.
- Never allow someone to use your bank account to receive or forward money. You may be used as a money mule.
- Independently confirm changes to payment instructions, especially for property, renovation or professional invoices.
- Do not assume an e-transfer request is genuine because it appears in an existing email conversation; an account may have been compromised.
- Check investment sellers and registrations through provincial securities regulators before sending money.
- Be wary of guaranteed returns, secret systems, celebrity endorsements and pressure to recruit others.
- Recovery services that promise to retrieve lost money for an upfront fee may be a second scam.

Large transfers

For a major payment, confirm the recipient and account details by a separate, trusted method. Consider asking your bank to place reasonable transaction alerts or limits on your accounts.

EMOTION CAN HIDE THE WARNING SIGNS

Romance friendship and caregiving scams

A scammer may build trust for weeks or months before requesting money. They may claim to be working overseas, serving in the military, facing a medical crisis or waiting for an inheritance.

Common patterns

- The relationship becomes intense unusually quickly.
- Video calls are repeatedly avoided or fail for convenient reasons.
- Stories are dramatic but difficult to verify.
- Money is requested for travel, customs, medical care, legal costs or an investment opportunity.
- The person discourages you from discussing the relationship with family.
- A new friend, helper or caregiver begins controlling mail, banking, transportation or contact with others.

Protect your independence

Never send money or share banking access with someone you know only online. If a new relationship affects your finances, talk privately with a trusted person or professional before signing or transferring anything.

YOU CONTROL YOUR FRONT DOOR

Door to door and home service pressure

A visitor may claim that your furnace, roof, water heater, alarm system or utility account needs immediate attention. Legitimate businesses do not require an instant decision at your door.

Your house rules

- Keep the door locked and speak through it, a camera or an intercom.
- Do not let an unexpected salesperson or contractor inside.
- Ask for written information, then research the company independently.
- Do not show bills, account numbers or identification.
- Never sign a contract just to make the visitor leave.
- Obtain more than one written estimate for major work.
- In British Columbia, door-to-door contracts are regulated and cancellation rights may apply. Consumer rules can change, so confirm current requirements with Consumer Protection BC.

If the visitor will not leave

Do not confront them. Call a neighbour, building manager or police. Call 911 if you feel threatened or someone is trying to enter.

LIMIT WHAT CAN BE STOLEN

Identity theft mail and personal documents

Identity information can be used to open accounts, redirect benefits, obtain credit or impersonate you.

Everyday protection

- Carry only the identification and cards you need.
- Keep your SIN, passport, birth certificate, tax records and unused cheques securely stored.
- Do not routinely use your SIN as identification. Ask why it is needed and how it will be protected.
- Shred statements, labels and documents containing personal or financial information.
- Collect mail promptly and investigate missing statements or redirected mail.
- Review bank and credit card activity regularly. Turn on transaction alerts.
- Review your credit reports and question accounts or inquiries you do not recognize.
- Do not post travel dates, full birth dates, addresses or answers to common security questions on social media.

If identification is lost

Contact the issuing organizations and your financial institutions immediately. If you believe your SIN is being used fraudulently, contact Service Canada.

SEEING AND HEARING ARE NO LONGER PROOF

AI voice cloning and deepfakes

Artificial intelligence can imitate a person’s voice or create convincing images and videos from material posted online. Treat urgent digital contact as a claim to verify, not proof.

A simple verification routine

- End the call and contact the person through a number already saved in your phone.
- Ask for the family safe word or a private detail that is not posted online.
- If a video call seems unnatural, ask the person to turn their head, wave, or answer a spontaneous personal question.
- Be suspicious when the person insists that the call must remain secret.
- Limit public voice clips, family details and travel information where practical.
- Never make an urgent payment based only on a voice, photo or video.

The old rule has changed

“It sounded exactly like them” is no longer enough. Verification through a separate channel is now essential.

SCAMS ARE NOT ALWAYS COMMITTED BY STRANGERS

Financial abuse by someone you know

Financial abuse can involve a relative, friend, caregiver, neighbour or person acting under a power of attorney. It may begin gradually and can be difficult to discuss.

Warning signs

- Unexplained withdrawals, transfers, debts or changes in spending.
- Pressure to sign documents, change a will, add a joint owner or transfer property.
- A person takes a bank card, withholds mail or monitors every conversation.
- Bills go unpaid despite adequate income.
- Possessions disappear or someone moves into the home without a clear agreement.
- The older adult becomes isolated, fearful or unusually dependent on one person.

Safer planning

Use a lawyer for powers of attorney and major property decisions. Choose trustworthy people, keep records and consider requiring regular statements or oversight. Speak privately with your bank, lawyer, doctor, police or the Seniors Abuse and Information Line if you feel pressured or unsafe.

ACT QUICKLY WITHOUT SHAME

What to do if you may have been scammed

Even if no money was lost, take action when information, passwords or device access may have been exposed.

Immediate danger	Call 911.
Money sent	Contact the bank, card issuer, wire service, cryptocurrency platform or gift-card company immediately. Ask whether the payment can be stopped or recalled.
Account exposed	Change the password using a trusted device, sign out other sessions and enable MFA. Start with email and banking.
Device accessed	Disconnect it from the internet and obtain help from a trusted technician. Use another device for banking and password changes.
Identity exposed	Contact financial institutions, credit bureaus and the organization that issued the identification. Monitor statements and credit reports.
Evidence	Save messages, receipts, phone numbers, account details, screenshots and dates. Do not continue arguing with the scammer.
Report	Contact local police if money, identity or safety is involved, and report to the Canadian Anti-Fraud Centre.

After the immediate actions

Once urgent calls have been made, create a clear record of what happened. This will make conversations with your bank, police, insurers and credit bureaus easier.

Your follow-up list

- Write a timeline including dates, times, names used, phone numbers, websites and payment details.
- Keep copies of receipts, account statements, emails, texts and screenshots. Do not alter the originals.
- Review recent bank, card and email activity for other changes you did not authorize.
- Ask financial institutions what monitoring, replacement cards, alerts or account changes they recommend.
- Tell a trusted person what happened so you do not have to manage the recovery alone.
- Watch for follow-up contacts that claim to be investigators, refund departments or recovery experts.

Do not pay a recovery agent

After a loss, scammers may contact you again and claim they can recover the money for a fee. Verify any recovery service independently and speak with police or your financial institution first.

Be patient with yourself

Scammers deliberately manipulate normal emotions and trusted systems. Reporting the incident promptly is responsible and may protect other people.

KEEP THIS PAGE HANDY

Canadian and British Columbia contacts

Emergency	911
Local police	Use the non-emergency number for your municipality when there is no immediate danger.
Canadian Anti-Fraud Centre	Report online at antifraudcentre-centreantifraude.ca or call 1-888-495-8501.
Service Canada SIN concerns	1-866-274-6627 if you suspect your SIN is being used fraudulently.
National Do Not Call List	lnnte-dncl.gc.ca or 1-866-580-DNCL (3625).
Consumer Protection BC	consumerprotectionbc.ca for BC consumer contracts and complaint guidance.
Seniors Abuse and Information Line	1-866-437-1940 in BC. A confidential resource for older adults and people concerned about them.
VictimLinkBC	1-800-563-0808 or text 604-836-6381 for information and referrals.
Credit bureaus	Equifax Canada and TransUnion Canada: use the official Canadian websites to request reports or fraud alerts.
Your bank or card issuer	Use the number printed on your card, statement or official website - never a number supplied by the suspicious caller.

Hours and services can change. Verify current contact details on the organization’s official website.

PREPARE BEFORE A CRISIS

Your family safety plan

Complete this page with someone you trust. Keep a copy near the telephone and another with important records.

Our family safe word or verification question

Trusted person 1 and phone

Trusted person 2 and phone

Bank fraud number from the back of my card

Local police non-emergency number

Trusted computer technician

Lawyer or financial professional

Where important documents are stored

Family agreement

We agree that anyone may pause a transaction or emergency request for independent verification. No one will be criticized for checking first or for reporting a mistake.

STOP BEFORE YOU ACT

One page scam defence checklist

☐ I was contacted unexpectedly.

☐ I am being rushed, threatened or asked to keep a secret.

☐ The caller wants money, personal information, a password or a verification code.

☐ The payment method is unusual or difficult to reverse.

☐ I was asked to click a link, install software or allow remote access.

☐ The caller ID, email address or website may be imitated.

☐ I have not verified the story using a number or channel I already trust.

☐ I have not yet discussed this with a trusted person.

If any box applies

STOP. End the contact. Do not pay, click, share a code or allow access. Call a trusted person, then contact the organization using information you find independently.

Three things no legitimate caller needs

- Your full password or banking PIN.
- A one-time security code to cancel fraud.
- Payment by gift card, cryptocurrency or a cash courier.

CANADA FOCUSED

Official sources and further reading

Canadian Anti-Fraud Centre

antifraudcentre-centreantifraude.ca

Canadian Centre for Cyber Security and Get Cyber Safe

cyber.gc.ca | getcybersafe.gc.ca

Canada Revenue Agency scam information

canada.ca/en/revenue-agency/corporate/scams-fraud.html

CRTC phone scam and caller ID guidance

crtc.gc.ca/eng/phone/telemarketing/

Financial Consumer Agency of Canada

canada.ca/en/financial-consumer-agency.html

Service Canada SIN protection

canada.ca/en/employment-social-development/services/sin/protection.html

Province of British Columbia seniors resources

gov.bc.ca/seniors

Consumer Protection BC

consumerprotectionbc.ca

Prepared September 2026. Scam methods and reporting procedures change. Consult the official sources above for current details.

About Mark Manuel

Mark Manuel is a licensed REALTOR® with more than 40 years of real estate experience and holds the Seniors Real Estate Specialist® designation. Through Seniors Real Estate Solutions, he helps older adults and their families make informed housing decisions with patience, clarity and respect.

seniorsrealestate.net | 604-657-7500 | markmanuelrealtor@gmail.com