Common Trends in Scams

Preventing Financial Fraud and Scams

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

This resource was created as part of an educational toolkit to increase awareness of financial abuse, scams, and frauds for older persons. Resources were created thanks to support from the Government of Canada's New Horizons for Seniors Program.

This document is designed to educate seniors about common trends in scams, so they recognize scams early and understand how to protect themselves.

The following tool kit is provided for informational purposes. The list of potential scams is not intended to be an exhaustive list. Should you have any concerns of a possible scam please contact the RNC at 709-729-8000.

The opinions and interpretations in this publication are those of the author(s) and do not necessarily reflect those of the Government of Canada.

Common Trends in Scams

Understanding Scams and Frauds

- Scams can happen online on the phone, at your door, or by mail.
- Scammers try to create fear, stress, or excitement to trick you.
- Scammers change tricks often and create new scams, but their goals are the same - to steal your money, or personal details.

Common Scam Trends

- Scammers call and pretend to be from the government, bank, technical support, or family.
- Emails or texts with a link to fake bills, unpaid amounts, or claim prizes.
- Romance or friendship scams asking for money.
- Fake investments, lotteries, or charities promising big returns or asking for “donations”.
- Home repair or service scams with strangers showing up without being asked.

Common Warning Signs

- Pressure to act fast.
- They tell you to keep it secret (“do not tell anyone”).
- Ask to pay in odd ways: gift cards, wire transfers, cryptocurrency (digital money used online; not issued by banks or government).
- Bad grammar, spelling mistakes, or strange email addresses.
- They ask for personal information like Social Insurance Numbers (SIN), banking information, or passwords.
- Deals that sound like they are too good to be true.

How to Protect Yourself

- Take your time and do not rush into decisions.
- Hang up and call back using real company numbers.
- Never share passwords or Personal Identification Numbers (PIN) with anyone.
- Use strong passwords and change them often. Try to include a mix of capital letters, numbers, and unique symbols. (e.g., Coffee@ Midnight#9528!).
- Do not click unknown links or download files from strangers.
- Keep personal and financial information private.
- Keep your devices updated with security software. For example, regularly check for updates on your phone or computer by going to Settings › Software Update or Settings › Security, and install any updates you see.

What To Do if Unsure

- Talk to a family member, friend, or someone you trust.
- Look up the phone number, email, or offer online.
- Ask your bank directly before sending money.
- Stop all contact with the scammer.
- Report scams to police or anti-fraud centres.
- Change passwords and check your accounts.

Extra Tips

- If it feels wrong, it is likely wrong.
- A real company or government office will not ask for payment with gift cards.
- It is okay to hang up the phone, delete an email or message, or close the door.
- Scammers change their ways often so be careful and not fearful.
- Asking questions and taking your time can help stop fraud.

Romance Scams

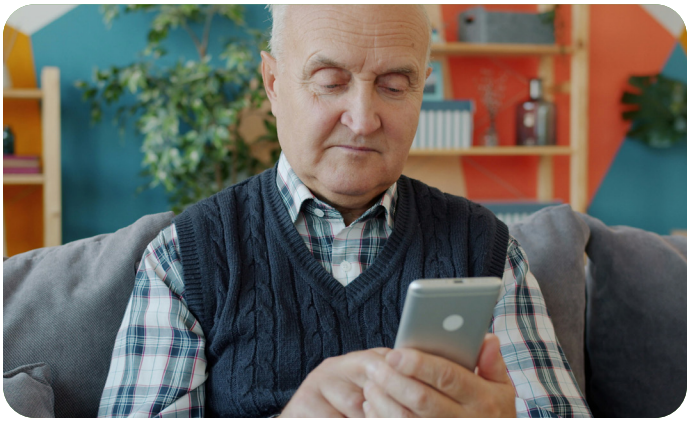
Scammers pretend to be interested in a romantic relationship online to gain your trust and steal your money.

Common Warning Signs

- State their love very quickly.
- Claim to live far away or have a job abroad.
- Avoid meeting you in person or on video calls.
- Claim to need money quickly (emergency, travel, accidents).
- Plan to visit but cancel because of unexpected situation/emergency.

Protection Tips

- Never send money or share your banking information with someone you have only met online.
- Be cautious if a new online friend tries to isolate you from family and friends.
- Watch for mistakes in stories or personal details.
- Talk to someone you trust if you are unsure. Do not keep it a secret.
- Remember that it is very unlikely that a genuine person will state their undying love to anyone after only a few letters, emails, phone calls, or pictures.



What to do if you think you have been scammed:

- Stop all communication. Do not send money.
- Keep evidence like messages, emails, and other records and do not delete them.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Share scams with others to prevent more victims.

Video link: Romance Scams
To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Grandparent or Emergency Scams

Scammers call seniors, pretending to be a grandchild or person of authority, claiming the grandchild is in trouble and urgently needs money for bail, hospital bills, or emergencies.

Common Warning Signs

- Unexpected call from someone claiming to be family.
- They need money quickly (for an accident, bail, or emergencies)
- The caller asks for secrecy and immediate action.
- They pressure you for money via wire transfer, e-transfer, or cash pickup.

Protection Tips

- Slow down, take your time, and check to see if the information is true.
- Ask questions that only a real family member would know the answer.
- End the call and call your grandchild / family member to confirm.
- Never send money or give personal information to strangers.
- Use code words with your family as proof of identity.

What to do if you think you have been scammed:

- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Video link: Emergency Scams

To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Canada Revenue Agency (CRA) Scams

Scammers pretend to be CRA officials and contact people by phone, text, or email. They claim you owe taxes, have a refund, or are under legal threat, demanding money, or personal info.

The Canada Revenue Agency will never:

- Use forceful language or threats (arrest, deportation, or send police).
- Ask for payment by Bitcoin, gift cards, e-transfer, or wire transfer.
- Use text messages to communicate.
- Ask to provide financial information in an email.
- Provide instructions to click suspicious links or download files.

Protection Tips

- Hang up and check directly: call CRA at 1-800-959-8281 or log-in on the official website and use the look up tool to check if it is the CRA calling: **https://www.canada.ca/en/revenue-agency/corporate/scams-fraud/verify-cra-contact.html**
- Do not share personal information or click on links in unexpected emails or texts.
- Never send money using a link or text message information.
- Stay informed by checking CRA and Canadian Anti-Fraud Centre updates.

What to do if you think you have been scammed:

- Stop speaking with the scammer immediately.
- Change passwords and notify your bank if you share any of your information.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Video link:
CRA Fraud Prevention
To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Video link:
Is the CRA Texting Me?

Service Canada Scams

Scammers pretend to be Service Canada officials and contact people by phone, email, or text, seeking Social Insurance Numbers (SIN), banking information, birthdates, or money using threats or false promises.

Service Canada Agents will never:

- Ask for your Social Insurance Number (SIN), password, banking details, or payment.
- Threaten of account closure, arrest, or loss of benefits.
- Demand payment in cryptocurrency, gift cards, e-transfer, or wire.
- Send messages with odd links, bad grammar, or urgent demands.
- Refuse or resist in confirming their identity.

Protection Tips

- Never share your SIN or financial information over unwanted calls, texts, or emails.
- Service Canada does not threaten arrest or ask for payment in gift cards or cryptocurrency.
- Caller ID may appear as local/government but may still be a scam.
- Do not click on links. Always access government sites through official channels.

What to do if you think you have been scammed:

- Hang up and call Service Canada directly at 1-800-622-6232 to verify.
- Make note of the scammer's information (calls, emails, numbers).
- Change passwords, alert your bank, and monitor accounts.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Phishing and Smishing Scams

Phishing: unexpected e-mails that claim to be from a real organization, e.g., banks, government agencies, asking for personal and/or financial information.

Smishing: Same thing but by text messages to your cell phone.

Both scams may be trying to get your online login information to online banking or social media.

Common Warning Signs:

- Say you owe money or that your account has been frozen.
- They have noticed some strange activity or log-in attempts.
- Your computer has a virus, or your account has been compromised.
- You have won something or have a "coupon" or "free gift" because you are a loyal customer.

Protection Tips

- Never click on links or open attachments from unfamiliar senders. Hover over the link to determine if it looks right.
- Do not share passwords or personal info via email, text, or suspicious websites.
- Confirm a request by contacting the company through its official contact information. Never reply directly to the message.
- Never use the phone number or email address provided in the suspicious message.
- Look for bad grammar, spelling errors, and general greetings ("Dear Customer").
- If it seems "too good to be true," like unexpected refunds, prizes, or contests you did not enter, then it really is.

What to do if you think you have been scammed:

- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Change passwords right away.
- Notify your bank and credit card company.
- Save emails, screenshots, and sender information in case further action is needed.
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Video link: Phishing Scams

To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Quishing Scams

Quishing or QR phishing is a cybersecurity attack that uses QR code to trick victims into visiting a malicious website or downloading malware (malicious software to gain unauthorized access to your device).

What is a QR code?

A QR (Quick Response) code is a display of black and white squares that you can scan with your phone to quickly open a website, text, or other information.

How to Spot a Fake QR Code

- Preview the website address after scanning to check where the QR code is directing you.
- Sent from fake, misspelled email addresses, usually without business domain.
- Signs of tampering, such as a sticker placed over the original QR Code.
- General design and website missing branding with poor grammar, spelling mistakes, a time limit to put in your details or other scary tactics.
- If the edges are not clear, sharp, and exact, it might be fake.

Protection Tips

- Only scan QR codes from trusted sources.
- Avoid scanning codes on public posters, parking meters, or random emails. If it does not come from a trusted source, do not scan it.
- Use your device's camera's built-in scanner instead of random apps.
- If scanning a QR code opens a website that immediately asks for personal, banking, or login information, do not enter any details and close the page.
- Avoid using QR codes to pay bills.
- Run your fingernail across the printed QR code (such as on a poster) to check if it is a sticker that is covering the original QR code.

What to do if you think you have been scammed:

- If a QR code leads to a suspicious site, disconnect from the internet or turn off Wi-Fi / mobile data to prevent further unwanted access.
- Install and run trusted antivirus or anti-malware software to check for threats.
- Change passwords for any affected accounts and monitor financial or online activity; notify banks if needed.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Artificial Intelligence (AI) Generated Scams

AI (technology that allows computers to think and learn like humans) scams use fake voices, images, videos, or messages that look and sound real to trick people online, in texts, or by phone.

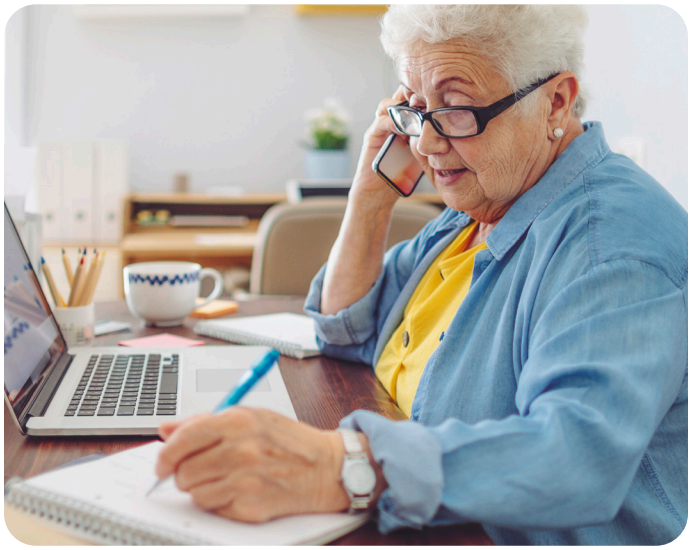
Scammers may pretend to be government officials, banks, companies, friends, or family members, even in live calls or video chats.

Common Tricks and Risks

- "Deepfake" videos or audio are of celebrities or loved ones asking for money.
- Emails, texts, or ads with perfect grammar, real photos, and convincing stories - sometimes with your name or personal details.
- Fake investment or job offers, prizes, urgent requests to "verify" accounts, or warnings about fake emergencies.

Protection Tips

- Beware of urgent, unexpected requests for money or information, especially from people you cannot verify in person.
- Never trust an unexpected email, text, or call just because it looks or sounds like it might be real. Always double check by contacting the person or company directly through official contact information.
- Do not click links or download files in suspicious messages, even if they seem convincing.
- Never share personal details, passwords, banking information, or send payments to new online contacts, especially if you feel rushed or pressured.
- Remember: Even "live" calls or videos can be faked with AI technology.



What to do if you think you have been scammed:

- Stop all contact and save any messages or evidence.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Video link: AI Generated Scams

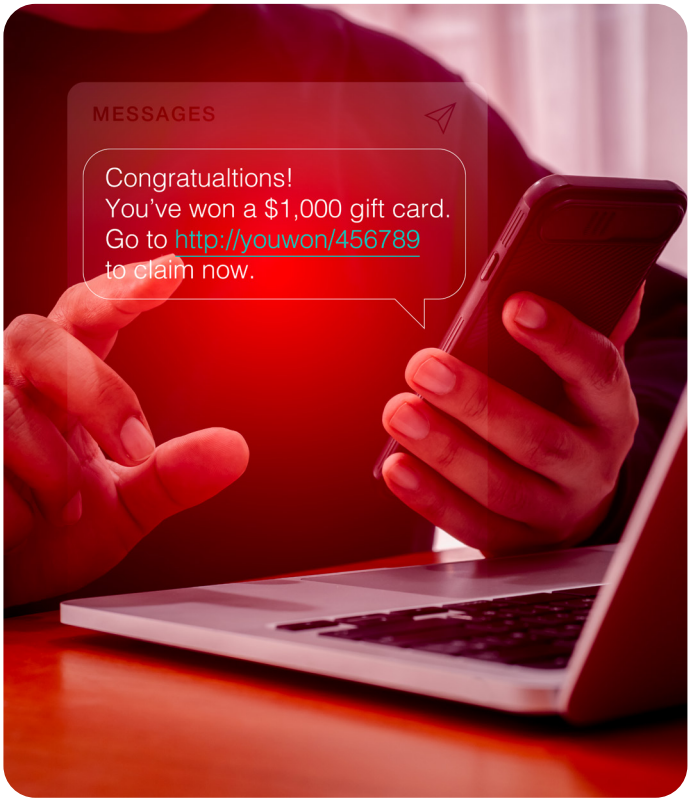
To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Lottery and Sweepstakes Scams

Lottery scams, or prize scams, target seniors by phone, email, mail, or even social media, informing them that they have won a lottery or sweepstake. They then ask for a fee to cover taxes or legal fees.

Common Warning Signs

- You receive an unexpected phone call, email, letter, or text saying you have won a prize.
- You are asked to pay fees, taxes, or shipping or handling charges before receiving your winnings.
- The caller pressures you to act quickly or keep your "win" a secret.
- You are asked to provide personal or banking details to claim the prize.
- The message contains spelling mistakes, generic greetings, or comes from a free web-based email (like Gmail, Yahoo, Outlook).
- You do not recall entering a draw.



Protection Tips

- Real contests never ask you to pay money upfront to receive a prize.
- Never share banking details or government identification numbers with unwanted callers or emails.
- Be careful if you receive unexpected claims that you have won something. Do not act quickly to get the prize. Ask questions and explore whether it is a scam.

What to do if you think you have been scammed:

- Stop all communication. Do not send money.
- Save any letters, emails, or messages as evidence.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Financial Service or Technology Support Scams

Scammers pretend to be from a bank, government agency, or computer company. They try to scare you into sending money, sharing personal information, or giving them access to your devices.

Common Warning Signs

- You receive an urgent call, email, or website pop-up claiming there is a problem with your bank account, taxes, or computer.
- The caller asks for your credit card, bank account, or Social Insurance Number.
- You are told your computer has a virus and asked to download software or give remote access.
- They may claim that a checking or savings account has been compromised and ask for personal information, such as a password, credit card, bank account, or Social Insurance Number, to "secure" it.
- They threaten legal action, account suspension, or you will lose money if you do not act quickly.
- Scammers often ask for payment in gift cards, wire transfers, or cryptocurrency.

Protection Tips

- Banks, government agencies, and real companies will never demand immediate payment or request gift cards.
- Do not click on suspicious links or download unknown attachments.
- Stop all contact and call your bank, government office, or service provider directly using a verified number.
- Keep your computer, phone, and security software updated.
- Talk to someone you trust before making payments or sharing information.

What to do if you think you have been scammed:

- Do not provide personal or financial information.
- Stop all communication and disconnect your device if remote access is granted. "Remote access" means someone is controlling your device from far away, using the internet or software, as if they are using the device or sitting in front of it.
- Save evidence such as emails, caller IDs, or pop-up screenshots.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Share scams with others to prevent more victims.

Investment Scams

Scammers offer fake investment opportunities promising high returns with little or no risk. The use of cryptocurrency (digital currency, such as Bitcoin) is common in investment scams.

Common Warning Signs

- Promises of certain or unusually high returns.
- Pressure to "act fast" or risk missing out.
- Requests to keep the opportunity secret.
- Unexpected calls, emails, or social media messages about investment opportunities.
- Limited or unclear information about the company or investment product.

Protection Tips

- Always research investment opportunities and the company that is offering them to ensure they are real.
- Beware of uninvited investment offers, even if they sound official.
- Never share banking, credit card, or personal information with people you don't know.
- Take your time and never let anyone pressure you into a quick decision.
- Ask questions and get independent financial advice before investing.
- Remember: High returns with little or no risk are usually scams.

What to do if you think you have been scammed:

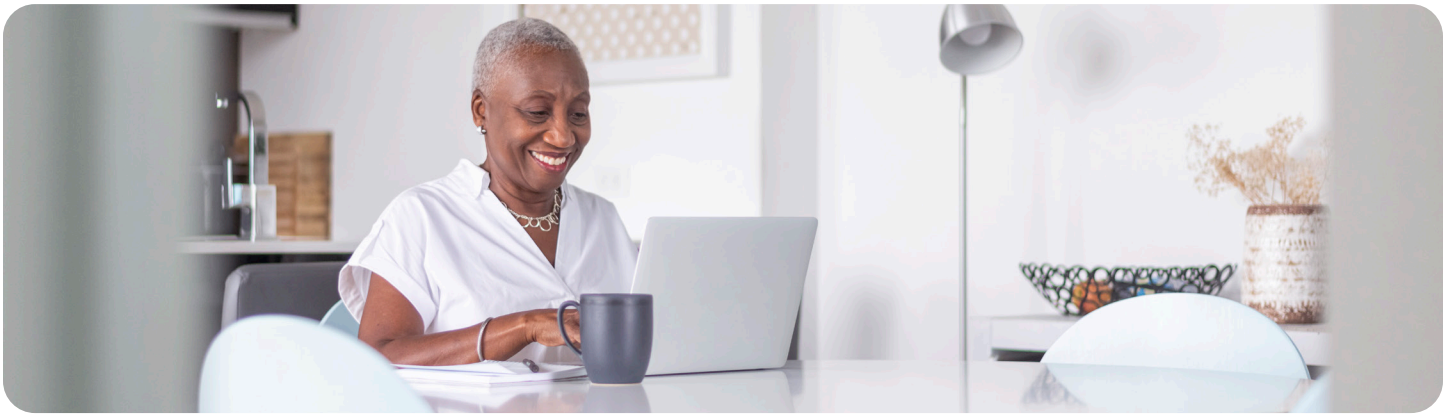
- Stop all communication and do not send money.
- Save evidence such as emails, messages, or transaction records.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Video link: Investment Scams

To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.



Home Repair, Improvement or Renovation Scams

A home repair, improvement, or renovation scam occurs when a person or company pretending to be a contractor unexpectedly offers you repair / renovation services that are unnecessary, overpriced, poorly done, or never completed after receiving payment.

Common Warning Signs

- Uninvited door-to-door or phone offers for home repairs or renovations.
- Request for large or full payment up front before work begins.
- Quotes or discounts that seem too good to be true compared to others.
- Contractors lack written contracts, licenses, or proof of insurance.
- High-pressure tactics or demands for immediate decisions.
- Refusal to provide references, reviews, or past project photos.
- Avoid questions about permits, inspections, or detailed costs.
- Avoid written communication and prefer cash payments.

Protection Tips

- Always get several quotes before hiring a contractor.
- Never pay large deposits or the full amount upfront; use staged payments after work milestones.
- Get everything in writing, including costs, timelines, and materials.
- Verify the contractor's business license and insurance coverage.
- Do not sign any document you do not fully understand. Ask a trusted family member or friend to review it.
- Beware of door-to-door offers or unexpected calls.
- Do not provide any personal and financial information until you confirm the company is real.
- If unsure about a company, ask for references and check reviews or ratings online.

What to do if you think you have been scammed:

- Gather all evidence, including any documents, receipts, emails, and text messages related to the scam.
- Contact your bank or financial institution immediately to report the scam and try to stop or recover any payments.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Password Protection

Avoid Weak Passwords

Weak passwords are made up of simple words, numbers, names, birthdays, or keyboard patterns and are easy for scammers to guess. Examples include:

- Password
- 1234
- qwerty
- jennifer1

Best Practices

- Using long passwords, minimum 12-16 characters is recommended. Longer is better for security.
- Instead of a password, create a passphrase that combines random words, numbers, and symbols that are easy to remember. Pass phrases are harder to guess. (e.g., Coffee@ Midnight#9528!).
- Never reuse passwords for multiple accounts to prevent one breach from affecting others.
- Do not use personal details (names, birthdays, favorite teams) in passwords.
- Avoid writing passwords down, use a secure password manager to store and generate passwords.
- Enable multi-factor authentication (MFA) wherever possible for extra protection. MFA means you will have to confirm your password in multiple ways such as using the password and providing a code only you would have received by your email address or a text message.
- Change passwords quickly if you feel your account was used or hacked by someone else.

Extra Tips

- Do not share passwords with anyone - keep them confidential.
- Use letters, numbers, and symbols to make it harder to guess.
- Pick security questions only you can answer and avoid those easily guessed or publicly available.
- Regularly monitor your accounts for breach alerts and take quick action if a password was used by someone else

Video link: How to Create a Strong Password

Another Video link: Short Introduction to Password Security

To watch the video, open your phone's camera and point it at the QR code (the square image that works like a link). Hold steady until a link appears, then tap it to open the video.

Tips for Staying Safe Online

Protect your devices:
Install and keep antivirus/security software updated.

Wi-Fi:
Avoid sensitive transactions (like online banking) while using public Wi-Fi.

Choose secure passwords:
Use different ones for different accounts and store them securely.

Enable two-factor authentication:
Add an extra layer of security on accounts like email, banking, or social media.

Beware of unknown senders:
Do not open emails from people or organizations you do not know. If you do, do not reply. Never click on links or attachments when you do not know the sender. Close the email and delete it.

Use secure websites:
Use websites with "https" - not "http" in their addresses when entering bank or credit info. The "s" generally means "secure".

Social media:
Do not accept friend requests from people you do not know in real life. Do not share your home address or other sensitive information on social media sites.

Think before you click:
Pop-ups or urgent messages asking for money or personal info are often scams.

Be mindful of downloads:
Only download apps and files from trusted sources like your device's official app stores or reputable websites (e.g., Apple App store, Google Play store).

Monitor your accounts:
Regularly check bank statements and online accounts for unusual activity.

Log out of accounts:
Especially on shared or public computers.
Watch for scams: Online deals that look "too good to be true" usually are.

Teach others:
Share these tips with friends or family who may be less tech-savvy.

Reporting Frauds and Scams

Why Reporting Matters

- The Canadian Anti-Fraud Centre estimates that less than 5% of the total number of fraud victims report their experiences.
- By reporting a scam, you provide law enforcement with the information they need to stop scammers and help prevent others from becoming victims.

What Should Be Reported?

- All suspected scams: online and phone fraud, phishing, financial fraud, identity theft, fake investments, and government impersonation.
- Any unexpected request for personal info, money, or account access.

Steps to Report a Scam or Fraud

- Collect information: Keep emails, texts, screenshots, phone logs, and receipts documenting the scam.
  - » Take note of the scammer's name, what they asked you to do and when.
  - » Write down or copy and paste the exact website address.
  - » If contacted by telephone, write down the phone number.
  - » If contacted by email, save a copy and take notes of sender's IP address, if possible.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Report the incident to the financial institution if money transfer has been made.
- Notify the website (e.g., Facebook, Kijiji, etc.) if the scam or fraud happened on a website.
- Notify your bank to flag unusual activity on your accounts and check your credit report.

Frauds and Scams

Scammers use emails, texts, websites, or social media to trick people into giving personal details, money, or clicking malicious links. Common scams include fake delivery updates, investment schemes, banking scams, job offers, government or prize notifications.

Common Warning Signs

- Unexpected contact from unknown numbers or addresses.
- Uses threats (“account suspended!”), urgent promises (“refund waiting!”), or rewards (“prize won!”).
- Demands immediate payment.
- Send you a link and ask you to click on it.
- Requests sensitive information like passwords,

  Social Insurance Number (SIN), or banking details.
- May request payments by cryptocurrency or gift cards.
- Caller ID or email sender that looks close to real but is off by a letter.

Protection Tips

- Never click links or download files from unexpected texts or emails.
- Do not respond to the scammer. Delete, or block their email address or number, and never share money or personal information.
- Double check sender addresses, website addresses and call known official numbers if unsure.
- Use strong and unique passwords or passphrases, enable multi-factor authentication, and keep devices and software up to date.

What to do if you think you have been scammed:

- Stop communication at once and save evidence (screenshots, emails, phone numbers).
- Change affected passwords, notify your bank, and check accounts.
- Report to local police and the Canadian Anti-Fraud Centre:

  Royal Newfoundland Constabulary:
  1-709-729-8000
  Deaf/Hard of Hearing TTY:
  1-800-363-4334

  Canadian Anti-Fraud Centre:
  1-888-495-8501
  Monday to Friday, from 9:00 a.m. to 4:45 p.m. (Eastern time).
- Speak with trusted friends or family.
- Share scams with others to prevent more victims.

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S