






Fraud awareness for seniors

Knowing how to identify, avoid and respond to fraud is essential for your safety and security. Whether you are a senior, or family member, caregiver or friend of a senior, learning about fraud and common scams will help protect you and those you care about. Use this information sheet to read about fraud prevention tips, common scam scenarios, and steps to take if you think you've encountered a scam.



Fraud prevention tips

-  **Watch out for unsolicited phone calls, text messages, emails and letters**
Fraudsters use different ways to reach out to potential victims and will typically create a sense of urgency in order to get a response.
-  **Protect your personal and banking information**
Many scams are designed to trick you into providing confidential information, such as your Social Security number or driver's license number, in order to steal your identity.
-  **Be cautious when making a payment**
Fraudsters will request untraditional forms of payment, such as wire transfer, preloaded cards, e-transfer, global money transfer or cryptocurrency, as these methods are often difficult to trace. Always ensure you know exactly who you're sending your money to and how your money will be used.
-  **Keep your contact information up to date**
Ensuring we have your correct contact information allows you to receive and respond to fraud alerts by text, email or phone to verify any suspicious transactions.
-  **Review your bill payments and bank statements**
Ensure all transactions on your account are accurate by regularly checking for any unauthorized charges.

Common scam examples

Grandchild emergency scam

You receive a call from someone claiming to be (or seeking assistance on behalf of) a grandchild or other family member. The fraudster requests funds due to a financial emergency. Common reasons for the request include bail money due to an arrest or funds for medical treatment related to an accident.

Prize or inheritance scam

You receive an unexpected call from someone claiming you've won the lottery or inherited a large sum of money; however, you are required to pay taxes or a "fee" in order to receive the funds.

Romance scam

You meet someone through social media or a dating site and spend time talking to them, building a trusting relationship. The person then fabricates a financial concern and asks for your help. Common requests relate to equipment they need urgently to secure a large project, taxes or fees that must be paid to receive an inheritance, or a medical emergency.

Service scam

You receive an unsolicited call from a computer or software company advising of security, warranty or other computer-related issues, or a pop-up on your computer may indicate a security issue and requests the user call a specific number for assistance. The fraudster will claim they need to fix these issues remotely and take over your computer.

Bank investigator scam

A fraudster calls you pretending to be a bank representative investigating a theft or fraud committed by an employee. You're asked to participate in the investigation to catch the employee by transferring funds using your personal bank account.

Signs of the scam

- You're asked to immediately send money
- You're asked to keep the situation a secret
- The person calling may claim to be an authority figure, such as a police officer or lawyer

- You don't recall entering a contest or lottery
- You're advised to respond quickly to claim the prize/inheritance or risk missing out
- You're asked to keep your winnings or inheritance confidential
- You're required to pay an upfront fee

- The person's online profile is new and lacks much of an online presence
- They quickly profess their love for you and avoid face-to-face interactions
- The person claims they need financial assistance for emergency situations

- You receive a pop-up warning on your computer providing you with a phone number for assistance
- You're contacted by a computer technician claiming your computer needs to be fixed
- You're asked to pay for the service by wire transfer, gift cards, prepaid cards or cryptocurrency

- You're asked not to tell anyone about the investigation
- The "bank representative" calls you and asks for your personal information, bank account information, online banking password
- You receive funds in your account as part of the investigation
- You're asked to purchase gift cards and provide the card information to the investigator or wire transfer a large sum of money

Common scam examples

Signs of the scam

IRS scam

You receive an unsolicited call, text or email from someone claiming to be from the Internal Revenue Service (IRS). The fraudster may insist that personal information is needed for you to receive a tax refund, or you must pay outstanding taxes immediately and may be threatened with legal consequences if you do not comply.

- You're threatened with aggressive language, legal action or arrest
- You received a text from the IRS; the IRS never communicates with taxpayers through text message or instant messaging apps, such as Facebook Messenger or WhatsApp
- You're told to make an immediate payment to the IRS by using a digital payment platform or app, wire transfer, prepaid card or cryptocurrency



If you think you've encountered a scam, stop all communication, don't send money or share any information, and investigate the situation further by taking these steps:

Take your time

Think about the situation you're in and avoid making any quick decisions. Ask yourself whether the situation you're in makes sense and question whether it could be a scam.

Do your research

Research the person you're talking to and the situation that you're in using online resources. If other people have been in the same situation, you may find more information online to confirm it isn't legitimate.

Talk to someone you trust

Ask for advice about your situation from a person you trust, such as a family member or friend. Getting an outside perspective on your situation will help you identify whether it may be a scam.

If you think you may be a victim of fraud, report it

Call CIBC at [1-877-448-6500](tel:1-877-448-6500) or visit your local banking center.