CHATS | Community & Home Assistance to Seniors

Common Frauds and Scams

Frauds and scams are common across Canada and change frequently. The examples below highlight some of the most common scams circulating. For more information and tips, visit CHATS Home & Community Resources.

1. Grandparent or Emergency Scam

- Usually happens over the phone and are effective because scammers use strong emotions and a grandparent's natural desire to protect their loved ones.
- The caller pretends to be your grandchild. They may say they are in trouble, for example, in jail, a car accident, or stranded, and that they need money now.
- The scammer uses fear and pressure, saying there is no time to check the story.
- The caller may already know your grandchild's name. Other times, they wait for you to say a name when you answer for example, *"Is this Patty?"* Once you do, they pretend to be that person.
- They may ask you to keep the call a secret *and* pretend to put a "lawyer" or "police officer" on the phone who demands immediate payment.
- Some scammers now use artificial intelligence (AI) to copy a loved one's voice, making the call sound very real and convincing.

Stay Safe: If you receive a call from a family member in distress, hang up and call them back on the number you have for that person, ask questions only they would know and that would not be shared on social media, ask for help even if they pressure you not to, and consider implementing code words with your family that they would use to verify who they are.

2. Romance Scam

- A romance scam happens when someone pretends to form a romantic relationship to steal money or personal information. These scams begin online through email, text, social media, or dating websites.
- The scammer uses a fake profile, builds trust, and talks about a future together.
- Once trust is built, the scammer asks for money. They may ask you to: Send cash or gift cards; Help with an "emergency"; Invest in a business or cryptocurrency; Move money or open accounts on their behalf.
- The scammer often has excuses for why they cannot meet face-to-face or speak on video, and they may suggest that you keep the relationship private.

Stay Safe: Don't accept any funds or send the person any money for any reasons. Scammers will use all kind of tactics to get to your money, bank accounts or credit cards.

3. Phishing scam

- Phishing is a common online scam designed to trick you into disclosing personal or financial information for the purpose of financial fraud or identity theft.

- Scammers will send an email that appears to be from a legitimate source and direct you to a fake website; or they'll call and direct you to a fake website. That fake website will look real by copying the brand name and logo of the real company. They then ask you for personal information such as credit card numbers, account numbers, passwords, date of birth, driver's license number, and social insurance numbers.
- While you may think you are giving your information to a valid company, instead, you may be providing it to a scammer.
- This is a popular tactic used against seniors who may be more trusting and have more time to respond to apparent offers or deals.

Stay Safe: Always stop and think before clicking on a link or file of unknown origin in an email. Don't feel pressured by any emails to click, login or provide any personal information. If unsure, call the company using the phone number on an account statement or other formal documentation to verify the information or offer and ensure that you are calling the correct company.

4. Tech Support Scam

- A tech support scam tries to scare you into thinking your computer, tablet, or phone has a serious problem.
- These scams often appear as pop-up messages on your screen or through the phone. The message may say you have a virus or that your device is in danger. It may include loud alarms, flashing warnings, or a voice telling you to act right away.
- The message usually tells you to call a phone number or click a link to fix the problem. If you call the number, you will reach a scammer pretending to be from a well-known company, such as Microsoft or Apple.
- The scammer may ask for your credit card information to "remove the virus" or "protect your computer." They may also ask you to share your screen or give them remote access, which allows them to see your personal information and take control of your device.

Stay Safe: Legitimate tech companies will never call you out of the blue to fix a problem you didn't report or spam your computer with pop-up messages. Do not click on pop-ups. If concerned you may have a virus, ask a family member for help or take your technology to a trusted shop to be checked and fixed such as Best Buy.

5. Investment / Financial Scam (Sometimes called Impersonation Scams)

- In this scam, the caller or message pretends to be from a trusted organization, such as a bank, mortgage company, government office, or debt collection agency.

- The scammer may contact you by phone, text, or email, and the message may look very real. They might say there is a problem with your bank account or that your money is at risk.
- The scammer may ask for personal information, such as passwords, PIN numbers, banking details, or your Social Insurance Number, claiming it is needed to "secure" your account.
- Some scammers promise better investment returns, lower mortgage rates, or special financial opportunities that sound too good to be true.
- Others use fear and threats, such as claiming you owe money or could be arrested if you do not pay right away.
- Scammers can fake Caller ID, email addresses, and official-looking messages. They often pressure you to act immediately and may demand payment by cash, gift cards, wire transfer, or cryptocurrency.

Stay Safe: Avoid mail or telephone solicitations, disguised as promotions or surveys, offering instant prizes or awards designed for the purpose of obtaining your personal details, including credit card numbers. If they've stated a problem with your bank, credit or any account, hang up and call the phone number on your last account statement to verify it's true.

6. Home Renovation Scam

- A home renovation scam often begins with a knock at the door from someone who claims to be a contractor working nearby. The person may say they noticed a problem with your roof, driveway, or chimney and offer a "special deal" because they have extra materials left over.
- These scammers often target older adults, assuming they may not know the true cost of repairs and use high-pressure tactics, such as telling you that you need to decide right away.
- The scammer may pressure you to sign a contract quickly or ask for payment upfront.
- They will demand cash up front, then never return. Or they may charge exorbitant fees for repairs and then do little, poor or no work and take your money.

Stay Safe: Do not be pressured into buying or signing anything. Request for the information they are providing you to be provided in writing on the company's official letterhead. Research the company and discuss the project with friends and family.

For more information and tips, visit CHATS Home & Community Resources.