




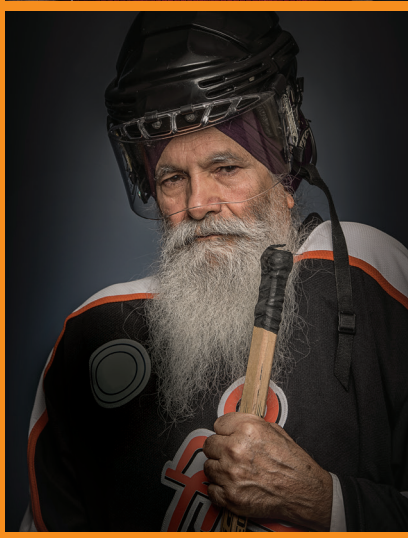

FRAUD & CYBERCRIME SAFETY TIPS

VANCOUVER POLICE

THERE ARE OTHER WAYS TO PROTECT YOURSELF

S.A.F.E.

Safety Awareness for Elders

8 WAYS TO PROTECT YOURSELF

1. *Get a mailbox with a lock and collect your mail every day.*

2. *Buy a good quality shredder and shred all personal or financial documents that you no longer need.*

3. *Beware of unsolicited emails, texts, or phone calls from someone saying they are with your bank, credit card company, or the government (i.e. Canada Revenue Agency). Do not give or confirm personal information.*

4. *Check your credit rating every year.*

FROM FRAUD & IDENTITY THEFT

5. *Keep your credit cards secure and with you.*

6. *Beware of scammers using emotion to create a sense of urgency and compel action.*

HOPE: *You have won a prize!*
FEAR: *You owe taxes!*
ALTRUISM: *Be our secret shopper!*

7. *Report all incidents of mail theft, fraud, and suspicious activity to local police.*

8. *Arm yourself with current, trusted information, and share it with your friends.*

8 WAYS TO PROTECT YOURSELF

1. *Fix security issues on your computer and other devices by keeping the operating system up to date.*

2. *Back-up your computer regularly, so you can restore or recover valuable documents and photos.*

3. *Use strong and different passwords for your online accounts. A passphrase (four words strung together) increases security greatly.*

4. *Ensure the router for your home network is secure and password-protected.*

FROM CYBERCRIME

5. *When shopping online, only purchase on trusted websites, and consider using a separate, low-limit credit card.*

6. *Ensure you have the highest privacy settings on your internet browser and your social media accounts.*

7. *Be careful of what you share on social media. Don't post personal information like your birthdate. Photos you post can have geotagging, which can reveal your location.*

8. *Report all incidents of cybercrime to your local police.*

COMMON SCAMS

1. INVESTIGATOR

You receive a call from someone claiming to be a bank investigator or police officer, who asks for your help in catching crooked bank employees.

They tell you to hang up and call your bank right away. They give you the number to call or offer to help you find it.

When you hang up the phone, the fraudsters stay on the line. The call remains "active" for long enough that when you pick up your phone again to call your bank, they are still on the line (dialing the number of your bank does not disconnect the call).

Another person may take the phone and pretend to be from your bank. They ask you to withdraw a large sum of money and send it to a foreign address, or to meet someone to hand over the money so it can be examined – all while promising to return the cash to you. After the money is sent, or handed over, you never get it back.

TO WATCH OUT FOR

2. ROMANCE

Some people looking for companionship online have been victimized. You may meet someone online who seems nice, and even develop strong feelings for them based on email correspondence and photos.

However, the photos may not be of the person you are communicating with. Usually, the fraudster will ask for money for things like an emergency loan to secure a business deal, or to get them out of trouble. They promise quick repayment once the crisis passes.

Unfortunately, many seniors have lost significant sums of money that can't be recovered.

3. SECRET SHOPPER

A person emails you asking you to be a secret shopper. They mail you a cheque as payment and instruct you to deposit it into your account. The amount will be more than you were promised. They ask you to send the overage back to them minus a token amount for your trouble. The original cheque will later be rejected by your bank as fraudulent and you will lose the money you sent.

4. HOME REPAIRS AND INSPECTIONS

This scam usually involves someone coming to your door offering home repairs or inspections.

They claim they are working in the area and can give you a special price. The scammers often ask for large advance payments, which they take without doing the work, or they perform minor or shoddy work.

Whenever you hire someone to work on your home, be sure to get a number of quotes for the job.

Ask for references and follow up on them. Remember, no reputable company would ask for payment up front. Contact the Better Business Bureau about potential contractors to make sure they are in good standing.

5. PAYMENT FOR LOTTERY

Anyone who calls, mails, or emails you advising that you have won a lottery is a fraudster. You cannot win a lottery that you haven't entered.

TO WATCH OUT FOR

The fraudster will advise you have won a significant sum and may ask you for a fee or taxes in order for your winnings to be sent to you. If you send money, they will request more by using new reasons (lawyer or banking fees, etc.). They will ask you to wire money within the country or outside of Canada.

6. EMAIL OR TEXT PHISHING

You may receive an email or text that appears to be from a Canadian bank, saying there is a problem with your account and asking you to confirm personal details and account information. This is always a scam. No reputable business or bank will contact you to confirm information they already have.

Check the email address. It may contain unusual numbers and letters and may show that the email address is not associated with the bank. Fraudsters will try to get personal information from you to steal your identity and commit fraud in your name.

7. HELP FROM GRANDPARENT

You receive a call from your "grandchild," who is in trouble. You may have been tricked into saying your grandchild's name, which the caller will use to further convince you the call is legitimate. They may tell you your grandchild is in jail, in hospital, or has caused an accident, and they don't want their parents to know. They need you to send money to help them out. A second person may get on the phone claiming to be a lawyer, telling you to send money. They instruct you to wire money, often outside of Canada. Many seniors have been victimized in this way as fraudsters prey on the love and concern you have for your grandchildren.

TO WATCH OUT FOR

8. CRA

You receive a call from a fraudster pretending to be from Canada Revenue Agency saying there is a problem with your taxes. They tell you there is a warrant for your arrest, or that you're facing deportation. The fraudster will demand payment to cancel the warrant or stop deportation. They instruct you to buy pre-paid gift cards and provide the code over the phone, or they may tell you to deposit cash into a Bitcoin ATM.

The CRA will never call you about outstanding taxes and will never threaten to arrest or deport you. The CRA does not accept payment by credit card, pre-paid gift cards, or Bitcoin.

RESOURCES

- **VPD.CA**
- **GetCyberSafe.ca**
- **AntiFraudCentre-CentreAntiFraude.ca**

For more information, call the VPD Financial Crime Unit at (604) 717-2569 and leave a voicemail with your name and number. Someone will call you back.

- **In an emergency, call 9-1-1**
- **For non-emergencies, call (604) 717-3321**

#BeSafeBeStrong

#BeSafeBeStrong

THANK YOU TO THE VANCOUVER POLICE FOUNDATION
FOR SUPPORTING THIS RESOURCE