DON'T BE SCAMMED!

There are many scams going around (some are repeats) and unfortunately seniors seem to be the most vulnerable. They come by telephone, snail mail, email, QR codes or by debit cards. Keep your wits about you. STAY ALERT, if in doubt, consult a family member or a friend.

Check out YouTube 60 minutes episode "Targeting Seniors." It is a game changer. The scammers get your voice from videos on social media or prior phone calls and create false statements with the "voiceprint." If you get a call from a scammer, it's best not to continue the call, because they can use your voiceprint for a future scam.

Someone in your family is in hospital, or in trouble, or has been arrested in some foreign country. You can hear him crying in the background. They say you need to send money right away for legal or medical or bail fees. Check with your family first!

The CANADA REVENUE AGENCY are threatening to have you arrested and jailed for some infraction. They are requesting you pay them immediately by Bit Coin or Gift Cards. THE CRA DO NOT CALL TO THREATEN, NOR DO THEY REQUEST PAYMENT BY BIT COIN OR GIFT CARDS.

Never give out personal information (SIN number, Date of Birth, Credit Card Number) over the phone or by email. This is information your Bank and Canada Revenue Agency already have.

Scammers can "spoof' or fake the phone number to say they are calling from a specific organization. A 416 area code could indicate to you it was from Toronto if they are pretending to be a government agency.

Links

If there is a link inside a suspicious email, it could be a scam. Do not click the link, for they could plant malware on your system. You can always check the actual link prior to clicking it. Just **hover your cursor over the link** in the email, and a window will pop up in the lower comer of your browser showing you the actual link.

If you get a text saying there is a problem with your **bank account, definitely do not click on the link.** Do not enter your bank account, username and password, so someone can get into your account. If you're not sure what to do, call your bank directly.

If you get a message from Amazon, Apple, Netflix, bank or credit card. You do not have to respond, call the bank, cell phone provider or check your Amazon, Apple or Netflix account. Opening the email won't put you in danger, but it will show your account is active, and you'll get more smishing texts. **Don't click on the "unsubscribe" links.** Just delete the email and block the sender.

If you have clicked on a link and were led to a website, temporarily disconnect from wifi or turn on airplane mode to delete any malware downloading.

Often spelling mistakes, odd punctuation and weird use of language are signs of a scammer. The majority of scams come from countries where English is not their native tongue.

If you do online ordering, make sure the website you are using starts with https://. The "s" means the site is secure. Don't just look at the name of the sender, check the email address. If it is not the one you know, it is probably fake.

QR codes

Scammers are creating QR codes that can lead to fake payment websites or download malware. Before you use a code, check the website address displayed. The url should start with "https."

Debit cards

A scammer might jam an ATM cardslot so you can't insert your card. A stranger might suggest you use the tap function. After the transaction is over unless you log out, the scammer has access to your account after you have walked away!

Check out the Website Canadian Anti-Fraud Centre which has plenty of information on fraud, www.antifraudcentre.ca

If you are a victim of a fraud, report it to police: 888-579-1520