Crime Prevention Safety Tips-Online Safety /Frauds and Scams

FRAUD

Definition: Sec 380 (1) Criminal Code

Everyone who ,by deceit,falsehood or other fraudulent means ,whether or not it is a false pretence within the meaning of this Act,defrauds the public or any person,whether ascertained or not,of any property,money or valuable security or any service, is guilt of the offence

“STREET WISE SMARTS”

Modern Technology has Changed our Day-today life, and its critical our that our “Seniors” become street wise, and know how to respond to these experiences

We all come from an era when a handshake sealed a deal, when basic trust and respect naturally and automatically came to us

Due to the Pandemic, and time or life moving forward, cellphones, computers ,tablets and landlines have become tools for scammers, and they are waiting for their next target.

Before you do anything..”THINK!..Stop and think some more before you act…Digest what is happening.

DON’T BE AFRAID TO CALL SOMEONE-OR GET A SECOND OPINION

WHY TARGET SENIORS AND THOSE VULNERABLE?

Excessive ability – home during the day

Trust – Older adults are often more trusting

Polite – Older adults are raised to be respectful

Finances – money or assets

Older people and seniors are more common targets –Why? (you have the money and the info vs younger people) Many “Hackers” target the older generation for these reasons

STOP-THINK-THINK SOME MORE!!

Do

Hang Up

Delete Emails

Keep Info Private-Social Media

Remain in Control-Be Assertive

Report immediately if you are a victim of Fraud / Identity Theft

Don't

Don't provide personal info (Banking,passwords or S.I.N)

Don't Click on links from unknown sources

Don't let strangers in your home

Don't Feel Threatened

Don't send money, provide Credit Card info or purchase Gift Cards as a form of payment

RED FLAGS!

REPORTING A FRAUD

Fraud is evolving. A fraud can often carry on over an extended period of time and is a crime that is difficult to recognize and report. To make reporting easier the CAFC suggests completing the following six steps:

Step 1: Gather all information pertaining to the fraud. More info at time of report is better

Step 2: Write out a chronological statement of events.

Step 3: Report the incident to your local law enforcement. Police Can't Help , if not Aware

Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.

Step 5: Report the incident to the Financial Institution or Payment Provider used to send the money.

Step 6: If the fraud took place online, report the incident directly to the appropriate website.

ONLINE SAFETY TIPS AND CONSIDERATION

Security Password/Login. Never make it easy for others to figure out (Think of your password, like the lock on the front door of your home (Are You putting a durable lock on? Or a weak /flimsy one) And be sure change it often

Don't share your password/login information with others (use special names/years/initials/places or colours) make it a combination of one or more. Never use simple things like current pet name your birthdate,home address etc..

Wifi-When its free, feel free to use it.."JUST DON'T ACCESS ANY PERSONAL ACCOUNTS, (ie:banking and other sites where your personal information may be stored) , and always clear your browser prior to accessing free wifi ANYWHERE!.

Never have your phone automatically connect you to wifi spots that you frequent or have used before, Keep WiFi turned off and only enable when in wifi to ensure that you are always asked/notified to join when wifi is enabled, and ONLY connect to trusted sites.

Always ensure Bluetooth is deactivated when not in use (Blue Scarfing)

Keep your device up to date, and only install reputable anti-virus software on the device you use for online activity

GIFT CARDS ARE FOR GIFTS NOT PAYMENTS

Won a Prize, but need to pay fees with a G/C

Caller claims to be from CRA-Request to Pay with G/C

Tech Support/Issue with Computer-Request to Pay G/C

Family Member Emergency-Request to Pay with G/C

Utility –Water Company-Request Payment with G/C

Online Purchase of item-Request you pay with G/C or

Someone wishes to Purchase and pay you with G/C

Sympathy Tragedy –Request you pay with G/C

Sends Cheque over-payment, request you send difference in form of G/C

Anyone who demands Payment by G/C is a SCAM!!!

GIFT CARD TIPS

Inspect Gift Cards before you buy, (Security stickers are intact, Pin tampered)

Keep the receipt with Gift Card

Use the Card as soon as you can

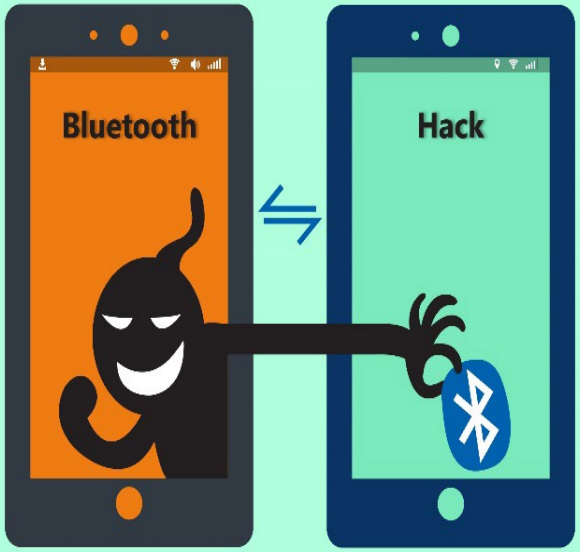
Treat Gift Card like you would cash

Read The Terms and Conditions

Buy Gift Cards from Sources You Know and Trust-Avoid online sales or auctions

NOTE-If you Paid a scammer with a Gift Card, Tell the Company immediately that issued the card, and tell them it was used in a scam. Ask them if they can refund your money, This “MAY” possible if you act fast enough!!!

BLUETOOTH HACKING-"BLUESNARFING"



Things to Consider

Always Ensure Bluetooth is turned off when it's not connected to a source

Phone can only be hacked through a laptop, and usually person is within 30 feet of your device-Be aware...BE ALERT!

If you like to connect to a vehicles wireless "Bluetooth", always ensure you do the following before exiting your vehicle

1.Disconnect –turnoff Bluetooth and delete phone from vehicle

2.Turn vehicle off

3.Disengage seatbelt

Rentals/Trade for Sale or Repairs –Things to Consider

1. Important to always go into the vehicle "Settings"/Bluetooth Icon and delete your phone and any other phones that have synced to that vehicle. Always do this before returning rental car, The sale of a personal vehicle, or when sending personal vehicle in for service..

Even if your phone is not insight , a hacker can steal your info by connecting to the vehicle Bluetooth system

Bluetooth mirrors your entire phone and all its information. Although you are no longer connected to the vehicle, you have left a picture perfect imprint of your phone and your personal information

Never connect to ride-share vehicles or plug into their USB ports

Security Settings should always be on highest

USE IT-THEN DISCONNECT AND DELETE

SHOPPING ONLINE

Make sure the address / website always starts with https (the “S” stands for secure), although many with just http(Hyper Text Transfer Protocol) are safe, best to give priority to the secure ones, Especially with online shopping. Ensure they are trusted sites to avoid giving away your bank account data to wrongdoers

Never save/create accounts with shopping services and DON’T save credit and/or financial info on the site. Big companies get hacked TOO !!

Although it may seem convenient and save you time, it will be way less convenient and task you so much more ,when you are attempting to get your money back

Be careful about gimmicks and items that seem to good to be true. No Deal is so time sensitive, that you must act NOW!!

Be careful and educated about cures/treatments or online purchasing of medical products. It’s illegal to sell/offer the vaccines on the internet. Always consult with a medical professional first

*REMINDER-CLEAR/CLEAN your browser. All websites have trackers, so clear out your browser to eliminate unsolicited add/websites.

TYPES OF ONLINE OR IN PERSON SCAMS

Home repairs/ renovations/hot water heaters..etc.. NO DEAL IS SO TIME SENSITIVE AT YOUR DOOR..wait and call around to a reputable company for a second opinion and also confide in a family member or friend

Family member is in trouble and/or incarcerated and requires money immediately to be released from jail, (person on phones requests etransfer, Western Union, Credit Card, Gift Cards or itunes cards)

Revenue Canada CRC Scam..fear of Police Persecution if debt is NOT paid immediately

Romance Scams (Dating Websites)

Financial institution Calls and requests you to confirm banking /credit info(Bank already has your info and will NEVER ask you to confirm unless YOU called Them!!

NEVER call back the number given to you over the phone or email, ALWAYS look the number up yourself for the institution and call yourself for confirmation

Distraction Thefts (usually in pairs) one person distracts while another steals purse/wallet

Hitman Scam

Lottery Scam, Refunds or Estate Money etc..DONT EVER Provide banking info or submit a request to pay taxes before money can be released into your account .YOU CAN'T win a lottery when you have NEVER filled out a ballot or bought a ticket. Its illegal in Canada to require a recipient of a prize to pay a fee before receiving winnings.

Tragedy-Charity Scams

Government Refunds/Rebates

EMAILS

Never click on email links or attachments from unknown sources

Signs of phishing emails-misspelled domain (move curser over email sender and ensure it is spelled correctly and includes actual name of company and not letters/numbers/characters)

Poorly written email-(spelling mistakes-refers to you as a costumer instead of customer)

Heightened sense of urgency (Act now ! or this deal will be gone, A family member or friend is in trouble, Respond /pay or you will be arrested !) CBSA, CRA

<u>BEWARE-"SPEED IS GREED"!!</u>

SOCIAL MEDIA SAFETY TIPS

Is your account private or public

What information is on there? (single,divorced,widow-er)

Pictures-family,children,pets

Grand-children,hobbies

Vacation photos

Address,City you live in

Never post places/vacations you are going to and/or during, “ALWAYS” post when you have returned home

This Information is what Scammers will use against and for you !!

ONLINE FRAUDS AND SCAMS

CRA-CERB Benefit (Canadian Emergency Response Benefit)..calling saying you have received a payment (NEVER PROVIDE BANKING INFO)

COVID Cures, remedies- “BE” careful what you read, watch and/or believe . Even during a Post Pandemic-Endemic, scammers will still utilize fear to take advantage of You

Deceptive emails..(Always scroll over the sender to also see if the sender email is the same as the company sending) when receiving phone calls or text messages, you can always do a google search of the number and see if others have reported it as a scam/fraudulent number

Puppy/Pet Scam..Never purchase a pet that you have never seen in person or met and viewed the breeder and location of animals being raised

Never send money to People you don’t know, click on links or download things from emails sent to you from people you don’t know!!!

DON'T FEEL PRESSURED

No Deal is too GOOD to be passed up

If they say the deal will expire once you hang up or they walk away, it probably wasn't that good anyways!

NEVER give out your personal information, SIN or any banking information(PIN ,Account Numbers) to anyone EVER!!!!!

Your bank already has everything and will never ask you to confirm over the phone UNLESS you call them directly from the number on the back of your card

(ie: date of birth ,card number and home address for purpose of identifying customer)

It is estimated that fewer than 5% of victims file fraud reports

TOP 10 FRAUDS AFFECTING CANADIANS 2021

Top 10 frauds affecting seniors based on dollar loss in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Investments	487	449	$38 M
Romance	332	251	$19.1 M
Service	1525	1051	$4.9 M
Extorsion	2483	391	$4.5 M
Bank Investigator	858	339	$2.5 M
Prize	580	165	$2.5 M
Timeshare	30	25	$2.1 M
Foreign Money Offer	112	13	$2 M
Emergency	573	181	$1.9 M
Grant	227	117	$1.5 M

ESTIMATED LESS THEN 5% Report –WHY?

THANK YOU

Crime Prevention Officer-Community Safety Branch

Sr.Cst.Darryl RICE#3309

Durham Regional Police Service

drice@drps.ca

905-579-1520

Ext 5660