FRAUD AWARENESS

TOP FRAUDS AFFECTING SENIORS

Preface:
RCMP 'E' Division Federal Policing Prevention and Engagement (FPPE) works with both public and private sectors to survey the landscape on crime trends and promote targeted prevention messaging. If you are a victim of fraud or any other crimes, we encourage you to contact your local police. We also encourage you to contact the Canadian Anti-Fraud Centre if you are a victim of fraud and to visit their website to keep current on the trends.

How Fraudsters Are Reaching Victims:

In Person:

Traditionally fraudsters have operated door-to-door, at parking lots, or at events to sell you stolen or inflated goods, services that don't exists, or invests in fraudulent schemes.

Recommendations: Do not allow fraudsters to pressure you or threaten you; remember the old adage "if it's too good to be true"; do your research before committing to a contract or deciding to invest.

By mail: Another traditional method that could reach more potential victims then the in-person approach. Scammers have used this method in ransom or lotter frauds.

Recommendations: Remember, you cannot win a contest if you did not enter; contact your local police if you receive suspicious and threatening letter.

By SMS Text Messages:

Fraudsters are using technology to reach more potential victims. SMS texts are sent to the cellphones of potential victims using automation. The messages appear to come from legitimate companies, financial institutions and government agencies but direct victims to websites set up by fraudsters for nefarious reasons.

Recommendations: Inspect these messages closely, ignore, delete and mark the message as "Spam" (for Android Phone users). Be aware that the originating number can be falsified to come from legitimate source (Spoofing).

By Emails: Fraudsters are sending emails en-mass to potential victims posing as legitimate companies or financial institutions. Their goals include adding malicious software to steal your information or through further deception have you send funds to them.

Recommendations: Avoid opening unsolicited emails or clicking on suspicious links. Hover over an email address or link and confirm that they are correct. Mark or move suspicious emails to your Junk Folder before deleting it.

By Phone: Fraudsters use technology to automate mass calls to potential victims. The calls contain recorded messages posing as legitimate businesses, financial institutions or government agencies. They may direct you to press a button to speak to a live agent who will attempt to convince you that you are in trouble and ultimately obtain your funds.

Recommendations: Do not follow their instructions and hang up. Be aware that the caller's number can be falsified (Spoofing). Do not provide personal information over the phone to an unknown caller. Police and other government agencies will not call to threaten you or demand payment in crypto assets or gift cards.

FRAUD AWARENESS

TOP FRAUDS AFFECTING SENIORS

#1 Investment Scams:

Investment scams are fraudulent schemes that aim to deceive investors and take their money, personal information, or both. There are many different types of investment scams, including crypto assets investment scams. Scammers use various methods to reach potential victims, such as text phishing, email phishing, and social media, just to name a few. Recent trends have seen a nexus with romance scams. They make incredible claims of guaranteed returns with low risks. They use pressure tactics, including claims of limited opportunity/time, trying to get victims to act immediately. Sometimes they deploy deceptive techniques, such as spoofing and deepfakes.

Recommendations:

Conduct a thorough research from credible sources before you decide to invest. Avoid unregulated exchanges and brokers. Avoid advice and offers to invest from social media or dating sites. Be skeptical of guaranteed returns.

#2 Romance Scams:

Fraudsters contact their potential victims through all forms of social networking and dating sites. A relationship is fostered and love is quickly professed, however, love is not what they are after. Fraudsters would use this emotional connection as leverage to ask for financial assistance. Usually claiming some form of emergency. They would continue to extract money from the victim sometimes over a long period even though they have never met in person. They may make excuses as to why they cannot meet in person. Fanciful claims of military service, employment overseas or successful business people are popular.

Recommendations:

Recognize the signs. Beware of individuals who quickly profess their love. Beware of individuals who claim to be wealthy but need to borrow money. Never send intimate photos or video of yourself as they may be used to blackmail you.

#3 Service (Tech Support) Scams:

Service scams encompasses a variety of frauds involving services from telecommunication to technical support. Fraudsters may use automated calls with recorded message or a Windows pop-up that appears to be a system generated warning with a phone number for victims to call. They may claim to be from Microsoft or other well known companies. The criminals may try to get permission to remotely access the victim's computer to steal information and money. Be aware of unsolicited calls claiming to provide technical support.

Recommendations:

Hang up. Close the Windows pop-up. Do not call the number on the Windows pop-up. Microsoft and other companies will not display a phone number for you to contact them. Check to see if it's a real systems warning. Re-start your computer and run a virus scan. Never allow strangers to remotely access your computer.

FRAUD AWARENESS

TOP FRAUDS AFFECTING SENIORS

#4 Extortion - SIN Scam:

Fraudsters use automated calling with a recorded message advising you that it is Service Canada and that there is an issue with your Social Insurance Number. The caller's phone number appear to be a local number, it may even appear to come from Service Canada. If you follow their instruction to press a button, a live person will come on the line and speak with you. This person is a fraudster and will threaten you and make up stories to get you to provide your information, transfer funds at their bank account or go a Bitcoin ATM to send them crypto assets. CRA Scam follows a similar MO.

Recommendations:

Hang up. Police and Government agencies will not call you with an automated message to threaten you with legal actions / arrests. Police and Government agencies will also not demand payment in Bitcoin (crypto assets) or gift cards.

#5 Emergency Scams:

Fraudsters will contact potential victims by phone, by email or even through social media platforms posing as families or friends asking for financial assistance due to an emergency. A version of this scam is hitting seniors and is called the "Grandparent" Scam. Fraudsters would pose as a grandchild and claim that they are in trouble. Perhaps an emergency that would require the grandparent to send funds to help them out such as an arrest from impaired driving or an emergency visit to a hospital.

Recommendations:

Don't give out your information. Don't let the fraudsters rush you. Confirm with another friend or family member. Guard your personal information on the internet (social media).

WHAT TO DO:

- Stay informed on fraud trends. Check the Canadian Anti-Fraud Centre (CAFC) to learn more.
- If you are a victim of fraud, report the incident to your local police and the CAFC.
- If you are not a victim, you can still report to CAFC. This helps inform law enforcement and the public of emerging trends.

Helpful Links:

Canadian Anti-Fraud Centre (CAFC) to learn more:
https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

BC RCMP:
https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=14&languageId=1&contentId=-1

BC Securities Commission: Investment Caution List | BCSC

Canadian Securities Administrators' National Registration Search: https://info.securities-administrators.ca/nrsmobile/nrssearch.aspx

RCMP ROYAL CANADIAN MOUNTED POLICE

RCMP 'E' Division Federal Policing Prevention and Engagement (FPPE) *E_FEDERAL_FPPE@rcmp-grc.gc.ca*