Anti-Fraud and Anti-Scam Information
Compliments of

National Association of Federal Retirees
Association nationale des retraités fédéraux

Central MB 32

In Partnership with

Stride CREDIT UNION

With branches in:
Portage la Prairie, Neepawa, Austin, Gladstone, MacGregor
877-228-2636
stridecu.ca

Craig Dunn "Still the Motor City" GM CANADA
CHEVROLET BUICK GMC

Located in:
Portage la Prairie
800-473-6050
cdmc.ca

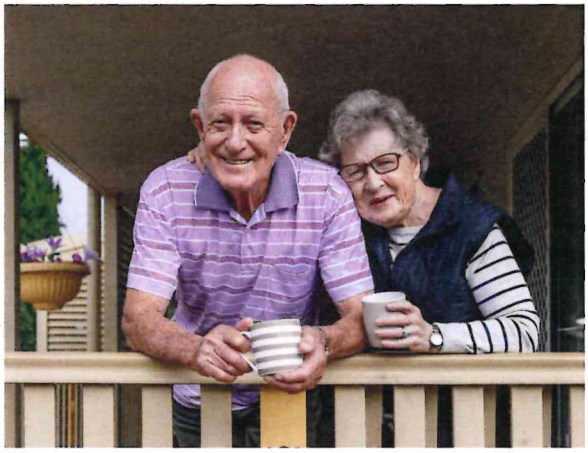
PETRO-CANADA **MAR-DEE ENTERPRISES**

With locations in:
Brandon, Portage la Prairie, Virden, Melita, Neepawa, Reston, Hartney, Austin
204-857-8764

If you think you are a victim of fraud:

1. **Immediately call your financial institution and/or credit card company**
2. **Call the RCMP or your local Police Department**
3. **Call the Canadian Anti-Fraud Centre 1-888-495-8501 to report fraud and scam phone calls**

Fraud Prevention Checklist



It's important that you protect yourself and your personal information, including your finances, from online and telephone fraud.

1 Protect your devices.

Install anti-virus and anti-malware software to protect your connected devices (like your mobile phone, desktop computer and tablet) and never skip an update. Install software updates as soon as they are available so you're protected against the latest threats. Even better - automate the updates so they're installed automatically.

2 Create unique, strong passwords.

Ensure you create strong, unique passwords for each account and website. This is important since a security breach at one site means your password could be handed to criminals who may try to use it at other sites - this is known as credential stuffing. If you suspect or know that your password has been compromised, be sure to change it on the affected account and any accounts where you may have reused it.

Fraud Prevention Checklist

6 Report lost/stolen cards immediately

Report lost/stolen credit and debit cards, drivers licence, social insurance card, passport and other documents with personal identification immediately. Review your bank and credit card statements regularly.

7 Strengthen social media security and privacy settings

Review the privacy and security settings available for all your social media accounts and tighten the default controls. Be sure you only accept "friend" requests from individuals you know and review your contacts every few months to ensure all your contacts are relevant.

8 Be wary when downloading online content

Malware like ransomware (that locks you out of your devices or files until a ransom is paid), spyware (that secretly monitors what you do online) and keystroke loggers (that secretly track what you are typing) can be hidden in downloaded files or apps and used to access personal information, such as passwords and financial information, Every few months, check through your devices and delete apps you no longer use so they don't become a security risk.

Scams

A scam refers to a fraudulent scheme or deceptive action designed to swindle someone out of money, valuables and personal information. Scams can occur in various ways, including via phone, email, in-person encounters and online platforms. The primary aim of scammers is to deceive the victim into providing something of value, typically through manipulation, false pretenses or outright lies. Keep reading to find out about popular scams affecting our neighbours.

1. Phishing

This involves sending emails pretending to be from a reputable company to trick individuals into revealing personal information, such as passwords and credit card numbers. Red flags to watch for:

a. **Demands and threats**: is the request for information from a legitimate source? Your financial institution will never send you a threatening email or call you on the phone demanding information like your password, credit or debit number, or your mother's maiden name.

b. **Suspicious senders**: check the "from" address by hovering your cursor over the sender's name. Some phishng attempts use a sender email address that looks legitimate but isn't.

c. **Suspicious links or attachments**: be wary of links or attachments that you weren't expecting and more importantly, never click or open them. Scam emails often include embedded links or attachments that look valid but are hosts for malicious websites or malware.

d. **Warnings**: warnings that your account will be closed or access limited are telltale signs of a phishing scam.

Scams

6. Tech Support Scam

The scammer claims to be from a well-known technical support company, saying there is a problem with the person's computer. This is a very common scam. They'll ask for remote access to your device or payment to "fix" non-existent problems. Sometimes they will claimg that your home computer has been hacked or is sending out viruses and will offer to help you fix the issue for a fee. Scammers are also sending out phishing emails with fake invoices claiming that your subscription to a computer antivirus support service has been renewed. They provide a phone number to call to cancel the service. Once the scammer has made contact with you, they'll request remove access to your computer where they will attempt to steal financial or personal information or they ask you to pay a fee to eliminate dangerous viruses on your computer.

- Be suspicious of unsolicited calls. Legitimate tech support companies don't make unsolicited phone calls.
- Never log into your accounts when using remote access or sharing your screen with someone.
- Run anti-virus to trace and monitor any vulnerabilities on your device.
- Do not call a number or click on a link presented in a suspicious form or contact or pop-up.
- Contact a verified company (like the maker of your device) for technical support and further information if necessary.

Scams

Grandparent Scam continued...

- Press your caller for details. If the person on the other end of the phone is explaining their story, ask them questions about their specific location or have them repeat their story. A criminal will have a hard time recalling details or coming up with them on the spot.
- Ask the caller a few personal questions that your real grandchild could answer but an imposter could not.
- Never wire money or send e-transfers under uncertain conditions.
- Never pay them with a gift card. An established business or government agency will never insist you pay them with this method.
- Don't provide your credit card number over the phone or internet unless you are sure about who you are giving it to.
- Never answer calls from numbers you do not recognize. Caller IDs can also be manipulated by scammers. Verify their identity by directly calling the number known to you.
- Never offer personal information or banking information.
- After you hang up, verify the story by calling the parents or other relatives of the "grandchild".

If you have been caught in a scam like this one, call your local police department. Your Credit Union or bank staff are aware of these kinds of scams and are trained to pay attention if a member makes an unusual transaction - for example, withdrawing more money than usual. Don't be afraid to ask for help and don't be embarrassed - let's get this fixed before it goes too far.

Scams

8. Romance Scam

- Does your new friend have an online profile? Look for inconsistencies between what they post, and what they tell you.
- If you receive a message from your friend and they use the wrong name, that may be a red flag. Many of these fraudsters are working on multiple victims at the same time.
- Scammers will claim that they live close to you but that they're working overseas. They do this so that they have numerous reasons to ask you for money. Be on your guard.
- If you receive a cheque or another form of payment from someone you've met online and they ask you to cash it and send a portion back to them - don't do it. This is another layer to the scam.

The romance scam extends to people who are just looking for a platonic relationship due to loneliness, the death of a partner, etc. It isn't always romantically driven. If you think you may be a victim of a romance scam or any other kind of fraud, it is important that you contact police immediately.

Scams

Ransomware scam continued...

- Check with your anti-virus provider - if you are familiar with data recovery, you may try to remove the malware yourself. Some anti-virus providers can detect this malware and may have instructions and software to help.
- Consult an IT security specialist - a professional may be able to help you remove the ransomware and restore your files if you have them backed up.
- Change your passwords - change all your online passwords. That can stop criminals from further accessing your accounts if they were able to access your passwords.
- Report the scam - alert your local police and the Canadian Anti-Fraud Centre.

The Canadian Anti-Fraud Centre contact information: 1-888-495-8501 or visit their website at www.antifraudcentre-centreantifraude.ca.

Scams

Fake websites continued...

Protect yourself while shopping online!

- Shop with a reputable and trustworthy retailers that provide a street address and a working phone number
- When looking for the shopping app of your favourite retailers, visit the retailer's website and look for the link to their legitimate app there - don't just search through the app store
- Look at the URL of the website to see if it starts with "https" and displays a padlock icon in the address bar. If it begins with "https" instead of "http" it means the site is secured using an SSL Certificate (the s stands for secure)
- Never respond to pop-up messages on a website or app that asks for your financial information
- Use your credit card and avoid websites and apps that request payment by wire transfer, prepaid debit or gift cards, cash only or through third parties.

Financial Abuse

Some warning signs:

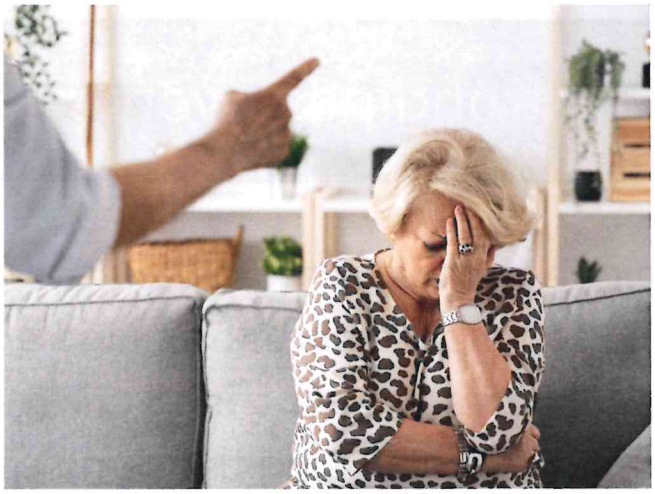
- A trusted person suggests that you make changes to important contracts - your Will, Power of Attorney, trusts, title to property, deeds or mortgages - that you do not want to make or are not in your best interest.
- You feel afraid or or pressured by a trusted person.

Examples of financial abuse

A trusted person may be a financial abuser if they:

- put pressure on your to give or lend them money, or to give them access to your financial information
- use a Power of Attorney for their own benefit
- force or trick you into signing something, including a contract, Will, letter or guarantee
- take assets or money without your permission
- misuse your bank card or credit card, or have you take out a loan to help them
- misuse joint accounts or pressure you to make your existing account a joint account
- forge your signature on cheques, including pension cheques or legal documents
- sell or transfer your property against your wishes or interests
- refuse to return borrowed money or property

Financial Abuse



Remember, financial abuse is a violation of your rights. It is not your fault, and you can get help. A list of contact information for each province is available on the CBA website at: https://cba.ca/where-to-go-for-help.

Tips to protect yourself

3 Ask for help

Never be afraid to ask for help. If you feel like something doesn't feel right, whether it be a scam of some sort, fraud or elder financial abuse, reach out to someone you trust. This could include someone at your financial institution, an RCMP officer or a trustworthy friend or family member. They will help get things sorted out and guide you in the right direction to take steps to protect yourself.

4 Take advantage of your Financial Institution's safeguards

At Stride Credit Union, we have safety measures in place to help protect our member's financial and personal information.

- Set up Two Step Verification. This is an added level of protection. This verifies you when logging in from an unknown location and also verifies certain transactions such as e-transfers, bill payments and adding payees.
- Lock'n Block. This gives MemberCard holders the ability to lock their debit card if it goes missing or is stolen. No transactions can take place while it is locked.
- Account Inactivity. Haven't logged in for awhile? After 90 days of inactivity, your account will move to an inactive state and you must call your branch to reinstate it.