Anti-Fraud and Anti-Scam Information
Compliments of

Stride
CREDIT UNION

In Partnership with

National Association of Federal Retirees
Association nationale des retraités fédéraux

Central MB 32

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**

877-228-2636 **stridecu.ca**

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

3 Shred papers with personal information

Destroy all your financial documents before putting them in the garbage or recycling. Safely shred, tear, or burn credit card, bank statements and any other documents with sensitive information on them.

4 Limit sharing of personal info online

Cyber criminals only need a small amount of your personal information to impersonate you online and commit financial crimes. Be careful what personal data you share online. Don't share your date of birth, home address, PIN or any personal or financial info that could be used to verify your identity in common account security questions. Only share necessary info privately with verified individuals with whom you have initiated contact.

5 Be careful on the phone

Never give your personal information over the phone, unless you initiated the call. Hang up on calls from phony bank employees or members of law enforcement who say they need you to withdraw your money from the bank to help with their investigation.

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.

Fraud Prevention Checklist

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

9 Don’t respond to suspicious emails, calls or texts

Your financial institution will never send you an email asking you to disclose personal information like your credit card number, online banking password or your mother’s maiden name. They will also never contact you to ask that you share a one time passcode that you previously requested as part of an account verification process.

It is important that you protect yourself and your personal information, including your finances, from online and telephone fraud. If it seems to good to be true, it probably is. And alternatively, if it sounds questionable, it probably is. Don’t be afraid to ask for help.

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

2. Lottery or Prize Scams

Victims are told they've won a large sum of money or a prize but they must pay a fee or provide personal information to claim it. Reputable companies will not award you a prize in exchange for payment or information. Hang up on these calls.

3. Email Imposter Scams

Scammers send emails posing as companies and include PDF attachments stating that your account will be suspended or put on hold. These attachments prompt you to click on a fraudulent link to "update your account". These links lure you to provide personal information such as payment information or account login credentials. Do not click on them.

4. CRA Impersonation Scam

Scammers pretend to be Canada Revenue Agency (CRA) agents, alleging that you owe back taxes or owe money to the government, and threatening legal action or arrest unless the money is paid back immediately. Call the CRA yourself at 800-959-8281 to check on your account.

5. Social Insurance Scam

Callers pretend to be a government official with access to Social Insurance numbers and information, and state there is an issue with the person's SIN account. This can escalate to them threatening legal action while demanding personal information.

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

7. Grandparent Scam

It typically involves a fraudster calling and pretending to be a grandchild or another family member in a desperate situation. The call will often start with “Grandma? Do you know who this is?” to get the name of a grandchild, assume their identity and gain credibility with you.

The caller will claim to have an urgent need for money, such as for medical bills, bail or travel expenses. They’ll say they were in an accident, under arrest, or in jail in a city or abroad.

To make their story sound more credible, they may put someone else on the phone to impersonate a police officer, government official or a lawyer. Scammers often rely on emotional and manipulative tactics to convince you to send them money without double-checking if the story is true.

The caller will ask you to withdraw funds from your bank account and send the money through a wire transfer service. In some cases, the scammers may also arrange for someone to impersonate a courier or a government official to collect the money from your home.

How to protect yourself from the Grandparent scam:

- Never offer information to the caller. If they prompt you with a question like “Do you know who this is?” simply say no and have them tell you.

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

Romance scams are among the most common scams according to the Canadian Anti-Fraud Centre. They cost Canadians more than $59 million in losses in 2022, compared to approximately $28 million in 2020.

Typically the victim and criminal will meet through a social media or dating platform. The criminal will then try to develop a relationship with their victim, sometimes spending several months making the victim feel they are in a romantic relationship.

Often the scammer will say that they are in another city or country and that they eventually want to meet the victim in person. The criminal might note that they can't afford to travel and will seek assistance from the victim in covering travel costs.

Another example of this scam includes the criminal noting that there's an emergency, like a sick family member, that they need financial help from the victim to visit said family member.

How to protect yourself from the Romance scam:

- Check other platforms for your new friend's profile. Scammers will often not use other platforms or they will have newly activated accounts with very little information to try and mitigate suspicions.
- If your love interest asks you to send money, end communication and block them.
- Scammers tend to try and develop a quick relationship with you so be on your guard when someone professes their love to you shortly after meeting.

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

9. Ransomware Scam

Ransomware is a type of malware (malicious software). Once malware is on your computer, it can lie dormant until the hacker takes control and encrypts your files. When files are encrypted, it is very much like the files are locked, and scammers will demand a ransom payment to decrypt and unlock the files. These threats are meant to scare and intimidate you. Paying a ransom does NOT guarantee they will decrypt your files or that they won't sell or leak the information online.

To avoid downloading ransomware, install reputable and up-to-date anti-virus and anti-malware protection software on all your devices and keep on top of updates.

Backup your files frequently to an external source, such as an external drive or cloud-based storage that is not linked to your computer. If they are linked, your backed-up data could be encrypted too.

Be careful not to click on links or open attachments from unknown senders.

What to do if you are a victim:

- Don't pay the ransom - it can open you to further and repeat attacks. Criminals use your willingness to pay the ransom to demand more money.
- Disconnect all devices - ransomware can spread through devices and networks.

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

10. Fake Websites and Apps

Scammers create online shopping websites and apps that have a similar look and feel to genuine retailers under an intentionally misleading, legitimate-sounding name. These websites and apps are often just a front to steal your credit card details and sensitive personal information.

Signs of a fake shopping website:

- the site looks poorly designed, unprofessional and has broken links and spelling errors
- you can't find an address or phone number for the business
- sales, return and privacy policies are hard to find or unclear
- the back button is disabled
- you're asked for credit card information anytime other than when you are making a purchase

Signs of a fake app:

- the name of the app publisher (typically displayed under the app's name) is close to the retail app you're looking for but isn't quite right
- the app has a poorly written description or doesn't have any user feedback
- the app requires excessive number of permissions for installation
- the app has a lot of pop up ads or you are constantly being asked for personal information

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

Financial Abuse occurs when someone tries to take or control what belongs to you for their own benefit, not yours. This can include your money, your property or your personal information. Financial abuse is unethical and in many cases illegal.

Financial abusers can be a trusted person in your life: a spouse, adult child, grandchild or other family member, caregiver, friend or neighbour.

Some warning signs:

- A trusted person takes an undue interest or involvement in your financial matters.
- Your statements show account withdrawals or transfers you did not make.
- A trusted person suggests you have your bank statements sent to them.
- You start failing to meet your financial obligations, when you've never had problems before.

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

How can you prevent it?

- If you are able, do financial transactions yourself. Take advantage of online banking.
- When planning for your possible inability to manage your finances yourself, allowing a trusted person (or persons) to assist with your financial affairs can be helpful, but you must select your trusted person carefully
- Powers of Attorney, joint accounts or other arrangements may be useful, but you must be careful. It is generally safer to use a Power of Attorney - which allows a trusted person to act and make decisions for you and obligates them to act in your interest - instead of a joint account, which makes the trusted person a joint owner of your money and investments.
- You can say “NO” when someone pressures you for money or to buy something - even family members.
- Make sure you understand every document you sign -do not give anyone your bank card or PIN.
- Set up automated deposits and payments. You can have your income deposited directly into your bank account and have your money sent directly to your necessary bill payments.

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

1 Choose strong passwords

Choose strong, unique passwords for your sensitive online accounts. Using the same password for multiple accounts puts you at risk when a security breach happens as criminals may try to get into all of your online accounts using the same password. Use a variety of lowercase and uppercase letters, numbers and symbols where allowed.
Bad actors use a technique called credential stuffing to gain access to multiple of your accounts. They use automated tools to “stuff” your credentials into as many login pages as possible until a matcf is found. If you’re using the same password for many different websites, it’s more likely that fraudsters will be succesful in accessing your accounts.

2 Have a code word with family members

To help prevent scams such as the grandparent scam, pre-determine a “safe word” with select family members. You can reference a past memory or an event that happened, just ensure it’s not too generic or easy to guess. Saying something like “What happened on our road trip to Expo 86?” and the answer could be “Our suitcase fell off the roof of the car!” instead of “what is your favourite colour?” as this is fairly easy to guess.

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.

Resources

CBA: https://cba.ca/where-to-go-for-help

Financial Consumer Agency of Canada: www.canada.ca/en/services/finance/fraud.html

The Canadian Anti-Fraud Centre: 1-888-495-8501 or www.antifraudcentre-centreantifraude.ca

We hope this information has helped. It is so important to be aware and protect yourself. And never be afraid to ask for help.