

Protect Yourself

Be Fraud Smart



Identity theft and financial scams are growing rapidly.

Anyone can be a victim of financial fraud. Every year criminals use the latest technology, trends, and social media applications to defraud more Canadians. Protect yourself and your family by being aware and proactive.

Here are a few simple steps you can take to protect yourself by improving the security of your personal, confidential information. Your credit union is also taking steps to ensure your identity and financial information is protected.

We also provide a list of organizations you can turn to for more information, or for help if you become a victim of fraud.



What is Identity Theft?

Identity theft occurs when someone obtains your personal information such as: your driver's license, date of birth, health card number, Social Insurance Number (SIN), online passwords, credit card number, or debit card Personal Identification Number (PIN).

With just a few pieces of personal information fraudsters can begin to make financial transactions in your name. They might take money from your accounts, get a new credit card, take out a car loan, or even put a mortgage on your home. Often people don't realize what's happened until it's too late. You can lose money and your credit rating will be affected.

Your Credit Union helps protect you. Credit unions have processes and defences in place to detect and investigate irregular account activity.



Protect your identity

- Don't carry your SIN card or birth certificate with you. Keep them in a safe place
- Check your credit report at least once a year to spot any credit inquiries or charges you haven't authorized
- Delete any email or text message that asks for personal or account information
- Be careful what you share on social media. Fraudsters can use your birth date and other personal information to set up fraudulent accounts in your name
- Remember to shred mail with your personal address on it

We have your back!



Credit unions follow the Canadian Code of Practice for Consumer Debit Card Services which protects card holders from losses if their card is used fraudulently. You can read the code on the [Financial Consumer Agency of Canada's website](#).

If you lose your debit or credit card, or suspect someone has created a duplicate card, report this to your credit union immediately. Read your cardholder agreement for further details on your liability.



Protect your payment cards

- When you receive a new debit or credit card, sign it immediately
- Don't choose an obvious PIN, such as your phone number or birth date
- Only carry cards you use the most often. Leave others safely at home
- Check your accounts frequently and review your monthly statements. Notify your credit union if you see any unfamiliar transactions
- Notify your credit union if you are unable to retrieve your card from an ATM.

Be PIN smart

- Change your PIN at least twice a year
- Keep your card in sight when conducting a transaction
- Shield your PIN with your hand
- Memorize your PIN
- Change your PIN after traveling
- Use tap whenever possible
- Never share your PIN



WATCH FOR SKIMMING DEVICES

Card skimming occurs when criminals attach a device to a card reader so they can collect your data. If the ATM or point-of-sale (POS) device you are using looks like it has been tampered with, don't insert your card, or enter your pin



Stay safe online

Being proactive is the best line of defense to protect your online identity. Here are a few best practices to stay safe online.

- Change your passwords frequently
- Don't use public Wi-Fi to access mobile banking
- Never accept an e-transfer from someone you do not know
- Install anti-virus software and anti-spyware
- Use a firewall
- Never click on an ad or pop-up window that says "Agree," "OK", or "I Accept"

If an email looks suspicious, don't open it.

- Carefully review the information included in the email
- Check the branding and spelling for errors
- Contact the company directly to verify they sent an email
- Your credit union will never email you to confirm your personal information

Report phishing attempts or malware infection to the federal Spam Report Centre at: spam@fightspam.gc.ca



Bank online with confidence

Your credit union uses a variety of security measures to protect your financial information when you are banking online. Your information is encrypted so that it cannot be read or changed while being transmitted.

Common online scams

Anyone can be a victim of fraud. Here are a few common online scams to watch out for:

- **Email Scams**
- **Phishing**
- **CRA Scams**
- **Cyber Scams (ex. Covid-19 scams)**

WHAT IS Phishing

Criminals attempt to lure you with **emails**, often impersonating companies, banks, or government agencies. They may ask you to confirm your account information or log-in so they can **capture your personal information.**





For More Information

Canadian Anti-Fraud Centre
1.888.495.8501
antifraudcentre.ca

Competition Bureau of Canada
1.800.348.5358
competitionbureau.gc.ca

The Little Black Book of Scams
competitionbureau.gc.ca/blackbook

Credit Bureaus

To order your credit report or report identity theft:

Equifax Canada
1.800.465.7166

TransUnion
1.800.663.9980

CCUA
Canadian Credit Union Association

ACCF
Association canadienne des
coopératives financières

ccua.com

The information in this publication is summary in nature and does not constitute legal or financial advice. This brochure is provided by your local credit union and is designed to inform you about financial products. For more information about these or any other financial product, please contact our knowledgeable staff.



GLOBE IN HANDS Design is a trademark owned by the World Council of Credit Unions, used under license.
© 2022 Canadian Credit Union Association. All rights reserved.