

What is identity theft?

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

With a few pieces of personal information they can begin to make financial transactions in your name. They might open a new credit card account, take out a car loan or mortgage your home. You probably won't realize what has happened until it's too late and your credit rating is affected.

YOUR CREDIT UNION HELPS PROTECT YOU

Credit unions work actively to detect and investigate irregular account activity. Your member debit and credit cards contain the minimum information needed to securely make a transaction.

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 look for any credit inquiries or changes you have not authorized.
- Be suspicious of any **email** that asks for personal or account information.
- Don't overshare on **social media**. Scammers can use your birth date and other personal information to steal your identity.

Protect your payment cards

Canadians are one of the biggest users of debit cards, credit cards and ATMs in the world. And while INTERAC® services are among the most secure in the world, debit card fraud does occur.

Take these steps to protect yourself:

- When you receive a new debit or credit card, sign it right away.
- Avoid choosing an obvious PIN, such as your phone number or date of birth.
- Carry only the cards you use most often and leave any others at home in a safe place.
- Always check your monthly statements and 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 or if someone tries to distract you while using one.
- Be PIN smart.
 - Change your PIN at least twice a year
 - Shield your PIN with your hand, body or a piece of paper
 - Keep your card insight when conducting a transaction
 - Memorize your PIN
 - Don't disclose your PIN to anyone

WATCH FOR SKIMMING DEVICES

Card skimming occurs when a criminal attaches a device to a credit or debit card reader to collect data from the card. If the ATM or point of sale device looks like it's been tampered with don't insert your card or enter your PIN.



YOUR CREDIT UNION HAS YOUR BACK

Canadian credit unions adhere to the *Canadian Code of Practice for Consumer Debit Card Services* which protects card holders from losses should their card be used fraudulently. For more information go to: tinyurl.com/Canadian-Code

If you lose your debit card or credit card, or you suspect someone has created a duplicate card you should let your credit union know immediately. Refer to your cardholder agreement for further details on liability.

- Consider reporting phishing to the Government of Canada Spam Reporting Centre at spam@fightspam.gc.ca. Report additional specifics such as resulting malware infection online at fightspam.gc.ca/src
- Never click on a banner ad or pop-up window that says **Agree, OK** or **I accept**.

BANK ONLINE WITH CONFIDENCE

Your credit union uses a variety of security measures to protect your financial information when banking online.

Special encryption software scrambles your information to make sure it cannot be read or changed while being transmitted.

Stay safe online

Life is just a little easier when you use your computer and mobile devices to get things done online. But there are a few simple and sensible things you should do to protect yourself against risks.

- Change your passwords regularly.
- Don't use the same password for everything.
- Install anti-virus software to protect your data from viruses and malware. Apply security updates as soon as you receive them.
- Install anti-spyware software to keep others from gathering information about your online habits or making unauthorized changes to your computer.
- Implement a firewall to prevent unauthorized access.
- If an email looks suspicious, stop before you click.
 - Look carefully at what it claims and think about whether it makes sense.
 - Check the branding, language and spelling to judge whether it seems legitimate.
 - Call the company and make sure the email came from them.

Common online scams



- **Email scams**
- **Phishing**
- **Brand spoofing**
 - emails with fraudulent sender addresses

WHAT IS PHISHING?

Cybercriminals have become expert at luring people in with their emails, often impersonating well-known companies, banks and even government agencies. They may ask you to confirm your account information or log in to your account. If you take the bait, they've stolen your personal information.



What to do if it happens to you

Acting quickly can minimize the damage and help prevent further fraud or theft.

- 1** Notify your credit union immediately if you suspect fraud or identity theft. They can provide advice on how to limit access to your credit card or financial accounts and investments.
- 2** Call the police and file a report. Keep a copy of the report for your records.
- 3** Change your PIN and passwords immediately.

Keep a list of the people you speak to when reporting a fraud, recording all dates, names, phone numbers and what was said.



Where to get 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

Government of Canada (Public Safety Canada) resources on Identity Theft
publicsafety.gc.ca

Major Credit Bureaus

Equifax Canada
To order your credit report or to report identify theft:
1-800-465-7166
consumer.equifax.ca

TransUnion
1-800-663-9980
transunion.ca



† Trade-mark of Interac Inc. Used under license.

©* All trade-marks are owned by their respective owners. CCUA's use of the third party marks is not intended to indicate sponsorship or affiliation with the owner of the marks.

This booklet is provided to you courtesy of your credit union.

This publication is provided for informational purposes only. The information in this publication is summary in nature and does not constitute legal or business advice. Canadian Credit Union Association (CCUA) hereby disclaims all warranties as to the accuracy of any of the information in this publication and disclaims all liability for any actions taken in reliance on this information. Any copying, redistribution or republication of this publication, or its content, is strictly prohibited.