Simple habits that make a big difference

- **Guard your SIN:** Only share it when legally required. Keep your card at home, not in your wallet.
- **Use strong passwords:** Mix letters, numbers, and symbols. Do not use your birthday or name. Write it down and keep it somewhere safe at home.
- **Check your credit report constantly.** You are entitled to a free report from Equifax and you can get the TransUnion credit report from your choice of financial institution.
- **Never share personal details with someone who contacted you first, by phone, text, or email.**
- **Talk about it:** Having community conversations in your own language, with people you trust, is one of the most effective ways to stay informed and protect yourself.

What to do in case of suspected fraud

Step 1: Stop communication

Step 2: Do not click/respond

Step 3: Verify using the official number

Step 4: Report if needed

Step 5: Trust your gut, if it feels wrong, hurried , panicked and unsure, it probably is.

If your information has been stolen, act fast

- Contact your bank immediately
- Place a fraud alert on your credit file. Equifax: 1-800-465-7166 TransUnion: 1-800-663-9980
- Contact the CRA if your SIN may have been misused. 1-800-959-8281
- Report to the Canadian Anti-Fraud Centre.
  Phone: 1-888-495-8501
  reportcyberandfraud.canada.ca
- Talk to someone in your community.

For more information, connect with us online:

(825) 333 3900
operations@thefei.ca

The financial literacy initiative
thefei1
www.thefei.ca

The SENIOR SHIELD

Preventing Financial Exploitation for Seniors

Protecting Your Personal Information

- Recognize the signs
- Protect your finances
- Empower your decisions
- Support your community

Funded by the Government of Canada's New Horizons for Seniors Program | Canada

THE FINANCIAL Empowerment INITIATIVE

This guide helps you, as seniors to:

- Understand the importance of protecting your personal information
- Recognize what criminals want from you
- Understand how they steal your information
- Know how you can protect yourself and who to report to in case you need help

Your Information is a target

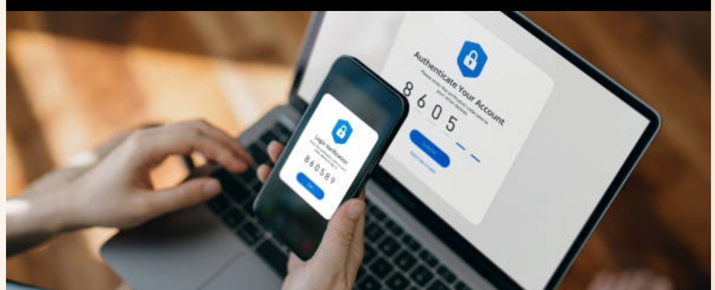
Identity fraud is the illegal use of someone else's personal information (like a name, ID number, or banking details) without their permission to commit a crime.

When a criminal gets your personal information, they can open bank accounts in your name, steal your tax refund, apply for loans, and drain your savings, sometimes without you knowing for months.

The good news is that you can protect yourself from these criminals.

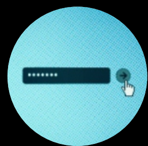
What Criminals Want From You

- **Your Social Insurance Number (SIN):** This can be used to steal your identity, file a fake tax return, or claim your government benefits.
- **Your banking details:** Account numbers, PINs, and passwords give direct access to your money.
- **Your passwords and email:** Once inside your email, a criminal can reset passwords on every account you own.
- **Your date of birth and address:** Combined with your name, this is enough to impersonate you.



Banks and Financial Institutions will never ask you for:

PIN



Full password

OTP codes

SIN over the phone/ email in most cases

Common ways your information gets stolen

1. Phishing emails and texts: A message looks like it is from your bank or the customer care officer, it asks you to click a link and enter your details. That link leads to a fake website built to steal your information.
   Tip: Never click links in emails. Go directly to your bank's website.

2. Phone calls: A caller claims to be from the government or your bank and asks you to confirm your SIN or account number.
   Tip: Hang up, visit the bank directly, or call an approved customer care number to make sure it was from your bank.

3. Mail theft: Bank statements, tax slips, and government letters left in an unlocked mailbox are an easy target.
   Tip: Collect your mail promptly and shred documents before disposing of them.