# CANADIAN ANTI-FRAUD CENTRE
# CENTRE ANTIFRAUDE DU CANADA

## Cyber Month Week 3: Protecting Your Personal Information

2026-10-20

FRAUD: RECOGNIZE, REJECT, REPORT IT  LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

The Canadian Anti-Fraud Centre (CAFC) wants to warn Canadians about the importance of protecting their personal and financial information. Fraudsters can collect information from many sources, including social media, fraudulent emails and text messages, online forms and surveys, data breaches and information that is publicly available. Details such as your name, date of birth, phone number, employer, family members, travel plans or social media activity may not seem sensitive on their own. However, when these details are combined, they can help fraudsters build a more complete picture of you.

Fraudsters can use the information they collect in different ways. Personal details can help them create more convincing stories, impersonate you or someone you know, or make an unexpected contact appear legitimate. More sensitive information, such as government-issued identification, Social Insurance Numbers (SINs), banking information and credit card information, can be used to commit identity fraud and other financial crimes. Information collected today may also be kept and combined with information obtained from other sources later. A fraudster does not always need one highly sensitive piece of information. In many cases, several smaller details can be just as useful when put together.

**Warning signs**

*Be cautious if:*

- You receive an unexpected request to provide or confirm personal or financial information.
- Someone asks you to provide a copy or photo of government-issued identification without a clear reason.
- An unsolicited email, text message or social media message directs you to a website or form asking for personal information.
- Someone uses personal details about you, your workplace or your family to gain your trust or make their story more convincing.
- You are pressured to provide personal or financial information immediately.
- You receive bills, statements or correspondence for accounts or services you don't recognize.
- You notice transactions, credit applications or other activity that you did not authorize.

**How to protect yourself**

- Think before you share. Consider what information you are making public and who can see it.
- Review your social media privacy settings and limit the amount of personal information available publicly.
- Be cautious about sharing your date of birth, travel plans, workplace, family information and other personal details online.

- Protect sensitive information, including your SIN, banking and credit card information and government-issued identification.
- Before providing personal information, ask who is requesting it, why it is needed and whether the request was expected.
- Don't provide personal or financial information in response to an unsolicited call, email, text message or social media message.
- Independently verify unexpected requests for information using contact information you trust.
- Avoid clicking unsolicited links or completing unexpected online forms that request personal information.
- Be cautious with surveys, contests and promotions that request more personal information than necessary.
- Regularly review your financial statements and credit report for activity you don't recognize.

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police. Also visit the Report Cybercrime and Fraud website to report online or by phone at 1-888-495-8501.