CANADIAN ANTI-FRAUD CENTRE
CENTRE ANTIFRAUDE DU CANADA

Cyber Month Week 1: Spotting Fraud in a Changing Digital Landscape

2026-10-05

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

Cyber Month is an opportunity to help Canadians learn how to recognize fraud and cyber threats and take simple steps to protect themselves. The 2026 Cyber Month theme, "**Your Best Defence Is You,**" highlights the important role we all play in protecting our personal, financial and account information.

Fraudsters continue to adapt their methods to new technology, current events and the ways Canadians communicate. They may contact you by phone, text message, email, social media or through a website. They may pretend to be a family member, financial institution, government agency, police service, business or another organization you know and trust.

Fraud can be difficult to recognize based on appearance alone. A message may be well written, a website may look professional, and a phone number may appear familiar. These details can make a request seem legitimate, but they do not prove that the person contacting you is who they claim to be.

Social engineering: influencing your decisions

Social engineering is when fraudsters use manipulation to influence your decisions or convince you to take an action. Fraudsters often rely on urgency, fear, authority, excitement and trust to get you to react before you have time to stop and think.

They may tell you that your bank account has been compromised, that you owe money, that a loved one is in trouble or that you must act immediately to avoid consequences. They may create excitement around a prize, investment or opportunity. In other cases, fraudsters may take time to build a relationship and gain your trust before asking for money or personal information.

The story may change, but the goal is often the same: to influence your emotions and get you to act before you verify the situation.

Artificial Intelligence (AI) can make fraud more convincing

Artificial intelligence is changing how convincing fraudulent content can appear. Fraudsters can use AI to create realistic messages, images, videos and voices. They can also combine these tools with information available online to make their approach more personal and believable.

For example, AI can be used to create a message that sounds natural and professional or imitate the voice of someone you know. Images and videos can also be created or altered to support a false story. This means some of the clues traditionally associated with fraud, such as spelling mistakes, unusual wording or poor-quality images, may not always be present.

A message, image, video or voice that appears real is not proof that it is real.

Warning signs

Be cautious if:

- You are pressured to act immediately or threatened with consequences if you don't.
- You are told to keep the situation secret or not speak with family, friends, your financial institution or police.
- You receive an unexpected request for money, personal information or financial information.
- You are asked to provide passwords, PINs or one-time verification codes.
- You are directed to click a link, open an attachment, download software or visit an unfamiliar website.
- Someone you know suddenly contacts you from a new phone number or account and asks for money.
- You receive an unexpected investment, prize, refund or financial opportunity that seems too good to be true.
- Something about the request doesn't seem right, even though the message or person appears convincing.

How to protect yourself

- Slow down. Don't let urgency, fear or excitement pressure you into making a quick decision.
- Verify unexpected requests. Use contact information you find independently, not information provided in the message.
- If someone claims to be a family member or friend, contact them directly using a phone number you already know.
- Don't rely on caller ID. The name or number displayed on your phone can be manipulated.
- Never provide passwords, PINs or one-time verification codes to an unsolicited contact.
- Avoid clicking links or opening attachments in unexpected messages. Go directly to the organization's official website or app.
- Be cautious about the information you share online. Fraudsters can use publicly available information to make their approach more believable.
- Before sending money or sharing sensitive information, talk to someone you trust.

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.