

Artificial Intelligence's (AI's) Emerging Role in Scams and Frauds



About this guide

Artificial Intelligence (AI) refers to technology that can create text, images, audio, and video. AI can also analyze information, answer questions, and generate content based on user instructions. As AI tools become more accessible, scammers are using them to make scams appear more convincing. This guide highlights common AI-enabled scams and ways to reduce the risks it can present.

Table of contents

How is AI Being Used in Scams and Frauds?	03
How to Spot an AI-Enabled Scam	05
Ways to support a client who has been a victim	06
Additional Resources and Supports	09

How is AI Being Used in Scams and Frauds?



AI tools are becoming increasingly accessible, and can now generate text, images, videos, and other types of media. Scammers can use these tools to imitate trusted individuals, organizations, or official communications, making scams more difficult to identify.

Newcomers are especially at risk for these AI-enhanced schemes due to things such as possible language barriers, an unfamiliarity with Canada’s media and reputable sources, and an unfamiliarity with government processes in Canada.

The following table describes four of the most common AI-based scams newcomers risk encountering.

	Deepfake Videos	AI Voice Cloning	AI-generated Images	AI-generated Messages
What it is	Videos that feature an imitation of an existing person through the use of AI-generated video and audio.	A copy of a person’s voice created using AI.	Images of people or scenarios created using AI.	Text generated using AI.

How is AI Being Used in Scams and Frauds?

	Deepfake Videos	AI Voice Cloning	AI-generated Images	AI-generated Messages
How scammers use it	Gives victims the impression that the scammers' requests are coming from a legitimate source or a trusted family member/friend. Deepfake videos can also be used to imitate the victim themselves for identity theft schemes.	Similarity of a cloned voice to the real voice of a family member, friend, or official could deceive the victim and make it easier to gain their trust. Scammers can combine this tactic with an urgent request to make it seem like a trusted person is asking for something such as money or bank account details.	AI-generated images can be used to increase the appearance of legitimacy in a scam/fraud scheme. AI-generated images can be used across many types of scams and frauds such as romance scams, identity theft, and celebrity scam endorsements.	AI-generated text can facilitate scammers' ability to run email and text-message scams. AI tools that generate text based off shorter prompts are easy to access, and their output can sometimes appear identical to an official source.
How it can affect newcomers	Newcomers mainly risk encountering these videos on social media or on scam websites. While non-newcomers are already regularly susceptible to these types of scams, newcomers who may be unfamiliar with Canadian media and trusted sources are often more vulnerable.	AI voice cloning can reach newcomers through phone call-based scams/frauds. These could be posing as a family member or a governmental agency trying to gain the victim's financial or personal information.	Just like Canadian citizens, newcomers can be deceived by scams employing AI images due to the legitimacy they can claim to hold.	AI-generated text can be used to make existing text-based scams that are aimed at newcomers even more deceptive. If a newcomer receives a message claiming to be the CRA or their bank, for example, AI-generated text can make the scam seem completely legitimate.

How to Spot an AI-Enabled Scam



**An example of an AI-generated video with noticeably unreadable text present.*

'Other völli & villi yout þou eisseu de tre sureat, mol ædo y ss ups mnotnad of the ttle doo, LEONORA CARRINGTON.'

Be cautious of unexpected messages, calls, or videos that create urgency, request personal information, or make offers that seem too good to be true. Look for these warning signs:

- **Videos:** AI-generated deepfake videos often showcase inconsistencies that would not be present in a real video filmed with a camera, such as abnormal body movements, lighting/shadow issues or unreadable text.
- **Audio:** Deepfake audio can be spotted when speech patterns sound unnatural, and the content is overly formal.
- **Images:** AI-generated images can show visual inconsistencies including missing body parts, lighting issues, and an artificial smoothness or sharpness to the subjects of the image.
- **Written Messages:** While AI-generated text can be harder to detect, text that is too perfectly or formally written could be a warning sign of AI use.

Learn More About AI Scams

[Government of Canada – Watch out for AI-generated government impersonators](#)

Provides information on the most common ways fraudsters use AI to impersonate government officials

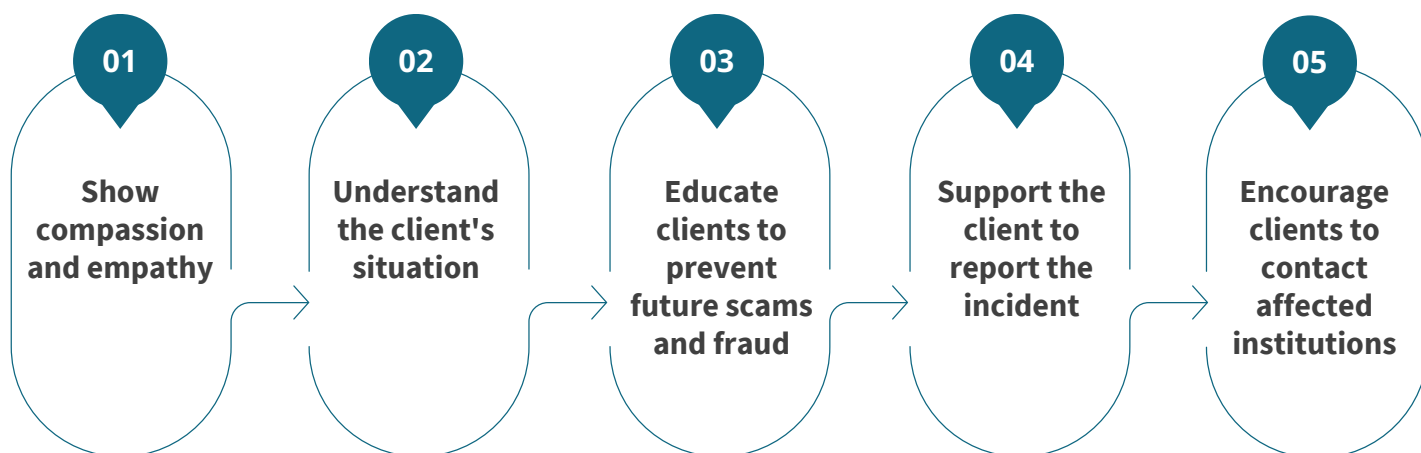
[RCMP – Don't take the bait: spotting AI scams before they spot you](#)

Provides information and links to further information on AI scams

[The rise of AI: Fraud in the digital age](#)

Provides information on the growing use of AI in scams and how to identify potential fraud.

Ways to support a client who has been a victim



01 Show compassion and empathy

Let them know that scams and fraud can happen to anyone, anywhere, at any time. Encourage them to acknowledge any feelings and practice self-care.

02 Understand the client's situation

Understand the client's situation and encourage them to collect and organize all information related to the incident, including:

- Details about what happened
- Supporting evidence. Advise clients not to delete any messages, emails, or other evidence related to the incident.
- Information that might reveal a suspect's identity (if available)

03 Educate clients to prevent future scams and fraud

Newcomers should be advised to limit the personal information that they post publicly online, as well as videos, audio clips, and images of themselves. Personal information can be used by scammers to learn more about victims' personal lives, while videos, audio, and photos can be used by scammers to impersonate victims' identities or those of their family and friends through AI.

Deciding on a "family password" with family members can help in verifying a caller's identity.

Settlement workers should emphasize the importance of waiting before acting on a possible scam post or message. Newcomers should avoid sharing personal/financial information with strangers unless their identity is confirmed. If a newcomer is unsure of the message, they should research the official website of the organization that the message claims to come from. There, they can confirm if official email addresses, names, and phone numbers align with the message's sender/author.

Ways to support a client who has been a victim

04 Support the client to report the incident

Clients affected by AI-based scams or frauds should be encouraged to report the incident to both:

Their local police

Particularly if:

- Money was lost
- Personal information was compromised
- Identity theft is suspected
- Threats or intimidation occurred

Let clients know that a police report may be required by banks or other organizations during their investigation or recovery process.

Emergency Situations: If a scam or fraud involves immediate danger or a crime in progress, call 911 for urgent police assistance.

Non-Emergency Situations: For scams and frauds that are not life-threatening, clients can contact their [Municipal police department](#) or [RCMP detachment](#).

Online reporting is available for minor impact scams and frauds. Follow this [RCMP Online Crime Reporting website](#)

The National Cybercrime Coordination Centre and the Canadian Anti-Fraud Centre

Use their [Online Reporting System](#) or report by phone at 1-888-495-8501.

They collect information on all types of fraud and can provide guidance on the next steps.

Witnesses can report as well. It is important to report even if no harm was done, or the client decides not to do it.

Reporting helps law enforcement; information could link several crimes together and/or help progress or complete an investigation.

Reports can be done anonymously.

Ways to support a client who has been a victim

05 Encourage clients to contact affected institutions

Encourage clients to contact any institution whose information may have been compromised to reduce the risk of further financial loss or identity theft.

Financial institutions

If they shared financial information, passwords, or transferred money, they should contact their bank immediately. Financial institutions may be able to:

- Freeze or secure affected accounts
- Stop or reverse certain transactions
- Monitor accounts for suspicious activity

Government institutions

If government-issued documents or personal information were shared, lost, or stolen, clients should contact the appropriate organization as soon as possible. Depending on the situation, this may include:

- Canada Revenue Agency (CRA) if tax-related information was compromised
- Immigration, Refugees and Citizenship Canada (IRCC) if immigration documents, permits, passports, or application information may have been misused
- Service Canada at 1-866-274-6627 if the newcomer suspects or knows that their Social Insurance Number is being used by anyone else.

If personal information has been compromised, encourage clients to:

- Place a fraud alert on their credit file. A fraud alert can help prevent criminals from opening credit accounts or obtaining loans using stolen personal information. Contact Canada's two national credit bureaus: [Equifax Canada](#) and [TransUnion Canada](#).
- Request a free copy of their credit report. This is a way to monitor unauthorized accounts or suspicious activity. Order a free credit report through the [Financial Consumer Agency of Canada](#).

Additional resources and supports to share with newcomers

- [VictimLinkBC](#): Call 1-800-563-0808 if a client is experiencing significant emotional distress following a scam or fraud. This free and confidential service is available 24/7 and provides crisis support, information, and referrals to victims of crime.
- [A Fraud Prevention Toolkit for Newcomers](#): Developed by the Canadian Bankers Association and Get Cyber Safe, this resource helps newcomers recognize common scams, protect personal information, and develop safe online and banking practices.
- [WelcomeBC - Fraud Awareness](#): This website provides an overview of many types of immigration fraud and how to report it.

Funded by / Financé par:
