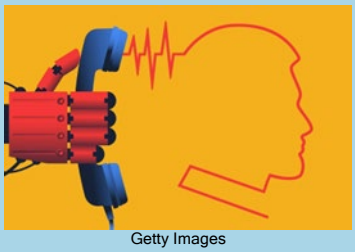
Scam Sense

Helping you to spot the fakes and stay safe - January 2026

DEEPFAKE



Getty Images

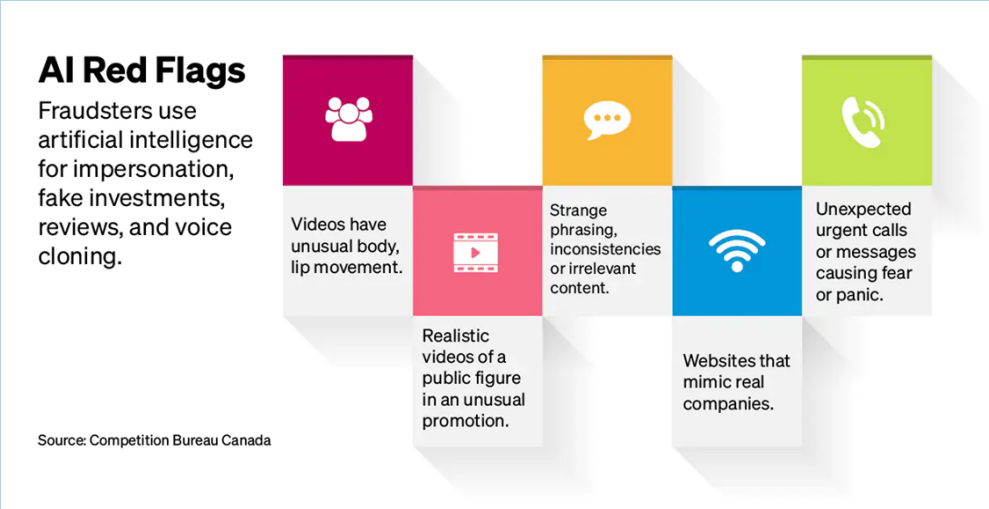
What Are Deepfakes?

Deepfakes are synthetic media—videos, images, or audio—created using artificial intelligence to mimic real people or events. These hyper-realistic fakes can be used to impersonate individuals, spread misinformation, or manipulate public perception. The term “deepfake” combines “deep learning” with “fake,” pointing to the machine learning techniques behind their creation. Machine learning focuses on creating systems that can learn from data and improve performance over time without being explicitly programmed.

How to Spot a Deepfake

While visual detection is becoming harder due to advances in AI, here are some signs to watch for:

- Unnatural blinking or eye movement
- Inconsistent lighting or shadows
- Lip-sync mismatches
- Lack of throat movement during speech
- Odd skin tones or facial distortions
- Body movements inconsistent with words



✅ AI Voice Cloning

🔍 How It Works

1. **Data Collection**: A sample of the target voice (sometimes just a few seconds) is recorded.
2. **Model Training**: Neural networks (often based on deep learning) learn the unique characteristics of the voice.
3. **Speech Synthesis**: Text-to-speech (TTS) engines generate spoken words in the cloned voice.

⚠️ Risks & Concerns

- **Fraud & Scams**: Criminals use cloned voices for impersonation in financial scams (e.g., calling relatives or employees).
- **Privacy Issues**: Unauthorized cloning of voices without consent.
- **Misinformation**: Fake audio clips can spread disinformation.

🛡️ Protection Tips

- Be cautious with voice samples shared online.
- Use multi-factor authentication for sensitive transactions.
- Verify suspicious calls through secondary channels (e.g., call back on official numbers, set up “code words” with friends and family.)

Signs of a Scam

Although there is a long list of different scams that target Edmontonians every day, there are commonalities between the scams. We've compiled a list of common red flags and signs that you may talking to a scammer.

Remember: scammers prey on emotions, whether that's fear, love, panic, or guilt. Take a step back from what they are telling you and think about the legitimacy of the situation. Pick up the phone and talk to someone you trust; family, friends, or us (780-423-4567).

When a scammer calls you and is:

- Threatening you with deportation, arrest, fines, etc.
- Requesting payment in unusual forms, like gift cards, Bitcoin, money orders, or commercial wire service transfer.
- Telling you to lie to your family, store clerks, bank employees, and police about what you're doing.
- Telling you not to talk to anyone about what you're doing.
- Telling you to pay them in order to get a job, receive a prize, get your money back, etc.
- Asking for personal information, your SIN number, and/or financial information.
- Leaving an alarming message, requesting you to dial a number to proceed or to call another number provided. These calls are being made to hundreds of thousands of people with hopes a few will comply with the request.
- Sending you money (e-cheque, e-transfer, or money transfer) with instructions to send back all or a portion in Bitcoin, gift cards, or any form of currency back.
- Pretending to be your grandchild or other family member and claims to be in trouble and asks for help. The scammer may try to convince you that your family member was in a car accident or had been arrested. You may be asked to wire money right away, without telling anyone

Beware of the Funds Recovered Scam

If you have been a victim of a scam, you may also be targeted for a **Funds Recovered Scam.** Scammers will claim to be a legitimate company to help you recover the funds you lost. They may even claim to be working with the local police service.

Protect Yourself:

- If they promise to recover the money, it's a scam as there is never a guarantee.
- If they are asking for any fees upfront, it's a scam.
- Verify the company, website, and email address.
- Never give your banking or credit card information for a request you weren't expecting.
- Police do not inform individuals of investigations over email.

💔 What is a Romance Scam

A romance scam involves a fraudster creating a fake online identity to build a romantic relationship with a victim—usually through dating apps, social media, or email—then exploiting that trust to request money or personal information.

Scammers may impersonate military personnel, professionals working abroad, or affluent individuals, often using stolen or AI-generated photos and elaborate backstories.

Common Red Flags

Quick professing of love or deep connection shortly after initial contact.

- Consistent excuses to avoid in-person or video meetings (e.g., working abroad, oil rig, military deployment).
- Sudden requests for money due to “emergencies” (medical, family, travel, visa) or “investment” opportunities.
- Pressure to move communication off-platform and onto private channels.
- Use of poorly written or inconsistent messages, often calling victims by wrong names.
- Attempts to isolate victims from loved ones or discourage them from seeking advice.

🛡️ Prevention Tips

- **Don’t send money or share financial info** with someone you haven’t met in person or video-chatted with.
- **Perform reverse image searches** for profile pictures to verify authenticity and detect fake accounts.
- **Keep communication on verified platforms** (avoid untested apps or phone/SMS).
- **Ask probing questions** to validate their identity and background; watch for inconsistencies.
- **Slow things down** and let trusted friends or family review your interactions.
- **Be alert to investment pitches** especially involving cryptocurrency.

What to do if you think you've been scammed

If you think you have fallen victim to a scam, that you have given remote access to your computer to a suspected scammer, or that your computer has been hacked:

- Alert your financial institution. If you have provided your account details to a scammer, contact your bank or financial institution immediately and let them know.
- We understand that falling victim to a scam can be embarrassing. If you, or someone you know, has fallen victim to a scam, we urge you to call the Edmonton Police Service using the numbers listed on this page.
- Get further assistance. Contact the Canadian Anti-Fraud Centre or call 1-888-495-8501.
- Get qualified computer help. If you have computer problems, seek help or advice from a qualified and reputable computer technician.
- File a complaint. You can report unwanted telemarketing calls at National DNCL or call 1-866-580-DNCL (3625).
- Contact law enforcement. If you think the call might be part of a fraud scheme, contact law enforcement authorities or the Canadian Anti-Fraud Centre) or call 1-888-495-8501.

Identity Theft and Fraud Victim Assistance Guide

Service Canada (personal documents) 1-800-622-6232 or 1-800-OCanada	**Canada Post** 1-800-267-1177 canadapost.ca/postalsecurity
Social Insurance Number 1-800-206-7218 servicecanada.gc.ca/eng/sc/sin	**Bills** - contact your bank/credit and debit card/utility/phone service providers
Service Alberta 780-427-7013 servicealberta.ca	**Equifax Canada** 1-800-465-7166 consumer.equifax.ca
Passport Canada 1-800-567-6868 passportcanada.gc.ca	**TransUnion Canada** 1-800-663-9980 transunion.ca

Non-Emergency
780-423-4567
Mobile Access
#377
Deaf or Hard of Hearing
780-425-1231
Crime Stoppers
1-800-222-8477

Call 911 for Emergencies Only

Connect on Social Media

Useful Websites:

www.antifraudcentrecentreantifraude.ca

www.standagainstscams.ca

www.edmontonpolice.ca/crimeprevention.ca

www.seniorfraudalert.ca