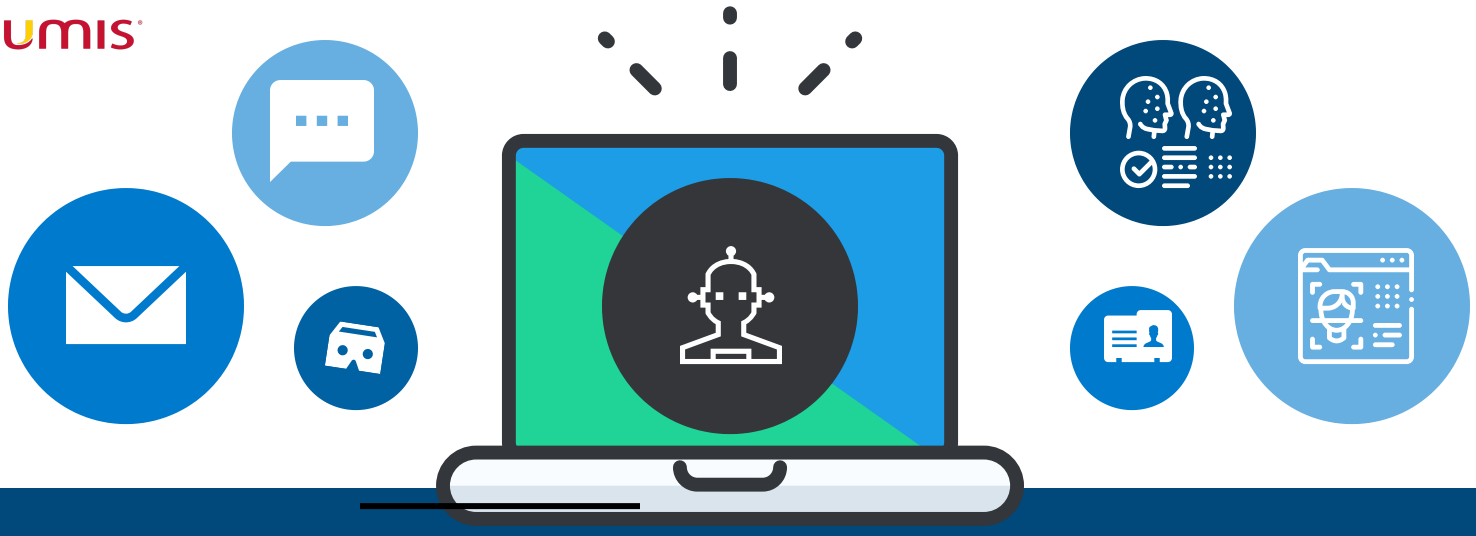
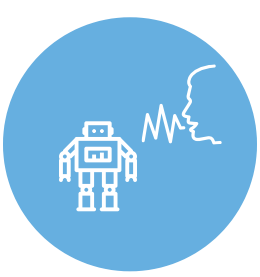


Spot the Signs: Don’t Get Fooled by AI-Generated Scams!

Fraudsters are increasingly using artificial intelligence to target Canadians for identity theft and other scams. AI enables them to mimic voices, create deepfake videos, and tailor their messages to appear more convincing and authentic. Stay one step ahead of the fraudsters by following these essential tips.



Check for Unnatural Language

AI-generated scams may have awkward phrasing, unnatural tone, or subtle grammar mistakes. Look out for robotic language that doesn’t sound quite right.

Be Wary of Impersonation

AI can mimic voices or writing styles to sound like someone you know or trust.
If a request seems unusual, verify directly through a known and trusted method (e.g., call the person or company yourself). It's also a good idea to establish a code word with your family and trusted friends that you can use to validate the legitimacy of an unusual call.

Watch for Phishing Links in Emails or Messages

AI-generated phishing emails may look more convincing, but always examine the sender’s email address and hover over links to check for suspicious URLs.
Don’t click links or download attachments unless you’re certain they’re safe!

Beware of Deepfake Content

Fraudsters can also use AI to create convincing deepfake videos to impersonate people and request money or sensitive information.
If you ever receive a video message urging immediate action, confirm its authenticity through other channels.

Always Trust Your Instincts

If something feels off, don’t ignore it. Even AI-generated scams can have small red flags that your intuition picks up on. Pause before acting on any suspicious request or communication.

Stay alert and double-check suspicious messages. Don’t let AI-generated scams trick you