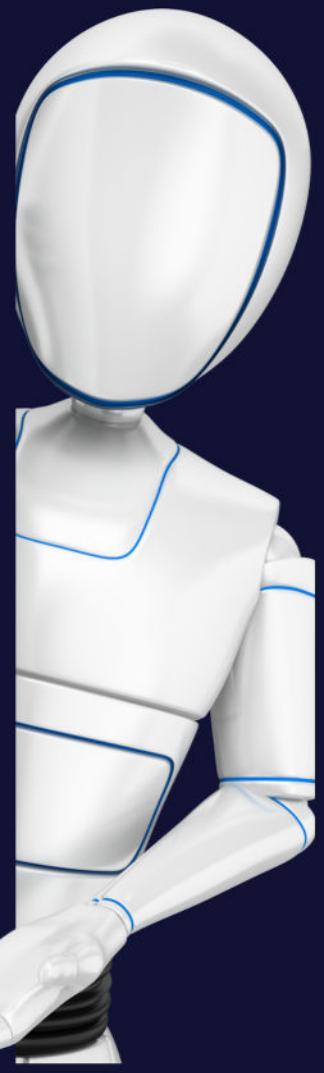
The Guide

of fraud prevention: Artificial Intelligence

March 2024 -vol 4

tonomsolution

Fraud in the age of artificial intelligence.

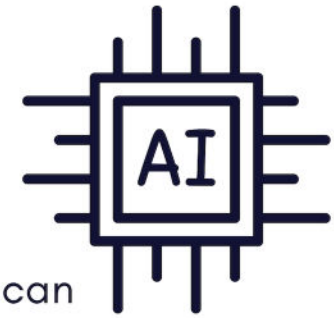


Every year, the World Economic Forum lists the 10 biggest risks facing humanity for the next two years as well as for the next decade. For the year 2024, we find "**cyber insecurity**" identified for both periods. (WEF, 2024). Artificial intelligence provides new tools for fraudsters that can make their activities much more credible and effective.

tonomsolution

The most common forms of artificial intelligence fraud.

Deepfaking



This method uses artificial intelligence to create images/sound clips that may seem **real.** These clips can be used to accurately recreate the voices of public figures or those close to you. This technique can therefore make anyone say anything, with the aim, for example, of making you invest in completely fictitious investments or to harm well-known personalities.

Identity Theft

This fraud occurs when fraudsters get their hands on **your username and password** for one of your online accounts. To do this, they may have found a loophole in the website and taken usernames and passwords. They then use bots to automatically check millions of usernames and passwords for different online accounts. If you've used the same password for multiple online accounts, especially a financial institution account, they can access it this way. They are then able to change your password and have full access to your account to carry out transactions.

Other
Common Frauds

Cryptoasset fraud

This fraud includes transactions that use cryptoassets. Fraudsters can operate from anywhere across the globe, inviting you to invest in fraudulent platforms. Once you have invested, it is very difficult **to trace the money** afterwards.

The “grandparent” fraud

Fraudsters specifically target seniors and pose as an immediate family member or someone close to them. They will claim to be in an **emergency situation** (an accident, theft, etc.) that requires immediate financial assistance. Accomplices can impersonate a professional (e.g. a police officer), in order to increase the credibility of the story. This stratagem therefore pushes the victim to act quickly, without having time to question themselves.

The love scam

The fraudster comes into contact with his victim through social media or dating apps. They then establish a bond of trust with the victim by complimenting them profusely to ultimately reveal romantic feelings to them. Once the virtual relationship is established, the fraudster then simulates various financial problems, in order to encourage the victim to **send money** to the fraudster.

Warning Signs

How to recognize a deepfake

- A **celebrity** promotes a high-yield, risk-free investment..
- You are asked to give **direct access** to your computer to assist you.
- You are encouraged to make a decision **quickly** to avoid missing out on a "unique opportunity"
- You are asked to make a **small initial deposit** to build your confidence. Be aware that scammers will often present fake account balances on fictitious investment websites to convince you to invest more than your initial deposit.

- You are allowed to **withdraw part of your earnings**, in order to build a bond of trust. However, once you invest larger amounts, the fraudsters cut off all communication with you.
- You receive an **unsolicited offer** to recover your losses, for a fee.
- A loved one calls you and asks for money due to a **personal emergency**.

Warning Signs

How to **recognize** an attempted ID theft?

- Do not respond to an **unsolicited** email without ensuring its authenticity. Do not use the contact details provided in the email or text message and do not click on the **hyperlinks** provided.

- You are offered a new social insurance number for a fee. Please note that Service Canada **does not issue** a new SIN following the leak or theft of personal information.

- You receive an email, text or call from someone who says they work for a financial institution and who wants to help you following an alleged case of fraud detected in your account. **Do not give** him any personal information. Instead, call your financial institution or the organization cited using an official number that you already have or that is listed on their website. **Make sure** you are dealing with the legitimate institution.

Precautions to take

- Use a **different** password for each online account.
- If necessary, use a **password manager**.
- Enable **multi-factor** authentication if possible.
- Sign up for a monitoring service.
- Be careful when on a **public** computer or **public wireless** connection.
- Be careful about the **personal information** you share in games, apps and on social media.

By the numbers

95 820

Number of **deepfake videos** offered on the internet in 2023

SOURCE : HOME SECURITY HEROES, STATE OF DEEPFAKES,2023.

100 000

Number of computer models **listed** that could produce deepfakes in 2023

SOURCE : KPMG, RAPPORT DEEPFAKES : REAL THREATS, 2023

550%

Increase in deepfake videos offered on the internet since 2019

SOURCE : HOME SECURITY HEROES, STATE OF DEEPFAKES, 2023

62 365

Number of fraud **reports processed** in Canada in 2023

SOURCE : Centre antifraude du Canada, Fraudes récentes, 2024.

41 111

Number of fraud **victims** in Canada in 2023

SOURCE : Centre antifraude du Canada, Fraudes récentes, 2024.

554 M$

In **financial losses** linked to fraud in Canada in 2023

SOURCE : Centre antifraude du Canada, Fraudes récentes, 2024.

In Case of Fraud

- Contact your financial institution **and/or payment provider**.
- The **Canadian Anti-Fraud Centre at**
  1 888 495-8501 ou en ligne au
  www.antifraudcentre-centreantifraude.ca
- Contact your **local** police station to report fraud.

Sources

1. Home Security Heroes, 2023. STATE OF DEEPFAKES.
2. KPMG, 2023. RAPPORT DEEPFAKES : REAL THREATS.
3. World Economic Forum. 2024. Top 10 risks. https://www.weforum.org/agenda/2024/01/global-risks-report-2024/
4. AMF. 2024. L'hypertrucage (deepfake). https://lautorite.qc.ca/grand-public/types-de-fraude/lhypertrucage-deepfake
5. AMF. 2024. Vol de renseignements personnels. https://lautorite.qc.ca/grand-public/types-de-fraude/lhypertrucage-deepfake
6. Centre antifraude du Canada. 2024. Fraudes récentes. https://antifraudcentre-centreantifraude.ca/index-fra.htm