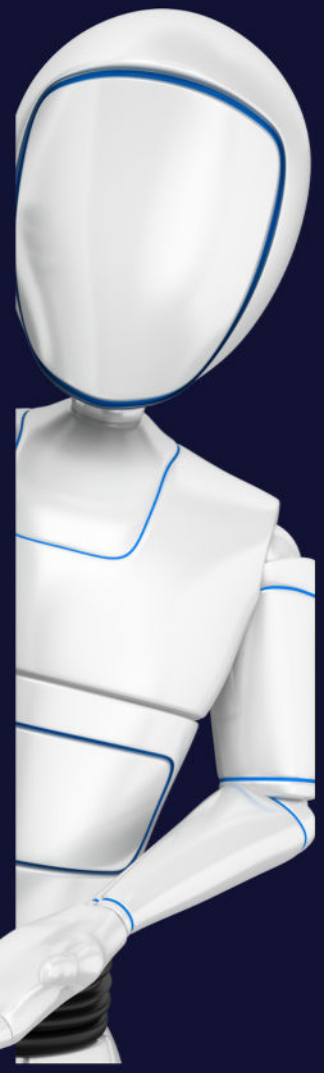
Le Guide

de prévention de la fraude: l'intelligence articielle

Mars 2024 -vol 4

tonomsolution

La fraude à l'ère de l'intelligence artificielle.



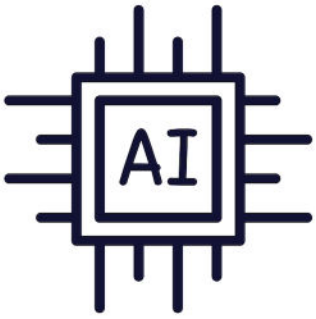
À chaque année, le Forum économique mondial dresse la liste des 10 plus grands risques encourus par l'humanité pour les deux prochaines années, ainsi que pour la prochaine décennie. Pour l'année 2024, on retrouve **«la cyberinsécurité»** d'identifiée pour les deux périodes. (WEF, 2024).

L'intelligence artificielle procure de nouveaux outils aux fraudeurs qui peuvent rendre leurs activités beaucoup plus crédibles et efficaces.

tonomsolution

Les formes de fraude les plus communes à l'intelligence articielle.

L'hypertrucage



Cette méthode utilise l'intelligence artificielle pour créer des images/des extraits sonores qui peuvent sembler **réels.** Ces extraits peuvent servir à recréer avec précision la voix de personnalités publiques ou même de vos proches. Cette technique peut donc faire dire n'importe quoi à n'importe qui, avec pour objectif, par exemple, de vous faire investir dans des investissments totalement fictifs ou pour nuire à des personnalités connues.

Vol d'identifiant

Cette fraude se produit lorsque des fraudeurs mettent la main sur **votre identifiant et votre mot de passe** d'un de vos comptes en ligne. Pour s'y faire, ils peuvent avoir trouvé une faille dans le site Web et s'être emparés d'identifiants et de mots de passe. Ils utilisent ensuite des robots pour vérifier automatiquement des millions d'identifiants et de mots de passe pour différents comptes en ligne. Si vous avez utilisé le même mot de passe pour plusieurs comptes en ligne, en particulier un compte d'une institution financière, ils peuvent ainsi y accéder. Ils sont alors en mesure de modifier votre mot de passe et avoir pleinement accès à votre compte pour y effectuer des transactions.

D’autres fraudes communes

La fraude liée aux cryptoactifs

Cette fraude englobe les transactions qui ont recours aux cryptoactifs. Les fraudeurs peuvent agir de partout à travers le globe en vous invitant à investir dans des plateformes frauduleuses. Une fois que vous avez investi, il est très difficile de **retracer l’argent** par la suite.

La fraude des « grands-parents »

Les fraudeurs visent spécifiquement les personnes aînées et se font passer pour un membre de la famille immédiate ou quelqu’un de leur entourage. Ils vont prétendre être dans une situation d’urgence (un accident, un vol, etc.) qui exige une aide financière **immédiate**. Des complices peuvent personnifier un professionnel (ex: un policier), afin d’accentuer la crédibilité de l’histoire. Ce stratagème pousse donc la victime à agir rapidement, sans avoir le temps de se questionner.

L’arnaque amoureuse

Le fraudeur entre en contact avec sa victime par l’entremise des médias sociaux ou d’applications de rencontres. Il établit ensuite un lien de confiance avec la victime en la complimentant abondamment pour ultimement, lui dévoiler des sentiments amoureux. Une fois la relation virtuelle établie, le fraudeur simule alors différents problèmes d’ordre financier, afin d’inciter la victime à lui **envoyer de l’argent**.

Les signaux d'alerte

Comment **reconnaître** l'hypertrucage?

- Une **célébrité** fait la promotion d'un placement à haut rendement et sans risque.

- On vous demande d'avoir un **accès direct** à votre ordinateur pour vous assister.

- On vous incite à prendre une décision dans de **brefs délais** pour éviter de passer à côté d'une « chance unique ».

- On vous demande d'effectuer un dépôt initial minimum pour vous mettre en confiance. Sachez que les fraudeurs vont souvent présenter de faux soldes de compte sur des sites Web de placement fictifs pour vous convaincre d'investir davantage que votre dépôt initial.

- On vous permet de **retirer une partie de votre gain**, afin de bâtir un lien de confiance. Toutefois, une fois que vous investissez de plus grosses sommes, les fraudeurs coupent toute communication avec vous.

- Vous recevez une **offre non sollicitée** pour recouvrer vos pertes, moyennant des frais.

- Un de vos proches vous appelle et vous demande de l'argent en raison d'une **urgence personnelle.**

Les signaux d'alerte

Comment **reconnaître** une tentative de vol d'identifiant?

- Ne donnez pas suite à un courriel **non sollicité** sans vous assurer de son authenticité. N'utilisez pas les coordonnées fournies dans le courriel ou le texto et ne cliquez pas sur les **hyperliens** proposés.

- On vous propose de vous offrir un nouveau numéro d'assurance sociale moyennant certains frais. Sachez que Service Canada **n'attribue pas** un nouveau NAS suite à une fuite ou un vol de renseignements personnels.

- Vous recevez un courriel, un texto ou un appel d'une personne qui dit travailler pour une institution financière et qui désire vous aider à la suite d'un supposé cas de fraude décelé dans votre compte. Ne lui donnez **aucun** renseignement personnel. Appelez plutôt votre institution financière ou l'organisation citée à partir d'un numéro officiel que vous possédez déjà ou qui figure sur leur site Internet. **Assurez-vous** de faire affaire avec l'institution légitime.

Les précautions à prendre

- Utilisez un mot de passe **différent** pour chaque compte en ligne
- En cas de besoin, utilisez un **gestionnaire** de mot de passe
- Activez si possible l'authentification à facteurs **multiples**
- S'inscrire à un service de surveillance.
- Être prudent lorsqu'on est sur un ordinateur partagé ou une connexion sans fil **publique**.
- Faire attention aux **informations personnelles** que vous transmettez aux jeux, aux applications et sur les médias sociaux.

En chiffres

95 820

Nombre de **vidéos hypertruquées** offertes sur l'internet en 2023

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

100 000

Nombre de modèles informatiques **répertoriés** pouvant produire des hypertrucages en 2023

SOURCE : KPMG, RAPPORT DEEPFAKES : REAL THREATS, 2023

550%

Hausse de vidéos hypertruquées offertes sur l'internet depuis 2019

SOURCE : HOME SECURITY HEROES, STATE OF DEEPFAKES, 2023

62 365

Nombre de **rapports traités** de fraude au Canada en 2023

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

41 111

Nombre de **victimes** de fraude au Canada en 2023

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

554 M$

En **pertes financières** liées aux fraudes au Canada en 2023

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

En cas de fraude

- Contactez votre institution financière **et/ou votre fournisseur de paiement**
- Le **Centre antifraude du Canada** au 1 888 495-8501 ou en ligne au www.antifraudcentre-centreantifraude.ca
- Votre poste de police **local** afin de dénoncer la fraude.

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