AUTORITÉ DES MARCHÉS FINANCIERS

L’hypertrucage : quand les apparences sont trompeuses

L’intelligence artificielle fait désormais partie de nos vies. Elle nous est utile, par exemple, pour faire des demandes vocales, utiliser un moteur de recherche sur le Web ou encore, créer des contenus de divertissement. Toutefois, l’intelligence artificielle peut également servir à tromper les gens lorsqu’elle est employée par des fraudeurs en quête de nouvelles victimes.

Qu’est-ce que l’hypertrucage?

L’hypertrucage, mieux connu sous l’expression anglophone « *deepfake* », est maintenant bien présent sur les réseaux sociaux et le Web. L’hypertrucage utilise l’intelligence artificielle pour créer des images ou des extraits sonores très réalistes concernant de faux événements, d’où le nom de *deepfake*.

L’hypertrucage peut servir à recréer avec précision la voix de personnalités publiques connues ou de vos proches, et de s’en servir pour réaliser des vidéos réalistes et convaincants. La tactique devient inquiétante puisque l’hypertrucage permet de faire dire n’importe quoi à n’importe qui. Des fraudeurs pourraient l’utiliser pour vous faire investir dans des placements qui n’existent pas, de discréditer des personnalités connues ou encore pour faire dire des faussetés à vos proches dans le but de vous soutirer de l’argent.

La fraude «grands-parents» est un classique. Un fraudeur peut facilement reproduire la voix d’un petit-enfant, s’en servir pour contacter ses grands-parents et leur demander de l’argent. La raison donnée aux grands-parents pourrait être, par exemple, des frais médicaux d’urgence ou une caution à payer rapidement, à la suite d’ennuis avec la justice.

Comment reconnaitre une fraude par hypertrucage?

AUTORITÉ DES MARCHÉS FINANCIERS

Soyez vigilant afin d'éviter de tomber dans le panneau. Voici quelques indices pouvant vous aider à prévenir la fraude :

- Une célébrité vous vante un placement à haut rendement et sans risque. Méfiez-vous de ce qui est trop beau pour être vrai.
- On vous demande l'autorisation d'accéder directement à votre ordinateur pour vous assister. Conservez vos renseignements personnels et identifiants personnels en sécurité.
- On vous fait une offre qui nécessite de prendre une décision rapidement pour ne pas rater une « occasion unique » ou l'on vous appelle et vous demande de l'argent pour une raison urgente. Prenez le temps de vous arrêter et de vous poser des questions.
- On vous demande d'effectuer un dépôt initial minime (environ 350 $ CA ou 250 $ US) 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. Gardez en tête que les fraudeurs poussent souvent leurs mensonges très loin.
- Pour gagner votre confiance et vous amener à investir davantage, on vous permet de retirer une partie de votre argent. Toutefois, au bout d'un moment, les fraudeurs coupent toute communication avec vous et conservent votre argent.
- Vous recevez une offre non sollicitée pour recouvrer vos pertes, moyennant des frais. Souvent, ce sont les mêmes fraudeurs qui vous soutirent davantage d'argent.

Comment vous protéger?

Sachez que l'Autorité des marchés financiers met à votre disposition un *Registre des entreprises et des individus autorisés à exercer*. Vérifiez toujours que l'entreprise ou l'individu qui vous contacte, ou vous fait une offre, y est réellement inscrit.

En cas de doute, contactez notre Centre d'information au 1-877-525-0337 ou consultez notre site Web lautorite.qc.ca.