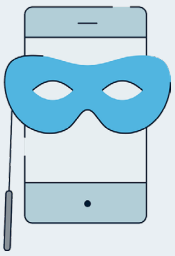
Escroquerie par hypertrucage



Au moyen de l'IA, les escrocs peuvent cloner les voix de personnalités (célébrités, représentants du gouvernement, hauts dirigeants) pour tenter de piéger les gens avec de faux appels ou de fausses publicités. La « personnalité » essayera alors de vous convaincre de réaliser un certain placement ou de contribuer à une œuvre de bienfaisance. Parce que les gens font souvent confiance aux personnes connues et respectées, ces hypertrucages peuvent être très efficaces pour les convaincre de se départir de leur argent. Lisez la suite pour savoir comment repérer les signaux d'alerte, ce que vous devez savoir et comment vous protéger.

Attention aux signaux d'alerte

- Incohérences dans la vidéo, restez à l'affût d'images et de mots qui semblent trop parfaits.
- Mouvements et expressions du visage non naturels.
- Audio qui ne correspond pas tout à fait au mouvement des lèvres.
- Tout message de nature urgente ou secrète.
- Le directeur demande des renseignements inhabituels et confidentiels.
- La demande est inhabituelle ou l'offre est trop belle pour être vraie.

À savoir

- L'hypertrucage désigne du contenu fictif conçu pour être impossible à distinguer d'une vraie personne. Les applications de permutation de visages et les vidéos de célébrités ou de politiciens qui font des choses inhabituelles sont des exemples d'hypertrucage.
- Au cours de la dernière année, les attaques par hypertrucage se sont multipliées. En effet, plusieurs personnes du monde entier ont été dupées par des clones audio et vidéo créés grâce à l'IA.
- Les hypertrucages peuvent servir à usurper l'identité d'un cadre supérieur, modifier le contenu audio ou vidéo pour autoriser des opérations et inciter des employés et des clients à révéler des renseignements confidentiels.
- De plus, les escrocs peuvent utiliser l'IA pour chercher des renseignements concernant vos profils en ligne et ainsi personnaliser les messages. Ils seront alors d'autant plus convaincants.
- Les hypertrucages peuvent se présenter sous diverses formes, notamment des images, des enregistrements vidéo et audio.

Façons de vous protéger

- ☐ Pour vous protéger, faites confiance à votre instinct et ne vous précipitez pas pour effectuer une opération, quelle qu'elle soit. Le plus souvent, c'est en prenant du recul pour évaluer une situation inhabituelle que vous éviterez de devenir la victime d'une escroquerie. Même une escroquerie qui repose sur l'IA.
- ☐ Avant d'effectuer une opération, d'envoyer de l'argent ou de donner des renseignements, assurez-vous de valider la demande auprès d'une autre source. Vérifiez l'identité du demandeur par des moyens indépendants avant de répondre.
- ☐ Examinez attentivement le contenu pour déceler les distorsions étranges, comme des doigts supplémentaires ou des visages flous. Ce sont des indices révélateurs que l'image est fausse.
- ☐ N'oubliez pas de faire une pause, de réfléchir et de signaler les hypertrucages pour vous protéger et protéger RBC.

Les meilleures pratiques de base en matière de cybersécurité jouent encore un rôle essentiel dans la réduction des risques :

- ☐ Continuez de vous tenir informé des dernières nouvelles sur les escroqueries et la cybersécurité en consultant le site rbc.com/cyberfute.
- ☐ Utilisez des mots de passe complexes.
- ☐ Renforcez vos paramètres de sécurité sur les réseaux sociaux.
- ☐ Limitez votre empreinte numérique et soyez prudent quant à ce que vous partagez en ligne.

Soyez cyberfuté RBC
rbc.com/cyberfute

RBC®