lefigaro.fr

Trompé par une fausse visioconférence, un employé vire 26 millions de dollars à des escrocs

Par Le Figaro avec AFP

5–6 minutes

Publié il y a 2 minutes, Mis à jour à l'instant

Les escrocs se sont fait passer pour le directeur financier de l'entreprise basé au Royaume-Uni. Valeriia / stock.adobe.com

L'employé d'un centre financier chinois, à Hong Kong, a cru participer à une réunion avec des cadres supérieurs de l'entreprise alors que tous les participants étaient des *«fake»* réalisés grâce à l'intelligence artificielle.

Des escrocs ont escroqué une multinationale de quelque 26 millions de dollars en utilisant une technologie deepfake pour se faire passer pour des cadres supérieurs de l'entreprise, a annoncé dimanche la police de Hong Kong, dans l'un des premiers cas de ce type dans la ville. Un deepfake est un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle. Il recèle un potentiel de désinformation et d'utilisation abusive, comme par exemple des images deepfake montrant des gens disant des choses qu'ils n'ont jamais dites.

Un employé d'une entreprise d'un centre financier chinois a reçu *«des appels par vidéoconférence de quelqu'un se faisant*

passer pour un cadre supérieur de son entreprise lui demandant de transférer de l'argent vers des comptes bancaires désignés», a indiqué la police à l'AFP.

Tous les participants de la visioconférence étaient des *«fake»*

La police a reçu un rapport sur l'incident le 29 janvier, date à laquelle quelque 200 millions de dollars de Hong Kong (26 millions de dollars américains) avaient déjà été perdus via 15 transferts. *«Les enquêtes sont toujours en cours et aucune arrestation n'a été effectuée jusqu'à présent»*, a indiqué la police, sans divulguer le nom de l'entreprise.

À lire aussiLes deepfakes pornographiques ciblant Taylor Swift provoquent une prise de conscience sur les dangers de l'IA

Un haut responsable de la police, Baron Chan, a déclaré que la vidéoconférence impliquait plusieurs participants, mais que tous, à l'exception de la victime, étaient des *«fake»*.

«Les escrocs ont trouvé des vidéos et des audios accessibles au public via YouTube, puis ont utilisé la technologie deepfake pour imiter leurs voix... afin d'inciter la victime à suivre leurs instructions», a déclaré Chan aux journalistes. Les vidéos deepfakes étaient préenregistrées et n'impliquaient aucun dialogue ni interaction avec la victime, a-t-il ajouté.

La rédaction vous conseille

- Les deepfakes pornographiques ciblant Taylor Swift provoquent une prise de conscience sur les dangers de l'IA
- «Une arme pour décrédibiliser un adversaire politique» : alerte contre les «deepfakes», ces vidéos truquées par intelligence artificielle

- Les «deepfakes», nouveau fléau sur internet