30.04.2024

Fraude au PDG 2.0

La fraude au PDG classique consiste à envoyer un mail à un employé pour le convaincre d'effectuer une opération bancaire en lui faisant croire qu'il agit sur ordre de son patron. L'Office fédéral pour la cybersécurité a recensé un cas dont le scénario est encore plus sophistiqué.

Le cas signalé à l'Office fédéral de la cybersécurité (OFCS) se distingue des autres attaques enregistrées jusqu'à présent. Contrairement au scénario habituel, la victime n'a pas été dissuadée ou empêcher de contacter son patron pour obtenir confirmation. Au lieu de cela, le collaborateur en question a été contacté par un prétendu avocat l'invitant à se connecter en vidéoconférence avec son chef. Lors de la réunion en ligne, l'employé a effectivement vu et parlé avec son supérieur à l'écran. C'est à cette occasion que ce dernier a tenté de convaincre la victime de procéder à des transactions financières.

Bien entendu, il s'agissait d'une fausse vidéo (ou « deepfake ») créée à l'aide de l'intelligence artificielle (IA). Bien qu'il reste encore à élucider la manière dont les criminels se sont procuré les images traitées, on présume qu'ils ont utilisé des séquences vidéo publiquement accessibles sur Internet.

Autre possibilité : passer des appels en amont pour enregistrer la voix et la copier. Ainsi, plusieurs entreprises ont récemment signalé que des inconnus avaient appelé pour demander des informations sur l'entreprise qui pourraient être utilisées pour des attaques ciblées. Une fois que la voix du patron est enregistrée, l'IA permet de la copier et de réaliser un deepfake.

Cet incident montre que les cybercriminels se servent de plus en plus de l'intelligence artificielle, même si son application n'est pas encore parfaite. Dans ce cas précis, la fraude a été découverte. Les fraudeurs s'étaient limités à manipuler le visage du chef d'entreprise. De plus, les vêtements qu'il portaient ne correspondaient pas à ses habitudes et sa voix n'était pas très bien imitée.

Comment reconnaître un deepfake :

- le mouvement des lèvres n'est pas synchronisé avec le son
- erreurs de prononciation
- formulations étranges ou inhabituelles
- vidéo de mauvaise qualité
- images provenant d'un tout autre contexte

Pour en savoir plus sur la fraude au PDG, et notamment sur la manière de s'en protéger, consultez notre article à l'adresse suivante : www.ebas.ch/ceofraud (http://www.ebas.ch/ceofraud)

Cliquez ici (https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/wochenrueckblick_14.html) pour accéder à l'article original de l'OFCS.

Copyright – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique