

# Les dangers des images générées par l'IA et les deepfakes

## Que sont les images générées par l'IA et les deepfakes ?

Les images générées par l'IA sont conçues à l'aide de millions d'images et exemples de visuels. Lorsque vous saisissez une requête, le générateur d'image artificielle construit un visuel répondant à votre demande en combinant en une seule image de nombreuses images différentes. Le « deepfake » est une technologie similaire, mais qui repose sur la manipulation de photographies et de vidéos réelles de lieux et de personnes. Cette technologie peut donner l'impression qu'une personne a fait ou dit quelque chose, alors que ce n'est pas le cas. Ces deux technologies peuvent être utilisées de manière inoffensive, mais les cybercriminels ont appris à les utiliser à des fins malveillantes.

## Escroqueries au deepfake

Grâce à la technologie du deepfake, les escrocs peuvent se faire passer pour des célébrités ou toute autre personnalité publique. Ce type d'escroquerie peut donner l'impression qu'une célébrité soutient un produit, alors que ce n'est pas vrai. Les escrocs utilisent cette technique pour tromper des personnes et les inciter à acheter un faux produit afin de voler leurs informations personnelles et bancaires. Les deepfakes peuvent également être utilisés pour des personnalités politiques. Un deepfake peut donner l'impression qu'un membre d'un gouvernement a fait ou dit quelque chose, alors qu'il n'en est rien. Ce type de vidéos peut être utilisé pour amener des personnes à consulter un faux site Web ou à cliquer sur de faux articles d'information.

## Escroqueries utilisant des visuels générés par l'IA

Les cybercriminels utilisent fréquemment l'IA lors des escroqueries sentimentales en ligne. Ils peuvent générer de fausses photographies utilisées sur des profils de sites de rencontre afin d'essayer de voler de l'argent et des informations à leurs victimes. Les cybercriminels exploitent également des événements actuels dans le cadre de leurs escroqueries. Ils exploitent l'IA pour créer des photographies réalistes de tragédies et d'autres événements. Ils publient les photographies sur de faux sites Web pour inciter les internautes à envoyer des dons à une organisation caritative. Bien entendu, l'organisation n'existe pas et les cybercriminels gardent l'argent des dons pour eux-mêmes.

## Comment puis-je me protéger ?

Suivez les conseils ci-dessous pour vous protéger des escroqueries aux images générées par l'IA :

- Les images générées par l'IA présentent souvent des imperfections ou des anomalies subtiles. Soyez attentif à tout ce qui vous semble inhabituel dans une photographie. Une main avec plus de cinq doigts, une photographie avec un éclairage ou des ombres étranges sont des indices courants qu'une image a été générée par l'IA.
- Prenez toujours le temps de faire une pause et de réfléchir avant de faire quoi que ce soit. Si une photographie ou une image vous semble bizarre ou trop belle pour être vraie, il peut s'agir d'une escroquerie.
- Chaque fois que vous le pouvez, consultez une autre source pour vérifier les faits. Par exemple, si vous voyez une vidéo dans laquelle une célébrité apporte sa caution, consultez le site Web officiel de cette personne pour vérifier qu'elle travaille effectivement avec le produit concerné.

