Apprenez une nouvelle compétence de survie : Repérer les Deepfakes

Que sont les Deepfakes ?

Le mot "deepfake" est une combinaison de "deep learning" et "fake". En français, on les appelle également les hypertrucages. Les hypertrucages sont des images, des vidéos ou des enregistrements audio truqués. Parfois, les personnes que vous pouvez voir ou entendre sont générées par ordinateur, de fausses identités qui ressemblent à de vraies personnes. Parfois, les personnes sont réelles, mais leurs images et leurs voix sont manipulées pour leur faire dire des choses qu'elles n'ont pas dites. Par exemple, une vidéo "deepfake" pourrait être utilisée pour recréer une célébrité ou un politicien disant quelque chose qu'il n'a jamais dit. En utilisant ces trucages très réalistes, les pirates peuvent créer une réalité alternative dans laquelle vous ne pouvez pas toujours faire confiance à vos yeux et à vos oreilles.

Certains "deepfakes" ont des objectifs légitimes, comme les films qui ramènent à la vie des acteurs décédés pour recréer un personnage célèbre. Mais les cyber-attaquants commencent à exploiter le potentiel des "deepfakes". Ils les déploient pour tromper vos sens, afin de pouvoir voler votre argent, harceler les gens, manipuler les électeurs ou les opinions politiques, ou créer des fake news. Dans certains cas, ils ont même créé des sociétés fictives composées d'employés d'hype. À la lumière de ces attaques, vous devez faire encore plus attention à ce que vous croyez lorsque vous lisez des informations ou les réseaux sociaux.

Le FBI prévient qu'à l'avenir, les deepfakes auront "un impact plus grave et plus étendu en raison du niveau de sophistication des supports synthétiques utilisés". Apprenez à repérer les signes d'un deepfake pour vous protéger de ces simulations très crédibles. Chaque forme de "deepfake" - image fixe, vidéo et audio - possède son propre ensemble de défauts qui peuvent la trahir.

Des images fixes

L'hypertrucage que vous pouvez voir le plus souvent est la fausse photo de profil sur les réseaux sociaux. L'image ci-dessous est un exemple d'hypertrucage sur le site thispersondoesnotexist.com. Sous l'image se trouvent cinq indices différents indiquant qu'il pourrait s'agir d'un "deepfake". Vous remarquerez que ces indices ne sont pas faciles à repérer et peuvent être difficiles à identifier :

1. Arrière-plan : L'arrière-plan est souvent flou ou de travers, et peut présenter un éclairage incohérent, comme des ombres prononcées pointant dans différentes directions.
2. Lunettes : Regardez attentivement le lien entre les montures et les branches près de la tempe. Les "deepfakes" ont souvent des connexions mal assorties, avec des tailles ou des formes légèrement différentes.
3. Yeux : les photos d'hypertrucage actuellement utilisées pour les fausses photos de profil semblent avoir les yeux au même endroit dans le cadre, ce qui donne ce que certains appellent le "regard Deepfake".
4. Bijoux : Les boucles d'oreilles peuvent être informes ou étrangement accrochées. Les colliers peuvent être enfoncés dans la peau.
5. Cols et épaules : Les épaules peuvent être difformes ou décalées. Les colliers peuvent être différents de chaque côté.

Vidéo

Des chercheurs du Massachusetts Institute of Technology (MIT) ont élaboré une liste de questions pour vous aider à déterminer si une vidéo est réelle, notant que les "deepfakes" ne peuvent souvent pas "représenter pleinement la physique naturelle" d'une scène ou d'un éclairage.

1. Joues et front : La peau semble-t-elle trop lisse ou trop ridée ? L'âge de la peau est-il similaire à celui des cheveux et des yeux ?
2. Yeux et sourcils : Les ombres apparaissent-elles dans des endroits auxquels vous vous attendez ?
3. Lunettes : Y a-t-il des reflets ? Trop de reflets ? L'angle de la lumière change-t-il lorsque la personne se déplace ?
4. La pilosité faciale : La pilosité faciale semble-t-elle réelle ? Les hypertrucages peuvent ajouter ou enlever une moustache, des pattes ou une barbe.

5. Les grains de beauté du visage : Le grain de beauté a-t-il l'air réel ?
6. Clignement des yeux : La personne cligne-t-elle assez ou trop des yeux ?
7. Taille et couleur des lèvres : La taille et la couleur correspondent-elles au reste du visage de la personne ?

Audio/voix

Les chercheurs affirment que des technologies comme les spectrogrammes peuvent montrer quand les enregistrements vocaux sont faux. Mais la plupart d'entre nous n'ont pas le luxe d'avoir un analyseur de voix lorsqu'un pirate appelle. Recherchez une voix monotone, une tonalité ou une émotion étrange, et l'absence de bruit de fond. Les voix fausses peuvent être difficiles à détecter. Si vous recevez un appel bizarre d'une organisation légitime, vous pouvez vérifier si l'appel est réel en raccrochant d'abord puis en rappelant l'organisation. Veillez à utiliser un numéro de téléphone fiable, tel qu'un numéro de téléphone figurant déjà dans votre liste de contacts, un numéro de téléphone imprimé sur une facture ou un relevé de l'organisation, ou le numéro de téléphone figurant sur le site web officiel de l'organisation.

Conclusion

Sachez que les pirates utilisent activement les hypertrucages. Ils peuvent créer de faux comptes sur les réseaux sociaux pour se connecter ou créer de fausses vidéos pour influencer l'opinion publique. Certains vendent même leurs services sur le dark web pour que d'autres attaquants puissent faire de même. Nous n'attendons pas de vous que vous deveniez un expert en deepfake, mais si vous vous armez des bases de l'identification des hypertrucages, vous serez bien plus à même de vous défendre. Si vous pensez avoir détecté un "deepfake", signalez-le au site web ou à la source qui héberge le contenu.

Rédacteur Invité

Kerry Tomlinson (@KerryTNews) est journaliste spécialiste de l'actualité cybernétique chez Ampere News et est certifié SANS Security Awareness Professional. Sa mission est de traduire ce qui se passe dans le monde numérique pour les personnes de tous niveaux de connaissances, avec des nouvelles convaincantes et perspicaces, et des présentations convaincantes.

Ressources

Ingénierie sociale: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
Pouvez-vous repérer le trucage ? (Actualités Ampère): https://www.amperesec.com/news/can-you-spot-the-fake
Le test de détection de deepfake du MIT (MIT): https://detectfakes.media.mit.edu/
Repérer le trucage: https://www.spotdeepfakes.org/en-US

Traduit pour la communauté par : Juliette Busson