

Un reflet contrefait

Les logiciels de reconnaissance faciale sont infiltrés et volent votre visage

Prédiction : Les hackers vont défier les systèmes de reconnaissance faciale, et les entreprises répondront en utilisant des systèmes de reconnaissance comportementale

Le vol d'identifiants est la plus vieille tactique qui soit, et les attaquants cherchent sans répit de nouvelles vulnérabilités pour voler les identifiants des utilisateurs. L'authentification à deux facteurs (2FA) a été affaiblie avec le développement des « SIM swaps » (échange de carte SIM). Les méthodes d'authentification comme les empreintes digitales et la reconnaissance faciale s'améliorent mais sont toujours vulnérables.

Les authentifications à deux facteurs et biométriques ne sont pas des remèdes magiques.

\$224 millions

Total des dommages/intérêts demandés par Michael Terpin, qui affirme que des malfaiteurs lui ont volé 24 millions de \$ en cryptomonnaies en effectuant un SIM Swap sur son compte AT&T.

\$450

le coût de création d'une version papier de votre empreinte digitale (ou celles de quelqu'un d'autre).

5.6 millions

Le nombre de personnes dont les empreintes digitales ont été volées lors de la compromission du Bureau de la gestion du personnel aux États-Unis.

\$9.78 milliards

Marché mondial estimé des logiciels de reconnaissance de visage d'ici 2023.

Le phishing

est toujours le premier allié du hacker.

12,4 millions

victimes potentielles de kits de phishing entre 2016 et 2017.

56 %

des décideurs en sécurité IT affirment que les attaques ciblées via phishing sont les menaces de sécurité les plus importantes qu'ils affrontent.

la reconnaissance faciale vaincue

En 2016, des spécialistes de la sécurité et de la vision informatique de l'Université de Caroline du Nord ont leurré des systèmes de reconnaissance faciale à l'aide de photos numériques accessibles à tous, issues de réseaux sociaux et de moteurs de recherche.