www.techradar.com /pro/security/your-biometrics-may-not-be-as-safe-as-you-think

Vos données biométriques ne sont peut-être pas aussi sûres que vous le pensez

Oui, votre empreinte digitale peut être volée

Lewis Maddison :

Crédit image : Shutterstock (Crédit image : Shutterstock)

L'utilisation de vos données biométriques, telles que votre empreinte digitale, pour vous connecter et authentifier votre identité peut ne pas être aussi sécurisée que vous le pensez.

C'est ce qu'affirme NordVPN, dont les chercheurs affirment avoir trouvé 81 000 empreintes digitales volées sur des forums du dark web.
Le fournisseur VPN a également ajouté que puisque les utilisateurs ne peuvent pas changer leurs empreintes digitales - comme ils peuvent un mot de passe compromis - ils risquent d'être compromis de manière permanente.

Tout en reconnaissant que la biométrie est généralement une méthode d'authentification très sûre, Adrianus Warmenhoven, expert en cybersécurité chez NordVPN, a déclaré que « toutes les données enregistrées sont piratables...
Les informations biométriques sont une cible précieuse pour les cybercriminels, et le piratage de ce type de données devient un moyen populaire de vol d'identité.

NordVPN a identifié 20 types différents de données biométriques pouvant être utilisés, les plus populaires étant les empreintes digitales, le visage et la voix.
Il affirme en outre que tous sont vulnérables aux compromis de différentes manières.

En ce qui concerne les empreintes digitales, une méthode courante de vol consiste à placer quelque chose appelé écumeur sur les guichets automatiques ou autres machines de numérisation d'empreintes digitales.
Cela recueille les empreintes digitales et les duplique pour que les cybercriminels les utilisent pour violer les comptes des victimes.

NordVPN note que l'utilisation de skimmers est un moyen démodé de voler des empreintes digitales, et que maintenant la technologie deepfake rend le vol de données biométriques encore plus facile à réaliser pour les acteurs de la menace.

Il dit qu'en prenant les photos et les vidéos d'une cible à partir de ses profils de médias sociaux, la technologie peut créer de fausses versions de son visage, de sa voix et même de ses empreintes digitales pour tromper les processus d'authentification.

Warmenhoven explique que « bien que nous soyons propriétaires de nos propres visages et voix, nous ne sommes pas les seuls à y avoir accès.
Au fil des années d'utilisateurs actifs des médias sociaux, les gens ont laissé tellement de données biométriques qu'avec les capacités actuelles de l'intelligence artificielle pour créer des deepfakes, cela devient une arme contre notre vie privée.

Les données biométriques stockées sur un appareil intelligent sont généralement assez sécurisées car elles sont cryptées.
Cependant, si des applications malveillantes ont accès à ces données, des développeurs peu scrupuleux peuvent les voler.

Même dans le cas d'applications sûres et fiables, si les données biométriques d'un utilisateur finissent par être stockées dans le cloud ou les serveurs du fournisseur d'applications, elles sont à nouveau vulnérables aux violations de la part des auteurs de menaces.
Lors de la transmission des données biométriques entre l'appareil et les serveurs, un acteur malveillant pourrait intercepter les données.

Par conséquent, Warmenhoven recommande aux utilisateurs de bien réfléchir avant d'accepter la demande d'une nouvelle application d'accéder à leurs données biométriques.
Il conseille également d'utiliser l'authentification à deux facteurs (2FA) ou l'authentification multifacteur (MFA) lorsque cela est possible, ainsi que des mots de passe forts, et d'utiliser un VPN pour empêcher les criminels d'intercepter les données en transmission.

- Ce sont les meilleures options de gestionnaire de mots de passe pour protéger vos informations d’identification.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230821
"C'est ensemble qu'on avance"