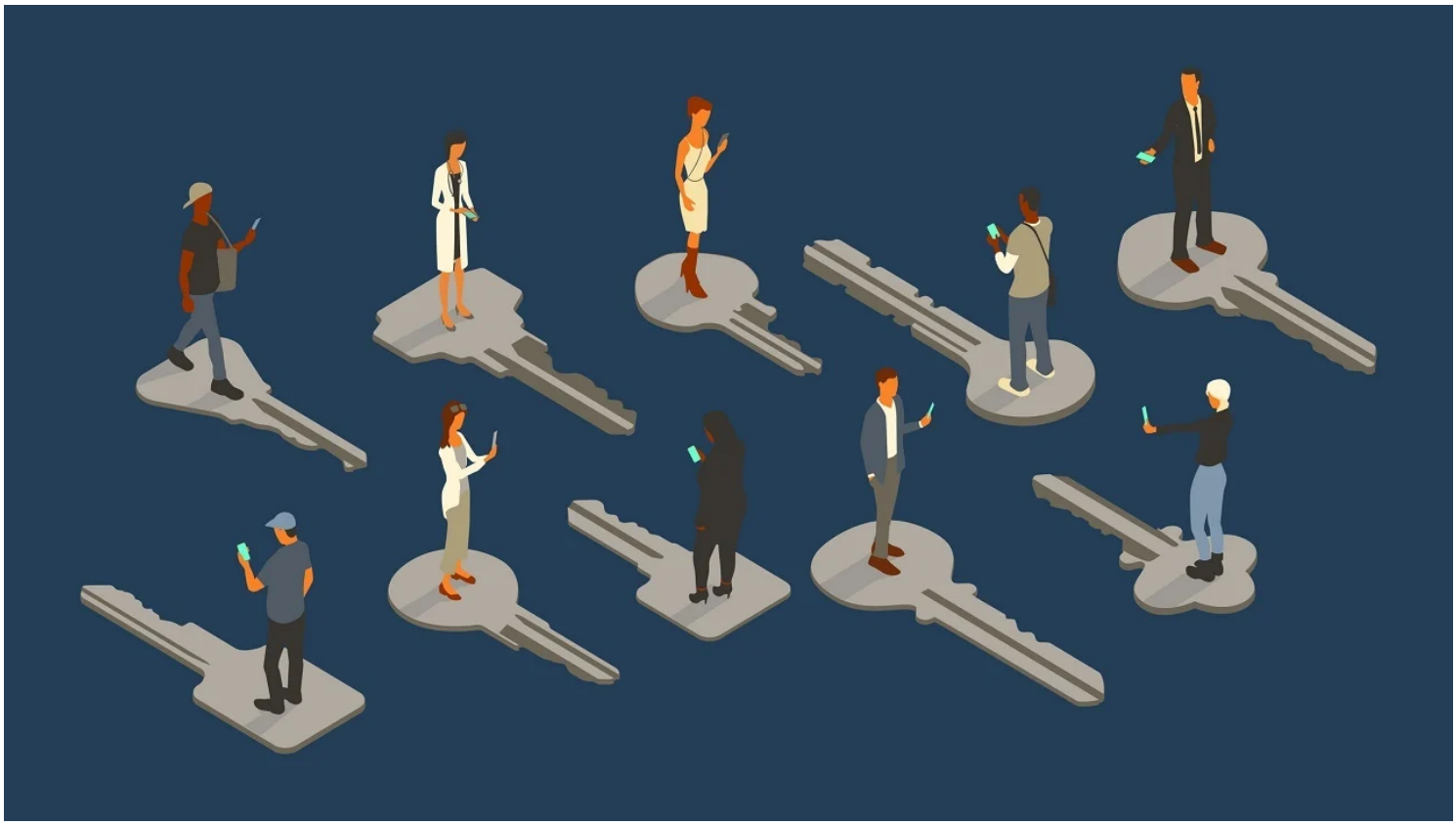
Clés d’accès (Passkey) qu’est-ce que c’est et pourquoi vous en avez besoin dès que possible

Nous vous expliquons ce que sont les clés d'accès, comment vous pouvez les obtenir et où vous pouvez les utiliser pour vous connecter en toute sécurité sans exposer votre adresse courriel ni créer de mot de passe.

Kim Key ⋮



J’en ai marre des mots de passe.
Ils sont en quelque sorte à la fois faciles à deviner et difficiles à retenir, et il est difficile de les garder hors de portée des criminels.
Pour résoudre ce problème, l’Alliance FIDO (Fast Identity Online) a développé des clés d’accès, une forme de technologie d’authentification sans mot de passe.
Les clés d’accès éliminent le besoin de saisir votre adresse courriel ou votre mot de passe dans les champs de connexion sur tout le Web, ce qui rend plus difficile pour les criminels de voler vos informations d’identification et d’accéder à vos comptes.

Les clés d’accès présentent de nombreux avantages ; par exemple, ils ne peuvent pas être devinés ou partagés.
Les clés d’accès résistent aux tentatives d’hameçonnage, car elles sont uniques aux sites pour lesquels elles

ont été créées, de sorte qu'elles ne fonctionneront pas sur les sites similaires frauduleux.
Plus important encore, à l'ère des violations de données quasi constantes, vos clés d'accès ne peuvent pas être volées en piratant le serveur ou la base de données d'une entreprise, ce qui rend les données extraites lors de ces violations moins précieuses pour les criminels.
Mais de quoi s'agit-il exactement ?
Nous sommes là pour vous expliquer.

Qu'est-ce qu'une clé d'accès ?

Une clé d'accès est un moyen de se connecter à des applications et à des sites Web sans utiliser une combinaison de nom d'utilisateur et de mot de passe.
Il s'agit d'une paire de clés de cryptographie générées par votre appareil.
Une clé publique et une clé privée se combinent pour créer une clé d'accès qui déverrouille votre compte.

Les applications ou les sites Web stockent votre clé publique unique.
Votre clé privée n'est stockée que sur votre appareil, et une fois que votre appareil a authentifié votre identité, les deux clés se combinent pour vous accorder l'accès à votre compte.
Nous vous expliquons comment mettre cela en pratique dans notre guide sur la configuration et l'utilisation des clés d'accès.

Habituellement, l'appareil ou le logiciel qui génère les clés d'accès utilise un outil d'authentification biométrique, tel que FaceID ou TouchID, pour authentifier votre identité. Si un gestionnaire de mots de passe est la source de la clé d'accès, vous pouvez vous connecter à l'application à l'aide d'un mot de passe principal fort au lieu d'une authentification biométrique.
Les clés d'accès sont uniques à chaque application ou site Web et stockées dans le coffre-fort d'un gestionnaire de mots de passe ou dans le trousseau de votre appareil.
Les clés d'accès peuvent être synchronisées entre les appareils, ce qui en fait un choix pratique.

Pourquoi avez-vous besoin de clés d'accès ?

L'adoption généralisée de l'authentification sans mot de passe comme les clés d'accès ne pouvait pas arriver à un moment plus critique.
Les chercheurs de Digital Shadows ont rapporté qu'en 2022, plus de 24 milliards d'identifiants de connexion avaient été exposés par des violations de données.
Ce nombre a augmenté de 65 % depuis 2020, et les chercheurs pensent que les attaques de logiciels malveillants, les escroqueries par ingénierie sociale et le partage de mots de passe sont à blâmer pour cette augmentation.

Le rapport conclut que l'adoption généralisée des clés d'accès par les utilisateurs et les propriétaires de sites Web est nécessaire pour empêcher les criminels de prendre le contrôle de comptes en utilisant des combinaisons de nom d'utilisateur et de mot de passe volées.
Les piratages de comptes et les incidents d'usurpation d'identité résultant de violations de données peuvent être atténués en activant l'authentification multifacteur pour vos comptes en ligne et en utilisant un gestionnaire

de mots de passe pour créer et stocker de nouvelles informations d'identification ou clés d'accès pour chaque page de connexion que vous rencontrez en ligne.

Où pouvez-vous utiliser les clés d'accès ?

Vous pouvez utiliser des clés d'accès pour vous connecter à de nombreux sites Web, notamment Best Buy, eBay, Google, Kayak et PayPal.
Les sociétés de gestion de mots de passe Dashlane ou 1Password gère un site communautaire où les utilisateurs peuvent signaler les sites Web qui acceptent les connexions à l'aide de clés d'accès.
À l'heure actuelle, certains des sites de cette liste, tels que Adobe.com, exigent toujours un nom d'utilisateur et un mot de passe traditionnels pour la création initiale d'un compte et les connexions, mais vous pouvez configurer une clé d'accès à utiliser pour les connexions futures en visitant le menu Paramètres.

Recommandé par nos rédacteurs

L'adoption rapide de la clé d'accès par les principales applications et sites Web est encourageante, mais l'adoption de la clé d'accès peut prendre du temps pour les sites Web appartenant à des particuliers ou à de petites entreprises.
Certains sites ne prennent même pas encore en charge l'authentification multifacteur, nous devrons donc peut-être attendre un certain temps pour que les dernières normes de sécurité FIDO éradiquent complètement les mots de passe.

La plupart des gestionnaires de mots de passe que j'ai examinés pour PCMag, tels que 1Password et Dashlane, peuvent stocker et créer des clés d'accès pour vous.
Si vous avez déjà un abonnement au gestionnaire de mots de passe, continuez comme ça !
Un gestionnaire de mots de passe facilite le stockage et l'utilisation de vos anciennes informations d'identification et de vos nouvelles clés d'accès lorsque vous vous connectez.
Si vous n'utilisez pas de gestionnaire de mots de passe, il n'est pas trop tard pour essayer d'être plus sûr avec vos données personnelles.
Les utilisateurs d'Android et d'iOS peuvent stocker leurs clés d'accès localement et y accéder à l'aide de l'application trousseau sur leurs appareils mobiles.

Donc, pour l'instant, utilisez des clés d'accès lorsque vous le pouvez et assurez-vous que l'authentification multifacteur est activée sur tous les comptes qui la prennent en charge. Vous devez également continuer à utiliser un gestionnaire de mots de passe pour créer et stocker vos informations d'identification jusqu'à ce que vous n'en ayez plus besoin.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231015
"C'est ensemble qu'on avance"