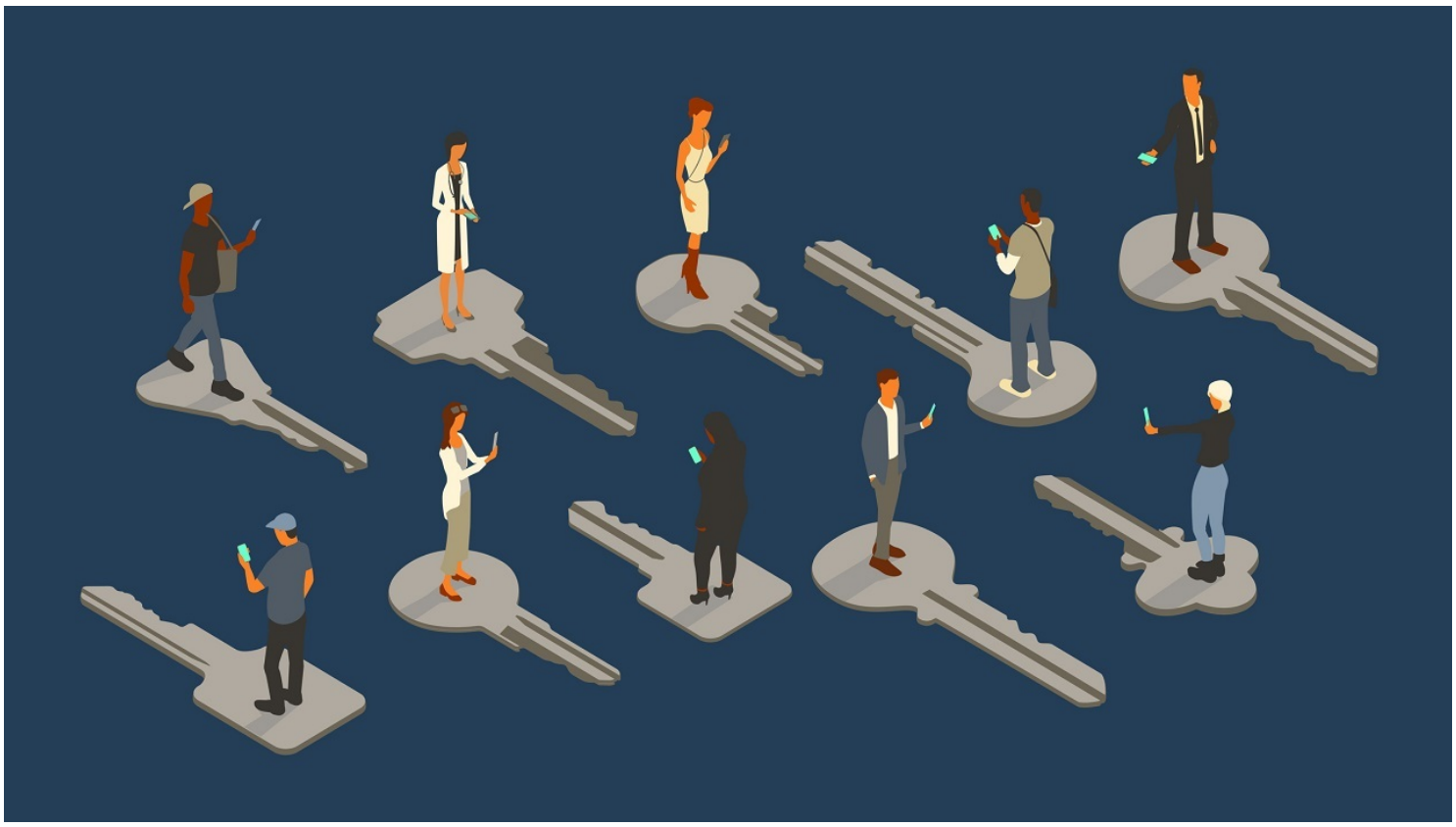
# Authentification sans mot de passe; qu'est-ce que c'est et pourquoi vous en avez besoin

***L'industrie de la cybersécurité a une vision pour un avenir plus sûr, qui implique de se débarrasser des mots 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 les garder hors des mains des criminels est difficile.
Au cours des dernières années, la Fast Identity Online (FIDO) Alliance a développé des normes technologiques d'authentification sans mot de passe.
L'année dernière, Apple a annoncé la disponibilité d'une nouvelle fonctionnalité de sécurité appelée clé d'accès pour les utilisateurs d'iOS 16.
Pendant ce temps, Google développe une solution d'authentification sans mot de passe pour Android.

Il est temps que davantage d'applications et de sites Web protègent les clients en adoptant des technologies sans mot de passe telles que les clés d'accès.
Les clés d'accès ne peuvent pas être devinées ou partagées entre les utilisateurs.
Ils résistent aux tentatives de phishing car ils sont tous uniques aux sites pour lesquels ils ont été créés, de sorte qu'ils ne fonctionneront pas sur des sites similaires frauduleux.

Plus important encore, à l'ère des violations de données quasi constantes, vos clés privées ne peuvent pas être volées en piratant le serveur ou la base de données d'une entreprise.

Nous voulons tous être plus en sécurité en ligne.
Lisez la suite pour savoir pourquoi vous devriez essayer l'authentification sans mot de passe dès que possible.

## Pourquoi avez-vous besoin d'une authentification sans mot de passe ?

L'adoption généralisée de l'authentification sans mot de passe ne pouvait pas arriver à un moment plus critique.
Les chercheurs de Digital Shadows ont récemment 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 l'origine de cette augmentation.

Le rapport conclut que l'adoption généralisée de l'authentification sans mot de passe est nécessaire pour empêcher les criminels de prendre le contrôle de comptes en utilisant des combinaisons de noms d'utilisateur et de mots de passe volés.
Jusqu'à ce que l'authentification sans mot de passe soit acceptée partout en ligne, les prises de contrôle de compte et les incidents de vol d'identité résultant de violations de données peuvent être atténués grâce à l'authentification multifacteur et à l'utilisation d'un gestionnaire de mots de passe pour créer et stocker de nouvelles informations d'identification pour chaque connexion.

## Qu'est-ce qu'une clé d'accès ?

Une clé d'accès est un moyen sans mot de passe de se connecter à des applications et des sites Web.
Une clé d'accès est un autre nom pour une paire de clés de chiffrement générées par votre périphérique authentifié.
Une clé publique et une clé privée se combinent pour créer une clé d'accès.

Votre application ou site Web cible stocke votre clé publique lorsque vous vous connectez.
La 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 donner accès à votre compte.
Lance Whitney de PCMag a écrit un guide pour la configuration et l'utilisation des clés d'accès.

L'appareil ou le logiciel générant les clés d'accès utilise généralement 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 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 le trousseau de votre appareil.
Les clés d'accès peuvent être synchronisées entre les appareils, ce qui en fait un choix pratique.

## Où pouvez-vous utiliser l'authentification sans mot de passe ?

À l'aide de clés d'accès, vous pouvez vous connecter à quelques sites, notamment Best Buy, eBay, Google, Kayak et PayPal.
Plusieurs gestionnaires de mots de passe, dont Bitwarden et Dashlane, lauréats du Choix de la rédaction, offrent à leurs clients un accès sans mot de passe aux coffres-forts Web via l'authentification biométrique.
D'autres sociétés de gestion des mots de passe, telles que NordPass, ont récemment annoncé qu'elles développaient des moyens de stocker des clés d'accès dans les coffres-forts des clients.

L'adoption rapide de la clé d'accès par les principales applications et sites Web est encourageante, mais cela peut prendre du temps pour une adoption généralisée sans mot de passe.
De nombreux sites plus petits n'offrent même pas encore de support pour l'authentification multifacteur, nous devrons donc peut-être attendre un certain temps pour que les dernières normes de sécurité FIDO tuent efficacement le mot de passe.

En attendant, utilisez des clés d'accès là où 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.

### Recommandé par nos rédacteurs

## Que se passe-t-il d'autre dans le monde de la sécurité cette semaine ?

Presque tous les utilisateurs de Coinbase s'appuient sur 2FA basé sur SMS, révèlent les statistiques de prise de contrôle de compte.
Coinbase exige que tous les comptes soient sécurisés via une authentification à deux facteurs; par défaut, ces codes arrivent par SMS.
Cette méthode, cependant, est vulnérable aux attaques d'échange de cartes SIM.

PayPal: 35 000 utilisateurs avaient des informations de sécurité sociale et fiscales exposées aux pirates.
Les pirates ont accédé aux informations en devinant avec succès les mots de passe des utilisateurs concernés grâce à une attaque de « bourrage d'informations d'identification ».

Le pirate a trouvé une liste d'interdiction de vol du FBI sur un serveur non sécurisé.
Le pirate a trouvé les données, qui contiendraient des centaines de milliers de noms et de dates de naissance après que la compagnie aérienne régionale CommuteAir les ait laissées sur un serveur ouvert.

Bonne nouvelle, mauvaise nouvelle pour les chercheurs en sécurité : les autorités sont moins susceptibles de vous inculper, les États sont une autre chose.
Lors de la conférence des hackers ShmooCon, l'avocat d'infosec Harley Geiger avertit que certaines lois étatiques continuent de menacer la recherche légitime, tout comme une récente réglementation chinoise.

À l’ère de la « crise permanente », les gens deviennent paresseux avec la sécurité sur le lieu de travail.

Quarante-cinq pour cent de ceux qui affirment éprouver une distraction « permacrise » disent qu’ils ne se soucient pas de toutes leurs règles de sécurité sur le lieu de travail, selon une enquête de 1Password.

*Recherche et mise en page par:*
*Michel Cloutier*
*CIVBDL*
*20231002*
*"C'est ensemble qu'on avance"*