Version en grands caractères
Version audio
(en anglais seulement)

Google

Les clés d'accès : un pas de plus vers un avenir sans mots de passe

Face à la montée en flèche des cyberattaques commanditées par des États et des actes malveillants en ligne, nous sommes plus que jamais déterminés à protéger les personnes, les entreprises et les gouvernements en leur permettant de profiter de notre expertise, en outillant la société, et en travaillant sans relâche pour faire progresser les technologies de cybersécurité afin de contribuer à bâtir un monde plus sûr pour tous.

Aujourd'hui, les mots de passe sont essentiels à la sécurité en ligne, mais les menaces telles que l'hameçonnage continuent d'augmenter. Google a identifié depuis longtemps ces problèmes et a encouragé l'utilisation d'outils d'authentification tels que la vérification en deux étapes (2SV), le gestionnaire de mots de passe Google, les clés de sécurité et, désormais, les clés d'accès.

Le défi

En informatique, les mots de passe sont utilisé depuis plus de 60 ans, mais aujourd'hui, ils ne suffisent plus à assurer la sécurité des données des utilisateurs et des organisations. Les attaques par hameçonnage continuent de prendre de l'ampleur et de se perfectionner en tirant parti des faiblesses de sécurité des mots de passe. Ainsi :

- En 2021, plus de **60 % des violations de données** résultaient du vol d'identifiants ou de l'hameçonnage[1].
- En 2022, les violations de données dues à l'hameçonnage ont coûté **en moyenne 4,91 millions $** aux organisations[2].
- En 2022, les attaques par hameçonnage ont augmenté de **61%** pour atteindre 255 millions sur une période de six mois[3].

La vérification en deux étapes et l'authentification à deux facteurs sont utiles, mais peuvent imposer des contraintes supplémentaires à l'utilisateur et ne protègent toujours pas totalement contre les attaques par hameçonnage et les attaques ciblées telles que les « échanges de cartes SIM » pour la vérification par messagerie texte.

La solution

En partenariat avec l'alliance FIDO, nous avons activé la prise en charge des clés d'accès, une solution de rechange aux mots de passe plus simple et plus sûre, qui permet à des milliards de personnes dans le monde de bénéficier d'une technologie à l'épreuve de l'hameçonnage. Avec les clés d'accès, vous n'avez plus besoin de votre mot de passe – vous utilisez votre empreinte digitale, la reconnaissance faciale ou le déverrouillage d'écran pour accéder à votre compte plus facilement et de façon plus sécuritaire.

Au début de l'année 2023, les titulaires de comptes Google personnels ont pu commencer à utiliser des clés d'accès, tout comme les quelque neuf millions de clients Google Workspace et les sites et applis tiers sur Chrome et Android.

Le moyen plus simple et le plus rapide de se connecter

Les clés d'accès sont **4 fois plus simples** à utiliser, puisqu'il n'est pas nécessaire de les mémoriser ou de les taper. Il vous suffit d'utiliser votre empreinte digitale, la reconnaissance faciale ou le déverrouillage d'écran pour vous connecter sur tous vos appareils et toutes vos plateformes[4].

Une sécurité d'accès de nouvelle génération

Les clés d'accès constituent la meilleure protection qui soit contre les menaces telles que l'hameçonnage. Et comme elles sont stockées sur votre appareil local, elles ne peuvent pas être devinées ou réutilisées, ce qui protège vos données contre le piratage.

Votre clé vous appartient

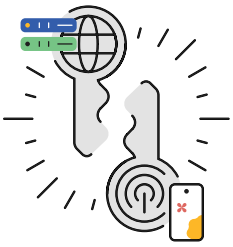
Votre clé d'accès demeure privée sur votre appareil personnel et n'est jamais communiquée à Google ou d'autres partenaires tiers. Il vous suffit d'utiliser votre empreinte digitale, la reconnaissance faciale ou le déverrouillage d'écran pour confirmer que c'est bien vous qui accédez à votre clé privée.

Sécurité accrue avec Google

Version en grands caractères
Version audio
(en anglais seulement)

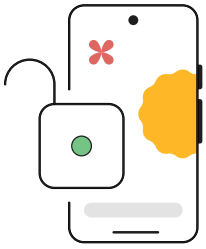
Google

Fonctionnement des clés d'accès

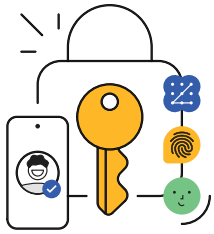


Une clé d'accès se compose de deux parties : une clé publique sur le serveur pour le site Web auquel vous accédez, et une clé privée correspondante sur votre appareil.

Lorsque vous vous connectez, le site Web vérifie que votre clé publique correspond bien à votre clé privée.



Pour vérifier que c'est bien le cas, on vous invite à déverrouiller votre appareil.



Vous pouvez ainsi accéder à votre compte, et votre clé privée et vos données biométriques sont conservées en sécurité sur votre appareil et ne seront jamais communiquées.

Favoriser un écosystème plus sûr

Les clés d'accès au service des entreprises et des gouvernements

Les clés d'accès présentent des avantages considérables pour les utilisateurs en termes de sécurité et de convivialité, et nous sommes heureux d'être le premier grand fournisseur d'infonuagique publique à proposer cette technologie à nos clients, qu'il s'agisse de PME, de grandes entreprises, d'établissements scolaires ou de gouvernements.

Un partenariat pour une connexion plus sûre et sans mots de passe sur Internet

Nous nous associons à des marques pour activer les clés d'accès sur les plateformes Chrome et Android et pour créer des connexions plus faciles et sécurisées pour leurs utilisateurs. Des partenaires des secteurs du commerce électronique, des technologies financières et du voyage, ainsi que d'autres fournisseurs de logiciels, se sont déjà engagés avec nous pour un avenir sans mots de passe, notamment 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal et Yahoo! Japan.

Vers un avenir sans mots de passe

Les clés d'accès nous permettent de faire un grand pas vers l'avenir sans mots de passe auquel nous travaillons depuis plus d'une décennie.

2008 — Lancement du Gestionnaire de mots de passe Google pour des connexions plus faciles et plus sûres.

2011 — Activation de la vérification en deux étapes pour les comptes Google.

2012 — Lancement des clés de sécurité à l'épreuve de l'hameçonnage pour les employés de Google.

2013 — Google devient membre de l'alliance FIDO pour favoriser la création de normes ouvertes favorisant un monde sans mots de passe.

2014 — Google étend l'utilisation des clés de sécurité à l'épreuve du hameçonnage à l'ensemble des utilisateurs.

2017 — Lancement du programme de protection avancée pour les utilisateurs à risque élevé.

2019 — Google étend la prise en charge FIDO aux appareils Android pour la réauthentification sans mot de passe sur les sites Web.

2023 — Activation des clés d'accès pour les comptes Google, les utilisateurs Workspace et les partenaires tiers sur Chrome et Android.

Même si les mots de passe continueront de faire partie de notre vie pendant la transition vers les clés d'accès, nous nous engageons à aider les utilisateurs et les autres acteurs du secteur à franchir le pas et à rendre les connexions plus faciles et plus sûres avec Google.

Sources : 1 - Verizon Data Breach Investigation report (Rapport d'enquête de Verizon sur les violations de données) 2022 | 2 - IBM Cost of Data Breach report (Rapport d'IBM sur le coût des violations de données) 2023 3 - CNBC's Cyber Report (Rapport de CNBC sur la cybersécurité) | 4 - Google Security Blog, May 2023 (Blogue de Google sur la sécurité), mai 2023.