



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

Face à la prolifération des cyberattaques orchestrées par des États et à la multiplication des acteurs malveillants sévissant sur le web, nous redoublons d'efforts pour protéger les personnes, les entreprises et les gouvernements. À cette fin, nous partageons notre expertise, créons les outils dont la société a besoin et faisons avancer la recherche en matière de cybersécurité afin de contribuer à la construction d'un monde plus sûr pour toutes et tous.

Si les mots de passe restent un élément essentiel de la sécurité en ligne, les menaces telles que l'hameçonnage continuent de proliférer. Google est depuis longtemps conscient de ces problèmes et encourage l'utilisation d'outils d'identification tels que la validation en deux étapes, le Gestionnaire de mots de passe de Google, les clés de sécurité et, désormais, les clés d'accès.

L'enjeu

Voilà plus de 60 ans que l'informatique compte sur les mots de passe. Malheureusement, ceux-ci ne parviennent plus à protéger efficacement les données des utilisateurs et des organisations. De plus en plus complexes et sophistiquées, les attaques par hameçonnage profitent des failles de sécurité présentes avec les mots de passe. Par exemple :

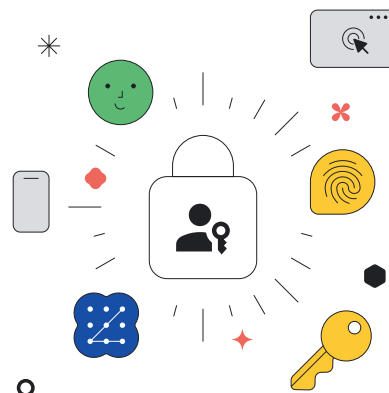
- ✓ En 2021, plus de **60 % des fuites de données** concernaient le vol d'identifiants ou l'hameçonnage¹.
- ✓ En 2022, les fuites de données dues à l'hameçonnage ont coûté **4,91 millions de dollars en moyenne** aux entreprises².
- ✓ En 2022, les attaques par hameçonnage ont augmenté de **61 %** à 255 millions de cas sur une période de six mois³.

Si la validation en deux étapes et la double authentification peuvent aider, elles représentent toutefois une contrainte supplémentaire pour les utilisateurs et restent insuffisantes face aux attaques par hameçonnage et aux attaques ciblées, comme le SIM swapping (ou attaque à la carte SIM) en cas de vérification par SMS.

La solution

En partenariat avec l'Alliance FIDO, nous avons déployé les clés d'accès, une méthode plus simple et plus sûre que les mots de passe, qui met à disposition de plusieurs milliards de personnes dans le monde une technologie résistante à l'hameçonnage. Les clés d'accès remplacent vos mots de passe par une méthode de connexion plus simple et plus sûre qui utilise votre empreinte digitale, votre visage ou le verrouillage de votre écran.

Depuis le début de 2023, les clés d'accès sont disponibles sur les comptes Google personnels, pour les utilisateurs de plus de neuf millions de clients Google Workspace ainsi que sur les sites et applis tiers de Chrome et d'Android.



La méthode d'identification la plus simple et la plus rapide

Comme vous n'avez plus besoin de les mémoriser ni de les saisir, les clés d'accès sont **4 fois plus simples** d'utilisation. Vous n'avez qu'à utiliser votre empreinte digitale, votre visage ou le verrouillage de votre écran pour vous connecter sur tous les appareils et toutes les plateformes⁴.

La sécurité nouvelle génération pour votre compte

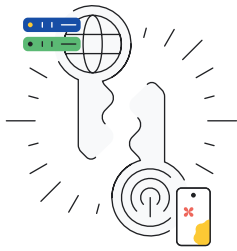
Les clés d'accès offrent le plus haut niveau de protection contre les menaces comme l'hameçonnage. Comme elles sont stockées sur votre appareil, il est impossible de les deviner ou de les réutiliser. Elles contribuent donc à protéger vos informations privées contre les pirates informatiques.

Une identification vraiment personnelle

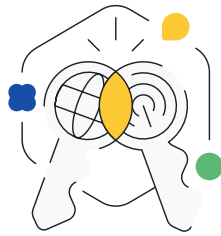
Votre clé d'accès reste privée sur votre appareil personnel. Elle n'est jamais partagée avec Google ni avec des partenaires tiers. Il vous suffit d'utiliser votre empreinte digitale, votre visage ou le verrouillage de votre écran pour prouver que c'est bien vous.



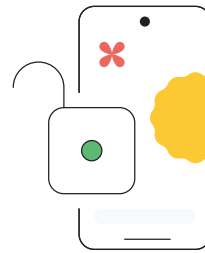
Comment ça marche ?



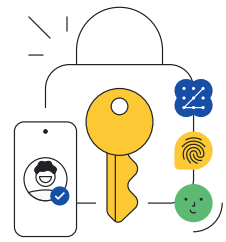
Une clé d'accès se compose de deux éléments : une clé publique stockée sur le serveur du site web auquel vous vous connectez, et une clé privée stockée sur vos appareils.



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



Pour cela, vous devez simplement déverrouiller votre appareil.



Une fois que vous êtes connecté à votre compte, votre clé privée et vos données biométriques sont stockées en toute sécurité sur votre appareil et ne sont jamais partagées.

Pour un écosystème plus sûr

Déployer les clés d'accès en entreprise et au sein des administrations

Les clés d'accès apportent des avantages tangibles en matière de sécurité et d'ergonomie. Nous sommes fiers d'être le premier grand fournisseur de cloud public à proposer cette technologie à ses clients, qu'il s'agisse de PME, de grands groupes, d'universités ou encore d'administrations.

Avancer ensemble vers une connexion sans mots de passe et plus sûre sur le web

En partenariat avec différentes marques, nous avons déployé les clés d'accès sur les plateformes Chrome et Android et proposons ainsi une méthode d'identification plus simple et plus sûre à leurs utilisateurs. De nombreux partenaires issus de secteurs très variés, tels que l'e-commerce, la fintech ou encore les voyages, nous ont rejoint dans cette aventure. Parmi eux, on peut citer 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal et Yahoo! Japan.

Vers la fin des mots de passe

Les clés d'accès nous rapprochent de plus en plus de l'avenir sans mots de passe sur lequel nous travaillons depuis plus de dix ans.

2008	2011	2012	2013	2014	2017	2019	2023
Lancement du Gestionnaire de mots de passe de Google visant à simplifier et à sécuriser les connexions	Adoption de la validation en deux étapes pour les comptes Google	Introduction des clés de sécurité résistantes à l'hameçonnage auprès des salariés de Google	Adhésion à l'Alliance FIDO pour favoriser des normes ouvertes vers un monde sans mots de passe	Élargissement des clés de sécurité résistantes à l'hameçonnage au grand public	Introduction du Programme Protection Avancée (PPA) pour les utilisateurs sensibles	Élargissement de l'adoption des normes FIDO sur Android pour permettre la réauthentification sans mot de passe sur les sites web	Déploiement des clés d'accès sur les comptes Google, les clients Workspace et les partenaires tiers sur Chrome et Android

Durant la période de transition vers la généralisation des clés d'accès, les mots de passe ne vont pas disparaître. Nous nous engageons à aider les utilisateurs et les acteurs du secteur à franchir ce cap pour une identification plus simple et plus sûre avec Google.

Sources: 1 - Rapport d'enquête Verizon sur les fuites de données, 2022 | 2 - Rapport IBM sur les coûts engendrés par les fuites de données, 2023 | 3 - Rapport cyber de CNBC | 4 - Blog sécurité de Google, mai 2023