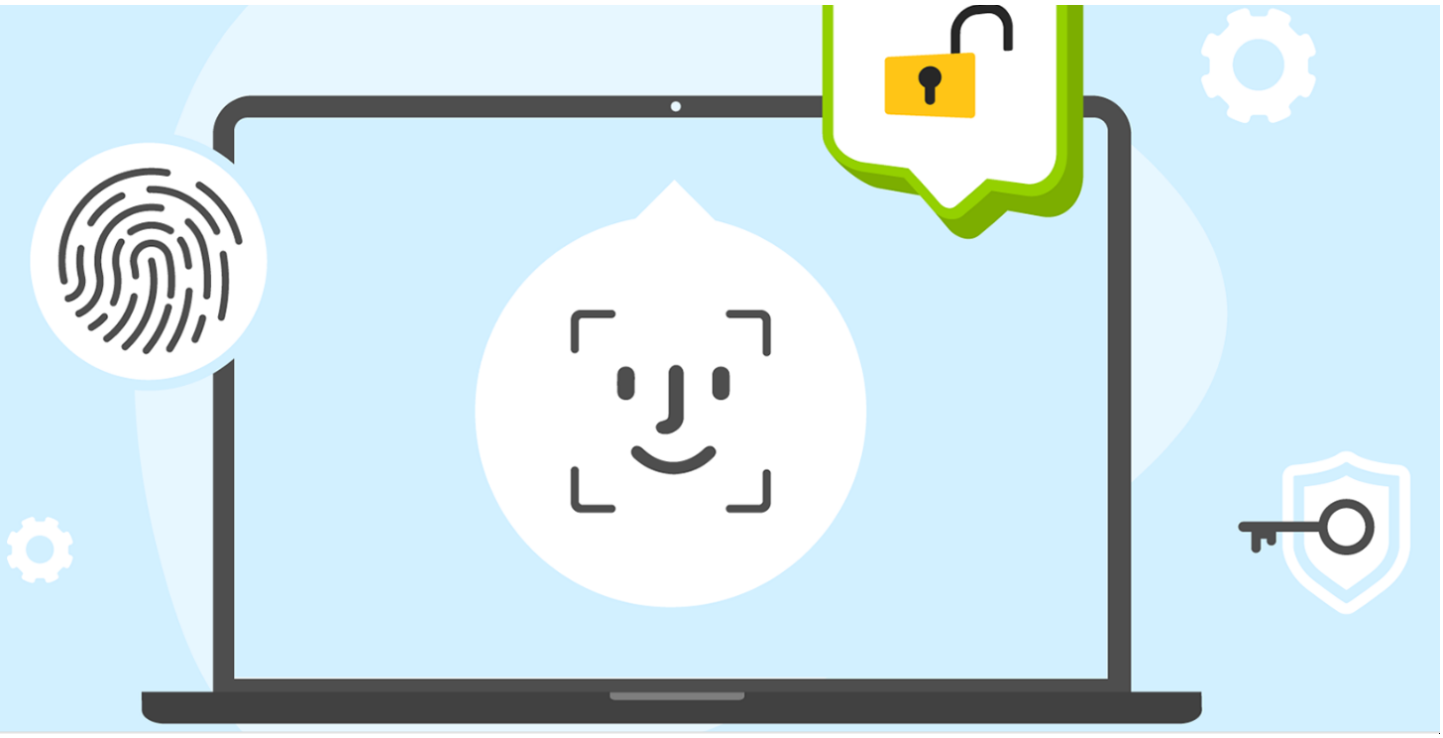
Clés d’accès, c’est quoi?

Ou “Passkeys”

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



Regarder la vidéo d’introduction d’une durée de 2 :43 minutes

Titre : Comment utiliser les Google Passkeys (sécurité renforcée)

Lien YouTube:

https://youtu.be/ht1xAiV6WT4?si=W9MKcr9tgMV6zswf

Référencement de Google :

Résumé :

Google promeut les clés d'accès comme une alternative plus sûre et plus facile d'utilisation aux mots de passe, protégeant les utilisateurs contre l'hameçonnage et les violations de données, et collaborant avec des partenaires pour un avenir sans mot de passe.

- Les mots de passe sont de plus en plus vulnérables aux cyberattaques, notamment l'hameçonnage, causant des pertes financières importantes pour les organisations.
- Les clés d'accès, une solution développée en partenariat avec l'alliance FIDO, offrent une sécurité accrue en étant stockées localement sur l'appareil de l'utilisateur.

- L'utilisation des clés d'accès est simplifiée par l'authentification biométrique (empreinte digitale, reconnaissance faciale).
- Google déploie les clés d'accès pour les comptes Google personnels, Google Workspace et des sites tiers sur Chrome et Android.
- Plusieurs grandes entreprises s'associent à Google pour adopter les clés d'accès, visant un avenir sans mot de passe.
- Les clés d'accès utilisent une paire de clés publique/privée pour l'authentification, la clé privée étant protégée sur l'appareil de l'utilisateur.
- Google travaille sur une transition vers un avenir sans mot de passe depuis plus d'une décennie.

Lien :

https://kstatic.googleusercontent.com/files/a121cdae11bf38d44f5c21a803808d77b59a70384cdc6a4f5a8fff65498d2eb669d01ce8a083e14edf9d814a5a0cdd6e545a9c0cdbc92b1ab21d7a1d9f9b4928

Google Blog sur la sécurité

Synopsis : Rendre l'authentification plus rapide que jamais : clés d'accès vs mots de passe

Lien : https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html

---

Titre : Méthodes d'authentification chez Google

Lien : https ://cloud.google.com/docs/authentication?hl=fr

Titre : Activer la vérification en deux étapes

Lien :
https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en&oco=0

La façon plus sécuritaire
de faire des recherches.

Lien : : https://safety.google/

Titre : Google annonce l'adoption de clés d'identification par plus de 400 millions de comptes

Lien : https://thehackernews.com/2024/05/google-announces-passkeys-adopted-by.html

---

Historique

- Les mots de passe sont utilisés depuis les années 60, mais ils présentent de nombreux inconvénients en matière de sécurité. Ils peuvent être facilement oubliés, volés ou devinés.
- Les clés d'accès ont été développées pour résoudre ces problèmes. Elles sont basées sur des normes ouvertes développées par le World Wide Web Consortium (W3C) et la FIDO Alliance*

*NDLR : La **FIDO (Fast IDentity Online) Alliance** est une organisation créée en 2012 qui vise à promouvoir des normes d'authentification forte et à réduire la dépendance aux mots de passe.*
Elle regroupe des entreprises, des organisations et des institutions qui travaillent ensemble pour développer des solutions d'authentification sécurisées, interopérables et faciles à utiliser.

- Google, Apple et Microsoft ont annoncé leur soutien aux clés d'accès en 2022, ce qui a accéléré leur adoption.

Raisons d'utiliser les clés d'accès

- **Sécurité accrue**: Les clés d'accès sont plus sûres que les mots de passe car elles sont stockées sur votre appareil et ne sont jamais transmises sur Internet. Cela signifie qu'elles ne peuvent pas être interceptées par des pirates.
- **Facilité d'utilisation**: Les clés d'accès sont plus faciles à utiliser que les mots de passe car vous n'avez pas besoin de les mémoriser. Vous pouvez vous connecter à vos comptes en utilisant votre empreinte digitale, votre visage ou un code PIN.
- **Protection contre le phishing**: Les clés d'accès sont résistantes aux attaques de phishing car elles sont liées à un site Web spécifique. Cela signifie que vous ne pouvez pas être amené à saisir votre clé d'accès sur un faux site Web.

Fonctionnement pour les aînés

Les clés d'accès peuvent être particulièrement utiles pour les aînés qui peuvent rencontrer des difficultés à mémoriser des mots de passe complexes.
Voici comment elles fonctionnent :

1. **Création d'une clé d'accès**: Vous pouvez créer une clé d'accès sur votre appareil, comme votre téléphone ou votre ordinateur.
2. **Enregistrement de la clé d'accès**: Vous enregistrez ensuite cette clé d'accès sur les sites Web ou les applications que vous utilisez.
3. **Connexion avec la clé d'accès**: Lorsque vous vous connectez à un site Web ou à une application, vous utilisez votre clé d'accès pour vous authentifier. Cela peut se faire en utilisant votre empreinte digitale, votre visage ou un code PIN.

Conseils pour les aînés

- **Choisissez un appareil de confiance**: Stockez votre clé d'accès sur un appareil que vous contrôlez et que vous protégez avec un code PIN ou un mot de passe fort.
- **Utilisez un gestionnaire de mots de passe**: Un gestionnaire de mots de passe peut vous aider à gérer vos clés d'accès et vos autres informations de connexion.
- **Demandez de l'aide**: Si vous avez des difficultés à utiliser les clés d'accès, demandez de l'aide à un membre de votre famille, à un ami ou à un professionnel de l'informatique.

Bien que les clés d'accès offrent une sécurité accrue et une meilleure expérience utilisateur, elles sont encore une technologie relativement nouvelle.
La plupart des sites Web et des applications continuent de prendre en charge les mots de passe traditionnels.

Voici quelques points à considérer :

- **Adoption progressive**: L'adoption des clés d'accès se fait progressivement.
  De plus en plus de sites Web et d'applications les prennent en charge, mais il faudra du temps avant qu'elles ne remplacent complètement les mots de passe.
- **Choix personnel**: Vous avez le choix d'utiliser les clés d'accès ou de continuer à utiliser les mots de passe.
  Si vous êtes à l'aise avec les mots de passe et que vous les gérez de manière sécurisée (en utilisant un gestionnaire de mots de passe, par exemple), il n'y a aucune obligation de passer aux clés d'accès.
- **Avantages de la transition**: Cependant, les clés d'accès offrent des avantages significatifs en termes de sécurité et de facilité d'utilisation.
  Si vous êtes préoccupé par la sécurité de vos comptes en ligne ou si vous trouvez les mots de passe difficiles à gérer, les clés d'accès peuvent être une excellente option pour vous.

En fin de compte, la décision d'utiliser ou non les clés d'accès vous appartient.

C'est une technologie encore assez récente, et les données sur son utilisation sont encore en train d'être collectées et analysées.

Cependant, voici ce que nous pouvons observer :

- **Croissance rapide**: L'adoption des clés d'accès est en forte croissance.
  Le soutien majeur de Google, Apple et Microsoft en 2022 a donné un élan important à cette technologie.
  De plus en plus d'utilisateurs découvrent les avantages des clés d'accès en termes de sécurité et de facilité d'utilisation.
- **Intérêt croissant**: L'intérêt pour les clés d'accès est grandissant, tant du côté des utilisateurs que des entreprises.
  Les entreprises cherchent des solutions pour renforcer la sécurité de leurs systèmes et protéger leurs clients contre les cyberattaques.
  Les clés d'accès offrent une réponse efficace à ces préoccupations.
- **Facteurs d'adoption**: Plusieurs facteurs influencent l'adoption des clés d'accès, notamment la sensibilisation du public, la disponibilité de solutions compatibles, et la facilité d'utilisation.
  Au fur et à mesure que la technologie se développe et se démocratise, on peut s'attendre à une adoption plus large.

Quelques indicateurs positifs :

- **Intégration dans les systèmes d'exploitation**: Les clés d'accès sont intégrées dans les derniers systèmes d'exploitation d'Apple, de Google et de Microsoft, ce qui les rend accessibles à un large public.
- **Support des navigateurs web**: Les principaux navigateurs web, comme Chrome, Safari et Edge, prennent en charge les clés d'accès.
- **Adoption par les grandes entreprises**: De nombreuses grandes entreprises, comme Google, Microsoft, eBay et PayPal, ont déjà adopté les clés d'accès pour leurs services.

En résumé, bien que nous ne disposions pas de chiffres précis sur l'adoption mondiale des clés d'accès, les indicateurs montrent une croissance rapide et un intérêt croissant pour cette technologie.
Il est probable que l'adoption des clés d'accès continue de s'accélérer dans les années à venir.

Il est important de bien comprendre les nuances entre ces différents moyens d'authentification. Voici un résumé des différences :

Mot de passe:

- **Définition:** Une séquence secrète de caractères (lettres, chiffres, symboles) utilisée pour vérifier l'identité d'un utilisateur.
- **Fonctionnement:** Vous créez et mémorisez un mot de passe, puis le saisissez pour accéder à vos comptes.
- **Faiblesses:**
    - Facile à oublier ou à deviner s'il est trop simple.
    - Peut-être volé lors de fuites de données ou par hameçonnage (phishing).
    - Doit être unique pour chaque compte pour une sécurité optimale, ce qui rend la gestion difficile.

Clé d'accès:

- **Définition:** Une méthode d'authentification plus sécurisée qui remplace les mots de passe. Elle est unique à chaque site web et liée à votre appareil.
- **Fonctionnement:** Générée et stockée sur votre appareil (téléphone, ordinateur), elle utilise la cryptographie pour vérifier votre identité sans transmettre d'informations secrètes sur Internet.
- **Avantages:**
    - Plus sûre que les mots de passe car elle ne peut pas être volée ou devinée.

- Plus facile à utiliser : authentification via empreinte digitale, reconnaissance faciale ou code PIN.
- Protège contre le phishing car elle est liée à un site web spécifique.

Authentification biométrique:

- **Définition:** Utilise vos caractéristiques biologiques uniques (empreinte digitale, visage, iris) pour vous identifier.
- **Fonctionnement:** Votre appareil scanne votre caractéristique biométrique et la compare à une donnée enregistrée pour vous authentifier.
- **Applications:** Utilisée pour déverrouiller des appareils, effectuer des paiements, accéder à des applications, et peut être combinée avec des clés d'accès pour une sécurité renforcée.

En résumé :

- La clé d'accès est une **alternative plus sûre aux mots de passe**.
- L'authentification biométrique est une **technologie** qui peut être **utilisée seule** (pour déverrouiller votre téléphone, par exemple) ou **en combinaison avec une clé d'accès** pour une authentification plus forte.

1) Types / modèles de clés d'accès:

Il peut y avoir un peu de confusion sur ce point, car le terme "clé d'accès" peut faire penser à un objet physique.
En réalité, il existe deux principales façons de "stocker" une clé d'accès :

- **Clé d'accès intégrée à votre appareil:** C'est la forme la plus courante.
  La clé est générée et stockée de manière sécurisée dans votre appareil (téléphone, ordinateur, tablette).
  Vous n'avez rien de physique à manipuler.
- **Clé d'accès sur une clé de sécurité physique:** Il existe aussi des clés d'accès qui peuvent être stockées sur un petit appareil physique, comme une clé USB ou un jeton NFC.
  Ces clés de sécurité se branchent sur votre appareil ou communiquent sans fil pour vous authentifier.
  Elles sont particulièrement utiles si vous devez vous connecter à des comptes sur des ordinateurs partagés ou non sécurisés.

Exemples de clés de sécurité physiques:

- Yubico YubiKey
- Google Titan Security Key

2) Clé physique (USB) vs. Clé d'accès:

Votre question est très pertinente ! Il est important de distinguer les deux :

- **Clé USB (stockage de données):** C'est un support de stockage physique que vous utilisez pour transporter des fichiers.
- **Clé de sécurité physique (clé d'accès):** C'est un appareil physique qui stocke une clé d'accès pour l'authentification.

Facilité d'utilisation:

Vous avez raison également sur ce point.
L'un des grands avantages des clés d'accès est qu'elles simplifient la connexion.

- **Pas besoin de mémoriser des mots de passe complexes**: La clé d'accès est stockée sur votre appareil et vous vous authentifiez avec votre empreinte digitale, votre visage ou un code PIN.
- **Processus plus rapide et plus fluide**: Plus besoin de taper un mot de passe, ce qui est particulièrement pratique sur les appareils mobiles.

Note : Il n'est pas nécessaire d'utiliser un gestionnaire de mots de passe payant comme Dashlane pour accéder aux clés d'accès virtuelles.

Voici pourquoi:

- **Fonctionnalité intégrée**: Les systèmes d'exploitation modernes (comme iOS, Android, Windows et MacOs) intègrent déjà des gestionnaires de clés d'accès.
  Vos clés d'accès sont stockées de manière sécurisée dans votre appareil et synchronisées entre vos appareils connectés au même compte (ex: compte Google ou Apple).
- **Navigateurs web**: Les navigateurs web comme Chrome, Edge et Safari incluent également des gestionnaires de clés d'accès.
- **Options gratuites**: Il existe des gestionnaires de mots de passe gratuits qui prennent en charge les clés d'accès, comme **Bitwarden** ou **1Password** (version limitée).

Quand un gestionnaire de mots de passe payant peut être utile:

- **Fonctionnalités avancées**: Si vous recherchez des fonctionnalités supplémentaires comme le partage sécurisé de mots de passe, la surveillance du dark web, ou un VPN, un gestionnaire de mots de passe payant peut être intéressant.
- **Support client prioritaire**: Les versions payantes offrent généralement un meilleur support client.
- **Préférences personnelles**: Vous pourriez préférer l'interface ou les fonctionnalités d'un gestionnaire de mots de passe payant spécifique.

En résumé:

- Vous pouvez utiliser les clés d'accès sans payer pour un gestionnaire de mots de passe.
- Les gestionnaires de mots de passe gratuits offrent une alternative valable.
- Les gestionnaires de mots de passe payants offrent des fonctionnalités supplémentaires pour ceux qui en ont besoin.

Types de clés d'accès numériques pour Google

Type de clé	Description	Avantages	Inconvénients
Mot de passe	Code secret choisi par l'utilisateur	Facile à utiliser	Peut être oublié ou piraté
Authentification à deux facteurs (2FA)	Combine le mot de passe avec un second élément de vérification	Plus sécurisé que le mot de passe seul	Nécessite un appareil supplémentaire
Google Prompt	Notification sur smartphone pour confirmer la connexion	Très simple d'utilisation	Requiert un smartphone
Code par SMS	Code envoyé par message texte	Familier pour beaucoup d'utilisateurs	Dépend de la réception du téléphone
Application d'authentification	Génère des codes temporaires sur smartphone	Fonctionne sans connexion internet	Nécessite l'installation d'une application
Clé de sécurité physique	Petit appareil USB à brancher lors de la connexion	Très sécurisé	Coût supplémentaire, risque de perte

---

<u>Référencement vidéo YouTube :</u>

(Accéder à YouTube et taper dans la barre de recherche, pour en ouvrir plusieurs)

Clé d'accès en français;

Clé d’accès Google

Titre : Comment utiliser les Google Passkeys (sécurité renforcée)

Lien YouTube : https://youtu.be/ht1xAiV6WT4?si=W9MKcr9tgMV6zswf

Titre: Qu’est-ce qu’une clé d’accès ? Expliqué en 2 minutes

Lien: https://youtu.be/O2UiBz2GJYA?si=lJEQs2OPp2T2GVg5

Conclusion :

1. Résumez les points clés :

- L'importance des clés d'accès pour la sécurité en ligne

- La simplicité d'utilisation par rapport aux mots de passe traditionnels

- Les avantages pour les aînés (moins à mémoriser, plus sécurisé)

2. Encouragez l'adoption progressive :

"Commencez par une seule clé d'accès, par exemple pour votre compte Google.
Petit à petit, vous verrez comme c'est simple et sécurisé !"

3. Rappelez le soutien disponible :

"N'oubliez pas, notre club CIVBDL est là pour vous aider.
Nous organiserons des sessions pratiques et un support continu."

4. Terminez sur une note positive :

"Ensemble, nous pouvons maîtriser ces nouvelles technologies et profiter d'une expérience en ligne plus sûre et plus agréable."

5. Ajoutez une touche personnelle :

"Chers membres du CIVBDL, votre curiosité et votre volonté d'apprendre sont inspirantes.
Continuons à explorer le monde numérique ensemble !"

Venez avec vos questions et votre enthousiasme !"

7. Remerciements :

"Merci de votre attention et de votre participation active.
C'est un plaisir de partager ces connaissances avec vous."

Cette conclusion résume l'essentiel, encourage l'action, offre du soutien, et termine sur une note chaleureuse et personnelle, adaptée à votre rôle de responsable du club et à votre public d'aînés.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
Rencontre Zoom du 20241016
"C'est ensemble qu'on avance"

Image créée par ideogram.ai