FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

Les clés d'accès: un atout pour sécuriser nos comptes en ligne

Préparé par: Denis Bergeron

23 Novembre 2023

Contenu

1. Présentation et fonctionnement des clés d'accès
2. Clés d'accès versus mots de passe
3. Sauvegarde de ses clés d'accès
4. Déploiement: où en sommes-nous ?
5. Trois exemples de création d’une clé d’accès
6. Réponses à quelques questions fréquentes
7. Deux exemples de connexion avec une clé d’accès
8. Conclusion

Présentation et fonctionnement des clés d'accès

- Terme anglais: « **Passkey** ».
- L’appellation « **clé d’identification** » est aussi fréquemment rencontrée en français.
- Les clés d'accès permettent de créer ou de se connecter rapidement à un compte (ou une application), parfois en une seule étape.
- Remplace les connexions nécessitant un nom d’utilisateur avec un mot de passe et, dans certains cas, élimine le recours à la double authentification.

Logo des clés d’accès

Présentation et fonctionnement des clés d'accès

- Cette méthode d'authentification est supportée désormais par tous les acteurs majeurs de l'industrie regroupés au sein de l'Alliance **fido** (**f**ast **id**entity **o**nline) dont l'objectif est de définir des standards d'authentification plus sécuritaires que ceux utilisant des mots de passe.

- L'Alliance **fido** regroupe notamment Apple, Google, Microsoft, Meta, 1Password, Bitwarden, Dashlane, eBay, Amazon, PayPal, American Express, etc.

- Le site web de fidoalliance fournit des informations détaillées sur les clés d'accès.

Présentation et fonctionnement des clés d'accès

- **Fonctionnement d’une clé d'accès:**
  - **C’est un identifiant de connexion** à un compte ou à une application, mais qui ne comporte aucun mot de passe.
  - **Nécessite l’utilisation d’un appareil authentificateur** (téléphone, tablette, ordi…) lors de la création du compte ou lorsque vous vous connectez à un compte existant au moyen de cette méthode.
  - **Lors de la première connexion**, l’authentificateur crée une paire de clés cryptographiques mathématiquement liées.
  - **Une clé cryptographique c’est quoi ???**…
    - C’est une longue série de caractères correspondant à un algorithme d’encodage.
  - **Cette paire de clés comprend** une clé privée (secrète) qui est sauvegardée dans l’appareil authentificateur et une clé publique qui est transmise au service en ligne auquel vous voulez vous connecter.

Présentation et fonctionnement des clés d'accès

Fonctionnement d’une clé d'accès:

- **Lorsqu’une demande de connexion est envoyée au site web**, celui-ci transmets un « défi » (données encodées) à l’authentificateur. Seulement la clé privée est en mesure de résoudre le défi (décoder les données) et ainsi retourner une réponse (ce qui équivaut à une signature). Le serveur vérifie la signature avec la clé publique et peut conclure ou non à l’authenticité de la demande de connexion.

- **L’utilisateur doit également prouver** qu’il est l’utilisateur légitime de l’appareil et approuver la demande de connexion en s’authentifiant par biométrie ou en saisissant le code de déverrouillage de l’appareil authentificateur (important d’avoir un code de verrouillage robuste !)

Présentation et fonctionnement des clés d'accès

- **Appareils avec lesquels vous pouvez créer des clés d'accès**:
  - Ordinateurs portatifs ou de bureau fonctionnant sous **Windows 10, macOS Ventura ou ChromeOS 109** (ou des versions ultérieures)

  - Clés de sécurité matérielles (ex: clé Yubikey) compatible avec le protocole **FIDO2**

  - Appareils mobiles fonctionnant sous **iOS16 ou Android 9** (ou des versions ultérieures)

  - De plus, les appareils doivent disposer d'un navigateur compatible: **Chrome 109, Safari 16, Edge 109**(ou des versions ultérieures), ou encore **Firefox et Brave** avec un appareil utilisant iOS et Android.
    Pour plus de détails, vois le site web passkeys.io

Clés d'accès vs mots de passe

- Parce qu'elles sont jugées plus sécuritaires, l'utilisation de clés d'accès pour accéder à nos applications et comptes en ligne est appelée à remplacer **progressivement** l'authentification par mot de passe au cours des prochaines années.

- Pourquoi sont-elles jugées plus sécuritaires ?

  - Les clés d'accès sont faciles à utiliser car vous n'avez pas de mot de passe à mémoriser. Quand vous vous connectez à votre compte, vous n'avez qu'à confirmer votre identité en déverrouillant votre appareil par biométrie ou en saisissant son code de déverrouillage.

  - De nombreuse personnes utilisent le même mot de passe pour plusieurs de leurs comptes, de sorte que lorsqu'un de ces comptes est compromis à la suite d'une fuite de données, tous les autres comptes utilisant ce mot de passe deviennent à risque. **Les clés d'accès quant à elles sont spécifiques à chacun de vos comptes.**

Clés d'accès vs mots de passe

- De nombreuse personnes choisissent de mots de passe « faibles » (123456 est encore le mot de passe le plus utilisé au monde!). Cependant, vous ne pouvez pas créer ou choisir une clé d'accès « faible ». Les clé d'accès sont créées par votre appareil et sont « robustes » par défaut. Et contrairement à un mot de passe, **les clés d'accès ne peuvent pas être lues ou « devinées » par un fraudeur**.

- Les clés d'accès ne peuvent pas être subtilisées lorsque vous êtes l'objet d'une tentative d'hameçonnage. La clé privé ne quitte jamais votre appareil et **elle peut se connecter uniquement au site web pour lequel elle a été créée**.

- Une fois en possession de votre mot de passe et de votre nom d'utilisateur, une fraudeur peut accéder à votre compte à partir d'un appareil qui ne vous appartient pas. Pour leur part, **les clés d'accès sont utilisables uniquement à partir de vos appareils ou d'un appareil préalablement autorisé**.

- Même si la clé publique associée à votre compte est « dérobée » lors d'une fuite de données, elle ne sera d'aucune utilité aux fraudeurs car ils ne connaissent pas la clé privée qui lui est associée et celle-ci ne peut pas être « devinée » ou déduite à partir de la clé publique.

Source: canva.com

Sauvegarde de ses clés d'accès

- Les clés d’accès peuvent être conservées dans l’appareil utilisé pour les créer.
- Tout comme pour les mots de passe, les clés d'accès peuvent être synchronisées entre tous vos appareils reliés entre eux par un service de cloud.
- Pour les appareils reliés à un même compte Apple, le trousseau iCloud peut être utilisé pour accéder à vos clés à partir de n’importe lequel de vos appareils.

- Pour les appareils fonctionnant sous Android et reliés à un même compte Google, il est possible d’accéder à ses clé d'accès avec tous ses appareils en sauvegardant ses clés dans le gestionnaire de mots de passe Google (ou Google Chrome).

- Il est possible également de sauvegarder ses clés dans la voûte d’un autre gestionnaire de mots de passe. Plusieurs d’entre eux prennent en charge ces clés actuellement et plusieurs autres le feront prochainement.

Déploiement: où en sommes-nous ?

- L'authentification avec clé d'accès est désormais disponible pour accéder aux comptes suivants:
  - **Apple** (prérequis: iOS 17 et macOS Sonoma, voir l'article de 9to5Mac),
  - **Google** (méthode par défaut depuis octobre),
  - **Microsoft**
  - **PayPal**
  - **Amazon**
  - **Adobe**
  - **Shopify**
  - Pour sa part, la messagerie **WhatsApp** de Meta a annoncé le déploiement de l'authentification avec clé d'accès pour les appareils fonctionnant sous Android (01net.com, 17 octobre 2023).
  - Une liste plus complète est disponible à passkeys.io

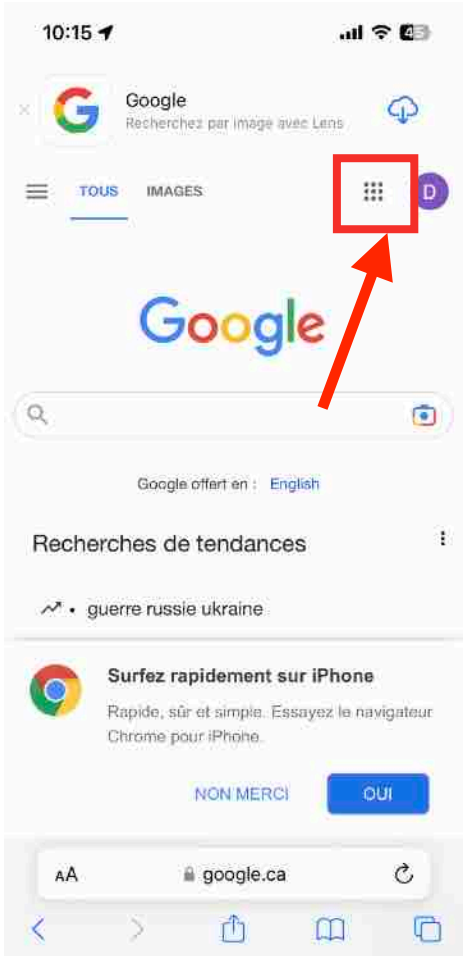
- Aux États Unis: outre les entreprises qui précèdent, Best Buy, eBay et Home Depot, entre autres, acceptent également les clés d'accès.

Déploiement: où en sommes-nous ?

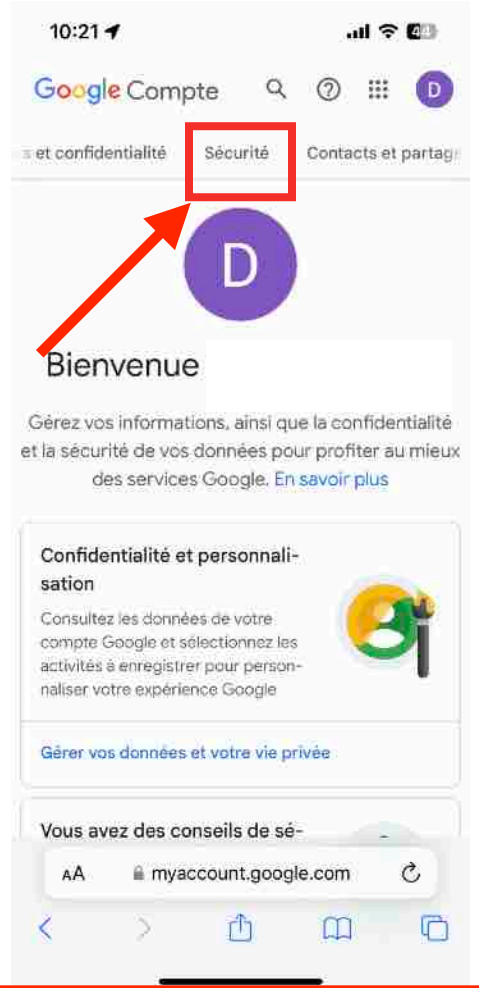
- Depuis l'arrivée de **iOS 17 et Android 14**, il est aussi possible d'utiliser si on le désire un gestionnaire de mots de passe tiers pour conserver et gérer l'utilisation de nos clés d'accès. Il n'est donc plus essentiel d'utiliser le trousseau iCloud d'Apple ou le gestionnaire de mots de passe Google pour cette tâche.

- Exemples de gestionnaires de mots de passe permettant de conserver et d'utiliser nos clés d'accès pour accéder à un de nos comptes:
  - **1Password**: indique en plus, parmi nos comptes, ceux acceptant l'authentifications avec clé d'accès.
  - **Dashlane**: offre en plus la possibilité d'utiliser une clé d'accès pour accéder à sa voûte.
  - **Bitwarden**: fonctionnalité disponible en utilisant l'extension Bitwarden de votre navigateur.
  - **Keeper**
  - **LastPass**
  - **NordPass**

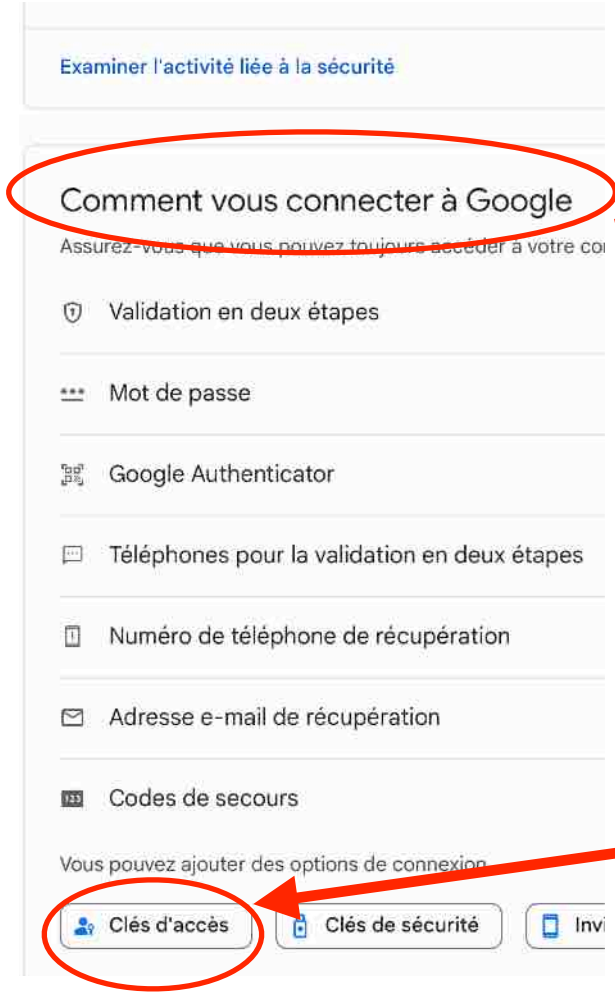
Google - création d'une clé d'accès



1. Accéder à votre compte, cliquer sur le damier et choisir l'application « Compte »



2. Dans l'application « Compte », choisir l'onglet « Sécurité »



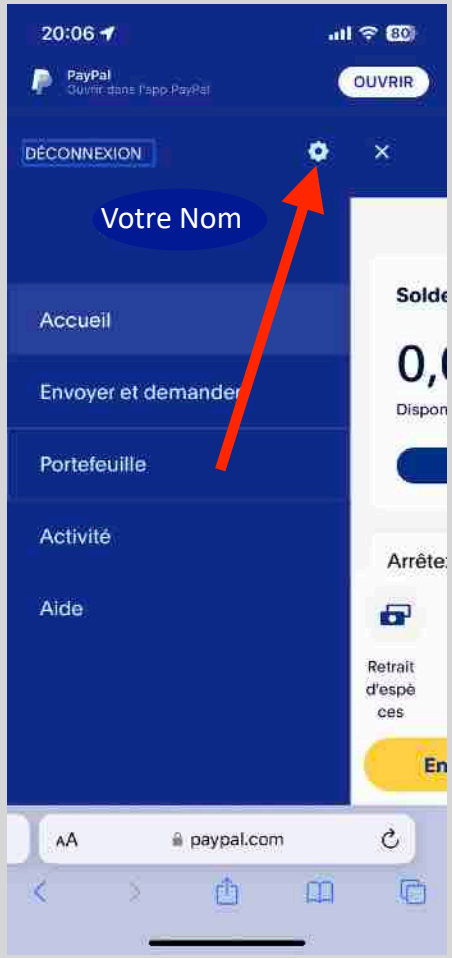
3. Dérouler la nouvelle page vers le bas jusqu'à la rubrique « Comment vous connecter à Google », cliquer sur « Clé d'accès » et suivre les instructions.

Trois exemples de création d'une clé d'accès

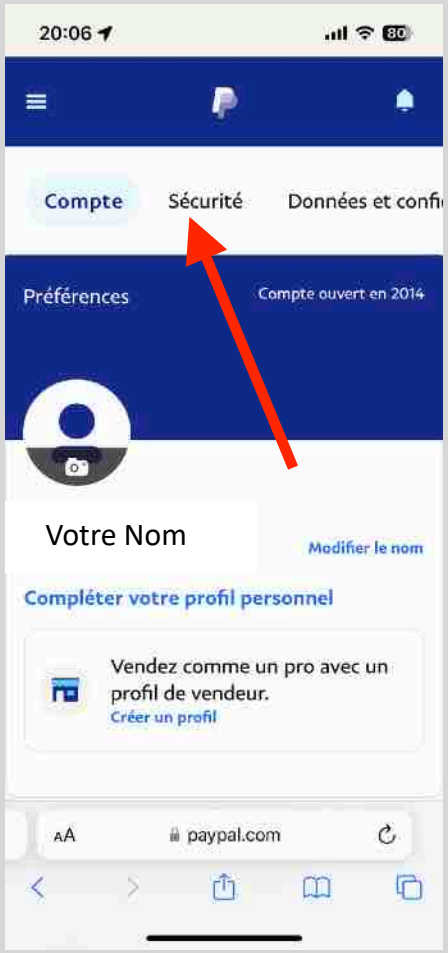
Procédure pour créer votre clé d'accès permettant d'accéder à votre compte Google

- Depuis octobre, l'authentification à l'aide d'une clé d'accès est la méthode d'authentification par défaut pour accéder à son compte Google.
- Avec votre appareil mobile, accéder à votre compte Google en tapant google.ca et en utilisant votre méthode d'authentification habituelle.
- Cliquer sur le petit damier dans le coin supérieur droit de l'écran, sélectionner l'application « Compte » puis choisir l'onglet « Sécurité » dans le menu situé à la gauche ou au haut de l'écran.
- Une nouvelle page s'affichera. Dérouler celle-ci jusqu'à la rubrique « Comment vous connecter à Google »: au bas de la rubrique, Google vous offre d'autres options pour vous connecter, dont la méthode par « clé d'accès ». Sélectionner cette option et suivre simplement les instructions.
- Google n'exige plus la double authentification lorsque vous vous connectez à votre compte avec une clé d'accès, estimant que le déverrouillage de votre appareil par une méthode biométrique ou avec votre code confirme votre identité.
- Cet article de 01net du 14 octobre 2023 explique plus en détail les différentes étapes à suivre.

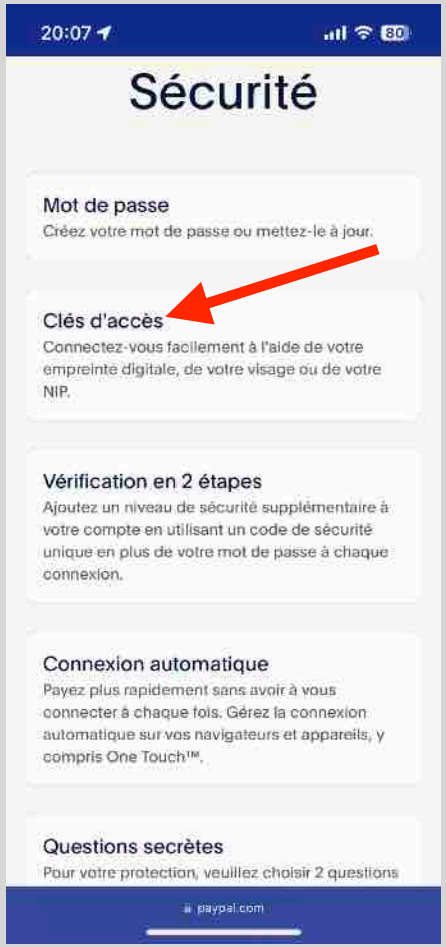
PayPal - création d'une clé d'accès



1

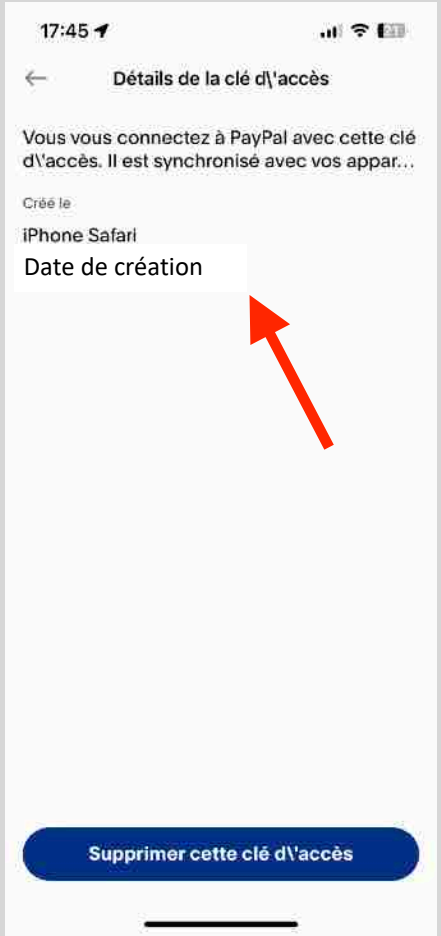


2



3

4



5

Trois exemples de création d'une clé d'accès

- **Procédure pour créer votre clé d'accès permettant d'accéder à votre compte PayPal**

  - Avec votre appareil mobile, accéder à votre compte PayPal en tapant paypal.com et en utilisant votre méthode d'authentification habituelle.

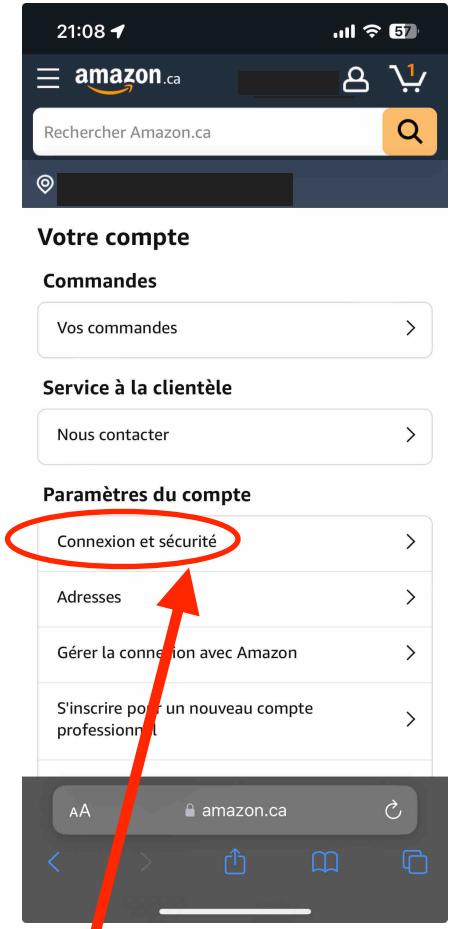
  - Cliquer sur la roue dentelée dans le coin supérieur droit de l'écran, sélectionner l'onglet « Sécurité » puis choisir la rubrique « Clés d'accès » sur la nouvelle page qui s'affiche. Suivre les instructions pour créer votre clé.

  - Contrairement à Google, PayPal continue d'exiger la double authentification lorsque vous utilisez un clé d'accès.

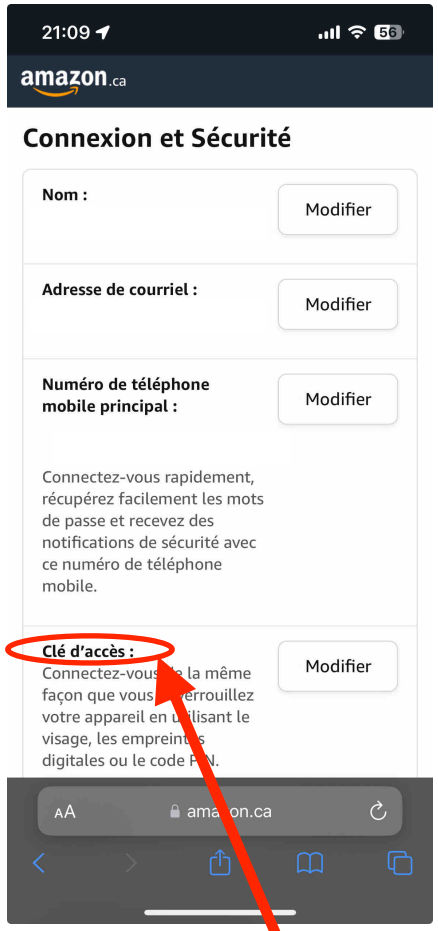
  - Si désiré, vous pouvez en tout temps supprimer votre clé d'accès et en créer une autre.

Amazon - création d'une clé d'accès

1. Accéder à votre compte, taper sur votre nom et à la rubrique « Votre Compte » sélectionner « Tout afficher »



2. À la nouvelle page affichée, choisir l'onglet « Connexion et sécurité »



3. Sélectionner la rubrique « Clé d'accès » et suivre les instructions.

Trois exemples de création d'une clé d'accès

- **<u>Procédure pour créer votre clé d'accès permettant d'accéder à votre compte Amazon</u>**

  - Avec votre appareil mobile, accéder à votre compte Amazon en tapant Amazon.ca et en utilisant votre méthode d'authentification habituelle.

  - Sélectionner la rubrique « Comptes et listes » ou « Compte » dans la partie supérieure de l'écran, sélectionner l'onglet « Votre compte », choisir ensuite la rubrique « Ouverture de session et sécurité » (ou « Connexion et sécurité ») et enfin aller à la rubrique/page « Clé d'accès ». Suivre les instructions pour créer votre clé.

  - Si vous aviez déjà activé la double authentification pour votre compte, elle continuera de s'appliquer lorsque vous vous connecterez avec votre clé d'accès.

  - Cet article de 01net du 19 octobre 2023 explique en détail les différentes étapes à suivre.

Quelques questions concernant les clés d'accès

- **Qu'arrive-t-il en cas de perte de l'appareil utilisé pour générer et conserver une clé d'accès ?**

  - Si vous utilisez le trousseau d'Apple ou le gestionnaire de mots de passe Google pour stocker vos clés, vous pouvez continuer à y avoir accès en vous authentifiant avec un de vos autres appareils utilisant le même écosystème. Si vous utilisez un autre gestionnaire comme par exemple 1Password ou Dashlane, vos clés sont conservées dans votre voûte et vous pouvez donc y accéder avec un autre appareil (et cela même si vos appareils ne font pas tous partie du même écosystème d'entreprise).

  - Si vous ne possédez pas d'autre appareil, si vous n'utilisez pas un gestionnaire de mots de passe pour conserver vos clés ou encore si vous choisissez de ne pas synchroniser vos clés via un service de cloud, vous pouvez suivre la procédure de récupération de votre accès spécifique à ce compte ou vous connecter avec une autre méthode d'authentification s'il y a lieu (par exemple avec un mot de passe si vous en avez un encore un).

Quelques questions concernant les clés d'accès

- **Peut-on supprimer ou remplacer une clé d'accès à un compte, par exemple à la suite du vol ou de la perte de l'appareil qui stockait cette clé?**
  - Oui. Il suffit de se connecter au compte en question, de vous rendre dans les paramètres ou les réglages de celui-ci et de sélectionner l'option permettant de supprimer la clé d'accès. Vous aurez alors la possibilité d'en créer une nouvelle ou, sinon, il faut vous assurer qu'une autre méthode d'authentification à ce compte (avec un mot de passe par exemple) soit activée.

- **Une même personne peut-elle avoir plus d'une clé d'accès pour un même compte ?**
  - Normalement oui, mais il peut y avoir des restrictions. Par exemple, vous pouvez créer plus d'une clé pour accéder à votre compte Amazon, mais elles ne peuvent pas être sauvegardées dans le même appareil ou encore dans le même compte de gestion de vos mots de passe.

Quelques questions concernant les clés d'accès

Comment procéder si je partage un compte avec une autre personne ? Puis-je partager une clé d'accès avec cette autre personne ?

- **Chaque personne peut choisir de créer sa propre d'accès** pour accéder au compte partagé et la sauvegarder dans son propre appareil ou dans son propre gestionnaire de mots de passe.
- Si vous utilisez le trousseau d'Apple pour stocker vos clés, vous pouvez aussi partager une clé avec une autre personne inscrite dans vos contacts en utilisant AirDrop, ou même partager cette clé avec un groupe de proches et d'amis.
- Si vous utilisez une autre plateforme de stockage, une vérification est nécessaire car les pratiques peuvent varier d'un gestionnaire à l'autre.

Y-aura-t-il encore des mots de passe pour mes comptes utilisant l'authentification avec clés d'accès ?

- La possibilité de se connecter avec un mot de passe pourrait ne plus être offerte lorsque l'utilisation des clés d'accès se sera généralisée. Toutefois, pendant la période transitoire qui s'amorce, les sites web peuvent continuer d'offrir la possibilité de se connecter avec un mot de passe tout en vous proposant ou non de vous connecter par défaut avec votre clé d'accès.
  Voir ces articles de 1password et de payPal.

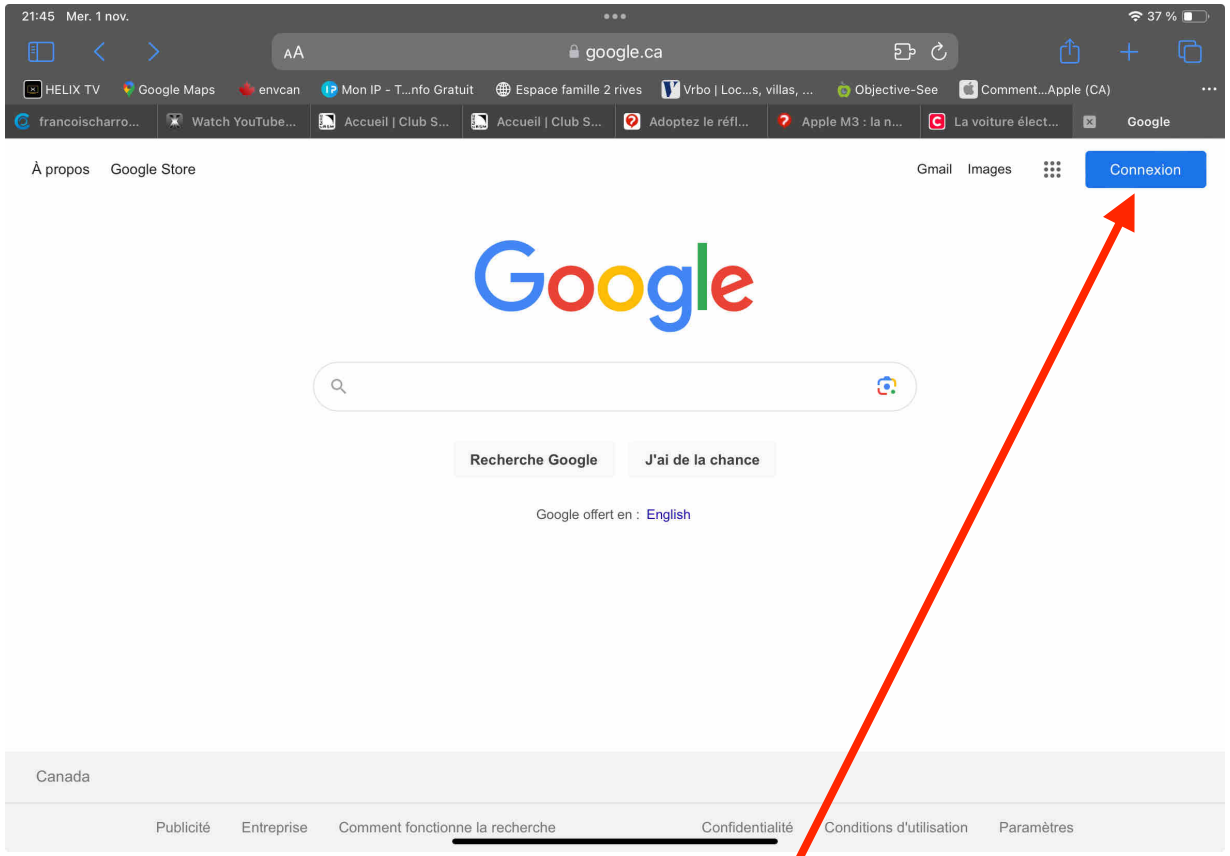
Quelques questions concernant les clés d'accès

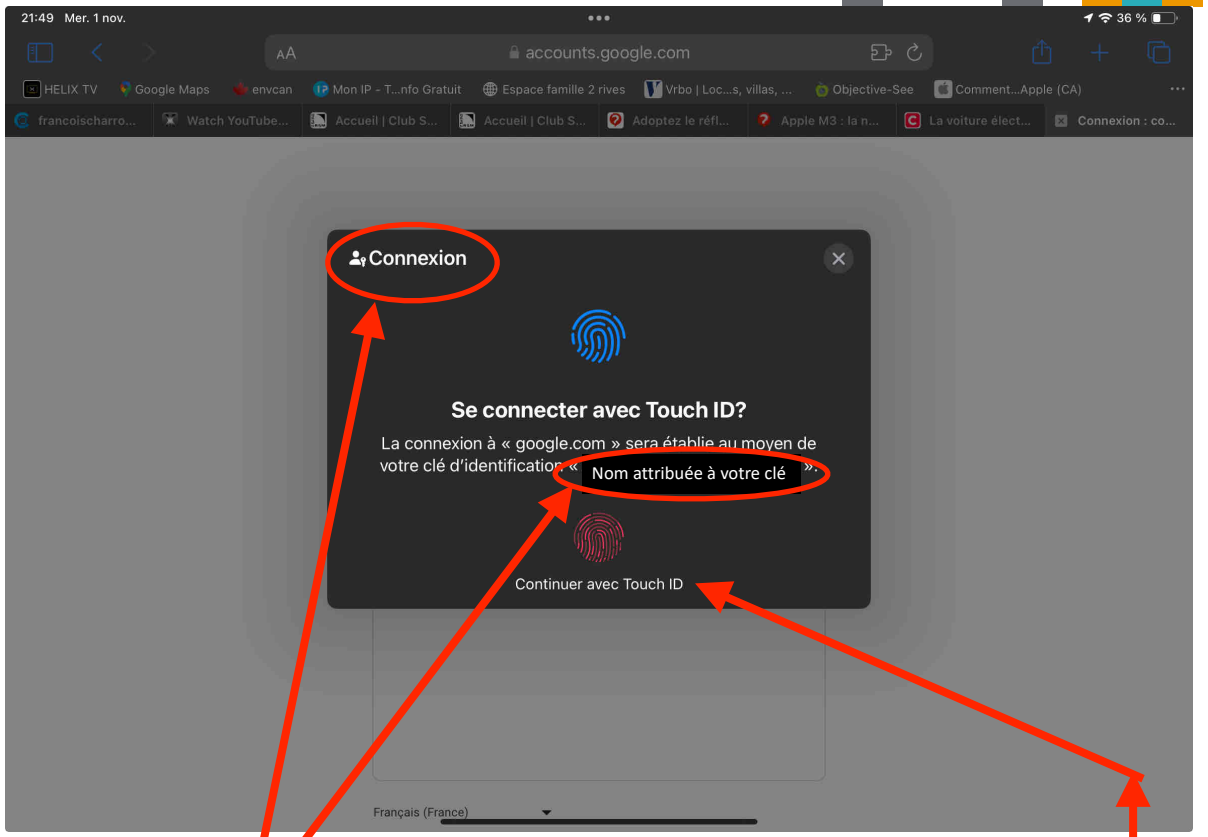
A-t-on besoin d’une connexion Bluetooth pour utiliser une clé d’accès ?

- Normalement non. Toutefois, le Bluetooth peut être requis si vous créez une clé d'accès à l'aide de l'une des solutions intégrées à Windows, iOS, macOS, Chrome ou Android - et que vous devez ensuite utiliser cette clé d'accès à partir d'un appareil qui se trouve dans l'écosystème d'une autre entreprise.

  Exemple: vous voulez vous connecter à un de vos comptes avec un ordinateur Windows appartenant à vous-même à une autre personne et la clé d’accès est sauvegardée dans votre iPhone. Dans un tel cas, le site web transmettra à l’ordinateur un code QR que vous pourrez lire avec votre téléphone. Le bluetooth est alors utilisé pour établir une connexion sécuritaire entre les 2 appareils.

Deux exemples d'utilisation d'une clé d'accès - google.ca





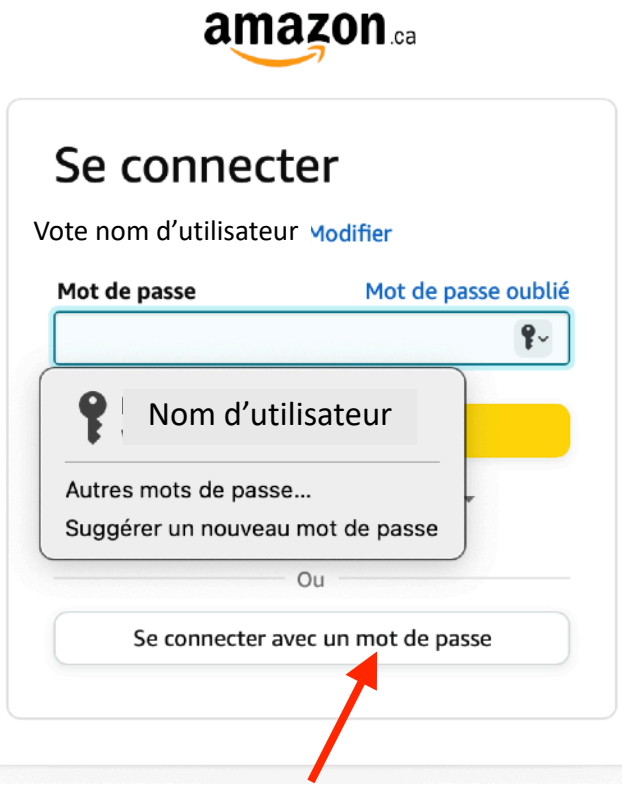
1: Allez à google.ca, sélectionnez le bouton de connexion à votre compte et saisir votre nom d'utilisateur lorsque demandé.

2: Le logo de connexion avec une clé d'accès s'affichera avec le nom attribuée à votre clé (votre nom d'utilisateur par exemple). Vous n'aurez qu'à autoriser la connexion en déverrouillant votre appareil de la manière habituelle.

Deux exemples d'utilisation d'une clé d'accès - amazon.ca

1: nom d'utilisateur

Sur la page de connexion à votre compte, entrer d'abord votre nom d'utilisateur



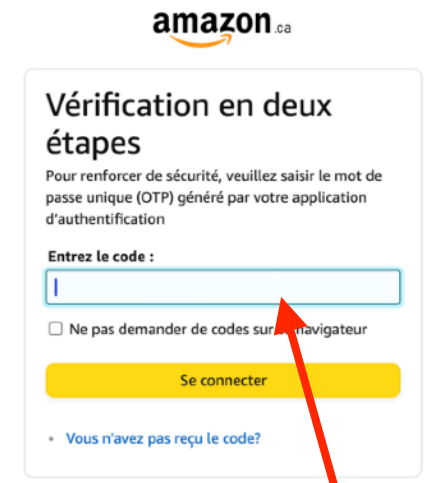
2: Choix du mode connexion

Erreur de traduction du site web: il faudrait lire « Se connecter avec une clé d'accès » ou « une clé d'identification ».

Sélectionner cette option pour utiliser votre clé d'accès.

3: Logo identifiant le mode de connexion avec le nom de votre clé d'accès.

Cliquer sur « Continuer » et déverrouiller votre appareil en vous authentifiant de la manière habituelle (TouchID, FaceID, etc.)



4: Si vous utilisez la double authentification, confirmer votre identité avec la méthode indiquée dans les réglages de votre compte.

Conclusion

- Nouvelle norme de connexion sécurisée développée par l'Alliance FIDO (Fast IDentity Online) et le World Wide Web Consortium permettant de se connecter à un compte en ligne avec les mêmes données biométriques ou le même code que vous utilisez pour déverrouiller votre appareil .

- L'utilisation de clés d'accès pour accéder à nos applications et comptes en ligne devrait remplacer **graduellement** l'authentification par mot de passe au cours des prochaines années, au fur et à mesure que la confiance en cette nouvelle approche se répandra et que les entreprises adapteront leur site web (et applications) en conséquence. On peut donc s'attendre à ce que les 2 méthodes coexistent pendant un certain nombre d'années.

- Cette méthode est jugée **plus sécuritaire** et plus facile d'utilisation que celle requérant un nom d'utilisateur et un mot de passe.

- Il est recommandé de ne pas utiliser cette méthode de connexion avec un appareil que vous ne contrôlez pas entièrement et de choisir un code de verrouillage **robuste** pour chacun de vos appareils utilisant des clés d'accès.

Références

1. *Passkeys - Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins, fidoalliance.org

2.*Grâce aux « passkeys », Google signe le « début de la fin des mots de passe ». 01net.com, 3 mai 2023.

3. Passwordless login with passkeys, developers.google.com

4.*Dashlane.com, Qu'est-ce qu'une clé d'accès et comment est-ce qu'elle fonctionne ?, 22 novembre 2022

5. *Comment se connecter à PayPal avec une clé d'identification, PayPal.com

6. *Passkeys FAQs: What they are, and other frequently asked questions, blog.1password.com

7. *Seven Misunderstandings About Passkeys, passage.1password.com

8. Partager en toute sécurité des clés d'identification et des mots de passe avec AirDrop sur l'iPhone, support.apple.com

Références

9. Partager des mots de passe ou des clés d'identification avec des personnes de confiance sur l'iPhone, support.apple.com

10. *Amazon:comment créer une clé d'accès pour se connecter sans saisir de mot de passe ?, 01net.com, 19 octobre 2023

11. *Utiliser des clés d'identification pour se connecter à des apps et des sites web sur l'iPhone, support.apple.com

12. *Rendre les clés d'identification et les mots de passe disponibles sur tous les appareils avec l'iPhone et le trousseau iCloud, support.apple.com

13. Kill passwords forever — here's how to set up passkeys on iPhone, iPad and Mac, tomsguide.com, 9 décembre 2022

14. *Manage passkeys in Chrome, support.google.com

15. Bitwarden releases new developer survey on generative AI, passkeys, and more. 9to5Mac, 18 octobre 2023.

16. *What is a passkey ?, passkey.io

QUESTIONS ?