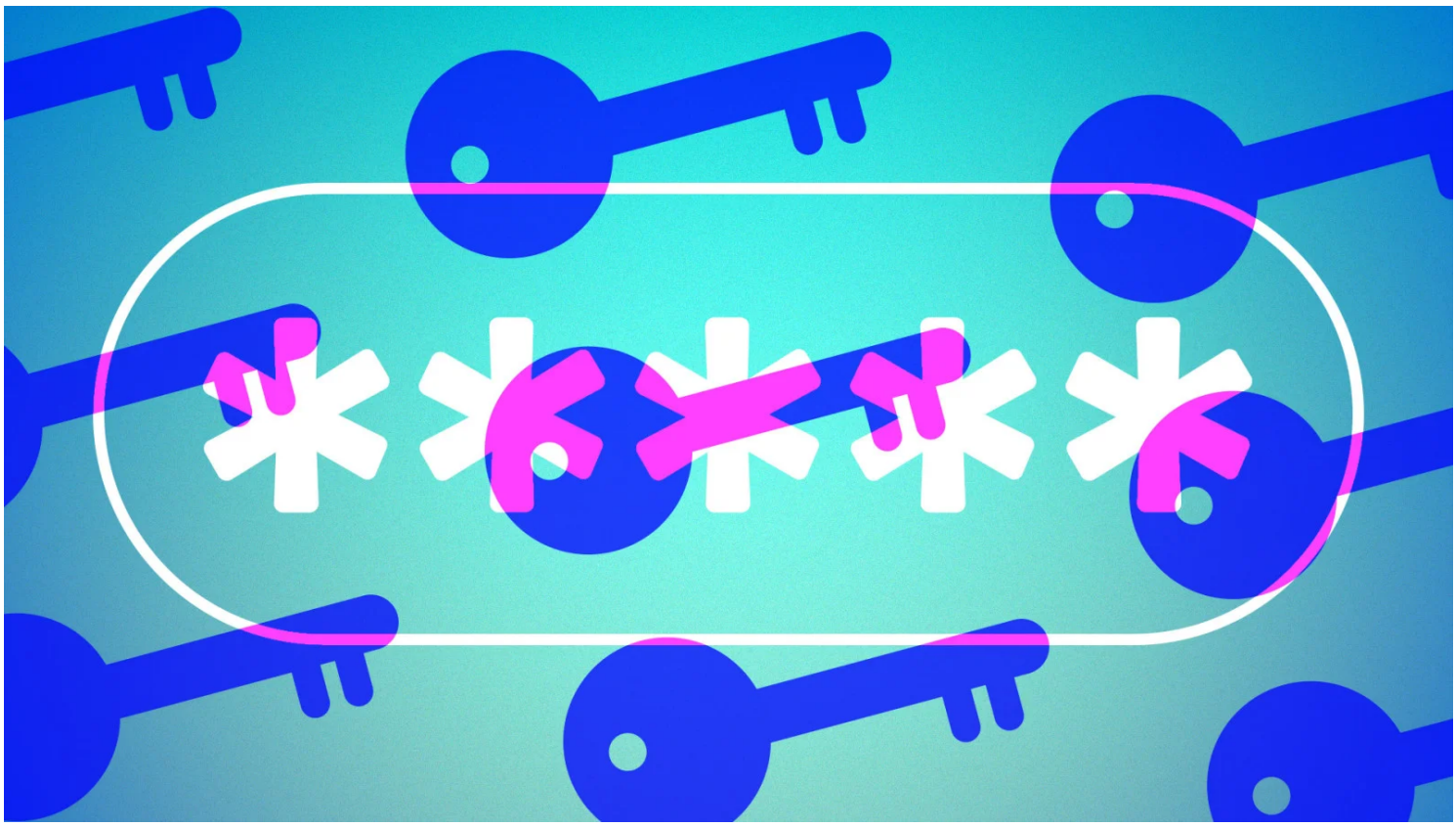
www.pcmag.com /how-to/set-up-passkeys-for-google-account

Comment configurer des clés d’accès pour votre compte Google

Les clés d’accès sont plus faciles à utiliser et plus sûres que les mots de passe, mais il n’est pas simple de les utiliser.
Nous vous expliquons comment configurer et utiliser les clés d’accès pour Google sur tous vos appareils.

Max Eddy :



Les mots de passe sont une réalité ennuyeuse et peu sûre de la vie avec la technologie. Personne ne les aime, mais il n’y a pas eu de véritable alternative – jusqu’à présent.
S’ils tiennent leur promesse, les clés d’accès peuvent éliminer la douleur et le risque de l’authentification grâce à un système simple et sécurisé construit sur des appareils de confiance.
Google est l’une des plus grandes entreprises activant les clés d’accès, vous pouvez donc maintenant essayer cette nouvelle technologie lorsque vous vous connectez à votre compte Google.

Que sont les clés d’accès ?

Les clés d’accès sont destinées à être plus sécurisées et plus faciles à utiliser que les mots de passe.
Au lieu de taper un mot de passe (ou de laisser un gestionnaire de mots de passe le faire) et de vérifier avec une méthode d’authentification multifacteur, les clés d’accès ne nécessitent qu’un appareil de confiance et une vérification biométrique ou par code PIN.

Une partie de la raison pour laquelle les clés d'accès semblent susceptibles de remplacer les mots de passe est qu'elles sont conçues par un consortium appelé FIDO Alliance et défendues par Apple, Google et Microsoft.
Ces trois sociétés ont déjà intégré la prise en charge des clés d'accès dans leurs navigateurs et leurs écosystèmes, ce qui signifie que pour la première fois, il existe une alternative viable aux mots de passe.
Cela dit, les clés d'accès n'ont pas encore été largement adoptées.

Dans quelle mesure les clés d'accès sont-elles sûres ?

Pour quiconque a travaillé dur pour protéger ses mots de passe contre l'hameçonnage et la devinette par force brute, cette nouvelle technologie peut sembler un peu effrayante.

Vous vous demandez peut-être ce qui se passe si quelqu'un vole l'appareil avec votre clé d'accès.
Comme les clés d'accès ne peuvent être créées que sur les appareils qui nécessitent une authentification pour se déverrouiller, toute personne qui trouve votre appareil devra d'abord y pénétrer pour usurper votre identité.
Bien qu'il ne soit pas impossible de contourner les verrous biométriques ou PIN sur les appareils, ce n'est pas un travail facile pour un escroc occasionnel.

Vous pouvez également vous inquiéter de ce qui se passe si un site est violé ou si votre appareil est attaqué.
Parce qu'ils sont réalisés à l'aide de la cryptographie à clé asymétrique, une violation de données n'expose aucune information qu'un attaquant pourrait utiliser pour usurper votre identité.
Même si votre clé d'accès était extraite de votre appareil, elle ne fonctionnerait pas sans l'appareil lui-même *et* votre autorisation biométrique ou PIN.

Les clés d'accès sont-elles pratiques ?

Même si vous surmontez ces peurs, il y a aussi la logistique à considérer.
Comment allez-vous vous connecter sur un appareil qui n'a pas de clé d'accès ?
N'ayez crainte, vous pouvez utiliser un appareil avec une clé d'accès pour autoriser temporairement un autre appareil qui n'a pas de clé d'accès.
La connexion est établie en toute sécurité via Bluetooth, mais la clé d'accès n'est ni transférée ni copiée.
Au lieu de cela, l'appareil récepteur n'est autorisé qu'à vous connecter, et juste pour cette fois.

“ Une partie de la raison pour laquelle les clés d'accès semblent susceptibles de remplacer les mots de passe est qu'elles sont conçues par un consortium appelé FIDO Alliance et défendues par Apple, Google et Microsoft. ”

Selon la plate-forme sur laquelle vous vous trouvez, les clés d'accès peuvent également être synchronisées entre vos appareils.
Par exemple, lorsque j'ai créé une clé d'accès sur mon iPhone, une alerte m'a informé qu'elle était enregistrée dans le trousseau iCloud et disponible également sur mes autres appareils Apple.

Votre appareil prend-il en charge les clés d'accès ?

Avant de commencer, vous devez vous assurer que les périphériques avec lesquels vous souhaitez créer une clé d'accès sont pris en charge.
La documentation de Google présente trois catégories importantes.
Vous aurez besoin d'au moins Windows 10 (2015) ou macOS Ventura (2022) pour les ordinateurs de bureau et portables.
Pour les appareils mobiles, vous aurez besoin d'au moins Android 9 (2018) ou iOS 16 (2022).

Vous pouvez également utiliser une clé de sécurité matérielle comme le Yubikey 5 pour stocker vos clés d'accès.
L'avantage est que vos clés d'accès ne vivent que sur un seul appareil que vous contrôlez, mais cela signifie également que vous perdrez toutes vos clés d'accès si vous perdez votre clé de sécurité.
Créer plus de clés d'accès sur d'autres appareils ou une clé de sécurité de sauvegarde est une bonne idée.
Les sites et les services qui utilisent des clés d'accès devront fournir une sorte d'option de secours pour des scénarios comme celui-ci, et cela signifiera probablement dépoussiérer votre ancien mot de passe ou le réinitialiser, si nécessaire.
Si vous utilisez une clé de sécurité, elle doit prendre en charge FIDO2.
La plupart des clés modernes prennent en charge cette norme, mais les clés plus anciennes peuvent ne pas l'être.

L'appareil que vous utilisez devra également répondre à certaines exigences de sécurité minimales.
Une fonction de verrouillage doit être activée pour un ordinateur portable, un ordinateur de bureau ou un appareil mobile.
Cela signifie que vous devez utiliser la biométrie ou un code PIN / mot de passe pour ouvrir l'appareil après qu'il ait été inactif.
Cependant, vous *n'avez pas* besoin d'une clé de sécurité prenant en charge la biométrie.

Comme indiqué ci-dessus, les clés d'accès peuvent être utilisées pour autoriser d'autres appareils dotés d'une connexion Bluetooth.
Donc, si vous voulez faire cela, vous aurez besoin d'un appareil avec Bluetooth activé.

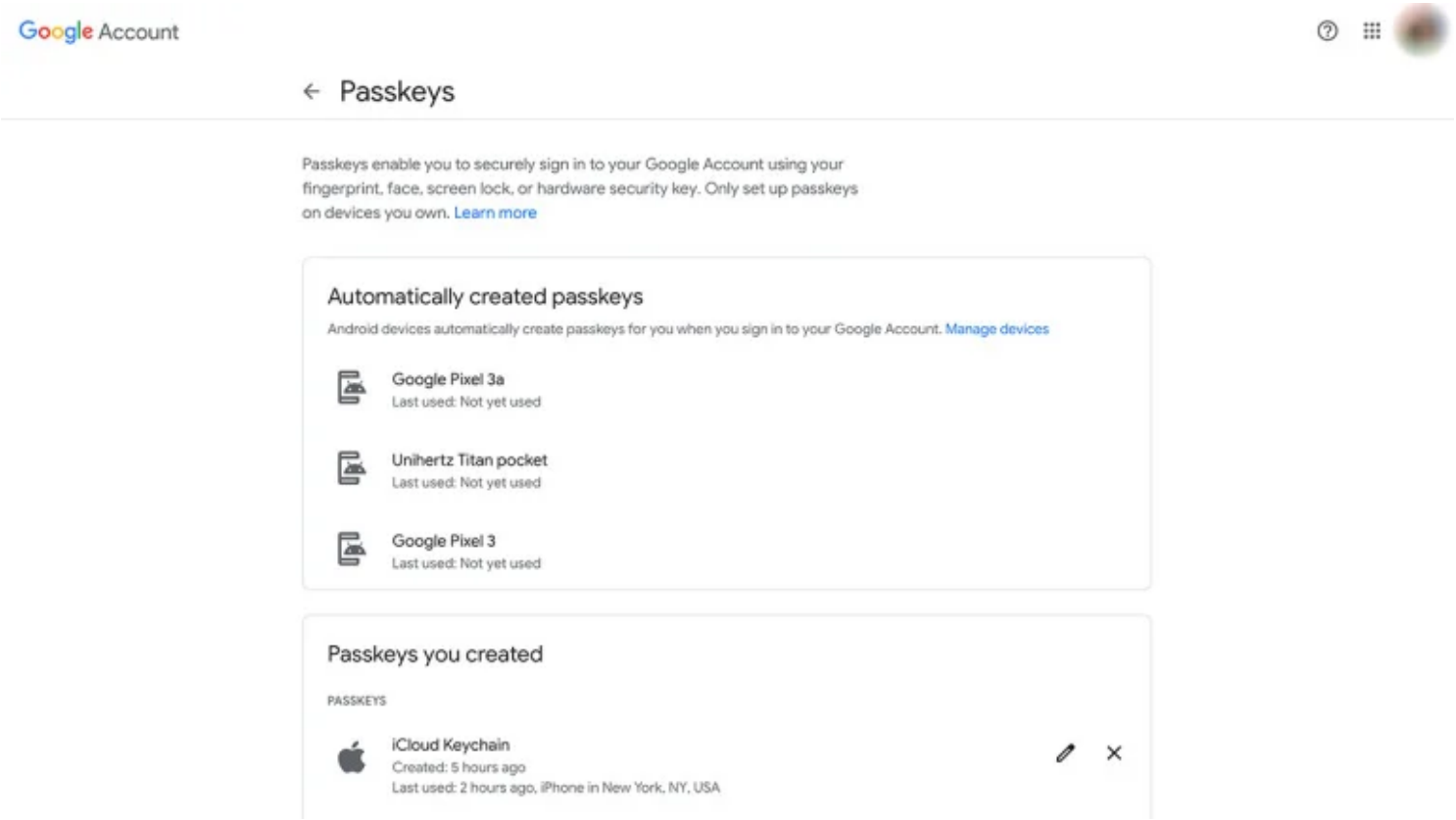
Enfin, si vous utilisez un navigateur, et c'est probablement le cas, il devra *également* prendre en charge les clés d'accès.
La documentation de Google indique que les clés d'accès sont prises en charge dans Chrome 109, Safari 16 ou Edge 109.
Firefox est remarquablement absent, bien que le développeur Mozilla affirme qu'ils sont sur la feuille de route.
Lors de nos tests, nous avons constaté que d'autres navigateurs basés sur Chromium peuvent également prendre en charge les clés d'accès.
Nous n'avons eu aucun mal à créer et à utiliser une clé d'accès avec la dernière version d'Opera, par exemple.

Notez que si votre compte Google est géré par un employeur ou une autre organisation, les clés d'accès ne sont pas une option.
Cependant, vous pouvez utiliser des clés d'accès à la place des clés de sécurité avec le programme de protection avancée de Google.

Prise en main des clés d’accès

Google a créé un tableau de bord spécial pour afficher et gérer les clés d’accès que vous avez créées pour vous connecter à votre compte Google.
Ceux-ci *sont uniquement pour votre compte Google,* pas pour toutes les clés d’accès pour d’autres sites et services sur votre appareil.

Pour le visualiser, connectez-vous à Google normalement (en utilisant, espérons-le, une authentification multifacteur et un gestionnaire de mots de passe).
Cliquez ensuite sur votre icône en haut à droite de l’écran et cliquez sur Gérer votre compte Google.
Sur l’écran suivant, cliquez sur Sécurité dans la colonne de gauche.
Dans la section intitulée Comment vous connecter à Google, vous verrez plusieurs options, dont l’une devrait être les clés d’accès.



Google vous permet de gérer toutes les clés d’accès que vous avez créées pour accéder à votre compte Google (Crédit : Google)

Si vous avez un appareil Android, la section supérieure de l’écran des clés d’accès est intitulée Clés d’accès créées automatiquement.
C’est juste; si vous avez connecté votre appareil Android à votre compte Google, cet appareil dispose déjà d’une clé d’accès et peut être utilisé pour vous connecter à votre compte Google.
Si vous y voyez des appareils que vous ne reconnaissez pas ou que vous n’avez pas utilisés depuis longtemps, cliquez sur le lien Gérer les appareils en haut de l’écran (ou visitez le gestionnaire d’appareils Google) pour les désinscrire.

La section intitulée Clés d'accès que vous avez créées affiche toutes les clés d'accès de votre compte Google, ainsi que des informations sur la plate-forme sur laquelle la clé d'accès a été créée, la dernière fois qu'elle a été utilisée et l'emplacement approximatif de son utilisation.
Si vous supprimez une clé d'accès ici, vous annulez l'autorisation de l'appareil qui a créé la clé.
C'est pratique si vous avez accidentellement créé une clé d'accès sur un ordinateur qui n'était pas le vôtre, ou si vous vous débarrassez d'une machine.

Si vous avez déjà enregistré une clé de sécurité matérielle en tant qu'appareil multifacteur avec votre compte Google, elle apparaîtra dans la liste ci-dessous.
Cela peut devenir un peu délicat ici, cependant.
Lors de mes tests, je n'ai pas pu utiliser une clé précédemment inscrite pour créer une nouvelle clé d'accès ou me connecter avec une clé d'accès.
Lorsque j'ai désinscrit la clé et que je l'ai ensuite utilisée pour créer une clé d'accès, cela a très bien fonctionné.

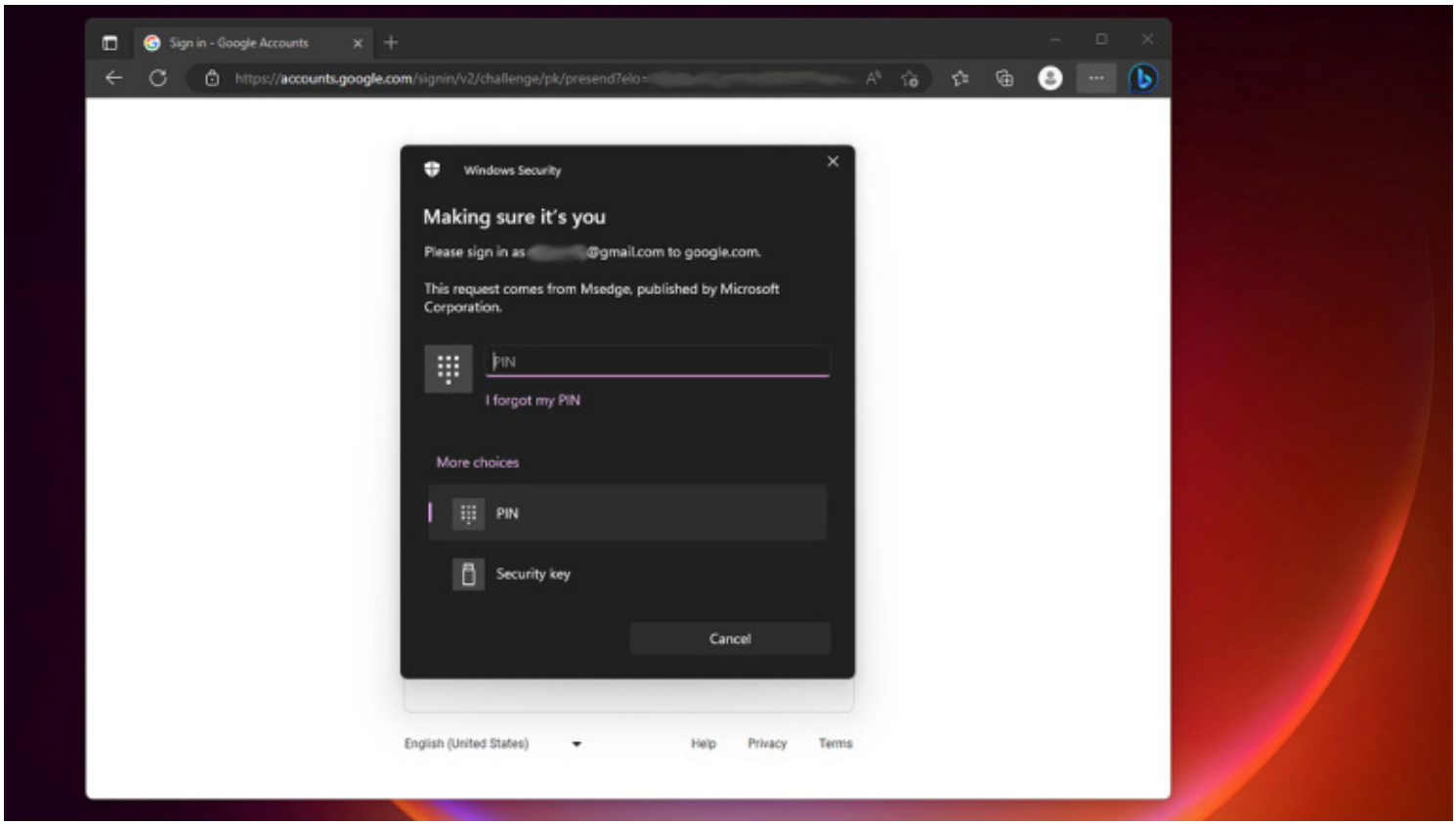
Tout en bas de la page se trouve la partie la plus importante: un bouton qui dit Créer une clé d'accès.
Cela fait exactement ce que cela ressemble et vous permet de créer une clé d'accès sur une clé de sécurité ou l'appareil que vous utilisez.

Comment créer une clé d'accès pour Google sous Windows

Tout d'abord, assurez-vous que votre ordinateur Windows est configuré pour prendre en charge les clés d'accès.
Plus important encore, vous devrez activer Windows Hello avant que votre PC puisse créer une clé d'accès.
Vous pouvez activer cette fonctionnalité dans les paramètres Windows.

À l'aide de Microsoft Edge, de Chrome ou d'un navigateur Chromium compatible, accédez à la page des paramètres de la clé d'accès Google et cliquez sur le bouton Créer une clé d'accès en bas de l'écran.
Vous pouvez également utiliser cette URL courte pour démarrer le processus : http://g.co/passkeys.

Vous serez d'abord invité à créer une clé d'accès, il vous suffit donc de cliquer sur Continuer.
Ensuite, une fenêtre contextuelle de sécurité Windows apparaîtra.
Ensuite, vous utilisez la méthode Windows Hello que vous utilisez pour déverrouiller votre PC.
Dans mon cas, j'ai entré mon code PIN et j'ai cliqué sur OK.



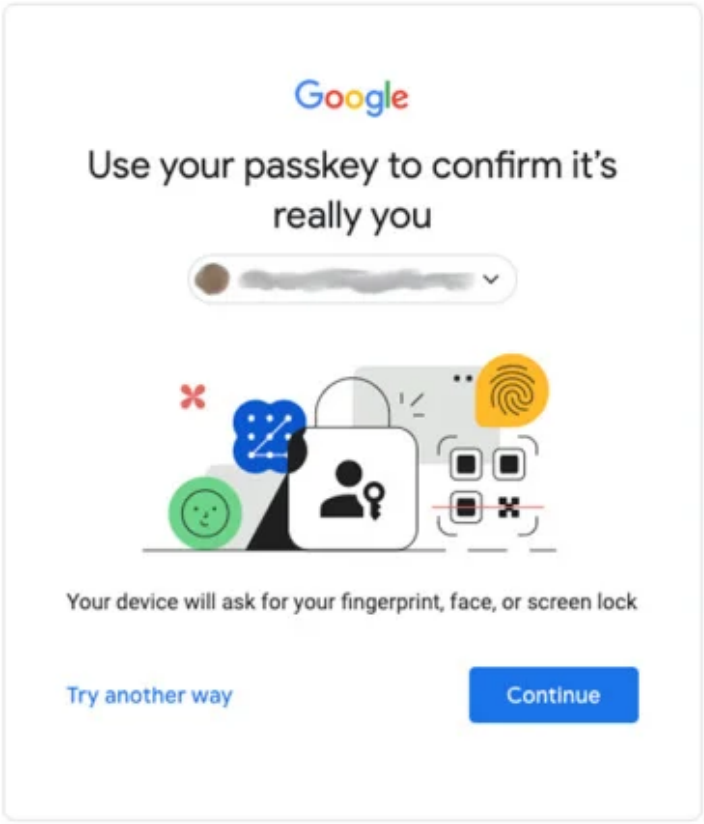
Windows Hello doit être activé pour créer une clé d'accès sous Windows (Crédit : Google/Microsoft)

Une clé d'accès pour Google est maintenant stockée sur votre ordinateur Windows.
Notez qu'à l'heure actuelle, Microsoft ne synchronise pas les clés d'accès entre les appareils : vous devez créer manuellement des clés d'accès sur toutes vos autres machines Windows.
Vous pouvez suivre les étapes ci-dessus ou utiliser un autre appareil avec une clé d'accès pour que Google autorise votre autre machine, puis créer une nouvelle clé d'accès, comme je l'explique ci-dessous.

Comment créer une clé d'accès pour Google sur macOS

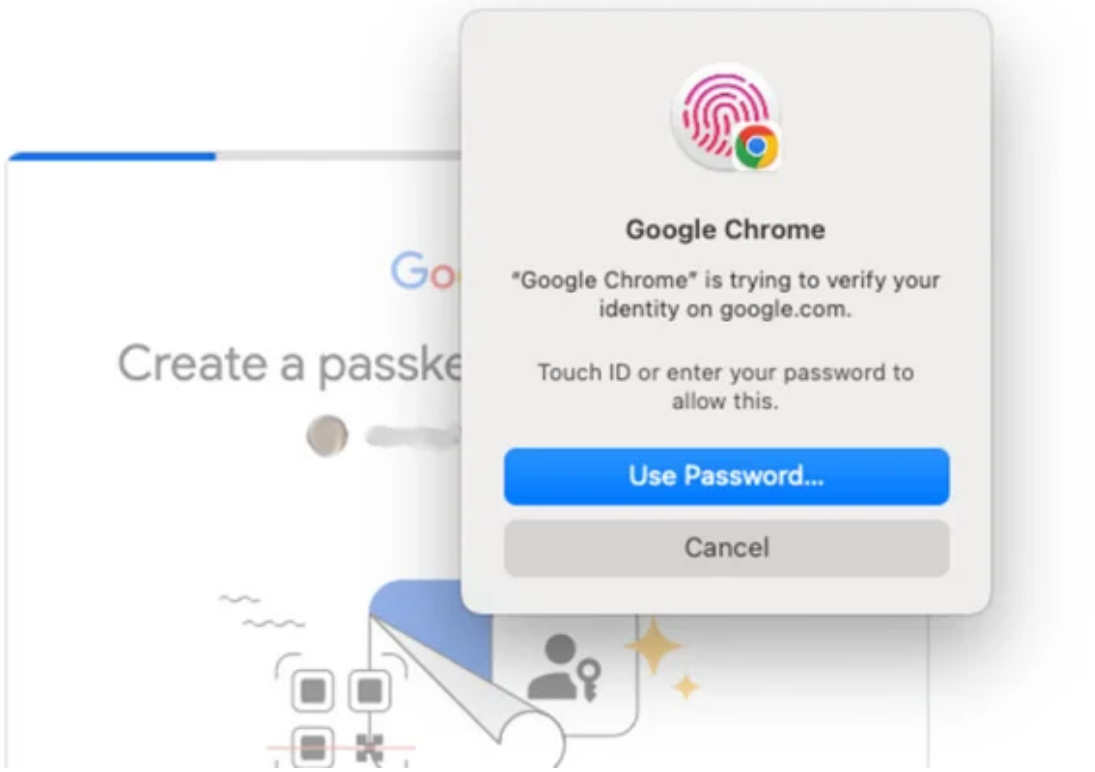
Vous pouvez utiliser Chrome, un navigateur Chromium pris en charge, ou Safari pour créer une clé d'accès sur macOS.
Assurez-vous que votre ordinateur utilise la dernière version de macOS et que vous avez activé un verrou biométrique ou un mot de passe pour sécuriser votre ordinateur.

Accédez au paramètre Clé d'accès ci-dessus et cliquez sur le bouton Créer une clé d'accès.
Vous pouvez également utiliser l'URL courte de Google https://g.co/passkeys.



Le premier écran lors de la création d'une clé d'accès sur Google Chrome pour macOS (Crédit : Google)

Vous serez invité à créer une clé d'accès sur votre Mac.
Une fois que vous avez appuyé sur le bouton Continuer, vous validez le compte Google pour lequel vous souhaitez créer une clé d'accès.
Ensuite, vous autorisez la création d'une clé d'accès avec le mécanisme que vous utilisez pour déverrouiller votre Mac.
Dans mon cas, j'ai utilisé le scanner d'empreintes digitales du MacBook Pro.



macOS générant une invite pour saisir une empreinte digitale ou un mot de passe (Crédit : Google)

La clé d'accès est maintenant stockée en toute sécurité sur votre Mac, et une nouvelle entrée apparaîtra sur la page des paramètres de la clé d'accès Google.

Comment créer une clé d'accès pour Google sur Android

Pour créer une clé d'accès sur votre appareil Android, vous n'avez rien à faire.
Si vous êtes déjà connecté à votre compte Google, cela signifie que Google a déjà généré une clé d'accès sur votre appareil.
Vous pouvez l'utiliser immédiatement pour vous connecter à Google en toute sécurité et autoriser d'autres appareils.

Comme je l'ai noté ci-dessus, comme il s'agit d'une procédure automatique, vous pouvez avoir des clés d'accès sur des appareils que vous n'utilisez plus ou que vous ne possédez même plus.
Assurez-vous de consulter la page des paramètres des clés d'accès Google et de supprimer tous les appareils que vous n'utilisez plus.

Comment créer une clé d'accès pour Google sur iOS

À l'aide des navigateurs Chrome (ou Chrome compatible basé sur Chromium) ou Safari sur iOS, accédez aux paramètres de la clé d'accès Google et appuyez sur le bouton Créer une clé d'accès ou utilisez le http://g.co/passkeys court.
Vous serez invité à créer une clé d'accès et à appuyer sur Continuer.
Maintenant, iOS prend le relais et vous avertit que votre clé d'accès sera ajoutée à votre trousseau iCloud et synchronisée avec tous vos appareils.
Appuyez sur le bouton sur le bouton, puis effectuez le rituel que vous utilisez pour déverrouiller votre appareil.
En ce qui me concerne, j'ai entré mon code PIN.
Voilà! Votre clé d'accès est créée et stockée.

Notez que vous pouvez également utiliser votre clé d'accès pour vous connecter à Google dans d'autres applications.
Par exemple, j'ai créé une clé d'accès dans Safari, puis je l'ai utilisée pour me connecter à Chrome pour iOS.

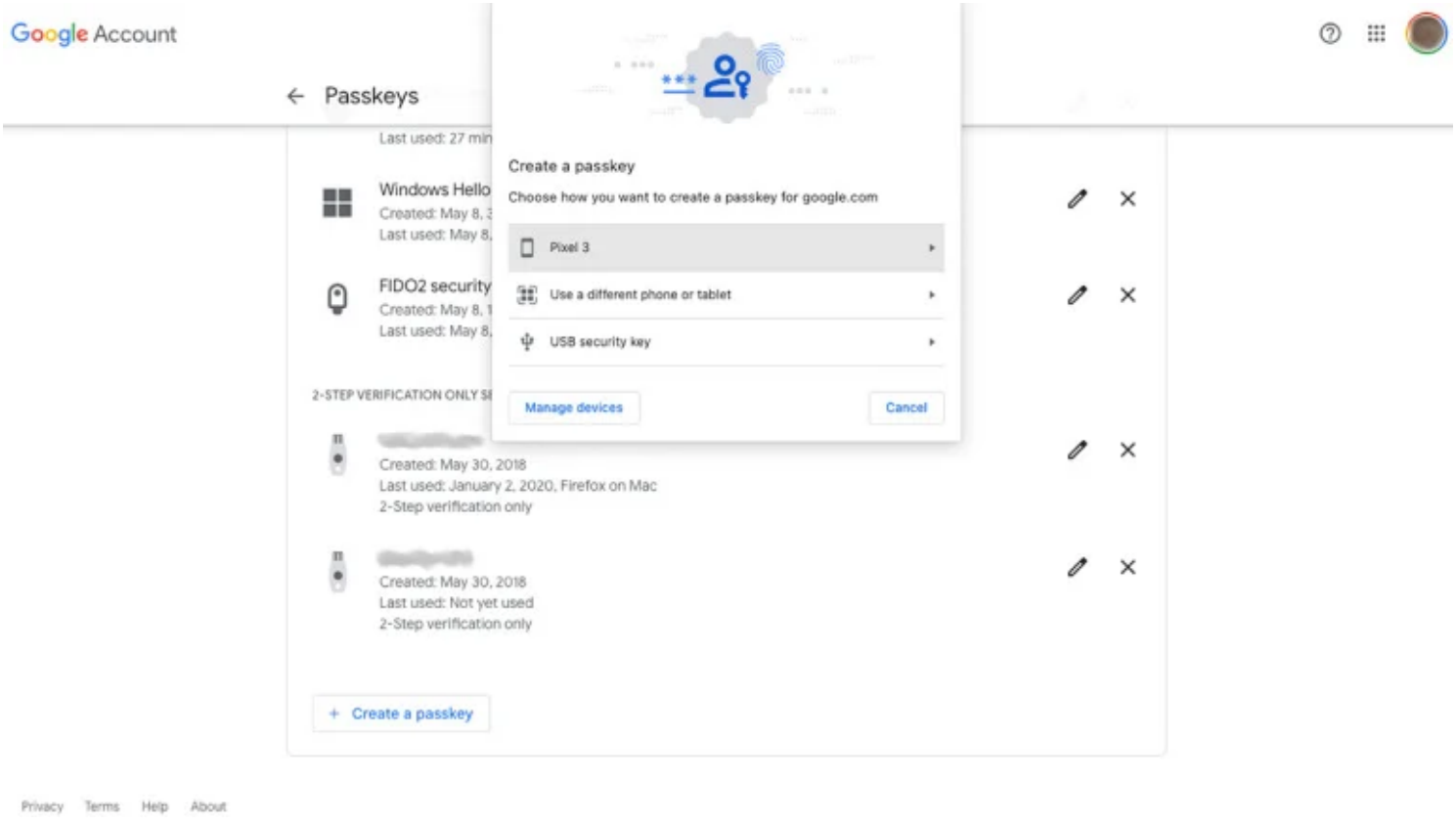
Comment créer une clé d'accès pour Google sur votre clé de sécurité

Vous pouvez utiliser une clé de sécurité matérielle comme la Yubikey pour stocker vos clés d'accès (Crédit : Max Eddy)

Avant de commencer, assurez-vous que votre clé de sécurité prend en charge FIDO2. Les anciennes clés ne fonctionneront pas.
Vérifiez également si vous avez déjà inscrit votre clé de sécurité auprès de Google en tant que dispositif d'authentification multifacteur.
Lors de mes tests, j'ai constaté que je ne pouvais pas utiliser une clé de sécurité que j'avais déjà inscrite pour

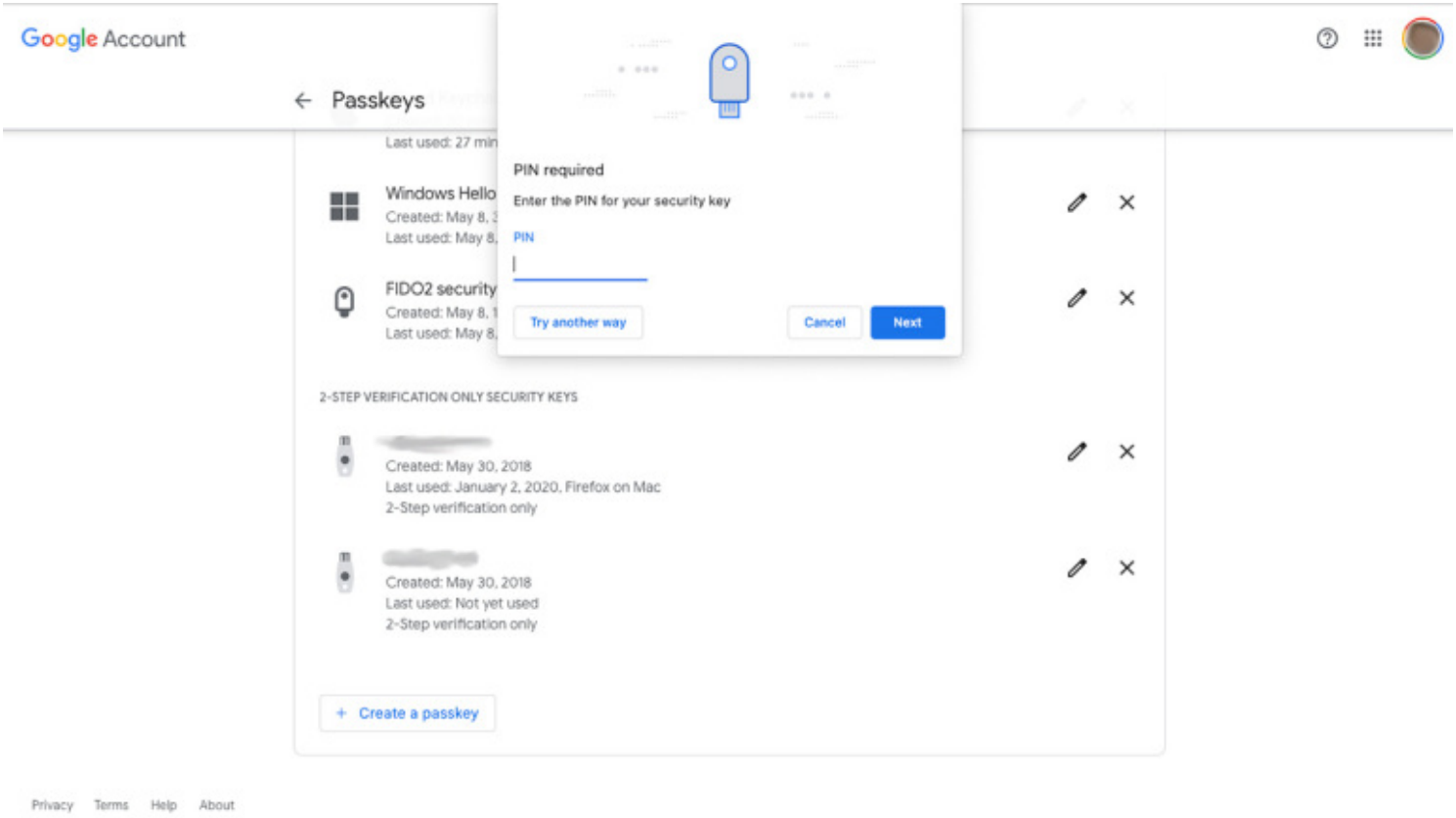
l'authentification multifacteur pour créer une clé d'accès. Cependant, j'ai simplement désinscrit la clé, puis j'ai créé une clé d'accès dessus. Bizarrement, j'ai dû réenregistrer séparément la clé pour l'utiliser comme dispositif d'authentification multifacteur.
Si vous avez besoin de faire cette astuce, je vous suggère fortement de disposer d'une autre méthode d'authentification multifacteur ou de créer d'abord une clé d'accès sur un autre appareil, afin de vous assurer que vous disposez d'un moyen sûr et fiable de vous connecter.

À l'aide d'un navigateur pris en charge, accédez à la page des paramètres des clés d'accès Google et appuyez sur le bouton Créer une clé d'accès ou utilisez l'URL courte : http://g.co/passkeys.
Lorsque vous êtes invité à créer une clé d'accès, *ne cliquez pas* sur Continuer.
Au lieu de cela, cliquez sur le lien Utiliser un autre appareil juste à gauche.
Dans la liste qui s'affiche, sélectionnez la clé de sécurité USB.



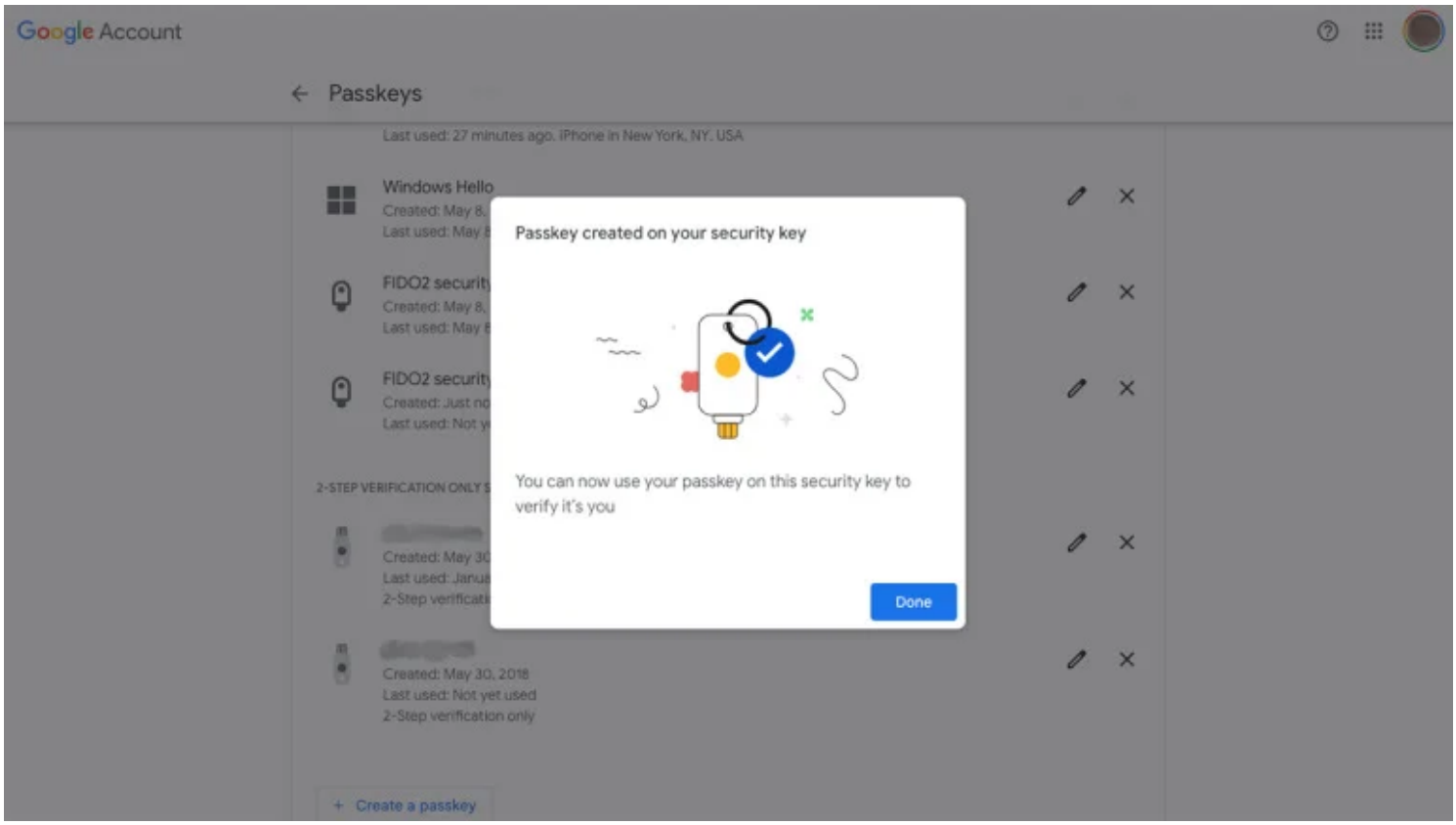
Cliquez sur Utiliser un autre appareil pour créer une clé d'accès dans Chrome (Crédit : Google)

Vous serez ensuite invité à brancher votre clé de sécurité et à appuyer sur son bouton tactile.
Si vous avez déjà créé un code PIN pour votre clé de sécurité, vous devez le saisir maintenant.
Dans le cas contraire, vous serez invité à définir un code PIN pour la clé.



Si vous n'avez jamais utilisé votre clé de sécurité pour une entrée sans mot de passe, vous devrez lui attribuer un code PIN (Crédit : Google)

Vous allez appuyer à nouveau sur la clé, puis appuyer sur Autoriser sur l'écran suivant qui vous demande l'autorisation d'accéder à votre clé de sécurité.
Une fenêtre s'affichera alors pour confirmer que la clé d'accès a été créée avec succès sur votre clé de sécurité.



La clé d'accès restera sur cette clé de sécurité (Crédit : Google)

N'oubliez pas que la clé d'accès que vous venez de créer *n'existe* que sur votre clé de sécurité, et non sur la machine que vous utilisiez.

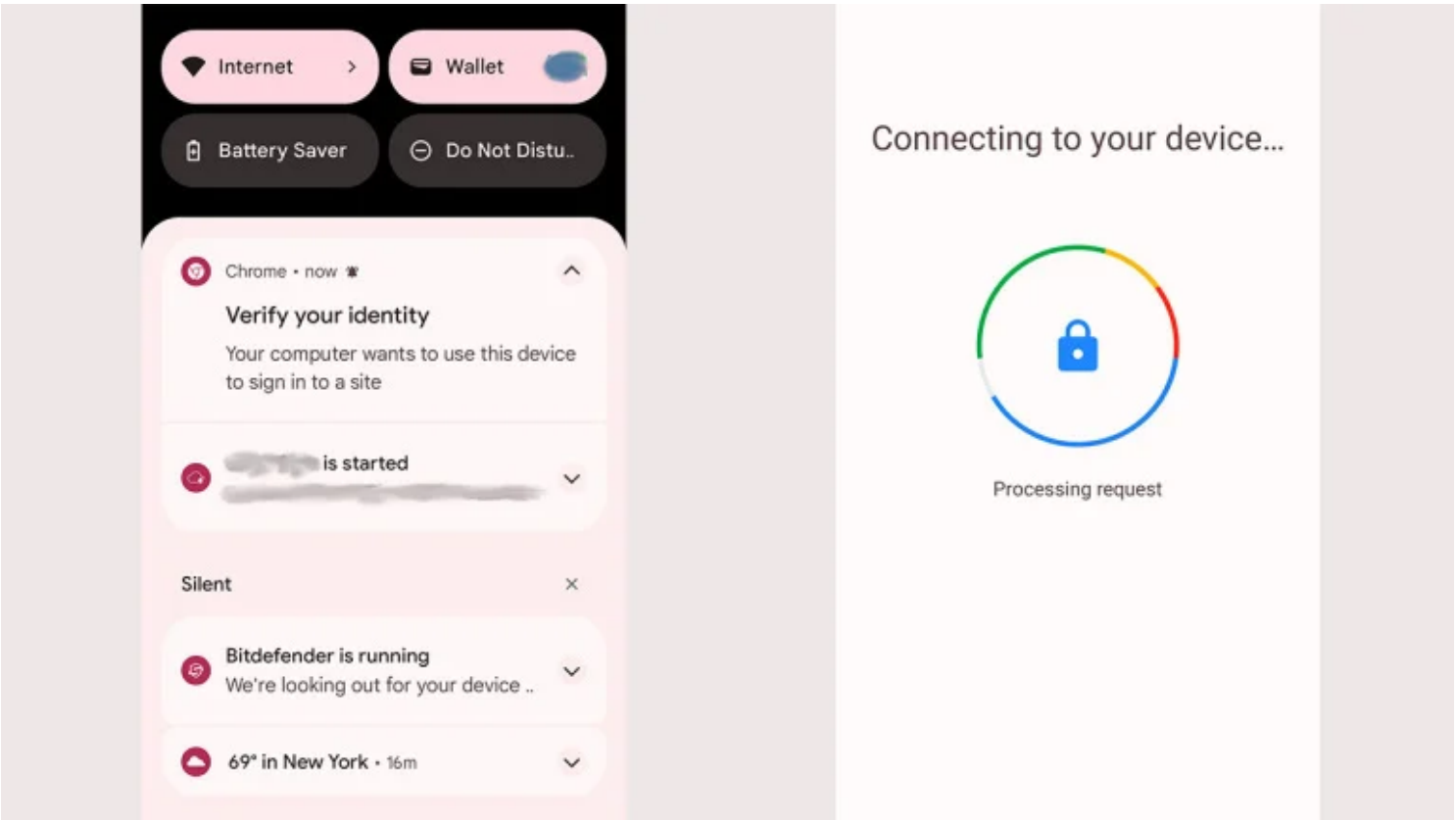
Comment utiliser une clé d'accès sur un autre appareil pour se connecter à Google

Pour vous connecter à Google sur un appareil à l'aide d'une clé d'accès stockée sur un autre, vous devez d'abord créer une clé d'accès à l'aide de l'une des méthodes ci-dessus. Vous devrez également activer le Bluetooth sur les deux appareils : celui avec votre clé d'accès et celui que vous souhaitez autoriser avec votre clé d'accès.
Si l'un de vos appareils ne prend pas en charge Bluetooth, cela ne fonctionnera pas. L'appareil qui contient votre clé d'accès a également besoin d'une caméra fonctionnelle.

Notez que si vous avez créé votre clé d'accès sur une clé de sécurité, vous pouvez simplement brancher la clé sur l'appareil et vous connecter.
Vous pouvez ensuite créer une nouvelle clé d'accès sur l'appareil avec lequel vous vous connectez si vous le souhaitez.

Lorsque vous commencez à vous connecter à Google, le site génère une invite indiquant que vous disposez d'une clé d'accès sur un autre appareil et vous propose des options pour vous connecter.
Selon l'appareil et le navigateur que vous utilisez, cela aura un aspect différent et aura différentes options.
Sélectionnez l'appareil sur lequel se trouve votre clé d'accès et continuez.

Si vous autorisez Google Chrome avec un appareil Android, une notification push s’affiche sur votre téléphone.

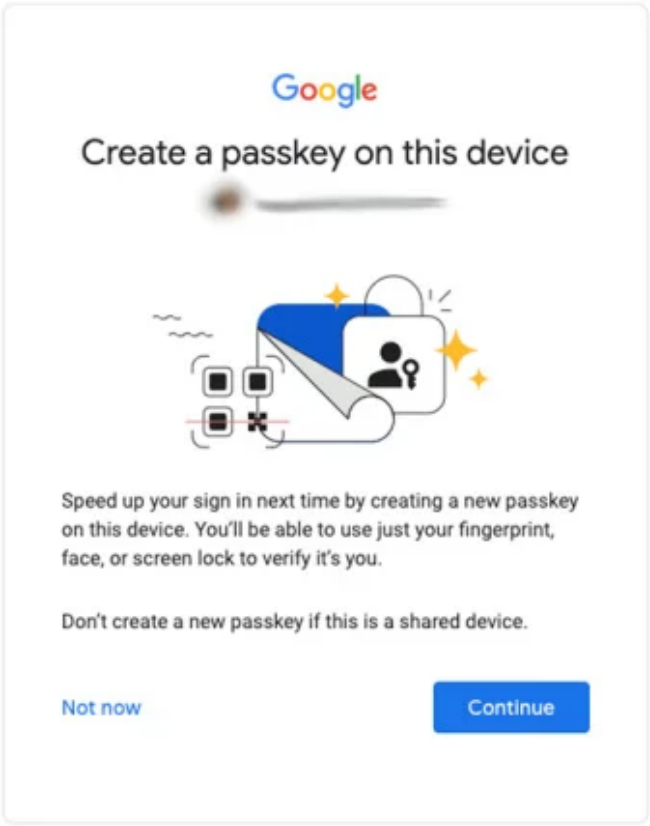


Si votre appareil Android est équipé d’une clé d’accès, le navigateur Chrome peut envoyer une notification push demandant l’autorisation (Crédit : Google)

Si vous utilisez une autre combinaison d’appareils, un code QR apparaîtra sur celui que vous essayez d’autoriser.
Scannez le code avec l’appareil qui possède déjà votre clé d’accès, puis utilisez le moyen que vous utilisez pour déverrouiller cet appareil.

En scannant le code QR, les deux appareils se connectent via Bluetooth (Crédit : Apple/Google)

Ensuite, vous pouvez créer une nouvelle clé d’accès sur l’appareil que vous venez d’autoriser.
Assurez-vous de ne pas créer de clé d’accès sur un appareil partagé ou sur un appareil qui ne vous appartient pas.
Si vous regrettez votre choix, il vous suffit d’utiliser la page des paramètres de la clé d’accès Google pour annuler l’autorisation de l’appareil.



Un appareil nouvellement autorisé peut créer sa propre clé d'accès (Crédit : Google)

Les clés d'accès pourraient bien être l'avenir

Les clés d'accès peuvent sembler étranges et intimidantes, mais après avoir fait les recherches et les tests pour cet article, je suis agréablement surpris de constater à quel point l'expérience est transparente et fluide. Nous sommes loin de nous libérer enfin de la misère des mots de passe, mais les clés d'accès sont notre meilleur pari pour le faire.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231015
"C'est ensemble qu'on avance"