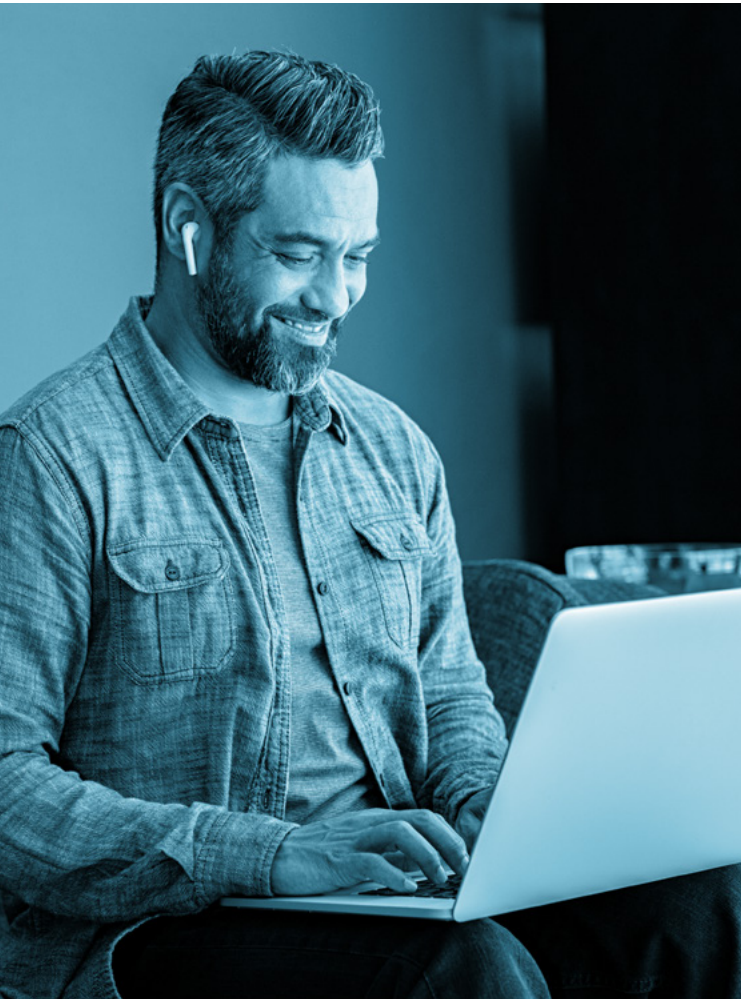
yubico

# Vous envisagez d'utiliser des passkeys synchronisées dans votre entreprise ?

## Évitez certains pièges qui entraînent une augmentation des risques et des coûts



# Différentes mises en œuvre des passkeys

Les passkeys sont des clés d'accès FIDO (Fast Identity Online) permettant de s'identifier sans mot de passe depuis un smartphone, une tablette ou un ordinateur portable, ou bien des systèmes d'authentification dédiés comme une clé de sécurité matérielle FIDO.

Les passkeys sont plus sûres que les mots de passe et permettent de s'authentifier sans mot de passe, pour davantage de sécurité et d'efficacité. Pour en savoir plus sur les fondamentaux des passkeys, cliquez ici.

Il existe deux types de passkeys : les passkeys synchronisées et les passkeys matérielles. Les passkeys synchronisées contiennent des informations d'identification pouvant être copiées et pouvant passer d'un appareil à l'autre, comme des smartphones, ordinateurs portables et tablettes connectés à un compte utilisateur. Ce type de passkey peut créer une faille de sécurité inquiétante pour votre entreprise.

Voici quelques scénarios courants dans lesquels les passkeys synchronisées peuvent vous rendre vulnérable :

1. **Risques liés au télétravail** : des risques de sécurité surviennent lorsque les employés travaillent depuis chez eux et qu'un pirate réussit à accéder à leurs informations d'identification depuis son appareil à cause de la facilité de copie offerte par les passkeys.
2. **Vulnérabilité de la chaîne d'approvisionnement** : des menaces internes apparaissent et l'intégrité de la chaîne d'approvisionnement est menacée lorsque les employés partagent des informations d'identification des passkeys synchronisées entre leurs comptes et appareils.
3. **Conformité et complexité du support** : la prolifération des écosystèmes de passkeys ouvre la voie à une foule de fournisseurs de passkeys. Par conséquent, il est plus compliqué de garantir la fiabilité, la conformité et le suivi des informations d'identification,et cela contribue à augmenter la charge de travail et les coûts du service d'assistance informatique.

Lisez les scénarios ci-dessous pour découvrir comment les passkeys synchronisées peuvent augmenter les risques et les coûts pour votre entreprise.

## Passkeys synchronisées et passkeys matérielles

### Passkeys synchronisées

Elles sont activées via un smartphone, une tablette, un ordinateur portable ou tout autre appareil et peuvent être copiées et synchronisées sur de nombreux appareils.

### Passkeys matérielles

Elles prennent la forme d'une clé USB ou tout autre matériel distinct des appareils du quotidien. La clé matérielle offre une sécurité renforcée.

Scénario 1

# Risques liés au télétravail

Les passkeys se synchronisent avec tous les appareils personnels connectés à un même compte iCloud. L'histoire de Jim, qui télétravaille à temps plein dans une entreprise technologique, montre le danger que posent les passkeys synchronisées. Jim travaille depuis chez lui et les membres de sa famille se partagent le même compte iCloud, accessible sur six appareils différents. Voyons comment un pirate peut exploiter les faiblesses des passkeys synchronisées.

1. Jim se connecte à son compte professionnel depuis son téléphone en utilisant une passkey. Il a ajouté son téléphone à son compte iCloud personnel, qui est également accessible sur d'autres appareils utilisés par les membres de sa famille.

2. Ben, le fils de Jim, reçoit un e-mail contenant un lien censé le rediriger vers l'application d'un jeu auquel il aime jouer. Il clique sur le lien.

3. Ben est incité à fournir le nom d'utilisateur et le mot de passe du compte iCloud, ce qu'il fait ; le pirate les a désormais en sa possession. Ben accepte la demande d'ajout d'un nouvel appareil, permettant au pirate d'accéder au compte iCloud de la famille depuis son propre appareil.


4. Puisque le contenu du téléphone professionnel de Jim est synchronisé avec le cloud, sa passkey professionnelle se synchronise automatiquement avec tous les appareils du compte iCloud. Dont l'appareil du pirate !

5. Une fois que le pirate dispose des informations d'identification professionnelles de Jim, il peut se connecter à des sites professionnels en se faisant passer pour Jim, puis chercher à obtenir d'autres informations d'identification disposant de droits d'accès plus importants.

**LE SAVIEZ-VOUS ?**

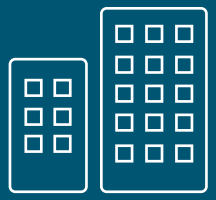
89 % des entreprises ont subi une attaque par phishing au cours de l'année dernière.

HYPR, Rapport sur l'état de la sécurité sans mot de passe en 2022

Scénario 2

# Vulnérabilité de la chaîne d'approvisionnement

Une passkey synchronisée peut facilement échapper au contrôle direct de son utilisateur principal et être utilisée sur un autre appareil via la fonctionnalité AirDrop d'un iPhone. S'il est pratique de partager une passkey dans certaines situations, elle peut être à l'origine de failles de sécurité importantes, telles que des menaces internes si les employés partagent des informations d'identification sans faire attention. Partager une passkey contribue à accroître les risques et affaiblir la confiance au sein de la chaîne d'approvisionnement. Découvrez l'histoire de Kira.



1. Un revendeur disposant d'une chaîne d'approvisionnement complexe autorise un fournisseur externe de matériel de climatisation, ventilation et chauffage à se connecter aux systèmes pour suivre les performances en temps réel.

2. Kira vient d'être embauchée. Elle n'a pas encore terminé la configuration de son compte auprès du revendeur, mais doit se mettre au travail. Elle demande donc à un collègue de partager sa passkey via AirDrop en activant le Bluetooth.

3. Quelques mois plus tard, Kira quitte son poste, mais elle peut toujours se connecter avec la passkey de son collègue depuis son appareil à elle, car il n'existe aucun moyen automatisé de révoquer son accès.

   L'entreprise ne peut pas forcer Kira à supprimer la passkey enregistrée sur son appareil.


4. Un réglage incorrect du système de CVC provoque une soudaine panne.

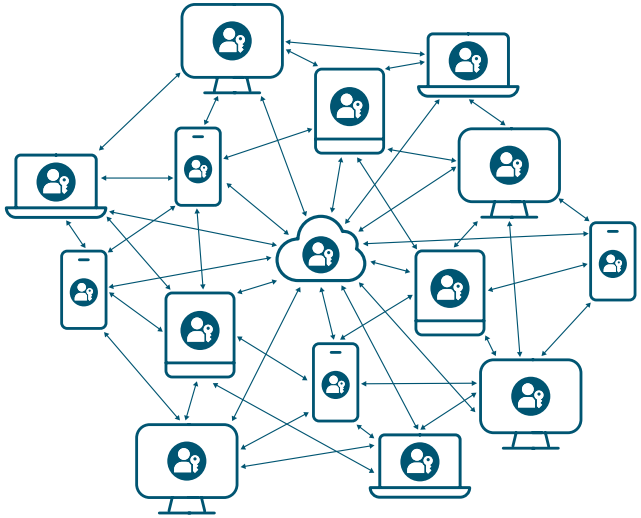
   La passkey est enregistrée dans au moins deux emplacements. Les journaux d'audit indiquent que la passkey a été utilisée, mais ils ne peuvent pas déterminer si la connexion a été effectuée par Kira ou son collègue.

5. Les risques juridiques augmentent lorsque les journaux d'audit sont moins fiables et que le fournisseur n'a plus la mainmise sur l'emplacement de stockage et de gestion des informations d'identification.

Scénario 3

# Conformité et complexité du support

Les passkeys sont déployées pour différents fournisseurs et produits. Les utilisateurs ne sont pas tenus d'utiliser un seul type de passkey. Cela signifie que les utilisateurs disposent potentiellement de nombreuses passkeys sur différentes plateformes et qui sont gérées par plusieurs gestionnaires de mots de passe. Sans visibilité, comment l'entreprise peut-elle savoir où sont stockées toutes ces passkeys et comment peut-elle aider les utilisateurs qui rencontrent des problèmes avec leurs passkeys ?



1. Le service informatique demande à Frank d'enregistrer des passkeys pour renforcer la sécurité de sa connexion professionnelle.

2. Frank opte pour trois fournisseurs de passkeys différents (Apple, Google, gestionnaire de mots de passe) pour pouvoir se connecter à l'écosystème de l'entreprise avec n'importe quelle passkey synchronisée.

3. Quelques mois plus tard, l'entreprise est victime d'une fuite de données et il est révélé que l'un des fournisseurs de services de passkeys de Frank a subi un incident de sécurité sur son système de gestion des passkeys.

4. En raison de la surexposition de l'écosystème, l'identité de Frank est vulnérable. Frank doit maintenant supprimer les passkeys synchronisées de ses trois fournisseurs et réenregistrer des passkeys pour se connecter à son compte professionnel.

5. Le service d'assistance de l'entreprise aura du mal à aider les employés comme Frank à résoudre leurs problèmes d'accès, car ils ne connaissent pas les différents fournisseurs de services de passkeys. Les entreprises devront également prendre en compte le coût de l'activation des passkeys synchronisées.

# Quelles passkeys sont adaptées à votre entreprise ?

## Les 5 points à retenir

Les passkeys sont plus sûres que les mots de passe, car elles sont basées sur des protocoles FIDO modernes et offrent une protection plus forte contre le phishing.

Voici les cinq principaux points à retenir sur les passkeys synchronisées et pourquoi les clés de sécurité matérielles répondent mieux aux besoins de sécurité et de conformité des entreprises ! Toutes les passkeys ne se valent pas et nous conseillons aux entreprises d'éviter de recourir aux passkeys synchronisées.

- Les passkeys permettent de s'identifier sans mot de passe, mais pour les entreprises qui exigent un contrôle strict de l'identité des utilisateurs, l'utilisation de passkeys synchronisées peut entraîner un risque accru.
- Les passkeys synchronisées passent d'un écosystème à l'autre et sont plus proches d'une identification classique que d'une identification à deux facteurs.
- Les passkeys synchronisées peuvent amener les entreprises à faire appel à des tiers qui ne sont pas spécialisés dans les solutions de sécurité.
- Les passkeys synchronisées permettent aux utilisateurs de partager plus facilement leurs informations d'identification, ce qui peut les encourager à utiliser ce type de passkeys s'ils en ont la possibilité.
- Les passkeys matérielles, telles que les clés de sécurité FIDO modernes et portables, offrent un niveau de protection plus élevé et répondent mieux aux besoinsde conformité des entreprises.

**Contactez-nous**
yubi.co/contact-fr

**En savoir plus**
yubi.co/passkey

## Comment choisir la bonne solution de passkey

### FOURNISSEURS DE SERVICES

**Utilisateurs grand public**

La plupart des utilisateurs grand public devraient préférer les passkeys synchronisées aux mots de passe classiques.

**Utilisateurs à risque**

Les utilisateurs à risque, par exemple les journalistes, devraient se tourner vers des passkeys qui offrent une sécurité renforcée, comme les clés de sécurité matérielles

### ENTREPRISES

**Travailleurs de première ligne**

La plupart de ces employés ne peuvent pas utiliser leur téléphone ou ordinateur portable personnel dans le cadre de leur travail. Il leur faut donc une passkey qui ne soit pas synchronisée avec ces appareils.

**Employés de bureau**

Ces professionnels ont besoin de clés de sécurité matérielles pour s'assurer que leurs informations d'identification ne peuvent pas être copiées

**Utilisateurs à haut niveau d'accès**

Ces utilisateurs présentent les plus grands risques et ont besoin de clés de sécurité matérielle pour savoir où leurs informations d'identification sont stockées

yubico

**Yubico** (Nasdaq First North Growth Market Stockholm : YUBICO), l'inventeur de la YubiKey, fait figure de référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, prévenant les piratages de compte et simplifiant la sécurisation des connexions pour tous. Depuis sa création en 2007, il a joué un rôle de premier plan dans la mise en œuvre de standards mondiaux pour l'accès sécurisé aux ordinateurs, aux appareils mobiles, serveurs, navigateurs et comptes sur Internet. Yubico est l'un des créateurs et principaux contributeurs des standards d'authentification ouverts FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F), et un pionnier de l'authentification par passkeys matérielles moderne et sécurisée à grande échelle, avec des clients dans plus de 160 pays.

Les solutions de Yubico permettent des connexions sans mot de passe utilisant la forme la plus sécurisée de la technologie passkey. Les YubiKeys sont prêtes à l'emploi dans des centaines d'applications et de services destinés aux particuliers et aux entreprises, faciles et rapides à utiliser, et offrent une sécurité rigoureuse.

Fidèle à sa mission de sécuriser Internet pour tous, Yubico fait don de YubiKeys à des organisations qui aident les personnes à risque par le biais de l'initiative philanthropique Secure it Forward. Ses sièges sociaux sont situés à Stockholm et à Santa Clara, en Californie. Pour plus d'informations sur Yubico, rendez-vous sur: www.yubico.com.