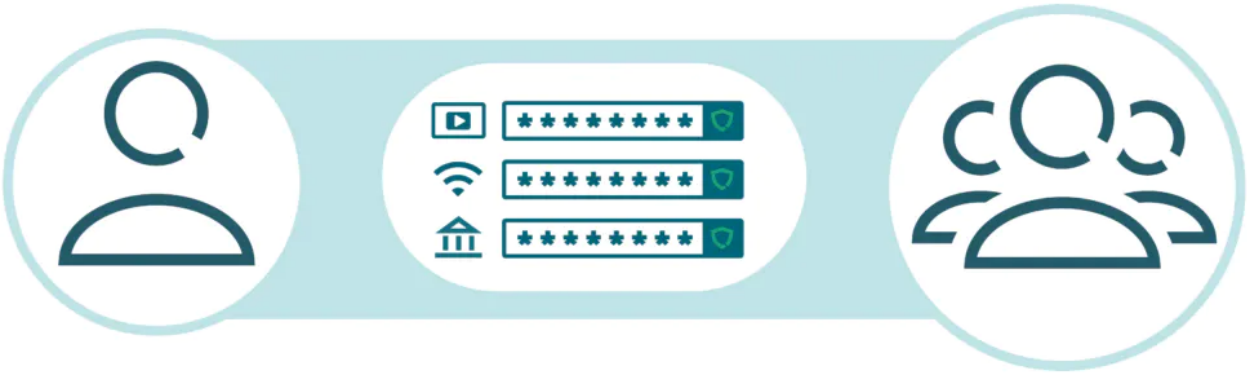
Restez protégé en évitant les 7 erreurs les plus courantes en matière de partage de mots de passe

W. Perry Wortman :

Partager des identifiants avec des personnes de confiance peut sembler inoffensif, mais cela peut entraîner des risques et des vulnérabilités en matière de sécurité.
Examinons de plus près les erreurs à éviter, ainsi que les bonnes pratiques en matière de partage sécurisé des mots de passe.

Les mots de passe pour les services de streaming (comme Hulu), les comptes de vente au détail (comme Amazon), ainsi que les réseaux Wi-Fi et les outils numériques sur le lieu de travail (comme le compte Twitter de l'entreprise), sont couramment partagés avec des amis, des membres de la famille ou des collègues.
Le partage des mots de passe est presque inévitable pour bon nombre de ces comptes, car créer des comptes et des mots de passe individuels pour chaque utilisateur peut s'avérer peu pratique ou inabordable.
Cependant, ce n'est pas parce que c'est une pratique courante que la sécurité est garantie.
Pour minimiser les risques auxquels vous vous exposez, vous devez apprendre à partager des mots de passe en toute sécurité.

Attitudes à adopter lors du partage des mots de passe



Avant de pouvoir partager en toute sécurité des mots de passe, vous devez renforcer l'hygiène de vos mots de passe.
Cela suppose d'établir et de maintenir de bonnes habitudes en matière de cybersécurité pour éviter le piratage, les failles de données et le vol de mots de passe, autant de choses qui peuvent être favorisées par le partage de mots de passe.
Les bonnes pratiques en matière de mots de passe sont les suivantes :

- **Créer des mots de passe forts :** un mot de passe fort comprend au moins 12 caractères et un mélange aléatoire de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux.
  Un mot de passe sécurisé laisse de côté les chaînes de caractères séquentielles telles que 12345 et les

phrases correspondant à des noms ou des adresses qui peuvent être liées à votre identité.
Si vous partagez des mots de passe faibles, vous exposez tous ceux avec qui vous avez partagé le mot de passe à des tactiques de piratage telles que les attaques par force brute et les attaques par dictionnaire qui s'attaquent aux mots de passe faibles et couramment utilisés.

- **Créer un mot de passe unique pour chaque compte :** avec autant de comptes et de mots de passe à gérer, la réutilisation des mots de passe est une habitude facile à adopter.
  Comme le partage de mots de passe, la réutilisation des mots de passe amplifie votre vulnérabilité. Si un mot de passe répété est perdu ou volé, les mêmes identifiants peuvent être utilisés pour pirater plusieurs comptes.
  L'outil d'analyse des mots de passe de Dashlane vous aide également à éliminer la réutilisation de mots de passe en fournissant des listes actualisées de vos mots de passe faibles, compromis et réutilisés.
- **Respecter la politique de mots de passe de votre lieu de travail :** l'établissement de règles de partage de mots de passe sur le lieu de travail est l'une des fonctions les plus importantes d'une politique de mots de passe en entreprise. Ces politiques aident à développer une culture de la sécurité pour renforcer les habitudes positives en matière de mots de passe.
  Elles peuvent également être utilisés pour éduquer les employés sur les dangers du partage de mots de passe lorsque les employés (ou les anciens employés) partagent des mots de passe de manière non sécurisée sans en informer l'équipe informatique.
- **Configurer la double authentification (2FA) :** la double authentification (2FA) utilise un deuxième identifiant, comme une notification push envoyée via une application ou un SMS, pour confirmer l'identité de l'utilisateur.
  Cela peut prolonger de quelques secondes votre temps de connexion, mais empêche presque totalement des intrus d'accéder à vos comptes sans avoir votre appareil en leur possession.
- **Modifier les mots de passe après une faille de données :** certaines entreprises persistent à imposer des règles obsolètes telles que des intervalles de 30 / 60 / 90 jours pour les réinitialisations des mots de passe.
  L'obligation de changer fréquemment de mot de passe peut en fait entraîner la création de mots de passe moins sécurisés si les utilisateurs effectuent de simples modifications, comme l'ajout d'un chiffre ou d'un symbole à la fin du mot de passe. Cependant, vous devez toujours modifier votre mot de passe immédiatement si vous pensez ou savez qu'il a été touché par une faille de données, et dire à toute personne avec qui vous avez partagé de faire de même.
- **Utiliser un gestionnaire de mots de passe :** lorsque vous apprenez à partager en toute sécurité des mots de passe, un gestionnaire de mots de passe facilite la création et la saisie automatique de mots de passe forts et leur enregistrement dans un coffre-fort chiffré.
  Des fonctionnalités telles que la double authentification, un score de sécurité et un portail de partage de mots de passe sécurisé et chiffré peuvent vous aider à améliorer l'hygiène de vos mots de passe afin de minimiser les risques associés au partage de mots de passe.

Attitudes à éviter lors du partage des mots de passe

Les risques liés au partage des mots de passe peuvent être minimisés en évitant quelques erreurs courantes et pratiques dangereuses.
Pour effectuer un partage sécurisé des mots de passe, assurez-vous d'éviter les habitudes suivantes :

1. **Noter les mots de passe et les exposer à la vue de tous :** le travail à distance et les listes de mots de passe de plus en plus longues ont entraîné une certaine négligence dans la gestion des mots de passe, comme le fait de les noter dans un carnet ou sur des notes autocollantes.
   Cela permet aux stratégies de vol de mots de passe démodées comme le shoulder surfing de rester efficaces à l'ère numérique.
2. **Partager des mots de passe par courriel :** les courriels sont-ils un moyen sécurisé de partager des mots de passe ?
   Non, la richesse des informations confidentielles partagées par courriel fait de ces comptes une cible de choix pour les pirates et les escrocs qui utilisent des méthodes telles que les attaques de phishing pour voler des mots de passe.
   Si vous partagez un mot de passe par courriel, les identifiants non chiffrés seront facilement détectables en cas de faille.
3. **Partager des mots de passe par SMS :** plus de 270 000 messages texte sont envoyés chaque seconde dans le monde, mais ils ne sont pas le meilleur moyen de partager des mots de passe.
   Tout comme les courriels, les SMS sont stockés indéfiniment dans un format non chiffré, et de nombreuses personnes enregistrent des SMS contenant des mots de passe pour s'y référer ultérieurement.
   Le partage de mots de passe par SMS les expose également en cas de perte ou de vol de votre téléphone portable.
4. **Partager des mots de passe sur Slack :** des entreprises de tous types utilisent des plates-formes de communication en ligne comme Slack pour collaborer et partager des informations en temps réel.
   Certaines personnes peuvent penser que ces fora sont également sécurisés pour le partage de mots de passe, mais ce n'est pas le cas.
   Le partage de mots de passe via Slack est risqué, car les messages non chiffrés sont stockés indéfiniment.
   De plus, de grands groupes d'utilisateurs peuvent avoir accès aux canaux Slack et augmenter le risque que des mots de passe tombent entre de mauvaises mains.
5. **Partager des mots de passe via un réseau Wi-Fi non sécurisé :** les réseaux Wi-Fi publics dans des endroits comme les aéroports, les cafés et les hôtels sont sensibles aux tactiques d'interception de données comme le spoofing du réseau Wi-Fi.
   Faites attention aux informations que vous partagez lorsque vous êtes sur un réseau Wi-Fi public et utilisez un VPN dans la mesure du possible.
   Un VPN réduit le risque d'interceptions de données en chiffrant toutes les données qui entrent ou sortent de votre appareil et en les acheminant via un portail sécurisé.

Le spoofing de réseau Wi-Fi se produit lorsqu'un cybercriminel crée un réseau sosie pour imiter un véritable réseau et inciter les gens à s'y connecter.

6. **Enregistrer des mots de passe dans un fichier partagé non chiffré :** les entreprises et les organisations à but non lucratif comme VillageReach ont appris d'office que les portails de partage de mots de passe ne sont pas sécurisés, à moins qu'ils n'incluent un chiffrement et des commandes d'accès adéquates.
   Les coffres de mots de passe en accès ouvert permettent aux utilisateurs de modifier les mots de passe stockés qui peuvent être utilisés par d'autres personnes ou de les copier et de les coller dans des gestionnaires de mots de passe non protégés de votre navigateur.
7. **Perdre la trace de qui a quel mot de passe :** lorsque le partage de mots de passe n'est pas contrôlé, il est difficile de se souvenir des personnes avec lesquelles vous les avez partagés et de savoir si les informations les concernant sont à jour.
   Cela peut créer un désagrément mineur pour les amis et les membres de la famille lorsque des mots de passe de streaming ou de Wi-Fi sont modifiés, mais pose un risque de sécurité plus grave pour les entreprises lorsque les employés quittent l'organisation alors qu'ils sont en possession d'identifiants de comptes actifs de l'entreprise.

FAQ sur le partage de mots de passe

Avez-vous d'autres questions sur la gestion de mots de passe de comptes partagés et comment partager en toute sécurité des mots de passe ?
Cet important problème de cybersécurité a fait l'objet de plusieurs foires aux questions :

- **Quels sont les risques de sécurité liés aux mots de passe partagés ?**

Les risques de sécurité accrus dus au piratage et aux failles de données peuvent en fin de compte entraîner une perte de données, d'argent ou de la confidentialité pour plusieurs utilisateurs.
Les mots de passe partagés augmentent également le risque de verrouillages de compte lorsque les mots de

passe sont mis à jour.
La traçabilité des transactions importantes est également diminuée lorsque plusieurs utilisateurs partagent des identifiants de compte ou de système.

- **Les mots de passe partagés sont-ils plus facilement piratés ?**

Oui. Les mots de passe partagés sont plus faciles à pirater, en particulier lorsque des mots de passe faibles sont utilisés par commodité ou que la double authentification n'est pas déployée.
L'acte de partage introduit des opportunités d'escroquerie et de piratage si l'on n'utilise pas un portail sécurisé et chiffré.
Les méthodes de partage non sécurisées augmentent également la vulnérabilité face au vol de mots de passe physiques et aux failles de données.

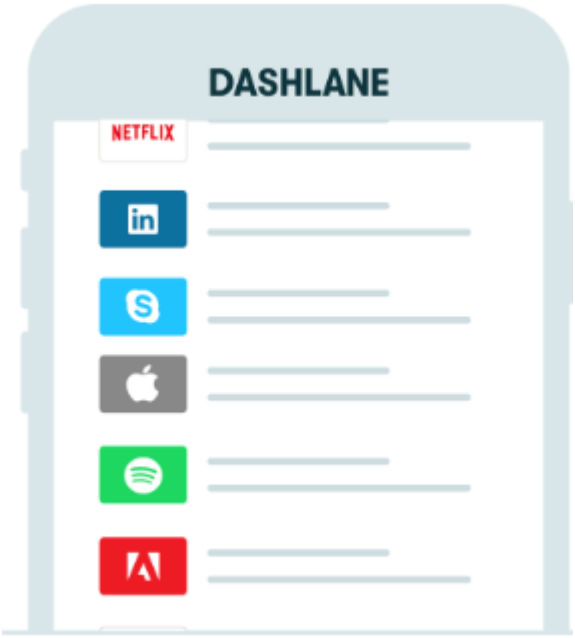
- **Quels types de mots de passe sont les plus fréquemment partagés ?**

Les mots de passe les plus couramment partagés sont faciles à deviner, car nous sommes nombreux à les avoir nous-mêmes partagés.
Les comptes d'abonnement (Amazon, Hulu), le Wi-Fi et les comptes financiers sont en tête de liste à la maison, tandis que les mots de passe des médias sociaux, des cartes de crédit et des applications professionnelles sont couramment partagés sur le lieu de travail.

- **Quelle est la fréquence du partage de mots de passe ?**

Une étude récente a montré que 79 % des Américains partagent leurs mots de passe. Cela n'est pas surprenant, étant donné l'opinion dominante selon laquelle le partage de mots de passe est inévitable.
Plus inattendu est le fait que seulement 7 % de ces personnes interrogées sont préoccupées par le piratage informatique.
Cette divergence suggère un manque de sensibilisation aux risques liés au partage de mots de passe.

- **Comment un gestionnaire de mots de passe rend-il le partage de mots de passe plus sûr ?**



Un gestionnaire de mots de passe sécurise le partage de mots de passe en générant des mots de passe forts et aléatoires et en fournissant des coffres sécurisés pour le stockage et le partage de mots de passe, de sorte que vos données sont chiffrées et protégées en toute sécurité.
Des fonctionnalités supplémentaires, y compris la double authentification, un VPN et un score de sécurité, vous protègent des attaques externes tout en améliorant l'hygiène et la productivité des mots de passe.

Dashlane fournit également la surveillance du dark Web pour analyser les profondeurs d'Internet à la recherche de vos identifiants et vous alerte s'ils y sont détectés.
Le portail de partage chiffré de Dashlane utilise une architecture brevetée « zero-knowledge » pour s'assurer que personne (y compris Dashlane) n'a accès à vos mots de passe non chiffrés et à vos messages privés
Vous pouvez partager des mots de passe avec d'autres utilisateurs Dashlane via le portail sécurisé et chiffré et éviter les habitudes de partage de mots de passe non sécurisées.

Références

1. Dashlane, « 7 Password Hygiene Best Practices to Follow », février 2023.
2. Dashlane, « 10 Bad Password Examples: Avoid These Common Mistakes » (10 exemples de mauvais mots de passe : évitez ces erreurs courantes), mars 2023.
3. Dashlane, « How Password Reuse Leads to Cybersecurity Vulnerabilities », mai 2023.
4. Dashlane, « Understanding Your Dashlane Password Health Score, » octobre 2020.
5. Dashlane, « Créez une politique de mots de passe que vos collaborateurs suivront à la lettre », juillet 2022.
6. Microsoft, « What is two-factor authentification », 2023.
7. Dashlane, « Changez toujours vos mots de passe après une faille de données », mars 2020.
8. Dashlane, « Build the Case for a Password Manager in 8 Steps », 2023.
9. Experian, « What is Shoulder Surfing? » octobre 2020.

10. Dashlane, « What To Do If a Scammer Has Access To Your Email » (Que faire si un escroc a accès à votre adresse e-mail), avril 2023.
11. True List, « Texting Statistics – 2023 », février 2023.
12. Dashlane, « Le partage de mots de passe sur Slack : une pratique risquée », novembre 2019.
13. NIST, « Man-in-the middle attack (MITM) », 2023.
14. Dashlane, « Pourquoi avez-vous besoin d'un VPN ? Ses 3 grands avantages pour votre sécurité », août 2020.
15. Dashlane, « Étude de cas : VillageReach élimine des centaines de mots de passe réutilisés et renforce la sécurité de son personnel dans le monde entier », février 2022.
16. Dashlane, "Best Way to Store Passwords at Home or Work", septembre 2022.
17. Dashlane, « What Is Password Sharing & When Should I Use It », [Qu'est-ce que le partage de mots de passe et quand dois-je l'utiliser ?] février 2023.
18. The Zebra, « 79% of Americans Share Passwords, But Only 13%Are Worried About Identity Theft », janvier 2023.
19. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.
20. Dashlane Dark Web Monitoring: Your Employees Are Likely Using Compromised Passwords », juillet 2022.
21. Dashlane, « 7 Dangers of Sharing Passwords Without a Password Manager », mars 2023.
22. Dashlane, « Partager vos éléments enregistrés dans Dashlane », 2023.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230930
"C'est ensemble qu'on avance"