Avantages et inconvénients du gestionnaire de mots de passe Google

W. Perry Wortman ⋮

L’utilisation du gestionnaire de mots de passe Google est-elle sécurisée ?
Le gestionnaire de mots de passe intégré à Google Chrome est une option populaire pour des millions d’utilisateurs, alors examinons ses avantages et ses inconvénients, ainsi que quelques alternatives.

Avec nos listes grandissantes d’identifiants et une foule de tactiques de piratage à surveiller, nous avons tous besoin d’un gestionnaire de mots de passe pour sécuriser notre navigation et nos transactions en ligne.
Les principaux développeurs de navigateurs tels que Google proposent dès lors un gestionnaire de mots de passe intégré.
Ces options intégrées :

- **Sont automatiquement installées et activées par défaut.** Si vous utilisez Google Chrome et avez créé votre propre compte Google, vous êtes déjà prêt à utiliser le gestionnaire de mots de passe Google intégré qui est activé par défaut.
  À moins de désactiver manuellement cette fonctionnalité, une boîte de dialogue familière continuera de s’afficher pour vous demander si vous souhaitez que Google enregistre vos identifiants chaque fois que vous vous connectez à un compte en ligne.
- **Facile d’accès, pour tout le monde.** L’enregistrement des mots de passe dans Chrome est-il sécurisé ?
  Si vous avez utilisé le gestionnaire de mots de passe Google dans le passé, vous savez probablement

que votre liste de mots de passe enregistrés est seulement à quelques clics dans le menu Paramètres. C'est vrai pour vous, ainsi que pour toute personne qui obtient l'accès à votre appareil.

- **Saisissez automatiquement vos informations.** Une fonctionnalité connue sous le nom de saisie automatique, courante pour les gestionnaires de mots de passe, vous permet de saisir automatiquement les noms d'utilisateur et les mots de passe enregistrés lorsque vous revenez sur le même site Web, éliminant ainsi la nécessité de mémoriser des mots de passe ou de les noter.
  Cette fonctionnalité particulièrement pratique peut devenir problématique si un pirate informatique accède à votre compte Google et que les mots de passe pour les comptes privés apparaissent automatiquement.
  Les gestionnaires de mots de passe comme Dashlane utilisent des méthodes de saisie automatique plus sécurisées pour protéger les données de ses clients, telles que la non-saisie automatique sur les formulaires invisibles, le fait de vous avertir si vous essayez de saisir automatiquement un identifiant sur un nouveau site Web et également d'empêcher l'accès aux données du coffre-fort par le biais d'un site Web avec un menu de saisie automatique.

Voulez-vous en savoir plus sur l'utilisation du gestionnaire de mots de passe Dashlane pour particulier ou pour entreprise ?

Découvrez nos forfaits pour gestionnaires de mots de passe pour particulier ou commencez avec un essai gratuit pour les entreprises.

Les avantages de l'utilisation des gestionnaires de mots de passe de navigateur

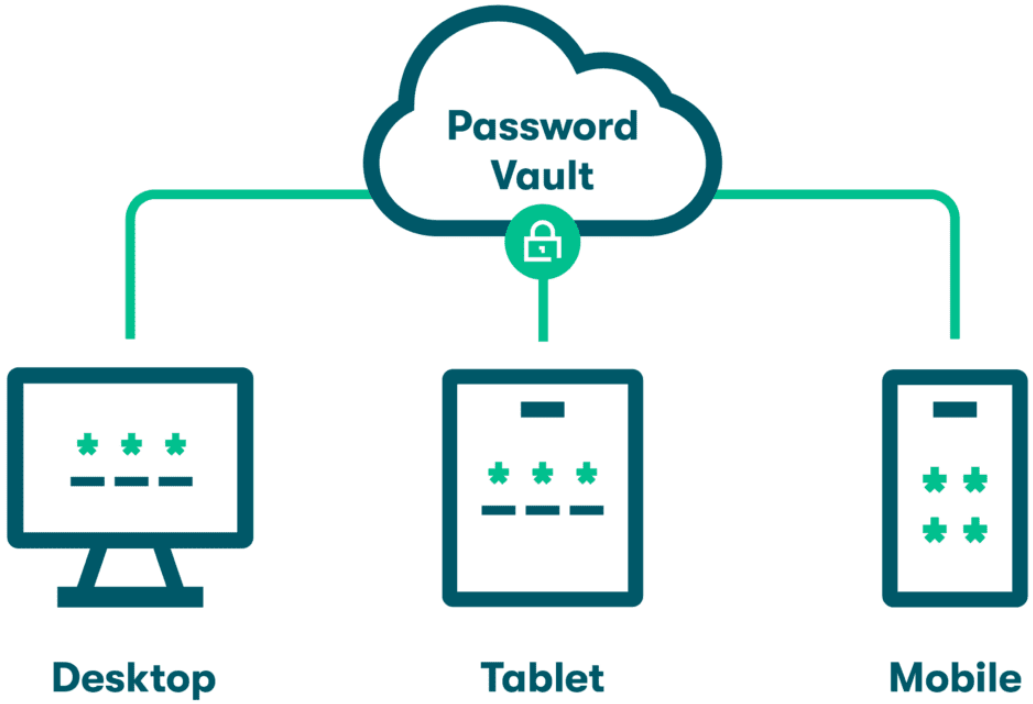
De nombreuses personnes qui choisissent d'utiliser uniquement Google Chrome ou un autre navigateur majeur aiment la simplicité offerte par une option de gestion de mots de passe intégrée.
Les avantages de l'utilisation des gestionnaires de mots de passe de navigateur comprennent :

- **Commodité :** il n'y a rien à installer ou à configurer avec les gestionnaires de mots de passe de navigateur.
  Certains font le choix de cette commodité plutôt que des fonctionnalités de sécurité d'un gestionnaire de mots de passe autonome.
  Ceux qui ont déjà stocké plusieurs identifiants dans leur navigateur pourraient également préférer poursuivre cette utilisation plutôt que de prendre le temps d'exporter leur liste de mots de passe lors du passage à une option autonome.
- **Gratuit :** le gestionnaire de mots de passe Google, comme les autres gestionnaires de mots de passe intégrés à votre navigateur, est toujours totalement gratuit, et les clients peuvent envisager cet avantage dans leur choix de gestionnaires de mots de passe.
  Ce n'est pas un hasard si près de 95 % des applications iOS dans l'Apple Store sont toujours offertes gratuitement.
  En effet, de nombreux clients préfèrent sacrifier les fonctionnalités souhaitées pour éviter un engagement financier, même minime.

Les inconvénients de l'utilisation des gestionnaires de mots de passe de navigateur

L'utilisation du gestionnaire de mots de passe Google est-elle sécurisée ?
Tous les gestionnaires de mots de passe de navigateur intégrés ne disposent pas de fonctionnalités et d'avantages importants en matière de sécurité.
Cela devrait être soigneusement pris en compte lors du choix entre les gestionnaires de mots de passe de navigateur et les gestionnaires de mots de passe autonomes.

- **Fonctionnalité limitée :** les fonctionnalités de base d'un gestionnaire de mots de passe de navigateur comprennent la génération de mots de passe, le stockage de mots de passe et la saisie automatique.
  Mais est-ce que cela suffit ?
  Les fonctionnalités incluses avec les gestionnaires de mots de passe autonomes forment une solution de cybersécurité plus complète.
  Ceux-ci peuvent inclure des portails de partage sécurisé de mots de passe, un score de sécurité des mots de passe pour surveiller l'hygiène de vos mots de passe, un VPN, une authentification unique (SSO) et la surveillance du dark Web pour scanner les recoins cachés d'Internet à la recherche de vos informations privées.
  De plus, un gestionnaire de mots de passe autonome se synchronise sur tous vos appareils et comptes en dehors de Chrome.



- **Vulnérabilités de sécurité :** aucun examen du gestionnaire de mots de passe Google ne serait exhaustif sans aborder certaines des vulnérabilités connues à Google Chrome.
  L'utilisation d'un navigateur pour la gestion de mots de passe expose vos identifiants si les faiblesses du

navigateur lui-même sont exploitées.
En 2022, les chercheurs ont découvert une vulnérabilité dans le navigateur Chrome qui aurait pu permettre de voler des milliards de fichiers si elle n'était pas corrigée. De plus, Chrome peut être ouvert en un seul clic, ce qui peut exposer vos données sensibles de mots de passe un peu trop facilement.

Comment utiliser en toute sécurité le gestionnaire de mots de passe Google

Pour ceux qui choisissent cette option, prendre quelques précautions de sécurité supplémentaires peut aider à compenser certains des risques et des vulnérabilités.

- **Envisagez de ne pas l'utiliser :** les fonctionnalités de sécurité limitées et les vulnérabilités connues vous rendent plus vulnérable à une cyberattaque.
  Le choix le plus sûr est d'éviter d'utiliser les gestionnaires de mots de passe de navigateur de tout type et d'effacer tous les mots de passe enregistrés dans les navigateurs pour éviter qu'ils ne soient exposés à l'avenir.
  Au lieu de cela, utilisez un gestionnaire de mots de passe autonome.
  Un gestionnaire de mots de passe autonome et intuitif renforce la sécurité de tous vos mots de passe.
  Les meilleurs gestionnaires de mots de passe créent des mots de passe complexes pour vos comptes, puis les chiffrent et les enregistrent en toute sécurité dans le cloud pour les protéger du piratage et des failles de données.
- **Utilisez des mots de passe forts :** le gestionnaire de mots de passe Google vous permet de poursuivre l'utilisation de vos mots de passe précédemment créés, même s'ils sont faibles ou réutilisés, bien qu'il vous fournisse une fonctionnalité de générateur de mots de passe.
  C'est donc à vous de créer des mots de passe forts que les pirates informatiques ont plus de mal à deviner et qui ne déverrouillent pas plusieurs comptes.
- **Ne prêtez pas votre ordinateur :** avec des mots de passe et des informations enregistrées sur les comptes facilement accessibles via le menu Paramètres de Chrome, partager votre ordinateur ou votre appareil avec d'autres personnes signifie également partager votre liste d'identifiants.
  Il est plus sage d'éviter de prêter votre ordinateur au vu des risques de compromission de confidentialité, même avec vos amis et vos proches, si vous utilisez le gestionnaire de mots de passe Google.
- **Ne partagez pas vos mots de passe :** partager des mots de passe avec vos amis et les membres de votre famille est une pratique courante, surtout pour des choses telles que les comptes de vente en ligne et les services de streaming.
  Le partage de mots de passe augmente votre degré d'exposition si les personnes avec qui vous partagez vos mots de passe sont les cibles d'un cybercrime.
  À la différence des gestionnaires de mots de passe de navigateur, les meilleurs gestionnaires de mots de passe autonomes incluent des portails de partage sécurisé et chiffré de mots de passe qui vous permettent de transférer des identifiants en toute sécurité.
  Par exemple, le portail de partage Dashlane peut être utilisé pour partager des notes sécurisées et des mots de passe avec d'autres utilisateurs de Dashlane.
- **Sécurisez votre compte Google :** dans quelle mesure le gestionnaire de mots de passe Google est-il sécurisé ?

Cela dépend en partie de la sécurité générale de votre compte Google, puisque toutes les applications que vous utilisez via le compte sont connectées.
Vous pouvez sécuriser votre compte Google et optimiser la sécurité du gestionnaire de mots de passe Google en créant un mot de passe fort et unique pour votre compte Google, en mettant en place une double authentification (2FA), en veillant à ce que votre adresse courriel de récupération soit à jour et en gardant un œil sur toutes les applications tierces qui ont l'autorisation d'accéder à votre compte Google.

Pourquoi les gestionnaires de mots de passe autonomes sont plus sécurisés

Avec autant de fonctionnalités avancées en matière de sécurité et de confidentialité pour vous protéger du piratage et sécuriser vos données, les meilleurs gestionnaires de mots de passe autonomes sont tout simplement plus sécurisés que le gestionnaire de mots de passe tels que celui de Google Chrome.
Un bon gestionnaire de mots de passe autonome :

1. **Inclus un stockage sécurisé :** les gestionnaires de mots de passe autonomes de haute qualité chiffrent vos mots de passe sur votre appareil ou votre ordinateur avant de les transporter vers un serveur cloud protégé pour le stockage.
   Dashlane utilise une architecture « zero-knowledge » brevetée pour s'assurer que personne (pas même Dashlane) ne peut accéder à vos informations non chiffrées. L'utilisation de votre mot de passe Maître ou de la SSO sécurisée est la seule façon dont vos données stockées peuvent être déverrouillées.

2. **Réduit la réutilisation des mots de passe :** avec une personne moyenne jonglant maintenant avec plus de 240 comptes en ligne, la réutilisation des mots de passe est une habitude de plus en plus courante.
   Cette pratique peut nous rendre plus vulnérables aux tactiques de piratage telles que le credential stuffing, car plusieurs comptes peuvent être touchés.
   Les fonctionnalités de surveillance fournies avec les meilleurs gestionnaires de mots de passe autonomes, comme le score de sécurité des mots de passe Dashlane, découragent la réutilisation des mots de passe en vous fournissant une liste actualisée de vos mots de passe faibles, compromis et réutilisés.
3. **Fonctionne avec tous les navigateurs** : comme les autres gestionnaires de mots de passe intégrés aux navigateurs, celui de Google ne fonctionne que lorsque vous utilisez le navigateur Chrome.
   Les mots de passe enregistrés deviennent inaccessibles dès que vous quittez Chrome.
   L'extension du navigateur Dashlane fonctionne avec tous les principaux navigateurs et systèmes d'exploitation, notamment Chrome, Firefox, Microsoft Edge, Linux et Chromebook, de sorte que vos fonctionnalités de génération, de stockage et de saisie automatique de mots de passe vous accompagnent lorsque vous naviguez sur différentes plates-formes et appareils.
4. **Fonctionnalités supplémentaires :** d'autres fonctionnalités précieuses que vous ne trouverez pas toujours dans les gestionnaires de mots de passe de navigateur incluent la double authentification, la SSO, le partage sécurisé de mots de passe, la synchronisation automatique des mots de passe sur tous les appareils, la surveillance du dark Web et un VPN.
   Un VPN vous protège du piratage et des interceptions de données lors de l'utilisation des réseaux Wi-Fi publics en chiffrant toutes les données qui entrent ou sortent de votre appareil et en les acheminant via un portail sécurisé.
   Un VPN masque également votre adresse IP pour faire en sorte que votre navigation reste privée.

Dashlane optimise la sécurité des mots de passe sans compromettre sa commodité en combinant les meilleures fonctionnalités de sécurité du gestionnaire de mots de passe autonome disponibles avec les avantages d'un score de sécurité des mots de passe, d'un portail de partage sécurisé de mots de passe et d'une génération de mots de passe personnalisables et de paramètres de saisie automatique.
Comme Dashlane fonctionne avec n'importe quel navigateur majeur, ces avantages vous accompagnent 24 heures sur 24.

Bien que les cybercriminels se perfectionnent, c'est aussi le cas des outils qui protègent vos ressources en ligne.
En suivant six règles de cybersécurité essentielles**, vous pouvez nettoyer votre empreinte numérique et sécuriser vos données personnelles.**

Références

1. PC Magazine, « How to Master GooglePassword Manager », avril 2022.
2. Dashlane, « Le chiffrement expliqué par Dashlane » mars 2019.
3. Dashlane, « 6 Things a Safe Username Should Always Do », février 2023.
4. Statista, « Distribution of free and paid iOS apps in the Apple App Store as of March 2023 », mars 2023.

5. Dashlane, « Understanding Your Dashlane Password Health Score, » octobre 2020.
6. Dashlane « Percer l'obscurité du dark Web », juin 2022.
7. Computer Weekly, « Chrome vulnerability could have led to widespread data theft », janvier 2023.
8. Dashlane, « How to Erase Saved BrowserPasswords : Step-by-Step Guide », novembre 2022.
9. Dashlane, "How Strong Is Your Password & Should You Change It?" août 2022.
10. Dashlane, « Partager vos éléments enregistrés dans Dashlane », 2023.
11. Dashlane, « 4 Steps to Secure Your Google and Gmail Accounts », novembre 2021.
12. Dashlane, « Build the Case for a Password Manager in 8 Steps », 2023.
13. Dashlane, « A Deep Dive into Dashlane's Zero-Knowledge Security », juin 2022.
14. Dashlane « A look at Password Health Scores around the world in 2022 », 2022.
15. Dashlane, « The Best Browser Extensions for Digital Privacy », octobre 2020.
16. Dashlane, « Pourquoi avez-vous besoin d'un VPN ? Ses 3 grands avantages pour votre sécurité », août 2020.
17. Dashlane : « Do You Have These 6 Cybersecurity Basics Down ? », juin 2022.
18. Dashlane, « How to Export Google Chrome Passwords to a CSV », avril 2023.
19. Dashlane, « Guide de protection des mots de passe contre les pirates informatiques », février 2023.
20. PCMag, « How to Master Google Password Manager », avril 2022.
21. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.
22. Dashlane, « 7 Dangers of Sharing Passwords Without a Password Manager », mars 2023.
23. Dashlane, « A Beginner's Guide to Two-Factor Authentication », août 2022.
24. CrowdStrike, « Credential Stuffing », mars 2022.

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