
Votre bulletin mensuel sur la sensibilisation à la sécurité

# Gestionnaire de mots de passe

## Aperçu

L'une des étapes les plus importantes que vous pouvez prendre pour vous protéger consiste à utiliser un mot de passe unique et fort pour chacun de vos comptes et applications. Malheureusement, il est presque impossible de se souvenir de tous les différents mots de passe. De plus, nous savons que cela prend du temps de devoir constamment taper vos mots de passe sur différents sites, générer de nouveaux mots de passe, répondre aux questions de sécurité et autres étapes. Cependant, il existe une solution qui vous simplifiera la vie et la rendra beaucoup plus sûre : les gestionnaires de mots de passe.

## Gestionnaire de mots de passe

Les gestionnaires de mots de passe fonctionnent en stockant tous vos mots de passe dans une base de données, parfois appelée coffre-fort. Le gestionnaire de mots de passe crypte le contenu du coffre-fort et le protège avec un mot de passe principal que vous seul connaissez. Lorsque vous avez besoin de vos mots de passe, par exemple pour vous connecter à votre banque en ligne ou à votre boite mail, il vous suffit de taper votre mot de passe principal dans votre gestionnaire de mots de passe pour déverrouiller le coffre-fort. Le gestionnaire de mots de passe récupérera automatiquement le mot de passe correct et vous connectera en toute sécurité au site Web. Vous n'avez plus besoin de mémoriser vos mots de passe ou de vous connecter manuellement à vos comptes.

De plus, la plupart des gestionnaires de mots de passe peuvent être synchronisés automatiquement sur plusieurs appareils. De cette façon, lorsque vous mettez à jour un mot de passe sur votre ordinateur portable, ces modifications sont synchronisées avec tous vos autres appareils. Enfin, la plupart des gestionnaires de mots de passe détectent lorsque vous essayez de créer un nouveau compte en ligne ou de mettre à jour le mot de passe d'un compte existant. Ils mettent alors automatiquement à jour le coffre-fort pour vous.

Il est essentiel que le mot de passe principal que vous utilisez pour protéger le gestionnaire de mots de passe soit long et unique. D'ailleurs, nous vous recommandons de faire de votre mot de passe principal une phrase de passe. C'est un mot de passe long composé de plusieurs mots ou expressions. Si votre gestionnaire de mots de passe prend en charge la vérification en deux étapes, utilisez-le également pour votre mot de passe principal. Enfin, assurez-vous de bien vous souvenir de votre phrase de passe principale. Si vous l'oubliez, vous ne pourrez accéder à aucun de vos autres mots de passe.

## Choisir un gestionnaire de mots de passe.

Il existe de nombreux gestionnaires de mots de passe parmi lesquels choisir. Dans la section Ressources, nous fournissons un lien vers des avis sur des gestionnaires de mots de passe. En attendant, lorsque vous essayez de trouver celui qui vous convient le mieux, gardez à l'esprit les points suivants :

**Votre gestionnaire de mots de passe doit être simple à utiliser. Si vous trouvez la solution trop complexe à comprendre, trouvez-en une autre qui correspond mieux à votre style et à votre expertise.**

**Le gestionnaire de mots de passe devrait fonctionner sur tous les appareils sur lesquels vous devez utiliser des mots de passe. Il devrait également être facile de synchroniser vos mots de passe sur tous vos appareils.**

**Utilisez uniquement des gestionnaires de mots de passe connus et fiables. Méfiez-vous des produits qui n'existent pas depuis longtemps ou qui ont peu ou pas de commentaires de la communauté. Les cybercriminels peuvent créer de faux gestionnaires de mots de passe pour voler vos informations. Aussi, méfiez-vous des fournisseurs qui clament avoir développé leur propre solution de chiffrement.**

**Évitez tout gestionnaire de mots de passe qui prétend pouvoir récupérer votre mot de passe principal pour vous. Cela signifie qu'ils connaissent votre mot de passe principal, ce qui vous expose à trop de risques.**

**Assurez-vous que, quelle que soit la solution que vous choisissez, le fournisseur continue de mettre à jour et de corriger activement le gestionnaire de mots de passe. Soyez particulièrement sûr que vous utilisez toujours la version la plus récente.**

**Le gestionnaire de mots de passe devrait vous donner la possibilité de stocker d'autres données sensibles, telles que les réponses à vos questions de sécurité, les numéros de carte bancaire et les numéros de comptes.**

**Pensez à écrire votre phrase de passe principale dans une enveloppe scellée et à la stocker dans une armoire verrouillée ou un coffre-fort.**

Les gestionnaires de mots de passe sont un excellent moyen de stocker en toute sécurité tous vos mots de passe et autres données sensibles, telles que les numéros de carte bancaire. Cependant, assurez-vous d'utiliser une phrase de passe principale forte et unique et utilisez toujours la dernière version de la solution que vous choisissez.

## Rédacteur Invité

***Russell Eubanks*** *est un leader de la sécurité de l'information basé à Atlanta, avec plus de 20 ans d'expérience et détient de nombreuses certifications en sécurité. Il est gestionnaire au SANS Internet Storm Center et contribue aux contrôles de sécurité critiques. Russell peut être joint à @russelleubanks et à : https://www.securityeverafter.com.*

## Ressources

| | |
|---|---|
| Simplifier les mots de passe : | http://www.sans.org/u/10Uu |
| Héritage digitale : | http://www.sans.org/u/10Uz |
| Avis sur les meilleurs gestionnaires de mots de passe : | https://www.wired.com/story/best-password-managers/ |