Devriez-vous autoriser votre navigateur à se souvenir de vos mots de passe

Malwarebytes

Pieter Arntz :

Chez Malwarebytes, nous disons aux gens depuis des années de ne pas réutiliser les mots de passe, et qu'un gestionnaire de mots de passe est un moyen sûr de se souvenir de tous les mots de passe dont vous avez besoin pour vos comptes en ligne.

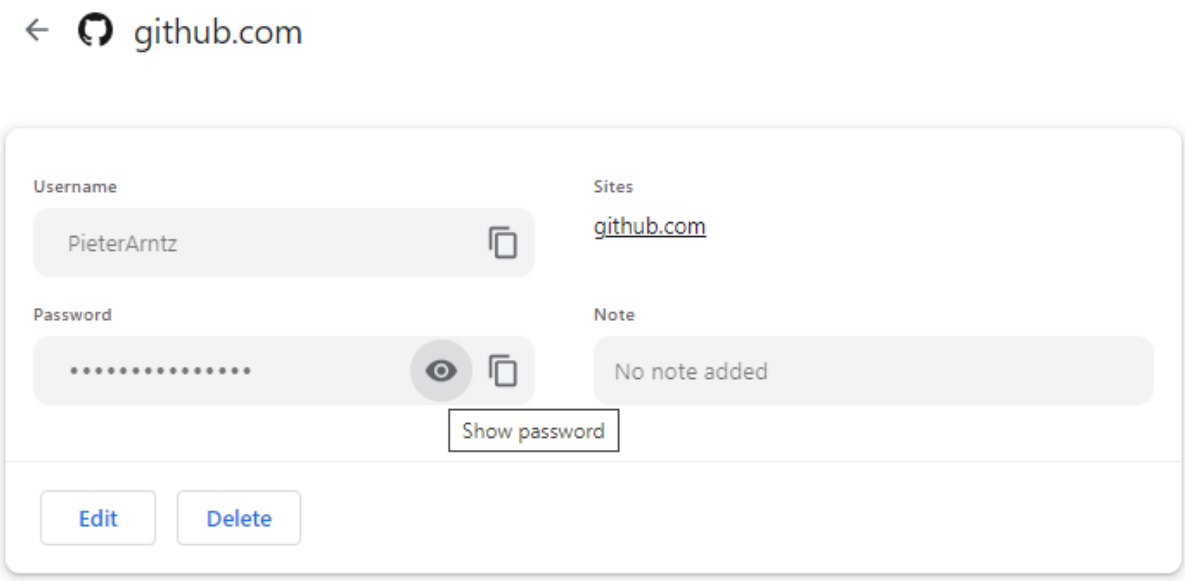
Mais nous savons aussi qu'un gestionnaire de mots de passe peut être accablant, surtout lorsque vous débutez.
Une fois que vous avez stocké vos dizaines, voire centaines de mots de passe, un gestionnaire de mots de passe est relativement pratique à utiliser et à mettre à jour.
Mais il faut d'abord arriver à ce stade et tout le monde n'a pas le même niveau de connaissances en informatique.

Alors, vous vous êtes peut-être demandé s'il y avait un autre moyen.
Sans aucun doute, vous aurez vu les fenêtres contextuelles dans votre navigateur vous demandant si vous souhaitez qu'il enregistre votre mot de passe pour la prochaine fois. En fait, de nombreux navigateurs s'y réfèrent comme à leur gestionnaire de mots de passe.

C’est très pratique, car votre navigateur est généralement l’application qui a besoin du mot de passe, mais est-ce une bonne idée ?

Comme d’habitude, il y a des avantages et des inconvénients.

Chiffrement. Avec un gestionnaire de mots de passe de navigateur, une personne ayant accès à votre navigateur pourrait voir vos mots de passe en texte clair, bien que Windows puisse être configuré pour demander une authentification (la même que celle que vous utilisez au démarrage de votre appareil).



L’option « Afficher le mot de passe »

Pour voir les mots de passe dans un gestionnaire de mots de passe réel, un attaquant aurait besoin de connaître le mot de passe du gestionnaire de mots de passe ou la phrase de récupération, qui sont généralement beaucoup plus difficiles à trouver que l’authentification Windows (si elle est définie).

Un mot d’avertissement ici, certains gestionnaires de mots de passe ont la possibilité de vous garder connecté pendant des heures, voire des jours.
S’il y a une chance que quelqu’un puisse obtenir un accès physique, de tels paramètres vont à l’encontre de la sécurité supplémentaire d’un gestionnaire de mots de passe, car l’attaquant pourrait ouvrir le gestionnaire de mots de passe et regarder vos mots de passe plus ou moins de la même manière qu’il le ferait dans votre navigateur.

Sites d’hameçonnage similaires:
Un gestionnaire de mots de passe autonome et celui de votre navigateur vous protégeront ici.
Ils ne rempliront pas votre mot de passe si le domaine ne correspond pas à celui pour lequel vous avez enregistré le mot de passe, ce qui pourrait indiquer un site d’hameçonnage.
Cela peut être très utile et c’est là que c’est mieux que d’écrire le mot de passe sur un morceau de papier ou de le stocker dans un fichier texte.

Je dois ajouter que les domaines pour lesquels il vaut la peine de créer un faux site sont généralement ceux auxquels nous vous conseillons d'ajouter l'authentification multifacteur (MFA).

Synchronisation:
Si vous avez stocké vos mots de passe dans le navigateur et que vous avez choisi de synchroniser votre navigateur entre les appareils, vos mots de passe seront également transférés.
C'est évidemment très pratique, mais c'est aussi un danger potentiel si quelqu'un accède à l'un de vos appareils.
Un véritable gestionnaire de mots de passe ne repose pas sur la synchronisation entre le même navigateur et différents appareils.
Une fois que vous avez installé le gestionnaire de mots de passe sur un appareil, vous pouvez l'utiliser dans n'importe quel navigateur ou d'autres applications.

Hors-ligne:
De nombreux gestionnaires de mots de passe mettent en cache vos mots de passe localement, de sorte que vous y avez toujours accès lorsque votre connexion est interrompue.
Le stockage des mots de passe du navigateur ne le permet pas.

Appareils professionnels:
Il est difficile pour le service informatique de savoir quel utilisateur a quels mots de passe enregistrés dans son navigateur.
Les gestionnaires de mots de passe pour les entreprises leur donnent un meilleur aperçu et facilitent la révocation des mots de passe en cas de besoin.

Voleurs de mots de passe:
Il existe des types de logiciels malveillants capables de collecter des mots de passe à partir de votre appareil.
Ils savent exactement où les navigateurs stockent leurs mots de passe et la clé de chiffrement, ce qui leur permet de voler et d'envoyer les informations d'identification à l'attaquant.
Les gestionnaires de mots de passe sont distincts du navigateur, ils ne sont donc pas exposés aux mêmes risques.

Violations de données:
Plusieurs gestionnaires de mots de passe vous avertiront s'ils constatent que vos informations d'identification sont impliquées dans une violation de données, afin que vous puissiez les modifier.
Le stockage du navigateur ne fait pas cela.

Mots de passe complexes:
Les humains sont mauvais pour créer et mémoriser des mots de passe complexes.
Un gestionnaire de mots de passe et certains navigateurs peuvent vous aider à créer un mot de passe qui répond à la complexité requise et à le stocker pour que vous n'ayez pas à vous en souvenir.

Attaques par canal auxiliaire:
Comme nous l'avons vu avec un bug récent dans Safari, les attaquants peuvent utiliser la fonction de remplissage automatique d'un navigateur pour collecter les identifiants de connexion d'un site.
Cela ne fonctionne que si vous avez activé la saisie automatique, donc pour rendre les choses un peu plus

sûres, vous pouvez demander à votre navigateur d'attendre votre OK avant de remplir les données.
Voici comment:

Comment désactiver la saisie automatique

- **Brave:**
  Paramètres > Saisie automatique et mots de passe > Gestionnaire de mots de passe > Paramètres.
  Désactivez l'option « Se connecter automatiquement »

- **Chrome:**
  Paramètres > Saisie automatique et mots de passe > Gestionnaire de mots de passe Google > Paramètres.
  Désactivez l'option « Se connecter automatiquement ».

- **Edge:**
  Paramètres > Profils > Mots de passe > Paramètres.
  Là, vous pouvez désactiver la saisie automatique pour les mots de passe et pour les données personnelles séparément.

- **Firefox :**
  Paramètres > Confidentialité et sécurité.
  Faites défiler vers le bas jusqu'à Identifiants et mots de passe et décochez « Remplissage automatique des identifiants et mots de passe ».

- **Opéra:**
  Paramètres > Paramètres avancés > Remplissage automatique > Gestionnaire de mots de passe > Paramètres.
  Désactivez l'option « Connexion automatique ».

- **Safari:**
  Safari (dans la barre de menus) > Réglages > Remplissage automatique.
  Décochez « Noms d'utilisateur et mots de passe » et « Cartes de crédit ».

Alors, devriez-vous permettre à votre navigateur de se souvenir de vos mots de passe ?

Le gestionnaire de mots de passe de votre navigateur vous offre une « facilité d'utilisation », mais cela vous coûte une partie de votre sécurité.
Bien sûr, les gestionnaires de mots de passe ne sont pas infaillibles non plus, il est donc important de décider vous-même où vous stockez vos mots de passe.

Si vous êtes sûr que le site Web est sûr et que toute personne qui peut y accéder sous votre compte n'apprendra rien de nouveau, n'hésitez pas à stocker le mot de passe dans votre navigateur, mais désactivez la saisie automatique afin que vous soyez celui qui a le contrôle.

Utilisez l’authentification multifacteur dans la mesure du possible.
Cela réduit considérablement le risque si quelqu’un met la main sur votre mot de passe. Et évitez d’utiliser le gestionnaire de mots de passe du navigateur pour stocker les détails de votre carte de crédit ou d’autres informations personnelles sensibles identifiables (par exemple, des informations médicales).

Nous ne nous contentons pas de signaler les menaces, nous les supprimons

Les risques liés à la cybersécurité ne doivent jamais dépasser les gros titres.
Éloignez les menaces de vos appareils en téléchargeant Malwarebytes dès aujourd’hui.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231108
"C'est ensemble qu'on avance"