

Chapitre 1 : Gestionnaire de mots de passe

De nombreux mots de passe et d'innombrables données d'enregistrement sont nécessaires pour utiliser régulièrement Internet. Un mot de passe doit être aussi sécurisé que possible et se composer de différents chiffres, lettres et caractères spéciaux.

En effet, grâce à la technologie actuelle, les cybercriminels ont de plus en plus de facilité à « cracker » les mots de passe simples. Ci-dessous, je vous montre un tableau qui indique qu'un mot de passe « normal » (formé de 8 lettres majuscules et minuscules, au hasard) peut être trouvé en moins d'une demi-heure...

Temps requis pour déchiffrer un mot de passe					
Traduction libre des données recueillies par Hive Systems via howsecureismypassword.net (2020)					
NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	7(10 ⁴⁸) ans

Un mot de passe compliqué est donc nécessaire pour sécuriser ses données. Mais qui peut se souvenir de plusieurs de ces mots de passe compliqués (par exemple 10 caractères avec symboles, chiffres, lettres)? La réponse à cette question importante est simple: **un gestionnaire de mots de passe!**

En effet, trouver un mot de passe compliqué comme « beeMQq6p6 » nécessitera 3 jours à un ordinateur actuel (et certainement moins de 6 heures pour les prochaines générations d'ordinateurs...). Alors que hacker un mot de passe plus compliqué comme « p3Z*U3qU4&a@ » nécessite environ **34'000 années** pour le trouver...

Voilà comment fonctionne un gestionnaire de mots de passe

Un grand nombre de foyers privés (ou d'entreprises) misent aujourd'hui sur des programmes intelligents capables de **générer des mots de passe** et de stocker des **données** dans un **coffre-fort numérique sécurisé**. Le logiciel possède un algorithme intelligent et sécurisé et peut générer des nouveaux mots de passe par simple clic.

Les utilisateurs peuvent définir eux-mêmes diverses options ou choisir les paramètres standards. La longueur des mots de passe, les majuscules et minuscules, les chiffres et les caractères spéciaux peuvent être utilisés. **Il suffit d'appuyer sur un bouton** pour que le gestionnaire de mots de passe génère un **mot de passe hautement sécurisé**, impossible à déchiffrer même par un **pirate informatique** professionnel.

Le programme stocke les mots de passe et autres données de connexion dans une banque de données sécurisée, un **coffre-fort numérique à cryptage SSL**. Le gestionnaire de mots de passe peut sauvegarder des données de connexion en ligne, des mots de passe et également des données de paiement et autres informations personnelles de manière sécurisée.

Grâce à la **fonctionnalité Cloud** et à une **synchronisation automatique**, les utilisateurs ont accès à leurs données enregistrées sur chaque appareil (ordinateur, smartphone,...). Cela ne fonctionne bien entendu que lorsque les utilisateurs indiquent leur **mot de passe maître (le seul mot de passe à se souvenir)**.

Le remplissage automatique de formulaires permet de gagner beaucoup de temps.

Chaque programme **génère** d'une part **des mots de passe sécurisés** et **gère** d'autre part **les données**. La disponibilité d'autres fonctionnalités dépend du gestionnaire de mots de passe choisi. De nombreux développeurs améliorent leurs logiciels avec le temps et leur ajoute des fonctionnalités utiles. Celle du **remplissage automatique de formulaire** est particulièrement pratique tout en faisant gagner du temps.

En effet, ces formulaires se retrouvent pratiquement sur tous les sites Internet (chaque fois qu'on vous demande votre identifiant / login et mot de passe). En commandant quelque chose en ligne, les utilisateurs d'Internet doivent à chaque fois renseigner leur nom, adresse et de nombreux autres champs. Le gestionnaire de mots de passe peut le faire à leur place et permet de leur faire gagner beaucoup de temps, et surtout sans se tromper.

La banque de données sécurisée contient toutes les informations de connexion et les mots de passe importants. Associé à une **extension de navigateur**, le gestionnaire de mots de passe peut indiquer ces données automatiquement sur tous les sites Internet. Ce qui signifie par exemple que lorsque vous utilisez Chrome ou Firefox, le site « reconnaît » votre profil et vous propose d'entrer le nom d'utilisateur et mot de passe associé.

Pourquoi tout le monde devrait utiliser un gestionnaire de mots de passe

Un gestionnaire de mots de passe est gratuit ou coûte **peu d'argent**. Les acheteurs profitent de **mots de passe sécurisés** et ne sont plus obligés de les mémoriser. Pour accéder à la banque de données cryptée, ils doivent impérativement indiquer leur **mot de passe maître** et peuvent **accéder** aux informations enregistrées **sur un grand nombre d'appareils**. Grâce au remplissage automatique de formulaires en ligne, surfer sur Internet devient beaucoup plus agréable et sûr.

Installation et utilisation

1. **Choix du gestionnaire de mot de passe**
2. **Téléchargement du gestionnaire sur l'appareil**
3. **Installation du gestionnaire de mots de passe**
4. **Installation des extensions de navigateur**
5. **Création du compte d'utilisateur**
6. **Génération d'un mot de passe maître sûr (ne doit pas être oublié)**
7. **Importation de toutes les données des navigateurs**
8. **Installation en option d'une application mobile**
9. **Sécurisation supplémentaire via l'authentification à double facteur (si disponible)**

Principaux gestionnaires de mot de passes

1. **Bitwarden (logiciel open source)**
2. **Dashlane**
3. **1Password**
4. **LastPass**
5. **Bitwarden**
6. **NordPass**
7. **RoboForm**

Mon choix : Bitwarden

Je vous laisserai aller regarder les comparatifs sur Internet. Mais j'ai choisi Bitwarden, car il est très performant, Open source, relativement simple d'utilisation, et très sécurisé. Il a de plus :

- Très bonnes évaluations de tous les testeurs
- Nombre quasi illimité de mots de passe et d'appareils
- Synchronisation du smartphone et du PC
- Remplissage automatique du login et mot de passe
- Proposition de mots de passe sécurisés, personnalisable
- Cryptage de toutes les données personnelles
- Possibilité d'entrer vos données comme cartes de crédit, etc...

Téléchargement (anglais) : <https://bitwarden.com/>