médiaTHEQUE
MUNICIPALE de
SAINT SYMPHORIEN
Jean Vautrin

Sécurité :
Les mots de passe
La solution Bitwarden

Octobre 2021

Publics		Niveau		Prérequis
Jeunes		Débutant	x	Windows
Adultes		Moyen	x	IOS
Tous	x	Confirmé	x	Android

Vous venez de participer à un atelier sur les mots de passe. Nous vous avons expliqué ce qu'est un mot de passe fort, les techniques pour le créer et s'en souvenir. Nous vous avons aussi présenté les aides matérielles pour ne plus les perdre, parmi elles, nous avons choisi de vous présenter le logiciel Bitwarden.

1 - Les règles pour un mot de passe fort

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde.

A - Les pires mots de passe en 2019

Voici un aperçu des mots de passe les moins sécurisés utilisés en 2020, ils sont à proscrire totalement :
123456 - qwerty - password - iloveyou - 111111 - 123123 - abc123 - 1q2w3e4r - admin - welcome - dragon - sunshine - liverpool - freedom - football - charlie - secret - nothing ...

B - Qu'est-ce qu'un mot de passe fort

- Un mot de passe est personnel et confidentiel, il ne doit jamais être divulgué
- Il doit être difficile à deviner, sans lien avec votre vie personnelle (prénom, date, ville, etc.)
- Il doit être long, 8 à 12 caractères
- Il doit être composé de chiffres, caractères spéciaux, lettres majuscules et minuscules
- Il peut être composé de plusieurs mots sans aucun rapport entre eux.

Pour des raisons de sécurité, il est préférable d'utiliser un mot de passe unique pour chaque service. Enfin, il faut le changer régulièrement (idéalement tous les 90 jours), pour le moins, au moindre soupçon d'utilisation frauduleuse.

C - Comment créer et retenir ses mots de passe

Vous trouverez ci-dessous quatre méthodes pour créer un mot de passe fort et s'en souvenir. Ces méthodes ne sont qu'indicatives, aucune n'est meilleure qu'une autre.
Libre à chacun de vous de créer votre propre technique et le moyen mnémotechnique de s'en rappeler.

- **Méthode 1 :** retenir la ou les premières lettres de chaque mot composant une phrase.

Ensuite, à chacun d'apporter sa petite touche personnelle en y incorporant quelques majuscules (une lettre sur deux, ou sur trois par exemple), et chiffres (remplacer certaines lettres par des chiffres dont la typographie est voisine s'avère très efficace).
Exemple : utilisons la phrase suivante : « L'œil ne voit rien si l'esprit est distrait » : En optant pour l'utilisation de la première lettre de chaque mot, d'une majuscule toutes les deux lettres, et des remplacements des O et des E par des 0 et 3, on obtient : L'0nVrSl'33D. Un tel mot de passe prendrait environ 500 millions d'années à être déchiffré par un ordinateur standard.

- **Méthode 2 :** l'utilisation de la phonétique.

En prononçant une phrase, chaque son générera l'un des caractères du mot de passe. Naturellement, toutes les phrases ne s'y prêtent pas, mais une fois le choix fait, la mémorisation sera aisée.
Exemple : on se basera sur la phrase suivante « J'ai acheté trois œufs et deux BD ce matin ». Toujours avec une majuscule toutes les deux lettres, on obtient : gHt3Eé2BdCeMaT1.

- **Méthode 3 :** l'utilisation d'une structure commune afin de gérer une diversité de mots de passe.

Il est possible de créer un tronc commun, complété d'une seconde partie propre à chaque service (Facebook, Twitter etc.). Exemple de tronc commun (fixe) : Deux mots sans aucuns rapport évident entre eux.

Exemple : Pluie&2fraises auquel on ajoute des lettres pour chaque service. Pluie&2fraisesFb (pour Facebook), Pluie&2fraisesGm (pour Gmail) etc...

- **Méthode 4 :** Choisissez un mot de passe « classique », puis décalez chaque lettre d'une touche vers la droite.

Exemple : en partant du prénom Jean-Claude, on obtient (toujours avec une majuscule pour deux lettres) KrZ,èVmZiFr.

Une fois le mot de passe choisi, n'hésitez pas à aller le tester sur un **vérificateur de mot de passe** (password.kaspersky.com/fr) qui informe de son niveau de sécurité et qui donne une estimation du temps nécessaire à le pirater. Vous percevrez alors rapidement la faiblesse de nombreuses combinaisons que vous considériez comme inviolables.

C - Comment retenir tous ses mots de passe

La quantité de sites internet nécessitant la création d'un compte avec mot de passe multiplie le nombre de mots de passe à retenir. Malheureusement, notre cerveau n'est pas aussi fiable que le disque dur de notre ordinateur, nous avons donc besoin d'aide.
Cliquer sur « Mot de passe oublié » n'étant pas une solution pérenne, il nous est obligatoire de chercher d'autres astuces :

- Les **moyen mnémotechniques**, les petites astuces personnelles peuvent être efficaces si nous n'avons que peu de comptes à gérer.

- Tout le monde s'est déjà servi d'un **carnet papier ou du bloc note de son téléphone** pour y enregistrer de façon plus ou moins claire ses précieux mots de passe. Il faut cependant noter que ces solutions ont aussi leurs limites : Carnet à la maison quand on a besoin du mot de passe, carnet égaré, fichier détruit par erreur, perte ou panne du téléphone et donc pertes des informations qu'il contenait…

- Demander à votre **navigateur d'enregistrer les mots de passe** pour vous est une solution bien pratique, à condition d'accepter de confier vos données personnelles à Google ou Firefox, avec les dangers bien connus de vols de données que rencontrent toutes ces grandes entreprises. De plus, votre ordinateur ne sera pas toujours à portée de main quand vous devrez vous connecter sur un service par le recours à un mot de passe.

- Le moyen le plus sûr, surtout dans le cadre professionnel, dans le cas d'un très grand nombre de comptes à retenir ou encore pour utiliser indifféremment plusieurs outils numériques, est le **gestionnaire de mots de passe**. Il permet de mémoriser les codes d'accès de tous les sites utilisés, au sein d'une même base de données, accessible elle-même à l'aide d'un unique mot de passe. De nombreux logiciels existent : *Bitwarden, KeePass, LastPass, ZenyPass, Password…*

2 - Utilisation d'un gestionnaire de mots de passe, l'exemple de « Bitwarden »

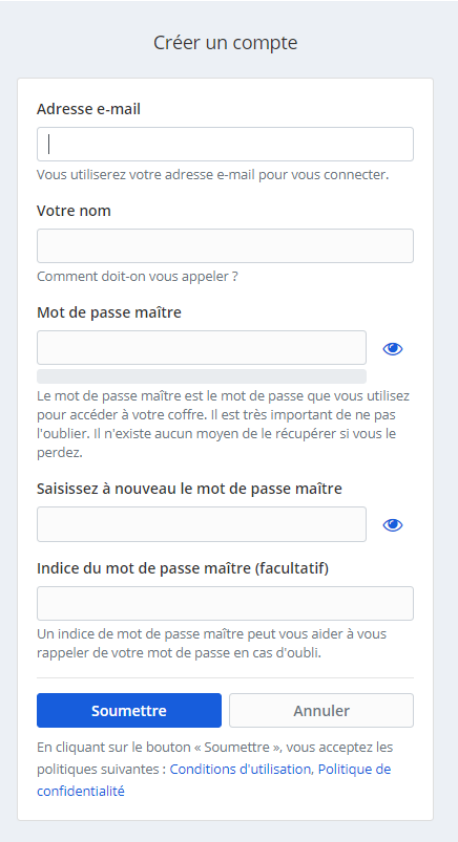
Bitwarden est un gestionnaire de mots de passe **gratuit et open source**.
Il fonctionne en mode **logiciel (Windows, Mac, Linux)** en mode **application (iOS et Android)** mais aussi en mode **extension pour les navigateurs Chrome, Firefox, Edge et Safari.**
Grâce au **cloud Bitwarden**, vous pouvez **synchroniser vos différents appareils** afin d'avoir vos mots de passe partout avec vous. Vous pouvez **générer des mots de passe complexes** et sécurisés et les stocker de manière illimitée. Vous pouvez également créer des notes sécurisées et gérer vos cartes de paiement et vos documents officiels.

A - Installez Bitwarden sur vos différents appareils

La fiche détaillée de PCastuces vous guidera dans cette entreprise : pcastuces.com/pratique/securite/mots_passe_bitwarden/page2.htm

La page de téléchargements pour toutes les plateformes se trouve à l'adresse suivante : bitwarden.com/download/
Pour vos appareils mobiles, vous pouvez vous rendre directement dans l'Appstore ou le Playstore de votre appareil mobile.

B - Créer votre compte Bitwarden



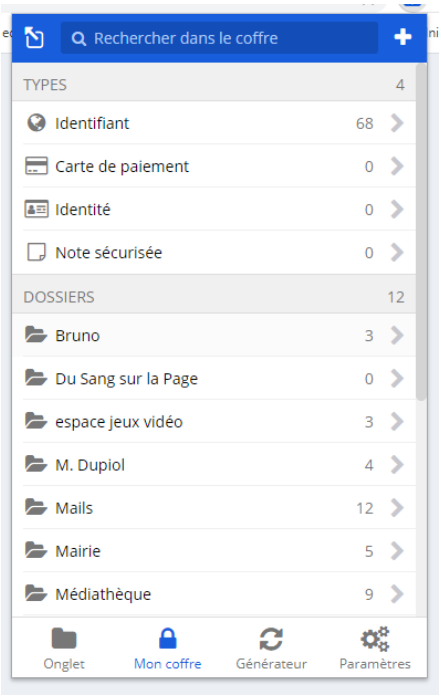
Afin de pouvoir utiliser le logiciel et de retrouver tous vos mots de passe sur tous vos appareils, il est obligatoire de **créer un compte**.

Pour cela vous devez remplir les champs : *« Adresse mail », « Votre nom »* (qui peut-être un pseudo), *« Mot de passe maître » et « Saisissez à nouveau le mot de passe maître »*. Attention, les deux champs correspondant au mot de passe maître doivent être **rigoureusement identiques** !

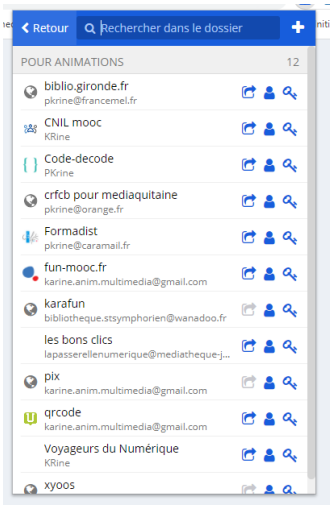
N'hésitez pas à mettre un **mot de passe complexe**, car c'est le seul dont vous devrez vous souvenir désormais. Mettez à profit toutes les recommandations précédentes. Si vous le souhaitez, vous pouvez entrer un « Indice du mot de passe maître » pour vous aider en cas de doute ultérieur.

Pour une utilisation simple et optimale de Bitwarden sur ordinateur, il est préférable d'utiliser l'extension de votre navigateur. Ainsi, au fur et à mesure de votre navigation, Bitwarden vous proposera de vous connecter aux services dont il conserve les mots de passe, ou d'enregistrer ceux qui ne sont pas déjà dans sa base de données.

C - Organisez vos mots de passe

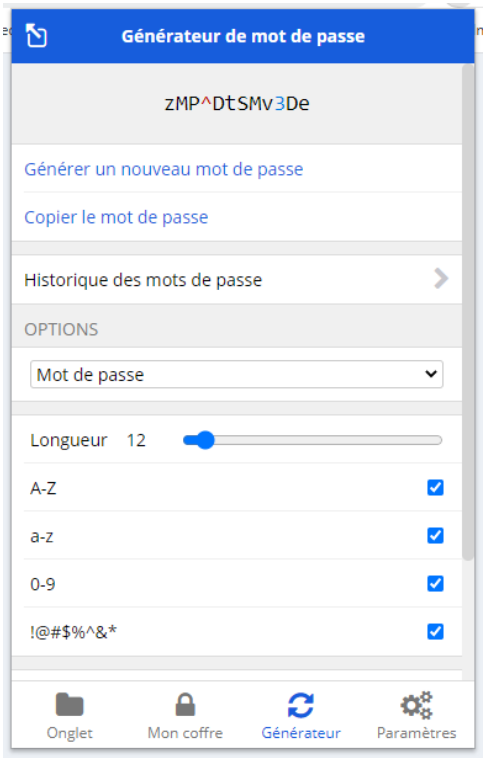


Dans l'onglet « *Mon coffre* », vous avez la possibilité de **créer et d'organiser les dossiers** afin de classer vos mots de passe par type ou thème.
En face de chaque dossier, le chiffre vous indique combien d'entrées contient le dossier.



En ouvrant le dossier, toutes les entrées disponibles apparaissent. Seuls sont visibles l'adresse du site et l'identifiant, le mot de passe reste masqué.

D - Générer un mot de passe



L'onglet *« Générateur »* permet de définir les **caractéristiques** nécessaires à la création automatique d'un mot de passe. Comme nous l'avons vu précédemment, dans l'idéal, il doit être composé de 8 à 12 caractères, et contenir des majuscules, des minuscules, des chiffres et des caractères spéciaux.

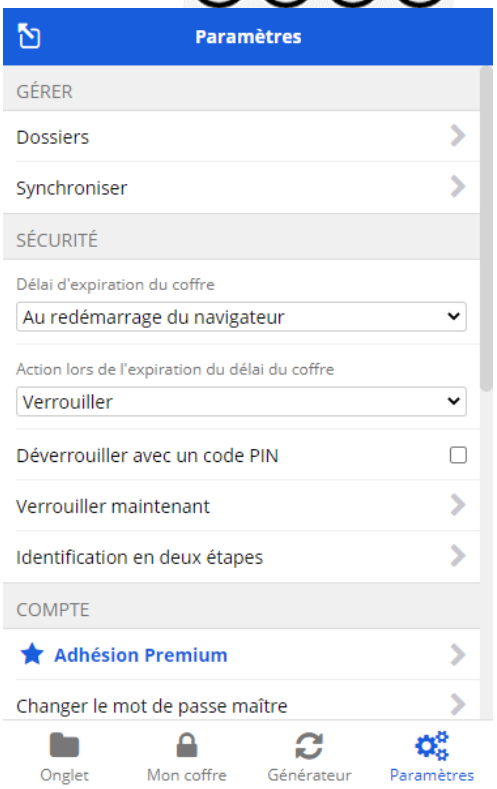
Une fois bien paramétré, le mot de passe généré peut facilement être copié pour la création d'un compte. Attention, ces mots de passe étant totalement aléatoires, vous n'avez aucune chance de vous en souvenir, alors n'oubliez pas de bien **enregistrer l'entrée** correspondante !

E - Les paramètres

a - Gérer

Cette zone permet de **gérer les dossiers** (Créer, supprimer, modifier le nom,…).
En dessous, **synchroniser** vous permet de synchroniser immédiatement votre base de données. Cette option est quasi inutile, en principe, Bitwarden synchronise en temps réel vos modifications et ajouts.

b - Sécurité



« Délai d'expiration du coffre » vous permet de définir à quel moment vous devrez de nouveau saisir votre mot de passe maître pour avoir accès à votre base de données. Plusieurs options se déroulent de *« Immédiatement » à « Jamais ».*

« Action lors de l'expiration du délai du coffre » vous propose de verrouiller votre base de données (le code PIN suffit à l'ouvrir de nouveau) ou de vous déconnecter du service (il vous faudra saisir votre mot de passe maître pour avoir de nouveau accès aux services de Bitwarden).

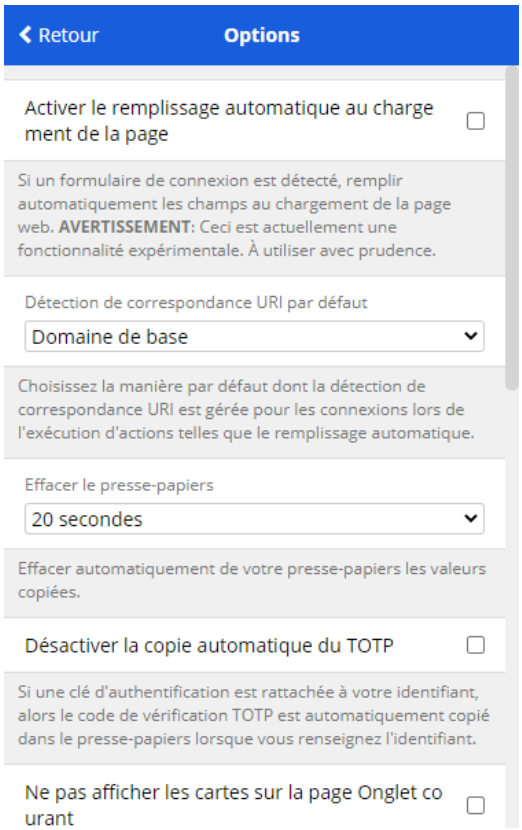
« Déverrouiller avec un code PIN » vous permet, si la case est cochée, de déverrouiller votre Base de données avec un code PIN que vous aurez choisi, plutôt que le mot de passe maître.

c - Compte

Vous aurez ici la possibilité de **changer votre mot de passe maître** et de vous **déconnecter** du service (utile si vous êtes sur un ordinateur public).

d - Outils

C'est dans cette partie des paramètres que vous aurez la possibilité d'**importer** vos mots de passe (de transférer la base de données d'un autre service comme Chrome, FireFox ou encore KeePass dans Bitwarden). A l'inverse, si vous souhaitez récupérer les données stockées sur Bitwarden pour les tranférer ensuite dans un autre service, il vous est proposé de les **exporter.**



e - Option

Ici, vous pouvez peaufiner les réglages de votre logiciel : activer le **remplissage automatique au chargement de la page** des données de connexion quand elles sont enregistrées dans votre base de données, choisir après combien de temps **effacer le presse-papiers** automatiquement, changer la couleur de l'application **(thème),** etc...