cybernews.com /best-password-managers/how-to-create-a-strong-password/

Comment créer de bons mots de passe forts Cybernews

Šarūnas Karbauskas Écrivain ⋮

Tout le monde a des données sensibles stockées sur des comptes en ligne qui nécessitent une protection infaillible.
Cependant, la plupart des internautes optent pour des identifiants de compte faciles et faciles à mémoriser, qui sont loin d'être des mots de passe vraiment forts.
De plus, beaucoup supposent que le meilleur mot de passe dans une situation donnée est peu pratique et difficile à mémoriser.

Heureusement, il existe de nombreuses façons et idées de créer des mots de passe forts, **comme l'utilisation d'un** outil de génération de mots de passe unique.
Ici, nous allons vous présenter nos conseils et astuces pour choisir et configurer des mots de passe forts et difficiles à deviner pour vos comptes en ligne.

Dashlane et 1Password sont des gestionnaires de mots de passe les meilleurs et les plus sécurisés avec des fonctionnalités multiplateformes.
Il met en œuvre un cryptage inviolable pour partager tous vos fichiers en toute sécurité et vous permet de remplir automatiquement toutes les informations nécessaires.
Il existe un essai gratuit de 14 jours pour essayer le gestionnaire de mots de passe sans aucun risque.

Et nous partagerons certaines de nos méthodes préférées pour protéger vos mots de passe et les moyens de vous assurer que vous n'aurez plus jamais à cliquer sur le lien « Mot de passe oublié ».

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

Un mot de passe fort est un mot de passe que vous **ne pouvez pas deviner ou déchiffrer à l'aide d'une** attaque par force brute.
Les pirates utilisent des ordinateurs pour essayer diverses combinaisons de lettres, de chiffres et de symboles à la recherche du bon mot de passe.
Les ordinateurs modernes peuvent déchiffrer des mots de passe courts composés uniquement de lettres et de chiffres en quelques instants.
Cela signifie que les progrès dans le domaine technologique conduisent également à des améliorations dans les arsenaux des pirates malveillants.

En tant que tels, les mots de passe forts consistent en une combinaison de lettres majuscules et minuscules, de chiffres et de symboles spéciaux, tels que la ponctuation.
Ils doivent comporter **au moins 12 caractères**, bien que nous vous recommandons de les rendre encore plus longs.

Dans l'ensemble, voici les **principales caractéristiques d'un bon mot de passe sécurisé :**

- Comporte au moins 12 caractères.
  Plus votre mot de passe est long, mieux c'est.
- Utilise des lettres majuscules et minuscules, des chiffres et des symboles spéciaux. Les mots de passe composés de caractères mixtes sont plus difficiles à déchiffrer.
- Ne contient pas de chemins de clavier mémorables.
- N'est pas basé sur vos informations personnelles.
- Les mots de passe sont uniques pour chaque compte que vous possédez.

Lorsque vous créez un compte en ligne, il y a souvent des invites vous rappelant d'inclure des chiffres ou un certain nombre de caractères.
Certains peuvent même vous empêcher de définir un « mot de passe faible », qui est généralement une combinaison de mots ou de chiffres facile à deviner.

Mais même si l'on ne vous rappelle pas de définir un mot de passe fort, il est impératif de le faire chaque fois que vous créez un nouveau compte en ligne ou que vous modifiez les mots de passe d'un compte existant.

Comment créer un mot de passe fort ?

1. Utiliser des combinaisons de mots de passe longs
2. Combiner des chiffres, des lettres minuscules et majuscules
3. Évitez les mots de passe populaires
4. Utilisez un gestionnaire de mots de passe sécurisé pour créer des mots de passe forts

Un mot de passe long est un bon mot de passe

Lorsqu'il s'agit de la sécurité des mots de passe, la longueur est essentielle.
Nous vous recommandons d'opter pour **un mot de passe d'au moins 12 caractères**, voire plus si vous le pouvez.

Chaque symbole supplémentaire dans un mot de passe augmente de manière exponentielle le nombre de combinaisons possibles.
Cela rend les mots de passe d'une certaine longueur essentiellement indéchiffrables, en supposant que vous n'utilisez pas d'expressions courantes.

Un mot de passe fort n'est pas évident

Un bon mot de passe doit être difficile à deviner ou à déchiffrer pour les personnes extérieures, alors **n'optez pas pour quelque chose de générique, comme « mot de passe » ou « 12345 ».**
Ces deux-là font également partie des mots de passe les plus populaires au monde, ce qui en fait de terribles choix de mots de passe.

Une autre catégorie de mots de passe populaire, peu exigeante et inefficace est **celle des chemins de clavier séquentiels**.
L'exemple le plus populaire est « qwerty », bien que d'autres options existent.
Ceux-ci sont exceptionnellement faibles et doivent être évités à tout prix.

Les mots de passe forts ne contiennent pas d'informations personnelles

Il est essentiel que vous **n'incluiez pas d'informations personnelles dans votre mot de passe**, comme un surnom, une date de naissance ou le nom de l'animal de compagnie.
Ces informations sont faciles à trouver pour les pirates simplement en consultant vos médias sociaux, en trouvant votre profil professionnel en ligne ou en écoutant une conversation que vous avez avec quelqu'un d'autre.

Un bon mot de passe est unique

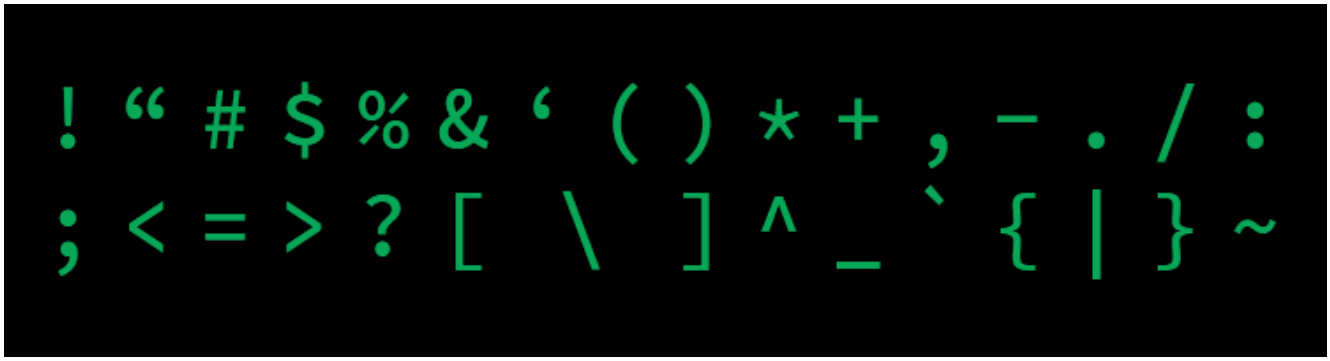
Une fois que vous avez créé un mot de passe fort, vous pourriez être tenté de l'utiliser pour tous vos comptes en ligne.
Mais, si vous faites cela, **cela vous rend plus vulnérable à de multiples attaques**.

Après tout, si un pirate parvient à découvrir votre mot de passe, il pourra se connecter à tous les comptes qui utilisent ce mot de passe, ce qui peut inclure vos courriels, vos réseaux sociaux et vos comptes professionnels.
Par conséquent, vous devez créer un mot de passe unique pour chaque compte que vous possédez.
Bien que fastidieuse, cette pratique est un élément essentiel d'une bonne hygiène en matière de cybersécurité.

Une autre **caractéristique cruciale des mots de passe uniques est qu'ils ne sont pas recyclés**.
Si les informations d'identification d'un ancien compte sont divulguées, les pirates ajouteront son mot de passe à une base de données d'options potentielles à tester lors du piratage d'autres comptes.
Ainsi, l'utilisation d'un mot de passe ancien et « fiable » pourrait entraîner votre perte.

Les mots de passe forts utilisent des caractères spéciaux

Bien que l'utilisation de caractères spéciaux dans vos mots de passe soit un excellent moyen de les rendre plus sûrs, tous les services en ligne ne permettent pas d'utiliser n'importe quel symbole que vous aimez.
Mais la plupart d'entre eux autorisent ce qui suit :



Les caractères spéciaux sont un excellent moyen d'ajouter du caractère aléatoire et imprévisible à vos identifiants de connexion, les rendant ainsi plus forts contre les attaques par force brute.
Il n'y a pas de règles que vous devez suivre pour un effet maximal ; Il vous suffit d'inclure quelques caractères spéciaux là où bon vous semble pour créer le mot de passe le mieux adapté à vos besoins.

Exemples de mots de passe forts

Vous trouverez ci-dessous quelques exemples de mots de passe efficaces et efficaces. Comme vous pouvez le constater, ils sont assez aléatoires et dénués de sens à première vue.
Bien que cela les rende difficiles à mémoriser, ils sont également beaucoup plus difficiles à déchiffrer pour les pirates malveillants.

- X5j13$#eCM1cG@Kdc
- %j8kr^Zfpr!Kf#ZjnGb$
- PkxgbEM%@hdBnub4T
- vUUN7E@!2v5TtJSyZ

Il s'agit d'une collection apparemment aléatoire et longue (plus de 15 caractères) de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
Ces mots de passe ne sont pas génériques et ne contiennent pas de chemins de clé mémorisables ou d'informations personnelles que les pirates pourraient utiliser.

Les meilleures idées pour créer un bon mot de passe

Il existe de nombreux outils que vous pouvez utiliser pour créer des mots de passe uniques et forts pour chacun de vos comptes en ligne.
Nous disposons d'un outil de génération de mots de passe prêt à l'emploi qui génère des mots de passe uniques et presque impossibles à déchiffrer.
Vous pouvez également suivre nos meilleurs conseils et idées sur la façon de configurer un bon mot de passe :

1. Utilisez un générateur de mots de passe

Si vous n'avez pas le temps de trouver vos mots de passe, un générateur de mots de passe **est l'outil parfait qui peut suggérer un mot de passe fort rapidement et facilement**.
Notre générateur de mot de passe sécurisé interne créera une séquence de caractères aléatoires.
Copiez-le et utilisez-le comme mot de passe pour votre appareil, votre courriel, votre compte de réseau social ou tout autre élément nécessitant un accès privé.

Certains outils de création de mots de passe incluent également des conseils sur la façon de se souvenir d'un mot de passe particulier.
Par exemple, la sortie :

K4k'F@F#>v_[2.z>

Est accompagné de l'indice suivant :

CORÉEN 4 coréen ' FRUIT @ FRUIT # > visa _ [2 .zip >

Il s'agit d'une bonne approche pour mémoriser les mots de passe forts que vous ne souhaitez pas stocker dans les gestionnaires de mots de passe pour une raison quelconque.

Les gestionnaires de mots de passe de premier ordre comprennent également des générateurs de mots de passe sécurisés.
Par exemple, Dashlane et 1Password peuvent vous aider à créer des mots de passe uniques et incassables ainsi que des phrases de passe.

2. Créez une phrase de passe forte plutôt qu'un mot de passe

Les phrases de passe sont beaucoup plus sûres que les mots de passe car elles sont généralement plus longues, ce qui les rend plus difficiles à deviner ou à forcer par la force brute.
Ainsi, au lieu de choisir un mot, choisissez une phrase et prenez les premières lettres, les premiers chiffres et la ponctuation de cette phrase pour générer une combinaison apparemment aléatoire de caractères.

Vous pouvez même remplacer plusieurs lettres d'un mot par des chiffres ou des symboles pour rendre le mot de passe plus imprévisible et, par conséquent, plus sûr.
Ou, essayez de remplacer les mots par de la ponctuation comme nous le faisions à l'époque de l'argot textuel, si vous vous souvenez d'aussi loin.

Il n'y a pas de règles spécifiques sur la façon de créer une phrase de passe forte, car les préférences de chacun varient. Idéalement, il devrait s'agir de quelque chose d'unique que vous seul pourriez imaginer et dont vous vous souviendrez.
Voici quelques exemples de la façon dont vous pouvez utiliser la méthode de phrase secrète pour créer des mots de passe forts :

Phrase	Mot de passe
Je suis allé à Disneyland pour la première fois quand j'avais 4 ans et cela m'a rendu heureux	I1stw2DLwIw8yrs&immJ
Mon ami Matt a mangé six beignets au café de la boulangerie et cela lui a coûté 10 £	MfMa6d@tbc&ich£10
Pour la première fois de son histoire, Manchester United s'est incliné 5-0 face à Manchester City	4da1sttymevaMU5:02MC

Remarque : n'utilisez pas d'expressions courantes, car elles sont vulnérables aux attaques par dictionnaire – les combinaisons aléatoires sont ce que vous voulez.

3. Optez pour une version plus sécurisée de la méthode du dictionnaire

Une méthode populaire pour choisir un mot de passe consiste à ouvrir un dictionnaire ou un livre et à choisir un mot au hasard.
Mais, aussi aléatoire que cela puisse vous paraître, un seul mot est en fait assez facile à deviner pour un pirate.

Donc, plutôt que d'opter pour un seul mot du dictionnaire, **choisissez-en quelques-uns et enchaînez-les avec des chiffres et des symboles** pour rendre la tâche beaucoup plus difficile à comprendre pour quelqu'un.

Voici quelques exemples de bonnes idées de mots de passe créés avec cette méthode :

Mots du dictionnaire	Mot de passe sécurisé
Puzzle, quête, trait, fourchette	Scie sauteuse%quest7trait/fork48
Aperçu, trucs, prix, koala	G1impse$tuff74Prize8Koala!
Trombone, poisson, rapide, à l'envers	Tr0mb0ne&Poisson? Qu1ck^côté

4. Jouez avec les phrases et les citations

Si vous voulez un mot de passe difficile à deviner pour les autres, mais facile à retenir, il peut être judicieux d'utiliser une variante d'une **phrase ou d'une citation significative**. Prenez simplement une phrase dont vous vous souviendrez et remplacez certaines lettres par des chiffres et des symboles.

Voici quelques exemples d'idées de mots de passe forts générés avec cette méthode :

Citation ou phrase	Mot de passe sécurisé
« Un pour tous et tous pour un » : Les Trois Mousquetaires	14A&A413Mu$keteers!

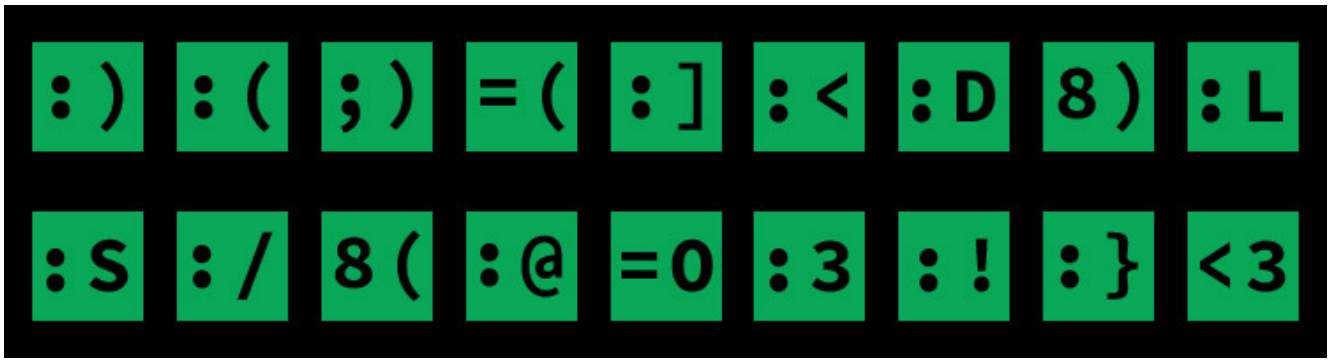
Citation ou phrase	Mot de passe sécurisé
« Pour la première fois depuis une éternité » : La Reine des neiges de Disney	4da1stTymein4eva-Congelé
« Twinkle twinkle little star, comme je me demande ce que tu es »: comptine	TW1nkle7ittle*comment1??UR

5. Utilisez des émoticônes

Si vous souhaitez ajouter des symboles à vos mots de passe sans les rendre plus difficiles à retenir, **vous pouvez toujours utiliser des émoticônes**.

Bien que vous ne puissiez pas ajouter d'emoji, vous pouvez utiliser des émoticônes, qui sont les versions codées, généralement composées de signes de ponctuation, de lettres et/ou de chiffres.

Voici quelques émoticônes que vous pouvez utiliser dans vos mots de passe :



6. Personnalisez vos mots de passe pour des comptes spécifiques

Une fois que vous avez trouvé un mot de passe fort dont vous vous souviendrez, vous devrez toujours **créer des mots de passe différents pour chacun de vos comptes en ligne**.
Mais, plutôt que de recommencer tout le processus, vous pouvez simplement ajouter un code différent dans votre mot de passe pour chaque compte en ligne.

Ainsi, par exemple, si votre mot de passe est cHb1%pXAuFP8 et que vous souhaitez le rendre unique pour votre compte eBay, vous pouvez ajouter £bay à la fin afin de savoir qu'il est différent de votre mot de passe d'origine mais qu'il reste facile à mémoriser.

Voici comment cela pourrait fonctionner :

Compte en ligne	Mot de passe avec code ajouté
Messagerie électronique	cHb1%pXAuFP8EMa1l
Amazone	cHb1%pXAuFP8AZN
eBay (en anglais seulement)	cHb1%pXAuFP8£Bay

7. Enregistrez votre mot de passe dans la mémoire musculaire

Si vous voulez vous souvenir de votre mot de passe, il peut être judicieux de **vous entraîner à le taper plusieurs fois**.
Finalement, si vous le tapez correctement suffisamment de fois, vous développerez une mémoire musculaire qui vous permettra de vous en souvenir beaucoup plus facilement.

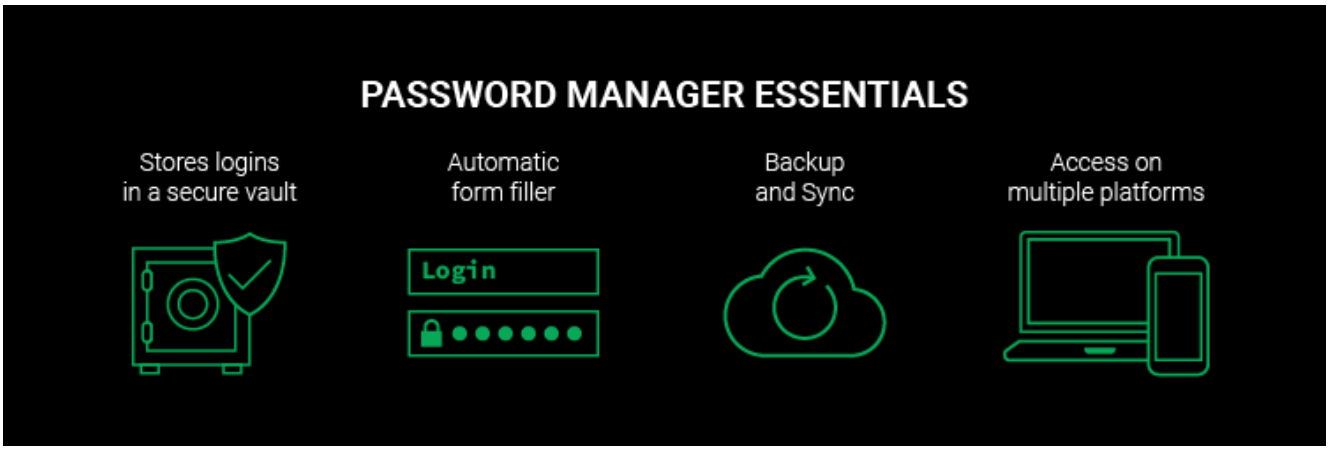
Cependant, il est tout un défi de se souvenir d'au moins une douzaine de mots de passe longs et uniques de tous vos comptes.
Ainsi, cette technique n'est applicable qu'avec des mots de passe courts, à 4 ou 6 chiffres, que vous utilisez pour déverrouiller votre appareil ou votre gestionnaire de mots de passe.

Comment protéger vos mots de passe

Maintenant que vous avez configuré un mot de passe fort pour chacun de vos comptes en ligne, l'étape suivante consiste à les protéger contre les pirates.

Voici quelques-uns de nos meilleurs conseils pour y parvenir :

1. Choisissez un bon gestionnaire de mots de passe



Que vous ayez généré vos propres mots de passe forts ou que vous recherchiez un service en ligne pour le faire pour vous, nous vous recommandons fortement d'utiliser un bon gestionnaire de mots de passe.
Un gestionnaire de mots de passe sécurisé **génère, stocke et gère tous vos mots de passe** dans un seul compte en ligne sécurisé.
C'est vraiment utile car cela vous permet d'utiliser autant de mots de passe uniques que vous le souhaitez sans jamais avoir à vous soucier de les mémoriser.

Tout ce que vous avez à faire est d'enregistrer tous vos mots de passe pour chaque compte en ligne que vous avez sur votre gestionnaire de mots de passe, puis de les protéger avec un « mot de passe principal ».
Cela signifie que vous n'avez qu'à vous souvenir d'un seul mot de passe fort au lieu de tous.

Une fois que vous avez configuré votre gestionnaire de mots de passe, chaque fois que vous vous connectez à l'un de vos comptes en ligne, il vous suffit de taper votre mot de passe principal dans votre gestionnaire de mots de passe et il remplira automatiquement vos informations de connexion pour ce compte.
Vous n'avez même pas besoin de vous souvenir de l'adresse courriel ou du nom d'utilisateur que vous avez

utilisé.
Un gestionnaire de mots de passe sécurisé remplira tout cela pour vous.
Voici quelques-uns des meilleurs gestionnaires de mots de passe en 2023.

Il peut sembler peu sûr de conserver tous vos mots de passe au même endroit. Cependant, un gestionnaire de mots de passe fiable comme Dashlane ou 1Password est l'endroit le plus sûr pour stocker vos informations d'identification.
Les fournisseurs ne conservent jamais le mot de passe principal de votre coffre-fort, de sorte que les pirates ne peuvent pas le voler même s'ils pénètrent dans la base de données.

2. Utilisez l'authentification à deux facteurs

Même si quelqu'un parvient à voler votre mot de passe, vous pouvez toujours l'empêcher d'accéder à votre compte **en ajoutant une couche de sécurité supplémentaire avec l'authentification à deux facteurs (2FA).**
Cela signifie que toute personne essayant de se connecter à votre compte devra saisir une deuxième information après le mot de passe correct.
Il s'agit généralement d'un code à usage unique qui vous sera envoyé directement.

Parfois, cela vous sera envoyé par SMS, bien que ce ne soit pas nécessairement le moyen le plus sûr de recevoir ce code.
Après tout, un pirate pourrait voler votre numéro de téléphone portable par le biais d'une fraude à l'échange de carte SIM et accéder à votre code de vérification.

Nous avons constaté qu'il est beaucoup plus sûr d'utiliser une application d'authentification à deux facteurs à la place, car ils sont beaucoup plus difficiles à intercepter.
Nos favoris sont les suivants :

- Authentificateur Google
- Microsoft Authenticator
- Authy

3. N'enregistrez pas vos mots de passe sur votre téléphone, votre tablette ou votre PC

Cela peut sembler évident, mais vous devez éviter d'enregistrer des mots de passe dans un document, un courriel, une note en ligne ou tout autre document que des personnes extérieures peuvent consulter sans autorisation.
Naturellement, cela s'applique aussi bien aux fichiers et aux notes numériques que physiques.
Même les fichiers zip protégés par mot de passe ne sont pas viables car ils utilisent un cryptage relativement faible.
En bref, **le seul coffre-fort numérique approprié est un gestionnaire de mots de passe de haute qualité**.

4. Vérifiez si votre e-mail a fait l'objet d'une fuite

Bien sûr, il est essentiel de se tenir au courant de toute violation de données qui a pu se produire, en particulier avec votre compte de messagerie.

Mais comment savoir si votre courriel a fait l'objet d'une fuite ?
Eh bien, nous avons un vérificateur de fuite de données personnelles en ligne, qui vous permettra de savoir si quelque chose de ce genre est arrivé à votre compte de messagerie.
Tout ce que vous avez à faire est d'entrer votre adresse e-mail, et nous serons en mesure de vous dire si quelque chose lui est arrivé.

5. Ne donnez pas votre mot de passe

Enfin, il est essentiel de préserver la confidentialité de vos mots de passe.
Même si vous faites entièrement confiance à la personne à qui vous donnez votre mot de passe, il est risqué d'envoyer un mot de passe par SMS ou par courriel au cas où quelqu'un l'intercepterait.
Même si tout ce que vous faites est de le lire au téléphone ou de l'épeler à la personne assise à côté de vous, il se peut que quelqu'un vous écoute et prenne des notes.

Conclusion : comment puis-je rendre tous mes mots de passe à l'épreuve du piratage ?

Les mots de passe sont comme la serrure de la porte de votre appartement : c'est la seule chose que les criminels doivent traverser si vous n'êtes pas chez vous.
Avoir un mot de passe faible, c'est comme un verrou faible.
Cela augmente considérablement le nombre de personnes qui ont les moyens d'accéder à vos comptes.

L'utilisation de toutes les astuces de cet article pour **créer des mots de passe forts et mémorables** est un bon point de départ pour renforcer votre sécurité.
Vous pouvez également vous procurer un gestionnaire de mots de passe puissant comme Dashlane ou 1Password et générer automatiquement tous vos mots de passe - de cette façon, vous n'aurez pas à vous en souvenir.

Quel que soit le cours que vous décidez d'adopter, ne le remettez pas à plus tard !
Des fuites et des violations de données se produisent tous les jours, et la prochaine pourrait contenir votre mot de passe.

Les meilleures offres de gestionnaires de mots de passe cette semaine :

Dashlane Password Manager

1Password

FAQ

Quel mot de passe serait un mot de passe fort ?

Un mot de passe doit **répondre à quelques critères pour être considéré comme fort**. Pour commencer, il doit être long, entre 12 et 16 caractères.
Deuxièmement, il doit être composé d'une combinaison de lettres majuscules et minuscules, de symboles et de chiffres.
Enfin, il doit être unique et impossible à deviner plutôt que quelque chose d'évident.

Quels sont les 10 pires mots de passe ?

Les 10 mots de passe les plus populaires en 2023 sont **123456, 123456789, qwerty, password, 12345, qwerty123, 1q2w3e, 12345678, 111111 et 1234567890.**
Les utiliser lors de la création d'un compte en ligne est sans doute la pire chose que vous puissiez faire en matière de cybersécurité.
Utilisez plutôt un générateur de mots de passe et un gestionnaire de mots de passe forts.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231016
"C'est ensemble qu'on avance"