Quel mot de passe choisir ?

Un bon mot de passe

« **Quel mot de passe choisir** ? », « Est-ce que les mots de passe de mes comptes Internet sont **vraiment efficaces** ? »…

Les mots de passe sont la **principale barrière de sécurité** de nos comptes.

Aujourd'hui plus qu'hier, le **choix d'un bon mot de passe** est primordial. Nous avons **de plus en plus de comptes** sur le Web : un compte bancaire, un compte Facebook, un compte Google, etc. Autant de comptes… et autant de portes d'entrée qu'il faut impérativement sécuriser.
Voyez vos comptes comme des **maisons (comptes)** qu'il faut protéger par des **verrous (mots de passe) efficaces**.

Les mots de passe faibles sont **l'une des failles les plus courantes** dans la sécurité informatique.
Je ne me sens pas concerné, j'utilise déjà des mots de passe **hyper-sûrs** !
Vous allez voir que ce n'est pas vraiment le cas 😉
Ce qu'on a appris à propos des mots de passe :

- Il faut qu'ils soient compliqués ;
- Il faut utiliser des chiffres, des majuscules et des caractères spéciaux ;
- Il faut les changer régulièrement ;
- Il faut utiliser des mots de passe différents pour chaque application et chaque compte Internet.

Malheureusement, ces directives ne sont pas efficaces, en plus d'être fastidieuses à appliquer pour les utilisateurs.
En juin 2017, le National Institute of Standards and Technology (NIST) a révisé ses lignes directrices pour la création de mots de passe, et les nouvelles recommandations divergent complètement des règles précédentes.
Les experts suggèrent maintenant de créer des mots de passe simples, longs et mémorables. Les caractères spéciaux et les mélanges de lettres majuscules et minuscules ne sont plus recommandés. Enfin, les mots de passe n'ont plus besoin d'être renouvelés après un certain temps.

« A travers 20 ans d'efforts, on a réussi à habituer les gens à utiliser des mots de passe qui sont difficiles à retenir pour les humains, mais faciles à deviner pour les ordinateurs » – Source : xkcd.com

Phrase secrète contre mot de passe

Qu'est-ce qu'une **phrase secrète** ? 🤔
Une phrase secrète (passphrase, en anglais) est un **groupe de mots et de caractères** utilisé comme moyen d'authentification pour prouver son identité lorsque l'on désire accéder à une ressource ou à un service dont l'accès est protégé. C'est **l'équivalent d'un mot de passe**, mais **en plus sécurisé**.
Les mots de passe sont généralement courts, **de 6 à 10 caractères**. Ces derniers sont généralement **suffisants** pour se connecter aux comptes utilisateur dans les systèmes d'exploitation (Windows, GNU/Linux, macOS…) lesquels sont programmés pour **détecter**

plusieurs tentatives d'accès incorrectes et pour **protéger les mots de passe stockés**. En revanche, ils ne sont **pas sûrs** pour une utilisation avec des systèmes de chiffrement.
Les phrases secrètes sont beaucoup plus longues, **de 25 à 64 caractères** (espaces compris). Leur **plus grande longueur** rend les phrases secrètes **beaucoup plus sûres que les mots de passe**.

Mot de passe	Phrase secrète
De 6 à 10 caractères	De 25 à 64 caractères
Souvent incompréhensible	Toujours significatif
Difficile à retenir	Facile à retenir
Facile à cracker	Difficile à cracker

Pour garantir une **meilleure protection contre les pirates**, la plupart des programmes de sécurité vous permettent d'ailleurs d'entrer une phrase secrète plutôt qu'un mot de passe, comme par exemple :

- Les protocoles de sécurité Wi-Fi WPA/WPA2 ;
- Les gestionnaires de mots de passe (LastPass, KeePass…) ;
- Les logiciels de chiffrement de données (VeraCrypt, Windows BitLocker…) ;
- Le logiciel de chiffrement cryptographique PGP, souvent utilisé pour signer, chiffrer et déchiffrer des e-mails ;
- Les cryptomonnaies (BitCoin).

A quoi ressemble une phrase secrète parfaite ?
Dans l'idéal, une phrase secrète devrait être :

- Connue uniquement par vous ;
- Assez longue pour être sûre ;
- Difficile à deviner – même par quelqu'un qui vous connaît bien ;
- Facile à retenir ;
- Facile à saisir.

☝ Comment faire pour **choisir une bonne phrase secrète** ?

Décidez du nombre de mots que vous voulez dans votre phrase secrète. Une phrase secrète avec **5 mots** fournit un niveau de sécurité bien supérieur aux mots de passe utilisés par la plupart des utilisateurs. Il est recommandé d'utiliser un minimum de **6 mots** pour une utilisation avec les programmes GPG, les protocoles de chiffrement Wi-Fi et les programmes de chiffrement de fichiers. Une phrase secrète de **7, 8 ou 9 mots** est recommandée pour les programmes qui requièrent une protection totale comme le chiffrement de disques ou BitCoin.
Lorsque vous avez terminé, les mots que vous avez trouvés forment votre **nouvelle phrase secrète** ! Mémorisez-les, puis détruisez le morceau de papier ou gardez-le dans un endroit vraiment sûr 😉

William Fourché - william@fourche.fr - 33 (0) 663 081 328
32 rue des Tilleuls 53160 Vimarcé - FRANCE

Générateur de phrase secrète

Diceware: https://www.rempe.us/diceware/#french.
Il suffit de cliquer sur le bouton correspondant au nombre de mots que vous souhaitez utiliser dans votre phrase secrète (**6 words**, **7 words**…), et le tour est joué !
Dans le même style, vous avez également : https://passwordcreator.org/fr.html !

Tester la force d'un mot de passe

Pour **comparer le niveau de sécurité** entre votre ancien et votre nouveau mot de passe, vous pouvez utiliser le **testeur de mot de passe** du site howsecureismypassword.net. Le site indique le temps que cela prendrait à un ordinateur pour trouver votre mot de passe.
Par exemple, voici la force de mon **ancien mot de passe** que je considérais comme sûr (c'était un mot de passe du type : `crabDU#8+`) :

Savoir si votre mot de passe a été récupéré par des pirates

https://haveibeenpwned.com/

William Fourché - william@fourche.fr - 33 (0) 663 081 328
32 rue des Tilleuls 53160 Vimarcé - FRANCE

Conseils sur les mots de passe

Si vous utilisez une phrase secrète pour le **chiffrement de disques ou de fichiers**, il est recommandé d'en **garder une copie écrite** dans un endroit sûr. Si vous ne le faites pas et que vous oubliez votre mot de passe, vos fichiers seraient **perdus pour toujours**.

Utilisez une **phrase de passe distincte** pour chacun de vos comptes.

N'utilisez pas de générateur de mot de passe qui vous fournira un mot de passe que vous n'allez jamais retenir.

Ne regroupez pas tous vos mots de passe sur le même morceau de papier. Utilisez plutôt un **gestionnaire de mots de passe** comme LastPass , Dashlane ou KeePass. Ce type de logiciel permet de stocker et de récupérer vos mots de passe de manière efficace et sécurisée.

Ne divulguez pas vos mots de passe, à qui que ce soit.

Au moment de préparer votre phrase secrete et pour une **sécurité maximale**, assurez-vous d'être seul et fermez les rideaux. Écrivez sur une surface dure – pas sur un bloc de papier. Après avoir mémorisé votre mot de passe, brûlez vos notes, pulvérisez les cendres et jetez-les dans les toilettes 🔥 💨 🚽
Si vous suivez toutes ces recommandations, je vous garantis que vos comptes seront **plus sécurisés que 99% des utilisateurs** et quasi-impossibles à pirater 🙂

Conseils sur les gestionnaires de mot de passe

Qu'est-ce qu'un gestionnaire de mots de passe ?

Un gestionnaire de mots de passe est un logiciel qui stocke tous vos mots de passe et vous évite de les retenir tous. Tous vos identifiants sont stockés dans une base de données, elle-même chiffrée et accessible par un mot de passe général. Une fois le logiciel déverrouillé, il remplit automatiquement les systèmes d'identification pour un site Internet ou une application sur smartphone. En outre, le gestionnaire de mots de passe enregistre également les nouveaux comptes automatiquement. Il permet également de stocker des documents ou des moyens de paiement. Les principaux gestionnaires de mots de passe sont Dashlane, LastPass, Keepass, 1Password, Keeper, Bitwarden, roboform...

William Fourché - william@fourche.fr - 33 (0) 663 081 328
32 rue des Tilleuls 53160 Vimarcé - FRANCE

Dashlane ou KeePass pour PC

Dashlane ou 1password pour Mac OS

En créant un coffre-fort avec un gestionnaire de mot de passe, verrouillé par la seule phrase secrète que à retenir, il est possible de stocker toutes autres les phrases secrète utilisées sur les sites qui les autorisent. Ainsi, il suffit de retenir la phrase secrète qui permet d'accéder au coffre-fort 🙂

William Fourché - william@fourche.fr - 33 (0) 663 081 328
32 rue des Tilleuls 53160 Vimarcé - FRANCE

Les pires mots de passe :

2019	*2024*
1. 123456	1. 123456
2. 123456789	2. 123456789
3. qwerty	3. azerty
4. password	4. qwerty123
5. 1234567	5. qwerty1
6. 12345678	6. azertyuiop
7. 12345	7. marseille
8. iloveyou	8. doudou
9. 111111	9. loulou
10. 123123	10. 12345678
11. abc123	11. 1234561
12. qwerty123	12. 000000
13. 1q2w3e4r	13. chouchou
14. admin	14. motdepasse
15. qwertyuiop	15. soleil
16. 654321	16. mypassphrase
17. 555555	17. 1234567
18. lovely	18. password
19. 7777777	19. nicolas
20. welcome	20. camille

On retrouve **qwerty123** qui est également "le mot de passe le plus utilisé au Canada, en Lituanie, Finlance, Norvège ainsi qu'aux Pays-Bas.

Face à cette débauche d'originalité, rappelons que 75% des mots de passe référencés par NordPass peuvent être devinés en moins d'une seconde par des cybercriminels via une attaque de type force brute, d'autant que chaque année les rapports de ce type se présentent comme du pain béni pour les hackers.

William Fourché - william@fourche.fr - 33 (0) 663 081 328
32 rue des Tilleuls 53160 Vimarcé - FRANCE