***MOTS DE PASSE conseils de la MAIF (janvier 2019)***

*Le mot de passe est rapidement devenu la brique de base de la sécurité sur internet. Pour que cela soit utile, encore faut-il respecter quelques règles simples.*

En moyenne, un internaute possède 90 comptes sur le net avec pour la plupart autant de mots de passe. Si l’on fait l’effort d’utiliser des bons mots de passe, il est impossible de tous les mémoriser (mais c’est un excellent moyen d’essayer d’améliorer notre mémoire).

Aucune solution n’est parfaite. Tout est question d’équilibre et de respect de certaines règles élémentaires pour éviter qu’il ne soit trop simple de prendre la main sur vos comptes.

**Un seul mot de passe : à bannir**

Il est parfois tentant de se simplifier la vie en n’utilisant qu’un seul et même mot de passe pour tous les comptes. C’est une erreur qui peut être lourde de conséquences : si un seul des comptes est compromis, les “pirates” pourront accéder à tous les autres !

Si idéalement il faut utiliser un mot de passe différent pour chaque compte, il est déjà raisonnable de définir des “niveaux de menace”. Un même mot de passe peut servir pour les comptes sans enjeux (comptes sans données personnelles ou bancaires), mais un mot de passe spécifique doit être déterminé pour chaque adresse mail, chaque réseau social et chaque autre compte important.

/ Lastpass, un gestionnaire de mot de passe efficace.

*Bon à savoir :  
Une étude américaine démontre la trop grande simplicité des mots de passe les plus utilisés pour les comptes piratés en 2017 : 123456, password, qwerty, letmein, football, iloveyou,… Ces mots de passe sont si souvent utilisés qu’il suffit de lancer un logiciel qui les teste automatiquement pour pouvoir se connecter à un très grand nombre de comptes et peuvent servir de base pour escroquer les proches de la personne piégée. (Source :* [*Smartlink*](https://www.smartlink.fr/voici-les-mots-de-passe-les-plus-pirates-en-2017/)*)*

**Évitez les mots de passe trop simples**

Les mots de passe suivants peuvent facilement être trouvés par des logiciels spéciaux conçus pour tester rapidement un grand nombre de combinaisons :

* les combinaisons clavier faciles ;
* les mots du dictionnaire, qui peuvent être tous testés par un logiciel ;
* les références culturelles (livre, série TV, film, théâtre…).

Il est important d’éviter également toute donnée vous concernant directement (date de naissance, nom de votre animal de compagnie) qui sont faciles à deviner en faisant quelques recherches.

**Évitez de crier votre mot de passe sur internet**

Vous ne vous rendez peut-être pas compte, mais le petit nom de votre chat, votre date de naissance, votre département ou votre pseudo ne doivent pas être des mots de passe. L’idée est de décourager la personne souhaitant accéder à vos données. Pas de les lui livrer sur un plateau.

Toutes les plateformes majeures de réseaux sociaux reçoivent constamment des tentatives d’attaque visant à récupérer les données personnelles des utilisateurs. C’est pourquoi il convient de prendre toutes les dispositions pour complexifier la tâche de ces hackers !

**Mettez toutes les chances de votre côté**

Les experts conseils les phrases de passe qui sont des phrases longues et faciles à retenir mais difficiles à pirater. Au lieu d’utiliser un mot de passe n’ayant aucun sens pour vous, choisissez une phrase de 4 mots plus facile à retenir.

Voici quelques conseils pour former un mot de passe sécurisé :

* 12 caractères minimums ;
* mélangez des chiffres, des majuscules et des caractères spéciaux ;
* créez un mot de passe ne voulant rien dire, ne se rattachant à aucune référence culturelle ;
* pas de données personnelles facilement retrouvables.

Prenons un exemple concret, avec les mots “tigre”, “vélo”, “école” et “pays” qui n’ont aucun rapport entre eux et ne sont pas une référence culturelle..  
Un mot de passe tel que “GarFi3LD^^”, qui peut être le nom de votre chat, sera plus simple à trouver qu’un mot de passe comme “TigreVéloÉcolePays”. Il suffit simplement de vous créer un moyen mnémotechnique : “Le tigre se rend en vélo à l’école dans tous les pays”. Cette phrase de passe est moins facile à craquer surtout si vous la complexifiez “Tigr3-Vél0@Éc0l3>P4y$”.

**Utiliser son navigateur pour enregistrer ses mots de passe ?**

Tous les navigateurs proposent d’enregistrer vos mots de passe afin de ne pas avoir à les retenir. Cette fonctionnalité est à utiliser avec prudence, uniquement pour les comptes peu importants. Quelqu’un qui prend la main sur votre ordinateur peut en effet accéder facilement à tous les mots de passe enregistrés.

**Utilisez un service de gestion de mot de passe et un système de double authentification**

Il existe des services très pratiques spécialisés dans la gestion et la sécurisation de vos mots de passe. Vous n’aurez plus qu’un mot de passe principal à mémoriser et ensuite il s’occupe de générer tous les autres sans que vous n’ayez besoin de les connaître ou de vous soucier de la sécurité. Ces services sont sécurisés et fiables (exemple : [Lastpass](https://lastpass.com/) et [Dashlane](https://www.dashlane.com/)).

Il existe également des techniques pour garantir une sécurité maximale comme le système de la double authentification. Il s’agit d’un processus qui permet d’ajouter un niveau de sécurité supplémentaire à un compte sur un réseau social ou sur un site, généralement grâce à votre numéro de téléphone portable ou à un mail, mais ces deux moyens ont également des failles. Il existe un troisième moyen, beaucoup plus sûr, l’utilisation d’une application dédiée à la double authentification. Ces applications génèrent un code unique à renseigner lors de la connexion en double authentification, ce qui est beaucoup plus sûr qu’un mail ou un numéro de téléphone pouvant être piraté.