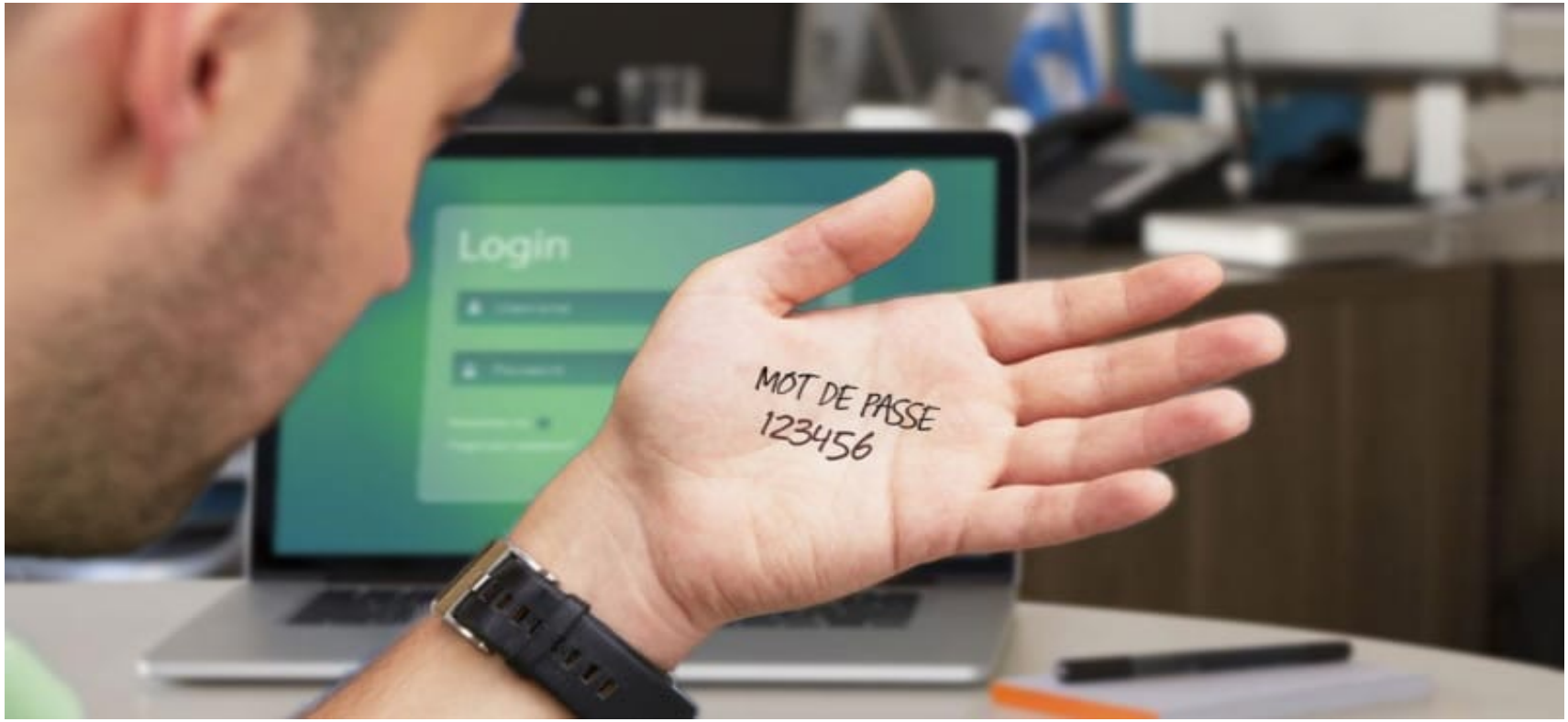
Les mots de passe …

Comment choisir ses mots de passe

Une centaine : c'est le nombre moyen de comptes et donc de mots de passes associés à chaque internaute. Choisir un mot de passe sécurisé pour chaque compte est donc primordial… et c'est un véritable casse-tête ! Or trop souvent les internautes négligent leur sécurité. On vous dit donc comment mieux choisir et gérer ses mots de passe.



Facebook, Twitter, Amazon, Netflix, Google, la Fnac, Cdiscount, Vente-privée… Nous utilisons en moyenne une centaine de services en ligne nécessitant chacun la création d'un mot de passe. Il en faut pour tout et n'importe quoi. Alors pour ne pas se prendre la tête, on utilise parfois un seul et même mot de passe pour plusieurs, voire parfois toutes ces plateformes.
De manière générale, nous manquons de vigilance, lorsqu'il s'agit de sécurité en ligne. Le site Cybermalveillance.gouv.fr a publié une série de conseils pour mieux choisir et gérer vos mots de passe. On vous dit tout sur **ce qu'il faut faire et ne pas faire lorsque l'on doit choisir un mot de passe**.

Les mots de passe à éviter coûte que coûte

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.

Ne jamais utiliser un mot de passe identique pour plusieurs comptes

Tout simplement parce qu'il suffirait à un pirate (ou un proche trop curieux) de casser l'un de vos mots de passe pour avoir accès à l'ensemble de votre vie privée. Autant lui rendre la tâche difficile et le faire travailler beaucoup plus. Voire, idéalement, le décourager complètement.

Autre erreur à éviter : utiliser des mots trop communs et trop courts

Les noms et prénoms de vos proches sont aussi à proscrire. Ça marche aussi pour votre chien, votre chat, votre hamster ou tout autre animal de compagnie, même une mygale (ça ne fera pas peur à un pirate). Evidemment ce sont des mots de passe plus simples à retenir mais plus facile à deviner également. La simplicité est souvent à l'origine des pires mots de passe du type 123456, 111111, 000000 ou encore chaton09. Ne riez pas… ils sont encore très fréquents.

Le simple fait de remplacer des lettres par des caractères spéciaux ne suffit plus

Tout va dépendre de ceux que vous utilisez et comment vous les insérez. Il faut donc éviter par exemple cette liste d'altérations courantes, qui ne corse pas vraiment beaucoup la difficulté dans le cadre d'attaques brute force :

- un e par un 3
- un a par un @
- un i par un 1
- un s par un $
- un o par un 0

Les ch@ton09 sont à bannir, tout comme les beaug0ssedu69 ou les $exyg1rldu57. Même s'ils sont faciles à retenir et qu'ils donnent l'impression d'être compliqués, ils ne le sont pas.

Comment choisir un bon mot de passe

C'est bien tout ça, mais alors comment choisir un bon mot de passe ? Bah oui c'est vrai ça ! Et bien de manière générale il faut faire exactement l'inverse de ce qui a été présenté plus haut.

Choisissez un mot de passe complexe, long et facile à mémoriser

Exit les noms communs trop courts, **il faut utiliser des mots de passe longs :** il est admis en effet qu'un bon mot de passe doit comporter **au minimum 12 signes** mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux. Ce qui ne signifie pas des mots de passe totalement impossibles à mémoriser non plus.

Il y a pour cela plusieurs techniques. Certains OS comme macOS proposent automatiquement des mots de passe forts que vous n'aurez jamais besoin de retenir – vous pouvez arriver au même résultat avec un gestionnaire de mots de passe, nous y reviendrons ci-après. Si vous devez choisir un mot de passe à la main, le meilleur conseil est le suivant :

Choisissez 5 mots au hasard pour en faire une phrase qui ne veut rien dire

Ajoutez des chiffres, majuscules et caractères spéciaux à des endroits que vous pouvez retenir

Exemple : *phonAndroidKernel_0téléphoneChienhiver*

L'entropie de ce genre de mots de passe est telle que cela corse considérablement la difficulté des pirates pour le deviner par toutes les techniques actuelles. Répétez la manipulation autant de fois que vous avez de comptes. Car oui, il faut un mot de passe différent pour chaque compte. Ça fait travailler la mémoire tout ça n'est-ce pas ?

Changez régulièrement de mot de passe et au moindre soupçon

Les fuites de données et leur revente par des pirates ne sont plus si rares. Or plus votre mot de passe existe depuis longtemps, plus il a potentiellement de chances de faire partie de fuites de données. Il est donc recommandé de changer régulièrement de mot de passe sur tous vos comptes – par de nouveaux mots de passes inédits. Certains comptes étant plus sensibles que d'autres, il conviendra de choisir une fréquence adaptée pour ces changements. Par exemple, pour votre adresse email, essayez de le changer au moins une fois par an.

Ne communiquez jamais vos mots de passe à un tiers

Ne donnez jamais un mot de passe à qui que ce soit… surtout si on vous le demande. Aucune entreprise ou organisation digne de ce nom ne vous demandera jamais votre précieux sésame, tout simplement parce qu'en cas de besoin ces dernières peuvent accéder aux informations nécessaires. Une « maintenance » ou un « dépannage » ne sont pas des raisons valables. Si par mégarde vous avez confié votre mot de passe à un tiers, veuillez le changer au plus vite.

Soignez particulièrement la sécurité du mot de passe de vos boîtes mail

Quel que soit le compte, mieux vaut privilégier sa sécurité. Il y a tout de même un type de compte sur lequel vous devez en particulier être intraitable et maximiser sa sécurité. Votre boîte mail est en effet liée à une grande partie de vos comptes. Si sa sécurité était compromise, un pirate n'aurait aucun mal à récupérer vos autres mots de passes par ce biais.

Comment mieux gérer vos mots de passe

Avec autant de comptes, retenir tous ses mots de passe est quasiment impossible. Du coup on change à nouveau, on opte pour quelque chose de plus simple, on refait les mêmes erreurs et on revient au point de départ. Jusqu'à être victime de piratage… Le problème est d'autant plus grave qu'il est conseillé de changer régulièrement ces mots de passe. De quoi vite s'embrouiller la mémoire !

Les plus organisés noteront les différents mots de passe sur des supports papier mais les post-it, calepins, cahiers, bouts de papiers ne sont pas sécurisés. Surtout parce qu'ils donnent potentiellement un blanc-seing à quiconque les trouverait à votre insu pour discrètement accéder à vos comptes.

Le pire, ce sont sans doute les applications de prise de note – qui disposent bien souvent d'une fonction de recherche et sont rarement protégés. Heureusement des spécialistes de la sécurité ont pensé à tout. Ils ont ainsi créé ce que l'on appelle des gestionnaires de mots de passe.

Utilisez un gestionnaire de mots de passe

Ces logiciels/applications pour ordinateurs, smartphones et tablettes sont en fait **des coffres-forts numériques**. Ils sont ultra-sécurisés et stockent tous vos mots de passe. Pour faire simple, ce coffre va retenir tous vos mots de passe à votre place. Vous n'aurez qu'un seul et unique mot de passe à retenir pour sécuriser le coffre-fort. Ce mot de passe doit être ultra-sécurisé et reprendre les règles citées plus haut. Vous devez créer le meilleur de vos mots de passe, le mot de passe unique qui va les gouverner tous.

Parmi ces gestionnaires de mots de passe, certains sont devenus des références.

Comme je ne souhaite pas faire de la publicité pour ces gestionnaires, faites vous-même une recherche de gestionnaires de mot de passe sur internet.

Activez la double authentification
Pour renforcer encore cette sécurité, **de nombreux services proposent également la double authentification.** Le principe est très simple : après la saisie de votre mot de passe incroyable et magique, une deuxième sécurité est demandée. Bien souvent il s'agit d'un code à plusieurs chiffres. Vous obtenez ce code soit par SMS soit via une application. Pour le recevoir par SMS il faut bien entendu avoir fourni son numéro au service au préalable.
Pour les applications, Google a par exemple un système extrêmement fiable baptisé Google Authentificator. Cette application génère un code de 6 chiffres renouvelé toutes les 10 secondes. Dès que vous rentrez votre mot de passe Google pour accéder à ses services, il faut ensuite lancer l'application pour obtenir le 2ème code et valider l'authentification complète.
Attention : depuis quelques temps **la double authentification par SMS est déconseillée en raison de sa faible sécurité** et le risque qu'un pirate parvienne à se faire passer pour votre numéro de téléphone afin de recevoir les SMS de connexion. Préférez toujours l'authentification par code fourni par une application. Ou, encore mieux, optez pour des clés physiques pour votre double authentification, comme YubiKey, lorsque la plateforme est compatible.

Voilà, avec tous ces éléments vous devriez pouvoir sécuriser tous vos comptes grâce à des mots de passes incroyables et magiques. N'oubliez pas que si la simplicité est tentante, elle a un impact important sur la sécurité. Je vous laisse, j'ai tous mes mots de passe à changer.