Vous et Votre Mac

Vous et Votre Mac

N° 145 • Juin 2018 100 % Mac en pratique

Quick Look

Êtes-vous sûr d'en tirer tout le parti ? Trucs et astuces pour l'améliorer et bien l'utiliser.

Rangement

4 utilitaires qui font le ménage et rangent eux-mêmes tous vos fichiers.

CRÉER DES MOTS DE PASSE TRÈS DIFFICILES À CASSER

MacBook iPad & iPhone...

Partir en vacances avec ses amis numériques

Tous nos conseils pour bien préparer ses bagages

HomeKit

Technos et matériels, ça bouge dans la domotique Apple !

Livres numériques

Zoom sur le lecteur et sur l'éditeur d'ePub de Calibre.

FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 145 H - F : 5,90 € - RD

PAGES 7, NUMBERS 5, KEYNOTE 8

NOUVEAU CRU 2018 D'iWORK

Prise en main des nouvelles fonctions des trois applications d'Apple. Et mise en œuvre pratique sur Mac et sur iOS.

Comment créer des mots de passe très difficiles à casser

Nous avons tous des dizaines de mots de passe à générer pour accéder à nos services distants et à chaque fois c'est un véritable casse-tête. Chacun à sa méthode pour établir un mot de passe : un générateur de mot de passe aléatoire, une table de conversion, comme le Leet speak qui utilise des caractères de substitution graphiquement voisins (5 pour le S, 7 pour le T), ou alors on fait appel à son imagination et on devient vite à court d'idées.

Il n'est pas étonnant que près de 50 % des internautes utilisent des mots de passe identiques pour tous leurs comptes ! Pourtant un mot de passe n'est jamais anodin. De sa solidité dépend la sécurité de vos données, de votre identité numérique et de votre vie privée. Alors, comment générer un bon mot de passe capable de résister aux attaques ? C'est ce que je vous propose d'approcher dans cet article. DENIS DUBOIS

Commençons par la définition d'un mot de passe… Chacun à sa petite idée de ce que ça peut être, mais Wikipédia nous précise : « ***Le mot de passe est un mot ou une série de caractères utilisés comme moyen d'authentification pour prouver son identité lorsque l'on désire accéder à un lieu protégé, une ressource ou un service dont l'accès est limité et protégé.*** ».

LES ERREURS À NE PAS COMMETTRE

De nombreux utilisateurs sont convaincus de ne pas être une cible intéressante pour les pirates, et **ne prennent pas la peine d'inventer des mots de passe un peu élaborés**. D'autres personnes pensent que concevoir un mot de passe qui a du sens, ou qui est généré selon certaines règles logiques (un algorithme simple, par exemple) est une très bonne idée. **Or, plus la structure du mot de passe est logique, plus il est à l'évidence facile à casser pour une machine**, et plus vous êtes vulnérable.

CRÉER UN (BON) MOT DE PASSE

La **CNIL** (Commission Nationale de l'informatique et des Libertés) édite des recommandations pour gérer ses mots de passe (**https://bit.ly/2jUdqfy**) **[1]**.
Pour la **CNIL**, un bon mot de passe doit avoir **une longueur minimale de 12 caractères** et contenir des **minuscules**, **majuscules**, **chiffres** et **caractères spéciaux**. Il peut être plus court (**https://bit.ly/2Hen8cC**) en cas de présence de sécurités complémentaires comme la double authentification ou le verrouillage du compte après plusieurs échecs. **Il ne doit dévoiler aucune information personnelle** comme le nom de votre chien ou celui de votre film préféré.
Pour les retenir, sans devoir les écrire, la CNIL préconise **d'utiliser la première lettre de chaque mot d'une phrase mémorisée**.
Enfin, elle recommande **l'utilisation d'un gestionnaire de mots de passe** (de préférence libre) ou d'**un trousseau d'accès chiffré** permettant de ne mémoriser qu'un unique mot de passe pour accéder à tous vos sésames.
La CNIL propose un générateur de mot de passe solide [2] (**https://bit.ly/2w2utDq**) qui donne quelques conseils supplémentaires pour renforcer votre mot de passe, comme l'utilisation d'émoticônes à la place de certains mots.
L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est chargée des questions de cybersécurité en France. Elle a notamment un rôle de conseil auprès des entreprises, et dans le domaine politique, diplomatique ou militaire. L'ANSSI a édité une note technique en juin 2012 (**https://bit.ly/2Hz81d8**) qui comprend des recommandations de sécurité relative aux mots de passe et suggère différentes méthodes pour créer un bon mot de passe. Elle aussi préconise **l'utilisation de mots de passe d'au moins 12 caractères** pour un usage local, voire 16 pour des mots de passe plus sûrs (connexions distantes).

1

LA MÉTHODE PHONÉTIQUE

Cette première approche consiste à utiliser **les sons de chaque syllabe** pour fabriquer une phrase facile à retenir. Par exemple, la phrase **j'ai acheté huit cd pour cent euros cet après-midi** donnera le mot de passe **ght8CD%E7am**.

LA MÉTHODE DES PREMIÈRES LETTRES

La méthode des premières lettres, recommandée aussi par la CNIL, consiste à garder **les premières lettres d'une phrase (proverbe, citation, paroles de chanson…) en veillant à ne pas utiliser que des minuscules**.
Ainsi, la citation **un tiens vaut mieux que deux tu l'auras** donnera **1tvmQ2tl'A**.

RENFORCER LA SOLIDITÉ D'UN MOT DE PASSE

Pour renforcer la solidité d'un mot de passe, il est souvent plus efficace d'allonger un mot de passe que de le rendre plus complexe, et donc difficile à retenir. En fait, **plus un mot de passe est long et moins il a besoin d'être complexe**. Dans les faits, on pourrait se contenter d'un mot de passe de 15 ou 16 caractères uniquement en minuscules !
S'il y a consensus dans le mode de composition d'un mot de passe mélangeant majuscule, minuscules et chiffres, c'est que **cela a été défini par le très sérieux NIST** (National Institute of Standards and

2

Technology) en 2003. Mais, à la surprise générale, Bill Burr, l'expert américain à l'origine de ces recommandations, **a fait un mea culpa en août 2017**.
Il reconnaît que ses préconisations n'étaient pas une bonne idée : leur complexité poussait les gens à les simplifier, voire à noter les mots de passe sur un support non chiffré ou sur un post-it collé sur le côté de l'écran. Il faut dire que leur renouvellement préconisé tous les 90 jours ne facilite pas leur mémorisation.
Depuis, **le NIST a défini de nouvelles règles** qui pourraient se résumer ainsi : **les mots de passe doivent être longs et faciles à retenir**.
Il est dorénavant préconisé **de concaténer quatre mots banals en une phrase sans aucun sens logique** comme : **plagepagodesoleilpelican**.
Il n'y a également aucun réel besoin de renouveler les mots de passe tous les 90 jours, **mais uniquement lorsqu'il y a suspicion de compromission**.
Ni la CNIL, ni l'ANSSI n'ont à ce jour intégré ces nouvelles préconisations du NIST.

ÉVALUER LA SOLIDITÉ D'UN MOT DE PASSE

Pour calculer la force d'un mot de passe, il faut prendre **le nombre de caractères possibles, élevé à la puissance de la longueur du mot de passe**.
Prenons un mot de passe comprenant des chiffres (de 0 à 9 soit 10 chiffres), des caractères minuscules (26 lettres) et des caractères majuscules (26 lettres) soit un total de 62 caractères.
Si le mot de passe fait 8 caractères comme v3DfmC45, le nombre total est de 628 soit 218.340.105.584.896 combinaisons possibles. En utilisant les caractères spéciaux usuels du clavier (!#$*%?), on monte à 70 voire 90 caractères en utilisant tous les symboles possibles, augmentant d'autant le nombre de combinaisons à tester pour l'attaquant et donc le temps nécessaire pour le trouver.

La force d'un mot de passe

Usuellement, il est encore souvent exigé au minimum un mot de passe de 8 caractères contenant des majuscules, des minuscules et des caractères spéciaux. Ce qui correspond, au mieux, à une clé de 52 bits. La solidité d'un tel mot de passe est très faible !
Un mot de passe de 16 caractères, comprenant les mêmes caractéristiques, correspond, au mieux, à une clé de 104 bits, ce qui est considéré comme une force « forte ».
Pour vous donner un ordre d'idée, pour arriver à une protection équivalente à un chiffrement AES-128 bits, il nous faudrait générer une clé de 20 caractères, utilisant tout le panel des caractères spéciaux disponibles - soit un alphabet de 90 symboles.

Les 8 recommandations de l'ANSSI

- Utilisez un mot de passe différent pour chaque service
- Choisissez un mot de passe qui n'est pas lié à votre identité (nom, date de naissance, etc.)
- Ne demandez jamais à un tiers de créer pour vous un mot de passe
- Modifiez systématiquement et au plus tôt les mots de passe par défaut
- Renouvelez vos mots de passe avec une fréquence raisonnable
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne mémorisent pas des mots de passe choisis.

La résistance d'un mot de passe s'évalue en fonction des capacités de calcul de l'attaquant. Les hackers peuvent, avec un équipement dédié, tester plusieurs milliards de combinaisons par seconde dans le cas d'une attaque par force brute. La résistance d'un bon mot de passe doit s'évaluer en nombre d'années.
Les nouvelles préconisations du NIST sont-elles vraiment efficaces ? **Nous allons comparer l'efficacité des deux méthodes en calculant leur entropie**, c'est-à-dire **la mesure de l'imprédictibilité d'un mot de passe**. C'est la difficulté qu'aura l'attaquant à découvrir ce mot de passe. **Elle s'exprime en bits**.
L'entropie du mot de passe aléatoire pris en exemple ci-dessus, est de 47 bits (je vous fais grâce de la formule à base de logarithmes !). C'est un bon résultat, mais ce mot de passe est difficile à mémoriser.
L'IETF, organisme qui participe à l'élaboration des nouveaux standards d'Internet, **recommande 29 bits d'entropie au minimum pour un mot de passe standard** afin de se prémunir d'une attaque « en ligne » (vers un serveur), voire 39 bits pour un mot de passe nécessitant davantage de sécurité.
Le schéma [3] compare (première ligne) un **mot de passe « classique »**, mélangeant majuscules, minuscules, chiffres et caractères spéciaux, à **un mot de passe constitué de 4 mots du dictionnaire anglo-saxon** (seconde ligne). Chaque petit carré représente un bit d'entropie.
Le premier mot de passe, qui semble a priori plus complexe à deviner, présente en fait **seulement 28 bits d'entropie**. Il sera facilement « cassé » en seulement 3 jours (sur la base de 1 000 essais/seconde). Le second, pourtant constitué de mots compréhensibles et facilement mémorisables, « pèse » **44 bits d'entropie**. Il faudrait 550 ans pour le casser !
Voici qui conforte les nouvelles préconisations du NIST.
En conclusion, sachez qu'il n'existe pas de mots de passe à toute épreuve, seulement des mots de passe qui résistent plus longtemps que les autres à l'attaque par force brute.

3