10 astuces pour créer des mots de passe solides

16 août 2021

Découvrez comment garantir la sécurité de vos comptes Internet.

Si votre activité numérique est limitée et que seuls quelques mots de passe vous suffisent, il n'est pas indispensable de faire appel à une appli spécifique.
Des principes élémentaires de sécurité s'imposent tout de même.

Dix points pour faire le tour de la question.

- **1. Assurez-vous que votre machine n'est pas infectée par des logiciels espions :** mettez à jour votre antivirus et lancez régulièrement une analyse avec.
- **2. Évitez les noms communs, les noms propres ou les marques commerciales** pour constituer vos mots de passe. L'une des méthodes des cyberpirates pour « craquer » ces derniers, l'« attaque par dictionnaire », consiste à essayer tous les mots de ces lexiques. Inutile de leur rajouter un ou plusieurs chiffres ou de remplacer les lettres a, i et e par, respectivement, @, 1, et 3 : les algorithmes de craquage ont prévu le coup !
- **3. N'utilisez pas les touches dans l'ordre de votre clavier.** Les mots de passe tels que 123456, AZERTY ou une combinaison des deux (A1Z2E3R4) sont très courants. De même, bannissez les formules type « motdepasse » ou « password », même accompagnées de chiffres.
- **4. Écartez l'idée d'utiliser, en guise de mot de passe, votre date de naissance,** celle de vos enfants, de vos parents ou l'année en cours ou précédente. Un algorithme spécialisé les a intégrées, toutes.
- **5. Employez le plus de caractères possible,** au moins douze dans l'idéal. Plus votre mot de passe sera long, plus il faudra de temps pour le

craquer lors d'une « attaque par force brute » (qui consiste à tester toutes les combinaisons possibles de caractères).

- **6. Combinez lettres minuscules, majuscules, chiffres et caractères spéciaux** tels &, #, * ou $. Là encore, cela allongera le temps de craquage.
- **7. Établissez des règles mnémotechniques pour faciliter la mémorisation** de vos mots de passe. Par exemple, prenez chaque première lettre des mots d'une phrase, d'un proverbe ou d'une citation, tout en ajoutant une pointe d'imagination personnelle pour tromper les algorithmes les plus malins. Ainsi, le proverbe « Un tiens vaut mieux que deux tu l'auras » peut se traduire par 1tvmq2tla, auquel vous pouvez ajouter un élément personnel (par exemple « à Marseille comme à Strasbourg » : aMca$).
- **8. Testez la robustesse de vos nouveaux codes** grâce aux vérificateurs de mots de passe de l'ONG Nothing2Hide ou de l'éditeur de logiciels Kaspersky.
- **9. Supprimez les post-it ou les feuilles de papier qui listent vos mots de passe** à proximité de votre écran. Personne n'est à l'abri d'un œil indiscret.
- **10. Enfin, n'utilisez jamais le même mot de passe pour plusieurs sites !** C'est particulièrement risqué car, si ce mot de passe est découvert, tous vos comptes seront accessibles.

Par 60 millions de consommateurs.

Qui n'a pas pesté devant son ordinateur au moment d'entrer un sésame dont on ne se souvient pas ?
Pour ne plus être bloqué, il existe des solutions : vous pouvez adopter une appli qui mémorise vos codes à votre place. Ce sont les gestionnaires de mots de passe. Nous abordons ces logiciels dans notre hors-série Internet plus rapide, plus sûr et facile.