5 règles pour créer un mot de passe sûr et introuvable… ou presque !

Créer un mot de passe sûr peut vite s'avérer compliqué, tant on entend tout et son contraire à ce propos. Un mot de passe sécurisé est pourtant un élément important pour que vos comptes soient bien protégés sur internet, tout comme la double authentification . Découvrez ces quelques règles simples qui permettent d'avoir un mot de passe fort dont vous vous souviendrez facilement !

5 règles pour créer un mot de passe fort

Pour que personne ne puisse accéder à vos comptes (que ce soit Facebook, Amazon ou Gmail), il est important de **trouver un mot de passe compliqué**. Mais comment faire pour générer un password qui soit à la fois sécurisé et simple à retenir ? Nous avons retenu 5 règles à utiliser :

1. **On mise sur la longueur du password**. Mais long, ça veut dire quoi ? Dans l'absolu, il faudrait que votre mot de passe ait plus de 10 voire 12 caractères. Le fait d'augmenter la longueur permet de rendre bien plus compliquée et longue l'utilisation de la brute force pour forcer votre mot de passe. Ici donc, plus c'est long... mieux c'est !
2. **On évite le nom de son chat**... mais aussi celui de son chien, de sa belle-mère ou sa date de naissance ! Le mot de passe ne doit pas contenir d'informations personnelles ou liées à vous. Celui-ci pourrait être trop facilement devinable, que ce soit par quelqu'un qui vous suivrait sur les réseaux sociaux ou en croisant des données.
3. **On mixe majuscules, minuscules, chiffres et caractères spéciaux**. Même si cette règle est couramment utilisée, elle augmente considérablement la difficulté de votre password. N'hésitez donc pas à ajouter de façon aléatoire des $, * ou encore 1 !
4. **On évite les substitutions communes**, c'est-à-dire qu'on ne remplace pas un O par un 0 ou A par un 4. Ce remplacement est bien trop simple à trouver, pour quiconque chercherait à trouver votre mot de passe. Comme indiqué précédemment, préférez l'ajout aléatoire de caractères spéciaux, de chiffres ou de majuscules pour complexifier votre password.
5. **On respecte la règle du mot de passe unique**, même si elle est particulièrement contraignante, on en convient. Il s'agit ici d'utiliser pour chaque site un mot de passe différent, qui ne sera jamais réutilisé. Ainsi, même si un de vos comptes se fait hacker, vous n'aurez pas à craindre que les pirates cherchent à réutiliser ce mot de passe sur d'autres sites ! Au minimum, utilisez un mot de passe différent pour vos adresses mails, puisqu'elles vous permettront de récupérer l'accès à vos autres comptes en cas de problèmes.

Trouver un mot de passe, et le retenir : pas si compliqué que ça !

Avec ces quelques règles en tête, il est très facile de **générer un mot de passe sécurisé**, que vous retiendrez très facilement. Il suffit pour cela de choisir une phrase d'une douzaine de mots, contenant au minimum un chiffre, un caractère spécial et une majuscule, puis de ne garder que le premier caractère (ou les deux premiers) à chaque fois !

Voici un exemple : *« **M**on **l**ivre **p**référé **e**st **H**arry **P**otter, par **J**-**K** **R**owling **e**n **1998** ! »* devient *« **MlpeHP,pJ-KRen1998** »*.

En plus d'être composé de caractères en apparence totalement aléatoires, ce mot de passe sera plutôt facile à retenir puisqu'il suffit de se souvenir de la phrase d'origine. C'est exactement ce que propose la CNIL avec son générateur de mot de passe , très pratique pour ne pas se tromper au moment de créer le mot de passe.

Et si vous avez peur de ne pas vous souvenir de ces mots de passe, n'oubliez pas que vous pouvez utiliser un gestionnaire de mot de passe qui le fera à votre place !