Créer le meilleur des mots de passe

Avec la multiplication des services en ligne, de nombreux comptes d'utilisateurs avec mot de passe sont créés. Il est important de respecter quelques règles lors de leur création.

Les mots de passe les plus utilités

Parmi les 25 mots de passe les plus utilisés au monde, « ***123456*** » et « ***123456789*** » reviennent respectivement en 1ère et 2éme position tandis que « ***password*** » , « ***motdepasse*** », « ***qwerty*** » ou « ***azerty*** » font partie du top 10.

Cela signifie que des millions de personnes partagent la même « *clé* » pour accéder à leurs comptes utilisateurs, leurs données personnelles, leur mails, leurs comptes en banque, les photos de leurs enfants, leurs documents administratifs, etc.

Et que bien évidemment, une personne mal intentionnée va commencer par tester les « *serrures* » de ces comptes en y inscrivant ces mots de passe ainsi que toutes les variantes qui y sont affiliées (par exemple « ***987654321*** » ou encore « ***m0t2passe*** »).

Méthodes de piratage

Il n'y a pas de mot de passe infaillible : il existe des programmes capables de calculer toutes les combinaisons de caractères possibles, notamment en passant en revue les mots des dictionnaires, et ce dans toutes les langues.

La faille de ces programmes est le **temps**. En effet, plus le mot de passe sera long et complexe, plus le programme devra mettre de temps afin de trouver la combinaison.

L'utilité de votre mot de passe : protéger vos accès, vos données et vos biens.

Pour protéger votre localisation

Si l'un de vos accès internet est mal sécurisé, il est possible de connaître votre adresse. Protéger sa localisation, c'est se protéger physiquement et se prémunir d'éventuels cambriolages.

Pour protéger votre identité

L'usurpation d'identité, c'est se faire passer pour vous sur Internet afin d'escroquer d'autres utilisateurs. Et il est souvent difficile de prouver que ce n'est pas vous derrière tout ça.

Pour protéger votre argent

Il est de votre responsabilité de sécuriser l'accès à vos données personnelles car elles servent de justificatifs pour s'assurer que vous êtes bien le titulaire des comptes en question.

Pour protéger vos proches

Vos photos sont des données pouvant porter atteinte à vos proches et notamment aux enfants. Les réseaux d'échange de photos d'enfants existent.

Pour protéger votre vie privée

Vos informations privées ne concernent que vous et il serait gênant voire compromettant pour vos relations et votre carrière professionnelle d'être étalées au grand jour.

Pour protéger vos contenus et votre identité numérique

Gardez le contrôle de l'image que vous véhiculez sur internet. Ne laissez à personne d'autre que vous l'accès à vos interfaces de modifications d'informations.

Gérer ses mots de passe

Bien évidemment, devant la complexité de création et de gestion des mots de passe, beaucoup préfèrent la facilité d'un code unique et simple au risque de perdre gros.

Pour vous aider à ne pas les oublier, il existe quelques outils.

- Le gestionnaire de mots de passe

C'est un logiciel qui sert de coffre-fort numérique. Il crypte vos données afin que vous seul puissiez accéder à vos mots de passe.

AVANTAGES

Il est lui-même protégé par un mot de passe.
Au lieu d'en retenir une multitude, il n'y en a plus qu'un seul à retenir.

INCONVENIENTS

Si vous perdez votre accès principal, vous n'accédez plus à vos mots de passe.
Si l'accès principal est découvert, tous vos autres mots de passe le sont aussi.

- Deux carnets

Un carnet bien caché à la maison, un autre à portée de main. Il suffit d'inscrire ses identifiants et mots de passe à chaque nouveau compte créé.

AVANTAGES

Permet de n'avoir plus rien à retenir.
Ne rend pas tributaire d'un appareil connecté.
Permet d'avoir accès à ses mots de passe où que l'on soit.

INCONVENIENTS

Peut se perdre ou se faire voler ! (D'où l'intérêt d'en avoir deux)
On peut parfois oublier d'actualiser l'un des deux répertoires.
Gestion assez contraignante.

- Une très bonne mémoire

Cela peut paraître amusant, mais certaines personnes y arrivent. En usant de moyens mnémotechniques efficaces ou de mémoire photographique

AVANTAGES

Votre tête est le meilleur des coffres-forts.

INCONVENIENTS

Demande une gymnastique cérébrale intense.
Ce n'est malheureusement pas un atout inné pour tout le monde.
Pensez à l'accident de santé et à la perte de mémoire !

Efficacité de votre mot de passe

En moyenne, nous possédons 25 comptes sur internet et nous n'utilisons que 6 mots de passes différents… Il ne faut jamais :

Laisser le mot de passe par défaut (même celui envoyé par courrier !)
Ouvrir la pièce jointe d'un email dont vous n'êtes pas certain de l'expéditeur : risque viral.
Laisser vos sessions internet sécurisées ouvertes.

Quel est le niveau de sécurité de votre mot de passe ?

Protéger la confidentialité de vos informations consiste à définir un mot de passe sûr.
Celui qu'un programme informatique ou une personne persévérante ne pourra pas deviner.
Voici des conseils pour la gestion de comptes utilisateurs.

Astuces pour définir un mot de passe sûr :

Votre mot de passe doit contenir **au moins 10** caractères
Utilisez un **mélange de majuscules, minuscules, chiffres et signes de ponctuation**.
Remplacez des caractères par d'autres **caractères d'aspect similaire**, comme zéro (**0**) pour la lettre « **O** » ou le signe **$** pour la lettre « **S** » ou **@** pour la lettre « **A** ».

Créez un **acronyme unique** :
Utilisez des **traductions phonétiques** : " *RD-V2m1n* " pour " *Rendez-vous demain* ".
La méthode des premières lettres : " *Un tiens vaut mieux que deux tu l'auras* ": **1tvmQ2tl'A**
ou phonétique : " *J'ai acheté huit CD pour cent euros cet après-midi* ": **ght8CD%€7am**

Actions conseillées :

N'utilisez **pas le même mot de passe** pour plusieurs comptes : personnalisez une base solide avec des lettres du site (par exemple : **Imp1tvmQ2tl'A** pour les Impôts et **Sécu1tvmQ2tl'A** pour la Sécurité Sociale)
N'utilisez pas les mots de passe proposés comme exemple.
N'utilisez pas de mot de passe contenant des **informations personnelles** (nom, prénom, date de naissance, numéro de téléphone, etc.).
N'utilisez pas de suite logique ou de mot entier **figurant dans un dictionnaire**
N'utilisez pas des touches du clavier (**azerty**) ou des nombres (**1234**).qui se suivent
N'utilisez pas un seul type de caractères. **Mélangez** nombres, majuscules et minuscules.
N'utilisez pas plusieurs fois les mêmes caractères (**aa11**).

Astuces destinées à préserver la sécurité de votre mot de passe :

Ne dévoilez jamais votre mot de passe à qui que ce soit.
N'enregistrez pas votre mot de passe dans votre navigateur
N'écrivez jamais votre mot de passe sur un papier.
N'envoyez jamais votre mot de passe par e-mail.
Testez et modifiez régulièrement votre mot de passe.
Modifiez votre mot de passe au moindre doute

Tests de complexité d'un mot de passe

Indice de sécurité " Inforisque "			Délai pour casser un mot de passe		
appoigny	=	8	**chapeau**	=	5 millisecondes
AppoignY	=	30	**Chapeau**	=	25 secondes
App01gnY	=	84	**Chapeau4**	=	2 heures
@pPo1gnY	=	176	**Ch@peau4**	=	9 heures
@pP°1§nY	=	264	**+Ch@peAu_4**	=	50 ans

Un mot de passe suffisamment sécurisé devrait avoir un indice supérieur à 200.

Ceci est à pondérer en fonction du nombre de caractères (à ce jour, 8 caractères minimum sont conseillés), plus il y en a, plus il est compliqué de " casser " le mot de passe.

Une astuce :
Pour mémoriser un mot de passe efficace il faut mémoriser une version longue (ex. 12 caractères) et la scinder en 3 pour avoir trois niveaux de sécurité :

Niveau 1 -> **m0nM** (pour des documents partagés) = 42
Niveau 2 -> **m0nMoT2p** (pour des documents personnels) = 84
Niveau 3 -> **m0nMoT2p@s5E** (pour vos comptes en banque) = 275

L'autre solution, certainement la meilleure, est d'utiliser une phrase :

" *jemappelToto&jesuis1exemple2mot2passe* ".

Avec une phrase de ce type, il est quasi impossible pour un ordinateur de casser le mot de passe.

Votre pire ennemi sera vous-même : ne laissez pas votre mot de passe sur un morceau de papier.

Les risques d'une session ouverte

Pourquoi ne faut-il pas laisser vos sessions internet sécurisées ouvertes ?

Voici un exemple concret :

Si vous laissez votre connexion *Gmail* ouverte, il est simple d'aller sur votre réseau social ou votre site de e-commerce préféré, de suivre la procédure « *mot de passe perdu* », saisir votre adresse email et attendre le message donnant le nouveau mot de passe.

Imaginez ensuite ce que l'on peut faire avec ce type de renseignements ; surtout si vous avez enregistré les caractéristiques de votre carte de paiement dans le site… ça ne vous fait pas peur ?