Créer le meilleur des mots de passe

Avec la multiplication des outils et services en ligne, de nombreux comptes d'utilisateurs sont créés et avec eux, des mots de passe. Mais savez-vous à quoi servent ces mots de passe et pourquoi il est si important de respecter quelques règles lors de leur création ?

Les mots de passe les plus utilités

Une étude de 2016 réalisée par une entreprise de gestion de mots de passe affirme que parmi les 25 mots de passe les plus utilisés au monde, « ***123456*** » et « ***123456789*** » reviennent respectivement en 1ère et 2éme position tandis que « ***password*** » (ou « ***motdepasse*** ») et « ***qwerty*** » (« ***azerty*** » pour les claviers français) font partie du top 10.

Qu'est-ce que 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

En théorie, il n'y a pas de mot de passe infaillible.

Il existe aujourd'hui des programmes capables de calculer toutes les combinaisons de caractères possibles afin d'accéder à n'importe quel mot de passe.

D'autres programmes passent en revue les mots du dictionnaires en plusieurs langues ainsi que les suites logiques les plus connues.

La faille de ces programmes réside dans le temps de traitement des données. En effet, plus le mot de passe que vous allez créer sera long et complexe, plus le programme mettra de temps afin de trouver la combinaison.

Un mot de passe sûr n'est donc pas un mot de passe inviolable mais un mot de passe dont la longueur et la complexité sont telles qu'un programme malveillant devra mettre plusieurs centaines voire milliers d'années avant de trouver la combinaison.

Pour quoi faire ?

A priori lorsque vous sortez de chez vous, vous faites en sorte de fermer votre porte à clé. Pour quelle raison ? Afin qu'on ne vous vole aucun bien et qu'on ne détruise ou n'utilise votre logement en votre absence, n'est-ce pas ?

C'est à peu de choses près la même utilité qu'a votre mot de passe : protéger vos accès, vos données et vos biens.

Pour protéger votre localisation

Sur internet, vos données personnelles sont nécessaires à l'utilisation de nombreux services. Qu'il s'agisse de vos comptes administratifs comme les impôts ou encore de sites d'achat et vente en ligne, votre adresse y est souvent renseignée. Si l'un de ces services est mal sécurisé, il est possible de connaître votre adresse et donc de vous retrouver. Protéger sa localisation, c'est se protéger physiquement mais aussi se prémunir d'éventuels cambriolages.

Pour protéger votre identité

C'est un phénomène de plus en plus récurrent. Votre nom, date de naissance, adresse, photo peuvent tomber entre les mains de personnes se faisant alors passer pour vous sur Internet afin d'escroquer d'autres utilisateurs. Il est souvent difficile de prouver que ce n'est pas vous derrière tout ça. Protéger vos données, c'est aussi vous prémunir d'éventuelles poursuites judiciaires.

Pour protéger votre argent

Lorsque vous effectuez des paiements en ligne, vos données bancaires sont transmises. Vous disposez peut-être même d'un porte-monnaie électronique. Ce sont des outils très pratiques nous facilitant l'achat et le transfert d'argent et ils font partie des services les plus sécurisés sur le net. Cependant, il est de votre responsabilité de sécuriser l'accès à vos données personnelles car elles servent souvent de justificatifs aux sites pour s'assurer que vous êtes bien le titulaire des comptes en question.

Pour protéger vos proches

Cela est un sujet sensible mais sachez que vos informations personnelles ne sont pas les seules choses convoitées. Vos photos sont aussi des données pouvant porter atteinte à vos proches et notamment aux enfants faisant partie de votre entourage. Les réseaux d'échanges de photos d'enfants existent malheureusement. Protéger les accès à ces données, c'est aussi protéger l'intégrité de vos proches les plus vulnérables.

Pour protéger votre vie privée

Messages personnels, photos de soirées gênantes, souvenirs de vacances en bikini, secrets entres amis, journal intime, confessions, etc. Toutes ces informations qui ne concernent que vous et qu'il serait gênant voire compromettant pour vos relations et votre carrière professionnelle d'être étalées au grand jour. Sécuriser vos comptes peut vous permettre d'étendre votre sphère personnelle sur internet en toute sérénité.

Pour protéger vos contenus et votre identité numérique

Sécuriser l'accès de vos réseaux sociaux et mails, c'est aussi garder le contrôle de l'image que vous véhiculez sur internet. L'identité réelle étant bien plus difficile à prouver sur Internet, seuls vos contenus et publications peuvent vous y définir. Il est d'autant plus important de ne laisser à personne d'autre que vous l'accès à vos interfaces de modifications d'informations.

Ces raisons sont bien sûr non exhaustives.

Elles n'ont pas pour but de vous couper de toute utilisation numérique mais de vous sensibiliser aux pratiques malveillantes existantes.

Un utilisateur averti en vaut deux.

Repensez-y la prochaine fois que vous direz « *Je n'ai rien à cacher ».*

Comment se protéger convenablement ?

Comme nous l'avons vu précédemment, il est possible de ralentir les programmes de décryptage en complexifiant les mots de passe. Pour cela, il suffit de :

Mélanger les signes et symboles

Majuscules, minuscules, chiffres, symboles de ponctuations variés. Le clavier AZERTY compte 142 caractères différents. Vous avez l'embarras du choix.

Ne jamais mettre moins de 9 caractères

Plus le mot de passe est long, plus il y a de combinaisons possibles. 14 caractères vous offrent une sécurité confortable. Vous pouvez bien évidemment en mettre plus mais songez que vous devrez retaper ce mot de passe à chaque nouvelle connexion.

Ne pas enregistrer le mot de passe dans le navigateur

Si quelqu'un d'autre que vous a accès à votre ordinateur à un moment ou à un autre, rien ne l'empêche de se connecter à vos comptes si votre mot de passe y est enregistré. Il semble pourtant bien pratique de procéder de cette façon, mais vous ne sortiriez pas de chez vous en laissant la clé sur la porte, n'est-ce pas ?

Ne pas faire de suite logique ou de mot entier

Les programmes recherchent aussi dans ce répertoire. Mettre un mot, une expression ou une suite leur faciliterait la tâche puisqu'ils les ont déjà dans leurs bases de données.

Ne pas mettre de numéros ou d'informations personnelles

Numéro de téléphone, date de naissance, de sécurité sociale, de compte bancaire, adresse, nom de famille, prénom des enfants, du chien, de l'entreprise, hobby, etc.

Pour la simple raison que si quelqu'un a accès à ces informations il peut avoir accès à vos comptes.

Et si un programme arrive à accéder à votre mot de passe, il a par la même occasion accès à vos informations personnelles.

Certains pirates retrouvent des mots de passe par le procédé de social-engineering (ingénierie sociale) : ils parcourent Internet à la recherche de toutes vos informations publiques, notamment sur les réseaux sociaux, et essaieront des combinaisons « *logiques* » : votre anniversaire + le nom du chien.

Dans 90% des cas de piratage c'est comme ça que le pirate a obtenu des accès.

Créer un compte = Un mot de passe différent

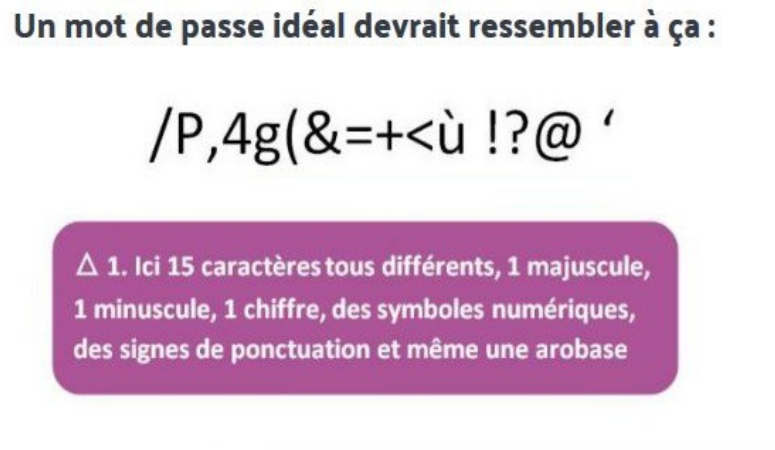
Des failles existent. Même si vous sécurisez parfaitement vos comptes, il arrive que des sites se fassent pirater et les données enregistrées sur leurs serveurs ne sont alors plus protégées. Si votre mot de passe est toujours le même, alors une personne malveillante n'aura aucun mal à accéder à tous vos autres comptes.

Ne jamais le communiquer, même à ses proches

Malgré toute la bienveillance dont vous pouvez disposer envers votre entourage, il n'y a pas de raison valable de leur communiquer vos mots de passe personnels. Cela peut même s'avérer plus néfaste que bénéfique, par exemple en cas de rupture ou de conflits internes. Beaucoup de personnes se font pirater leurs comptes personnels par des personnes qu'elles connaissent.

Lorsque vous créez votre mot de passe, ne l'écrivez jamais en clair

« *En clair* » signifie que vous pouvez voir les lettres, chiffres et symboles qui composent votre mot de passe. Si un site vous propose de vous montrer les caractères que vous tapez, déclinez. Vous devez toujours voir apparaître une suite de points ou d'étoiles lorsque vous le créez.



Mais vous pouvez vous contenter de **9 caractères**, avec a**u moins une majuscule, un chiffre et un caractère spécial**. Et surtout un moyen mnémotechnique pour s'en souvenir sans que ce soit trop évident pour autrui.

Modifier ses mots de passe existants

Maintenant que vous avez pris conscience de l'importance de créer des mots de passe complexes pour sécuriser vos comptes, vous songez peut-être à modifier ceux que vous avez déjà créés et qui ne remplissent probablement pas les conditions idéales pour protéger vos données.

Pour cela, il vous suffira la plupart du temps de cliquer sur l'icône *Paramètres* (qui est symbolisée par un rouage) de vos comptes, d'accéder à votre *Panneau de sécurité* puis de cliquer sur *Changer mon mot de passe*.

Gérer ses mots de passe

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

Pour vous aider à ne pas oublier tous ces mots de passe, il existe quelques outils.

	Gestionnaire de mots de passe	**2 carnets**	**Très bonne mémoire**
COMMENT CA MARCHE ?	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.	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.	Cela peut paraître amusant, mais certaines personnes y arrivent. En usant de moyens mnémotechniques efficaces ou de mémoire photographique
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.	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.	Votre tête est le meilleur des coffres-forts.
INCONVENIENTS	Si vous perdez votre accès principal, vous n'accédez plus à vos mots de passe. D'autant plus que si votre mot de passe principal est découvert, tous vos autres mots de passe le sont aussi.	Peut se perdre ou se voler ! (D'où l'intérêt d'en avoir deux) On peut parfois oublier d'actualiser l'un des deux répertoires. Gestion assez contraignante.	Demande une gymnastique cérébrale intense. Ce n'est malheureusement pas un atout inné pour tout le monde.

Efficacité du mot de passe selon Google

Il faut savoir, qu'en moyenne, nous possédons 25 comptes sur internet et nous n'utilisons que 6 mots de passes différents… Il est donc urgent que chacun prenne conscience des enjeux. Il ne faut jamais :

Laisser le mot de passe par défaut (même celui envoyé par courrier !)

Ouvrir une pièce jointe d'un email dont vous n'êtes pas certain de l'expéditeur : risque d'être infecté par un virus

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.

Un mot de passe sûr, signifie qu'un programme informatique ou une personne persévérante ne pourra pas le deviner rapidement.

Voici les conseils de sélection d'un mot de passe proposés par Google pour la gestion des comptes utilisateurs.

Astuces pour définir un mot de passe sûr :

Utilisez des **signes de ponctuation** et " **/ "** ou des **chiffres**.
Utilisez un **mélange de majuscules et de minuscules**.
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* ".

Actions déconseillées :

N'utilisez **pas le même mot de passe** pour plusieurs comptes importants, tels que Gmail et les opérations bancaires en ligne.
N'utilisez pas les mots de passe proposés comme exemples.
N'utilisez pas de mot de passe contenant des **informations personnelles** (nom, date de naissance, etc.).
N'utilisez pas de mot ou d'acronyme **figurant dans un dictionnaire**.
N'utilisez pas des touches séquentielles du clavier (**azerty**) ou des nombres qui se suivent (**1234**).
N'utilisez pas un seul type de caractères dans votre mot de passe. **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'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.

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 ?