



Choisir des mots de passe sécurisés et s'en souvenir sans effort !

Une à une, nos données personnelles sont confiées aux serveurs, aux nuages. Beaucoup de données sont ainsi concentrées à quelques endroits sur des serveurs. Il suffit alors à un hacker/dérobeur de rentrer sur un de ces serveurs pour dérober toutes les données qui y sont stockées.

Il y collectera vos mots de passe et/ou leur empreinte couplés à votre adresse mail et ... si vous êtes assez imprudent pour utiliser le même mot de passe sur tous vos comptes, il pourra très rapidement accéder à toutes vos données sur le Web.

Selon [Bruce Schneier](#), spécialiste en sécurité informatique et auteur de plusieurs livres sur la cryptographie,



"As insecure as passwords generally are, they're not going away anytime soon. Every year you have more and more passwords to deal with, and every year they get easier and easier to break. You need a strategy." soit en français (soit en français *"Même si les mots de passe ne sont globalement pas sûrs, ils ne vont pas disparaître de sitôt. Chaque année, vous avez de plus en plus de mots de passe à gérer, et chaque année, ils deviennent de plus en plus faciles à pirater. Il vous faut une stratégie."*)



"Pretty much anything that can be remembered can be cracked." soit en français



"Presque tout ce dont on peut se souvenir peut être cassé.)"

Ne soyez pas la porte d'entrée !

Pour accéder à un serveur, un client doit disposer d'un mot de passe. Un mot de passe est une clé d'accès et vous le savez, il y a clé et clé !

Le mot de passe idéal



- **est complexe**
 - **est long**
 - **est unique / n'est pas un "passe"** (doit être différent pour chaque compte)
 - **change régulièrement**
 - **n'est pas un mot d'un dictionnaire (linguistique, thématique, etc)**
1. Il est complexe : sa complexité dépend de la variété des caractères qui le compose: en plus des caractères alphabétiques (26), les décliner en Majuscules / minuscules augmentera la difficulté pour le hacker (26*2); vous pourrez aussi utiliser des caractères numériques (10) et idéalement des caractères spéciaux (comme = ou # ou - ou , ou _ ou ; ou : ou ! ou ? etc).
 2. Il est long : éviter les mots de passe de moins de 8 caractères et utilisez idéalement des mots de passe de 13 caractères et plus.
 3. Il change régulièrement : les risques de dévoiler son mot de passe sont nombreux, le changer régulièrement est donc prudent !
 4. Cela signifie une serrure = un clé et une clé = une serrure ..., * n'utilisez donc jamais le même mot de passe pour deux comptes différents.
 5. Éviter les prénoms, les titres, les noms propres, les chiffres successifs.



CRYPTOGRAPHIE

Longueur du mot de passe	NTLM		MD5crypt		SHA512crypt		Bcrypt N=5		Bcrypt N=12	
	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+	alnum	Alnum+
4	0,01''	0,18''	10''	2'43''	17'	4h31'	5'35''	1h30'	11h40'	7j18h
5	0,4''	12,9''	6''	3h15'	10h	13j13h	3h21'	4j11h	17j12h	2a
6	14,5''	15'29''	3h40'	9j18h	15j6h	3a	121h	323j	1,6a	110a
7	8'42''	18h35'	5j12h	2a	1,5a	193a	181j	64a	62a	8*10'a
8	5h13'	56j	198j	138a	54a	13*10'a	18a	4,5*10'a	2*10'a	5,73*10'a

Tableau 1 : Temps estimé pour effectuer une recherche exhaustive avec John the Ripper en fonction de la longueur du mot de passe et des caractères utilisables (h : heure ; j : jour ; a:année).

Comme pour les clés physiques, la solidité d'un mot de passe peut être mesurée par le temps mis à le casser. La plupart des mots de passe des utilisateurs d'outils et services numériques ne résistent pas plus de quelques secondes aux outils informatiques de cassage courants.

Une solution ?

Ou comment, gérer la sécurité de très nombreux comptes, qui évoluent au fil du temps, chez soi, au travail ou ailleurs ?

Voilà peut-être une solution originale: retenir une charade plutôt que 100 mots de passe !

Pas besoin de greffer une barrette mémoire supplémentaire à votre cerveau, nous pouvons tous concevoir et faire fonctionner une charade (un algorithme) et la mémoriser. Comme une recette de cuisine !

Niveau de sécurité acceptable

Les recommandations que je retiens pour mes mots de passe sont les suivantes :



- compose de **10 caractères minimum**,
- contient des chiffres, des lettres minuscules, des lettres majuscules,
- ne contient aucun mot figurant dans un dictionnaire (mots, noms propres, noms d'animaux, etc),
- ne contient **aucune date** (date de naissance, ...),
- ne contient **aucun code ou numéro** (numéro de Sécurité Sociale, plaque d'immatriculation de

- véhicule, ...),
- ne contient **aucune partie de mon adresse email**,
 - va changer tous les ans

Je peux décider que mon mot de passe sera composé de **4 parties** :

- la première sera les trois premières lettres de mon surnom (**Sur**)
- la deuxième sera le numéro de la maison que j'habitais quand j'étais enfant (**59**)
- la troisième aura les trois premières lettres du site pour lequel j'ai besoin d'un mot de passe (**???**)
- la dernière recevra les deux derniers chiffres de l'année en cours (**24**)
- je sépare chaque partie par un tiret

Par exemple, si je dispose d'un compte sur le site de [La Poste](#), d'une boîte mail chez mon *fournisseur d'accès*, d'un compte à la *SNCF* et un autre à la *FNAC* sans compter celui sur le site service public, mon mot de passe sera :

Sur-59-Lap#24	Pour mon compte chez Laposte	
Sur-59-Fre#24	Pour mon compte chez Free	
Sur-59-Snc#24	Pour mon compte à la SNCF	
Sur-59-Fna#24	Pour mon compte à la FNAC	
mon premier est	un indicateur de temps, trimestriel	1T19
mon deuxième est	le code pin de ma carte transpole (les 4 chiffres)	3348
mon troisième est	mon oiseau préféré (les trois première lettres)	mol
mon quatrième est	le site auquel je me connecte	meD
mon cinquième est	un caractère de début et fin	=

—> mon mot de passe pour la médiathèque est **=1T193348molmeD=** (1 million de million de million d'années soit 10 puissance 18 années)

— [André Vanderlynden](#) 2019/03/10 7:39   

From:

<https://informethic.net/dokuwiki/> - **Ethique et Informatique ...** **dietétique**

Permanent link:

<https://informethic.net/dokuwiki/doku.php?id=clicsetdeclics:motsdepasse&rev=1710926760>

Last update:

2024/03/20 10:26

