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.)”

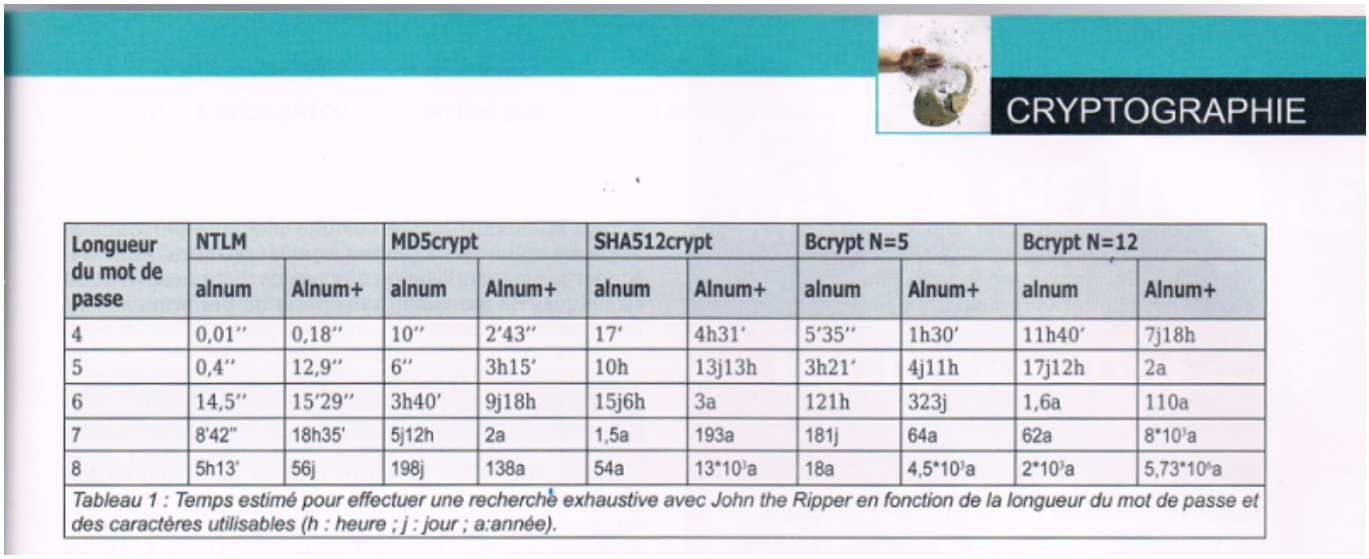
Ne soyez pas la porte d'entrée !

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.



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	$8*10^3$a
8	5h13'	56j	198j	138a	54a	$13*10^3$a	18a	$4,5*10^3$a	$2*10^5$a	$5,73*10^6$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 les 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 des dizaines ou centaines de 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
Sur-59-Gra#24	Pour mon compte à la Grand Plage

J'ai une solution pour tous les mots de passe nécessaires aujourd'hui comme pour ceux que je créerai à l'avenir.

Niveau de sécurité avancé

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

- contient 13 caractères minimum,
- comporte des chiffres, des lettres minuscules, des lettres majuscules,
- aucun mot figurant dans un dictionnaire (mots, noms propres, noms d'animaux, etc),
- aucune date (date de naissance, ...),
- ne contient aucun code d'identification ou numéro (numéro de Sécurité Sociale, plaque d'immatriculation de véhicule, ...),
- ne contient aucune partie de mon adresse email,
- va changer au minimum tous les ans

un exemple : je suis passionné par les arbres.
Parmi les arbres, je retiens l'**A**mandier, le **B**annanier, le **C**itronnier, le **D**attier, l'**E**ucalyptus, le **F**iguier, le **G**roseillier, le **H**oux, l'**I**f, le J**as**min, le **K**iwi, le **L**ilas, le **M**arronnier, le **N**oisetier, l'**O**rme, le **P**ommier, le **Q**uinina, le **R**obinier, le **S**ureau, le **T**illeul, l'**U**lmo, la **V**iorne, le **W**engé, le **X**anthoceras, le **Y**ucca, et le **Z**iziphus mais j'aime aussi tous les autres arbres.

Une charade un peu plus élaborée :
Mon mot de passe sera toujours composé de **4 parties** :

- la première partie sera les trois premières lettres du nom de l'arbre dont la première lettre est cella de mon identifiant (mon identifiant pour La Poste est alberteinstein –> je retiens les lettres **Ama**)
- la deuxième partie le numéro de la maison que j'habitais quand j'étais enfant (**59**)
- la troisième partie aura les trois premières de l'arbre dont la première lettre est celle du nom du site (laposte.fr –> **Lil**)
- la quatrième partie sera composée deux derniers chiffres de l'année en cours précédés d'un caractère spécial (**!24**)
- j'ajoute un caractère spécial en début et en fin de mot de passe (**#**)

#Ama59Lil!24#	Pour mon compte alberteinstein chez laposte.fr
#Lil59Fig!24#	Pour mon compte lea chez free.fr
#Ama59Sur!24#	Pour mon compte Ahmad chez sncf.fr
#Ama59Fig!24#	Pour mon compte Ahmad chez fnac.fr
#Ama59Mar!24#	Pour mon compte Ahmad chez mediathequederoubaix.fr (la Grand Plage)

Comment s'en souvenir ?
Ama (pour l'arbre qui commence par A comme alberteinsten (mon didentifiant)), **59** par que mes parents habitaient au au 59 quand je suis né, **Lil** pour l'arbre qui commence par L come laposte.fr, **!24** parce que nous sommes en 2024 (je le changerai en janvier 2025).
Vous préférez le foot, la philatélie, les papillons, les peintres, les auteurs, les compositeurs, les races de vaches ou de chiens, les pays du monde, les montagnes, les rivières, que sais-je encore, remplacez donc les arbres par vos compagnons préférés, ça marche aussi bien !
Vous n'avez maintenant plus un seul mot de passe à retenir, votre algorithme tout seul vous permet de les retenir tous.
Chaque année, je remplacerai les deux chiffres de l'année. Ainsi, en janvier 2025, mon mot de passe pour ma boîte mail à La Poste deviendra **#Ama59Lil!25#**

Et les vôtres ...

Construisez votre propre formule, avec les parties qui vous conviennent, dans l'ordre qui vous convient. Utilisez-la pour **TOUS** vos mots de passe.

Est-ce que ça marche pour tout ?

OUI ! <note>Pour les identifiants qui commencent par un chiffre (Sécurité Sociale, Banque) on

remplace 0123456789 par ABCDEFGHIJ

Allez plus loin

évaluer son mot de passe
évaluer son mot de passe, ses qualités, ses défauts
Modifier son mot de passe Gmail ... quitter Gmail c'est mieux
Comment changer votre mot de passe Windows 7 Windows 10 - Gmail - Outlook - Yahoo Mail - La Poste
Les conseils de la CNIL pour un bon mot de passe
[MISC n°89] Références de l'article « Cassage de mots de passe : que mettre dans votre boîte à outils ? »
Recommandations de sécurité relatives aux mots de passe du Secrétariat général de la défense et de la sécurité nationale

---

Quelques exemples

Exemple 1

mon premier est	un indicateur de temps, l'année	!24
mon deuxième est	la ville où je suis né (les 3 premiers caractères), la deuxième lettre sera en majuscule, les autres en minuscusles	rBx
mon troisième est	le site où je me connecte, les trois premières lettres, la troisième en majuscules	meD

—> mon mot de passe est #24rBxmeD

Exemple 2

mon premier est	un indicateur de temps, annuel	@24
mon deuxième est	la ville où je suis né(e) (les 3 premiers caractères), la deuxième lettre sera en majuscule, les autres en minuscusles	rBx
mon troisième est	le site où je me connecte, les trois premières lettres, la troisième en majuscules	meD
mon quatrième est	un séparateur (que je mets au début, à la fin et entre chaque partie de la charade	!

—> mon mot de passe pour la médiathèque est !@24!rBx!meD! (204 million années)

Exemple 3
… mon préféré …
Vous êtes (et je suis ;)) passionné par les oiseaux. Voici une liste alphabétique des oiseaux que je préfère: **Alo**uette des champs, **Béc**assine des marais, **Cyg**ne noir, **Din**don, **Épe**rvier d'Europe, **Fai**san obscur, **Gri**ve musicienne, **Hir**ondelle rustique, **Ibi**s sacré, **Jas**eur boréal, **Két**oupa brun, **Lin**otte mélodieuse, **Moi**neau domestique, **Niv**erolle alpine, **Oie** cendrée, **Per**drix grise, **Qui**scale rouilleux, **Rou**ge-gorge familier, **Sar**celle d'hiver, **Tou**rterelle turque, **Upu**pa epops, **Van**neau huppé, **Xen**us cinereus (Chevalier bargette), **Zon**otrichia albicollis (Bruant à gorge blanche)

mon premier est	un indicateur de temps, annuel	.24
mon deuxième est	le code pin de ma carte transpole (les 4 chiffres)	3348
mon troisième est	mon oiseau préféré (les trois première lettres)	moI
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 =.243348moImeD= (1 million de million de million d'années soit 10 puissance 18 années)

— *André Vanderlynden* *2024/03/10 7:39*