

Un mot de passe doit être :

Suffisamment fort

Un mot de passe doit comporter un minimum de 10 caractères composés de lettres majuscules, minuscules, de chiffres et si possible de caractères spéciaux.

Il faut, en moyenne, 5 minutes seulement pour craquer un mot de passe tel que «darren» et 41 jours pour un mot de passe tel que «Land3rz».

Difficile à trouver mais facile à mémoriser

Utiliser une méthode de construction de mots de passe ou un moyen mnémotechnique.

Différent selon les utilisations

Lorsqu'un mot de passe est utilisé, il faut que son domaine d'utilisation soit le plus restreint possible pour limiter le risque de divulgation. On associera donc à chaque usage un mot de passe différent.

Incessible

Un mot de passe est **strictement personnel** : ne le confier à personne (même à sa hiérarchie). Un service ne vous demandera **jamais** de communiquer votre mot de passe

Non enregistré

La plupart des navigateurs Internet proposent d'enregistrer les mots de passe, par le biais d'une petite case à cocher « retenir le mot de passe ». Si vous n'avez pas de mot de passe « master » pour protéger vos mots de passes enregistrés, n'importe quelle personne utilisant votre ordinateur pourra les consulter.

N'enregistrez vos mots de passe que dans un espace crypté fait pour cela tel qu'un coffre fort de mots de passe.

Et enfin... changé régulièrement !

Quelques méthodes de construction

La méthode phonétique ou syllabique

C'est un fameux trois-mâts, Hisse et ho ⇒ **c1famE3ma,is&o**
J'ai acheté huit CD pour cent euros cet après-midi ⇒
ght8CD%E7am

La méthode des premières lettres

Une souris verte qui courait dans l'herbe ⇒ **Usvqcdl'h**

Introduction de caractères spéciaux ou de chiffres

Mot-clé « secret » ⇒ **S1e2C3_r4E5t6**

Symboles remplaçant des lettres

@,4	3,€	!,	0,°	μ [	6,9	1,£	\$,5	*,><
A	E	I	O	U C	G,g	L	S	X

Attention tout de même, cette méthode de remplacement est très connue et les dictionnaires de mots de passe savent maintenant la gérer. Il ne faut donc pas utiliser cette méthode seule mais la combiner avec d'autres.

Combinaisons de plusieurs méthodes

Le mieux est encore de combiner plusieurs de ces méthodes.

Gérer ses mots de passe

Les coffres forts de mots de passe

Un coffre fort de mots de passe est un logiciel qui s'installe sur votre machine et qui peut stocker vos mots de passe en toute confidentialité et sécurité dans un système central auquel vous pouvez accéder à tout moment. Il suffit de ne retenir qu'un seul mot de passe, celui d'accès au coffre fort.

Exemple : Keepass (<http://keepass.info/download.html>)

Les différents types de piratage du mot de passe

Bruteforce

L'attaque par force brute consiste à tester tous les mots de passe possibles.

Attaque par dictionnaire

L'attaque par dictionnaire consiste à tester une série de mots issus d'un dictionnaire. Toutes sortes de dictionnaires sont utilisés pour cette attaque (dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...).

Plusieurs règles de transformation des mots du dictionnaire sont également utilisées par les outils automatisés pour augmenter le nombre de combinaisons possibles comme par exemple : le remplacement d'un ou de plusieurs caractères du mot du dictionnaire par une majuscule (uNiverSiTe) ou le remplacement de certains caractères par des chiffres comme par exemple le S en 5 ou le ! pour I (Un!verSiTe)

Social engineering

Le social engineering a pour but de vous soutirer des informations sans compétences techniques particulières. Grâce aux réseaux sociaux par exemple, il est devenu courant de récupérer le nom de jeune fille de votre mère ou le nom de votre animal de compagnie qui sert très (trop) souvent de réponse à la question secrète utilisée en cas de perte de mot de passe. Une question secrète doit donc avoir une réponse connue de vous seul.



Keylogger

Un enregistreur de frappes clavier, en anglais keylogger, est un dispositif logiciel ou matériel employé par une personne malveillante pour capturer ce qu'un utilisateur frappe au clavier.

Certains logiciels malveillants contiennent des keylogger. Pour vous en prémunir, assurez-vous toujours de la provenance et de la légitimité des logiciels que vous installez.

Phishing et autres attaques par ruse

Certains emails semblant émaner d'un organisme de confiance (votre banque, l'Université de Poitiers, etc.) vous indique qu'un problème est survenu sur son compte (dépassement de quota par exemple) et vous invite à renvoyer votre mot de passe ou à vous rendre sur un site et à remplir un formulaire en ligne.

Un organisme de confiance ne **vous demandera jamais** votre mot de passe par email, ne répondez donc jamais à ce type de demande !

Exemples de bons et de mauvais mots de passe

Quelques exemples de mauvais mots de passe :

Alice2007/04/15

Ce mot de passe est directement dérivé du prénom de l'utilisateur et d'une date.

K@nstitutionne1

Ce mot de passe est un mot du dictionnaire avec quelques caractères modifiés.

&Ntschuld|gung

Ce mot de passe est un mot du dictionnaire allemand avec quelques caractères modifiés (entschuldigung). Il ne faut pas oublier que tous les dictionnaires sont disponibles sur l'Internet.

Bob:0622780734

Ce mot de passe est un prénom et un numéro de téléphone où les « 0 » sont remplacés par des « O ».

CygW1n@mel.gouv.fr

Ce mot de passe est une adresse de courrier électronique.

c1famE3ma,is&o

Ce mot de passe est proposé en exemple dans ce document et ne doit donc pas être utilisé !

M&z0p0t@μ1e

Ce mot de passe pourrait être correct s'il n'était pas obtenu à partir d'un mot géographique (Mésopotamie) dans lequel six caractères sur 11 ont été remplacés selon des critères classiques (« & » pour « é », « 0 » pour « O », « @ » pour « a », « μ » pour « m », « 1 » pour « i »). Les outils de craquage par dictionnaire intègrent généralement ce genre de stratégie.

Quelques exemples de bons mots de passe :

H?cU@f1bv...

Avant d'avoir été rendu public, ce mot de passe était correct. Il comprend 13 caractères, intègre deux majuscules, 7 minuscules, un chiffre (1) et trois caractères spéciaux (?@%). Le moyen mnémotechnique utilisé est la première lettre de chaque mot de ces autres vers célèbres: « Heureux qui comme Ulysse a fait un beau voyage... »

Qj'M@f&rK0

Avant d'avoir été rendu public, ce mot de passe était correct. Il comprend le minimum de 10 caractères, intègre 3 majuscules, 3 minuscules, un chiffre (0) et trois caractères spéciaux ('@&). Le moyen mnémotechnique utilisé est le début du vers célèbre « que j'aime à faire connaître ce nombre utile aux sages » qui donne par le nombre de lettres de chaque mot la valeur des premières décimales de π : 3,1415926535...

Les mots de passe

Sécurité Informatique

MémoTICE n°3 :



Réalisation : *4*-médias