MÉTHODE STRATÉGIQUE POUR VOS MOTS DE PASSE

par Eric SOTOCA

Edition Sotoca-Online

Introduction

Consulter ses e-mails, son compte bancaire en ligne, accéder à un service payant, démarrer son ordinateur au bureau et même parfois à la maison : pour tous ces services, on a besoin d'un mot de passe… si possible différent à chaque fois. Or notre quotidien est déjà "envahi" par les codes secrets : des cartes bleues aux téléphones portables en passant par l'entrée des immeubles, les mots de passe et autres codes d'accès sont partout. Cela fait beaucoup pour nos fragiles mémoires…

Il nous faut une stratégie pour gérer nos mots de passe.

Dans cet ebook, je vous explique tout d'abord pourquoi votre stratégie actuelle a de grandes chances d'être vulnérable. J'ai recensé 7 raisons principales qui, je crois, touchent 90% des Français.

Constater que son mot de passe est "fragile" est une chose, déployer une stratégie pour le "solidifier" demande une certaine méthodologie.

Je vais vous accompagner, pas à pas, dans ce changement. La méthode demande certes une réflexion pour se l'approprier. Mais une fois en tête, c'est un gain de temps pour tout le reste de sa vie.

Dès que vous aurez à ouvrir un nouveau compte sur Internet vous saurez précisément quel mot de passe vous devez insérer.

Je vous souhaite un bon apprentissage :-)

Eric Sotoca

Sommaire

Partie 1 :

Pourquoi devez-vous changer votre Mot de Passe ? Maintenant !

Parce que votre mot de passe fait partie des plus utilisés.

Une analyse des listes de mots de passe les plus répandues dans le monde m'a permis d'établir une extrapolation spécifique pour la France.

Si votre mot de passe est composé à partir d'expressions du tableau suivant, sachez qu'il sera très facile pour un hacker de vous pirater. Ces derniers risquant de privilégier de forcer vos comptes avec les mots de passe les plus connus.

Extrapolation des mots de passe les plus courants en France

12345	**azerty**	**123abc**
123456	**mot2passe**	**starwars**
1234567	**football**	**passw0rd**
12345678	**jetaime**	**hello**
123456789	**iloveyou**	**bonjour**
00000000	**admin**	**motdepasse**
123123	**login**	**87654321**
123123123	**abc123**	**654321**

Conseils n°1 : ORIGINALITÉ

Ne pas choisir un mot de passe trop commun,
cela prend 5 min à quiconque de tester
une liste de quelques mots de passe !
Et moins d'une seconde pour un pirate !!!

Parce que justement vous n'avez qu'un seul mot de passe !

Pourquoi est-ce un problème ? Je vais vous donner 3 exemples de scénarios, tout à fait probables, pour vous montrer comment votre mot de passe pourrait vite vous échapper…

Scénario N°1 : L' Apprenti Hacker

Soif de savoir, l'Apprenti Hacker veut se tester en décodant par exemple les mots de passe rattachés à un site Internet.

Étant stagiaire ou salarié dans l'entreprise qui héberge le serveur du site, il peut copier le fichier concerné rassemblant tous les mots de passe. Et même si ce dernier est codé, il aura tout le temps nécessaire afin de tester des logiciels étudiés pour la circonstance.

Le plus grand défi des hackers est d'arriver à pénétrer les sites Internet, mais de l'intérieur, c'est beaucoup plus facile !

Il existe des magazines de hacking, en vente libre en France, dans n'importe quel tabac-presse.

Ils peuvent aussi se trouver par dizaine sur des sites de partage sur Internet, et ce, sans débourser 1 centime.

Toute personne peut ainsi s'initier et devenir un pirate en herbe et donc tenter de tester certains outils.

Scénario N°2 : Les Sites proposant des Films, Livres et Magazines piratés

Imaginons que vous avez entendu parler de sites sur lesquels vous pouvez télécharger facilement les derniers films, livres ou magazines (il en existe des dizaines). Au bout d'un moment, vous risquez d'être tenté !

Alors, petit à petit, vous prenez l'habitude de les utiliser, et un jour vous vient l'idée de vous inscrire gratuitement pour bénéficier d'un téléchargement plus rapide. Ceci pourrait être une erreur.

En effet lors de l'inscription, vous venez de donner votre mot de passe préféré sur un site plus que douteux. Qui sait ce qu'il va devenir à présent. Votre mot de passe peut rejoindre une base de données déjà conséquente créée pour être revendue sur Internet (ou même le Dark Web).

Scénario N°3 : Un site réputé et connu se fait pirater

En préparant cet ebook, j'ai été surpris de constater que le site du Monde avait une rubrique permanente sur le piratage. Les sites de Yahoo, L'équipe, British Airways,... apparaissent en première page ! Alors oui, aucun site n'est vraiment à l'abri. Un jour, il se peut que votre mot de passe fasse partie du butin.

Conseils n°2 : MULTIPLICITÉ

Avoir des mots de passe différenciés pour chaque site internet.

Parce que votre mot de passe a une structure commune.

Vous n'avez pas trouvé d'autres façons, pour vous rappeler de votre mot de passe, que d'associer un mot et nombre que vous appréciez bien car rattachés à des sentiments positifs.

Que ce soit le prénom de votre enfant, de votre animal de compagnie ou de la ville de naissance ou d'habitation, tous ces exemples peuvent apparaître dans des livres, des pages facebook et donc dans des "dictionnaires" de hackers.

Pourquoi est-ce un problème ?

Parce que les hackers vont utiliser des bases de données de dictionnaires de plusieurs langues. Quelques minutes suffisent à un ordinateur performant pour exécuter des millions d'opérations combinant et mixant des mots existants.

Evitez donc de choisir une des combinaisons suivantes, particulièrement ciblées :

Prénom, surnom, nom	+	Date ou jour de naissance
Fleur ou animal		Département d'habitation
Star		Département de naissance
Ville		Âge
Suite de lettre style "Abc"		Suite de nombre style "123"

Conseils n°3 : COMPLEXITÉ

Avoir des mots de passe qui soient formés d'aucun mot d'un dictionnaire.

Parce que vous notez tous vos mots dans un endroit précis.

Ok, vous faîtes partie de ceux qui ont des mots de passe différenciés pour chacun de vos sites, bravo !

Oui mais… vous avez tellement de créativité qu'aujourd'hui vous ne savez plus comment les retenir.

Cette technique était tout à fait opérationnelle lorsque vous aviez 5 comptes à gérer, mais aujourd'hui que ce nombre a doublé, voire triplé, ce n'est plus envisageable.

Alors vous avez dû, à regret, noter tous vos codes dans un petit calepin soigneusement rangé dans le tiroir de votre bureau.

Si vous êtes seul chez vous, peut-être avez vous préféré l'utilisation de post-it qui entourent les bords de votre écran d'ordinateur…

Le premier risque est de tout simplement perdre votre calepin ou même vous le faire voler.

Imaginez également qu'une personne mal intentionnée n'en prenne ne serait-ce que des photos pour avoir le loisir de s'introduire sur vos comptes en toute tranquillité…

Enfin, comment allez-vous faire lorsque vous devrez accéder à un site hors de chez vous ? Que ce soit en formation, chez un ami, en vacances, vous serez coincés !

Conseils n°4 : MÉMORISABLE

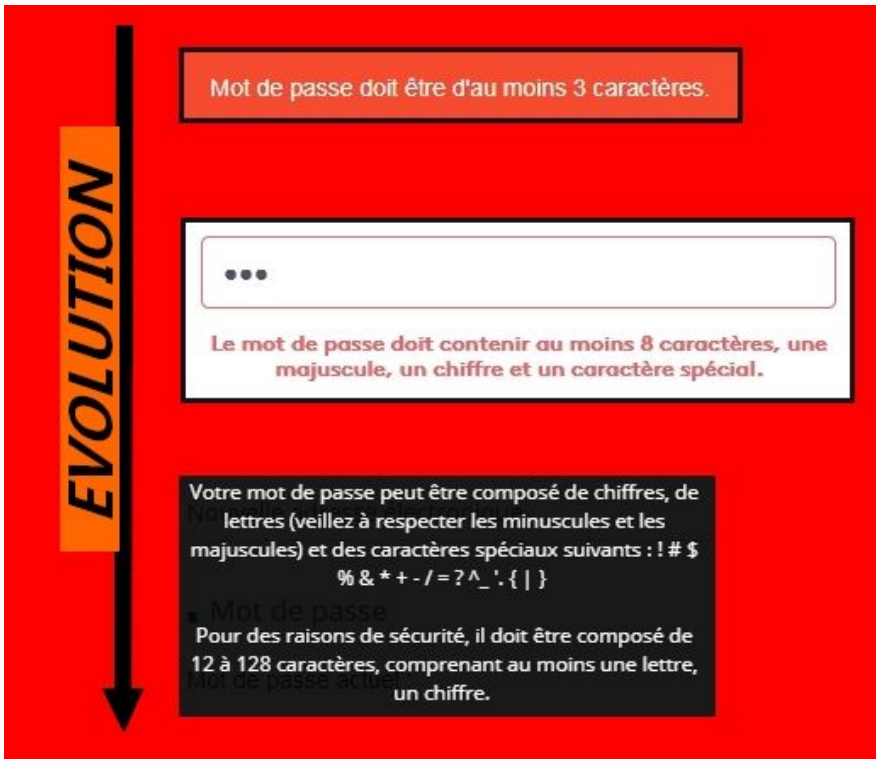
Choisir des mots de passe facilement mémorisables.

Parce que votre mot de passe ne passe plus.

De nos jours, il est de plus en plus demandé des mots de passe avec certains critères : des caractères spéciaux, des majuscules, un certain nombre de caractères…

Même en ayant pris le temps de réfléchir à une stratégie bien établie pour avoir des mots passe différenciés, il arrive que votre stratégie ne soit plus opérationnelle, c'est à dire utilisable quel que soit le site où vous souhaitez créer un compte.

Vous vous retrouvez alors avec une exception à votre règle et du coup, vous devez la noter quelque part. Mais comment faire alors pour que cet espace ne soit pas, à nouveau, une clé accessible et convoitée?



Conseils n°5 : ADAPTABLE

Prévoyez un mot de passe qui puisse s'adapter à un maximum de contraintes.

Parce que vous utilisez un gestionnaire de mots de passe.

Peut-être avez-vous lu cette information dans un magazine, les gestionnaires de mots de passe seraient LA solution pour gérer tous vos mots de passe.

Passpord Safe, Keepass, Enpass, tous ces logiciels sont gratuits et seraient là pour vous simplifier la vie. Ils rassemblent tous vos mots de passe au sein d'une base de données. Le stockage semble entièrement sécurisé puisque les données sont cryptées. Vous n'auriez ainsi qu'un mot de passe à retenir, permettant d'accéder à la base.

Autant vous dire que même si la solution paraît séduisante, attendez un peu avant d'embrasser la mariée…

En effet, du coup, ce super coffre fort devient la cible privilégiée de tous les hackers. Une seule porte à ouvrir pour accéder à toutes les données ! Une aubaine ! Et vu les progrès dans la rapidité de calcul des données, il semble peu probable que cette solution dite "entièrement sécurisée" le reste à long terme.

Sans parler que si vous oubliez le mot de passe "maître", vous n'avez accès à plus aucun site !

Ces logiciels sont installés sur votre ordinateur donc si vous devez utiliser un compte à partir d'un autre lieu que chez vous (vacances, formation, travail,…) comment faire ?

Enfin, ne vous faites pas voler votre ordinateur personnel ! Et que se passe-t-il si votre disque dur rend l'âme ?

Donc cette solution n'est pas non plus la plus conseillée.

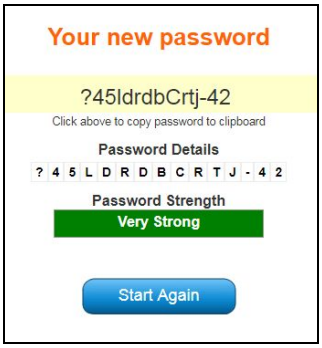
Conseils n°6 : SECRET

Ne pas mettre tous ses mots de passe dans le même endroit car cela devient un vrai enjeu pour les hackers.

Parce que vous utilisez un générateur performant.

Super ! Vos mots de passe sont générés de façon aléatoire. Ce sont des suites de lettres, de chiffres et de caractères spéciaux du style 1jjXkB@25M2QsX. Ces mots de passe sont parmi les plus difficiles à trouver, malheureusement ils sont aussi les plus difficiles à retenir.

Vous vous retrouvez dans le même contexte que la raison n°4 “Parce que vous notez tous vos mots dans un endroit précis”.



Comment faire autrement que de noter ces fameux mots de passe.

Si vous voulez voir à quoi ressemble un tel générateur, c’est par ici :

https://www.safepasswd.com/

Et qui ne vous dit pas non plus que ces services en ligne ne sont pas gérés par des pirates ! Il leur suffirait alors d’ajouter toutes les propositions générées dans leur base de données.

Alors non, les générateurs ne sont là encore pas LA meilleure solution. Vous devez avoir une bien meilleure stratégie.

Conseils n°7 : STRATÉGIQUE

Ne pas utiliser un générateur de mot de passe aléatoire.

Partie 2 :

La Méthode

Définir votre longueur optimale

Votre stratégie pour vos mots de passe va dépendre de votre propre utilisation d'Internet. Avez-vous des données ultra confidentielles ? Devez-vous régulièrement entrer vos mots de passe sur votre ordinateur ?

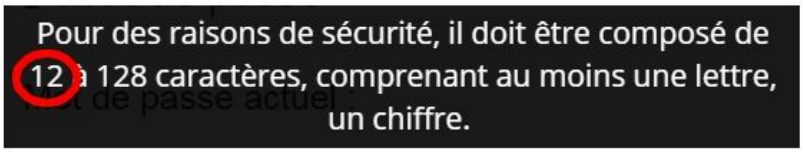
Car pour cette première étape, vous allez définir de combien de caractères votre mot de passe sera constitué. Attention, il faut savoir que l'idée est d'entrer, à chaque fois, votre mot de passe de façon manuelle.

Vous auriez préféré les enregistrer dans votre navigateur ? C'est plus facile en effet, mais beaucoup moins sécurisé ! Comme je vous l'ai expliqué dans la partie précédente, **dès qu'un mot de passe est sauvegardé ailleurs que dans votre tête, il y a un risque.**

Sachant que plus votre mot de passe sera long, plus il sera efficace, vous allez devoir choisir entre sécurité et confort d'utilisation.

> ***"Mon conseil est que la longueur de votre mot de passe soit comprise entre 12 et 16 caractères."***

Ça peut vous paraître beaucoup mais pour avoir étudié le top 50 des sites les plus utilisés en France, j'ai pu synthétiser les critères demandés et déterminer le nombre de caractères idéal à ce jour. Un exemple qui touche tout le monde ? Le site des impôts :



Etape n°1

Choisir un mot de passe qui comportera entre 12 et 16 caractères. 12, c'est génial, 16, au top !

La partie fixe, véritable clé de voûte

Vous le savez désormais : un bon mot de passe ne doit pas être un mot standard. Il est conseillé de mélanger des lettres, des chiffres et des caractères exotiques pour obtenir un code sûr. Par exemple, il sera très difficile à un pirate de deviner un code comme " ***1*&1Acof1PùA*** ". Mais le problème, c'est que vous aurez aussi du mal à vous en souvenir, surtout sachant qu'il faut, dans l'idéal, le noter nulle part !

Un code doit être facile à retenir mais difficile à deviner. Il existe des moyens pour créer des mots de passe complexes et facilement mémorisables. Notre objectif final est de concevoir des mots de passe de 12 caractères qui comprendront à la fois des lettres, des chiffres, des caractères spéciaux, des majuscules et minuscules. De plus, nos mots de passe seront différents pour chaque site !

Je vais vous proposer une méthode que je vous présente en 4 niveaux pour une meilleure compréhension. Le but étant d'utiliser le niveau 4 qui vous offre une sécurité optimale. Une fois cette méthode complètement assimilée vous pourrez la décliner à votre guise.

Niveau 1 : Ce niveau consiste à créer un code uniquement avec des lettres. Il sera constitué des **premières lettres de chaque mots** constituant une phrase clé choisie.

" Le fabuleux destin d'Amélie Poulain "	=>	lfddap
“ Trois petits cochons et un loup ”	=>	tpceul
“ Être né sous une bonne étoile “	=>	ênsubé
“ Comme une étoile dans la nuit ”	=>	cuédln
“ Plus dure sera la chute “	=>	pdslc

Niveau 2 : Ici le code sera constitué de lettres et de chiffres. Ainsi, **chaque mot représentant un chiffre** sera remplacé par la valeur.

" Le fabuleux destin d'Amélie Poulain "	=>	lfddap
“ Trois petits cochons et un loup ”	=>	3pce1l
“ Être né sous une bonne étoile “	=>	êns1bé
“ Comme une étoile dans la nuit ”	=>	c1edln
“ Plus dure sera la chute “	=>	pdslc

Niveau 3 : Ce niveau intègre également des **caractères spéciaux** comme @ & + - ‘ * / ; = % … Ainsi dès qu’un mot peut être remplacé dans la phrase, on le modifie. Et si une apostrophe est présente, on l’ajoute

" Le fabuleux destin d'Amélie Poulain "	=>	lfdd’ap
“ Trois petits cochons et un loup ”	=>	3pc&1l
“ Être né sous une bonne étoile “	=>	êns1b*
“ Comme une étoile dans la nuit ”	=>	c1*dln
“ Plus dure sera la chute “	=>	+dslc

Niveau 4 : Ajoutons pour ce niveau une majuscule **à la première lettre** du code.

" Le fabuleux destin d'Amélie Poulain "	=>	Lfdd’ap
“ Trois petits cochons et un loup ”	=>	3Pc&1l
“ Être né sous une bonne étoile “	=>	Êns1b*
“ Comme une étoile dans la nuit ”	=>	C1*dln
“ Plus dure sera la chute “	=>	+Dslc

Pour vous entraîner et trouver votre propre phrase, voici quelques liens où trouver des listes de phrases facilement mémorisables :

Les fables de la Fontaine	www.lesfables.fr	Les proverbes	www.unproverbe.com
Les expressions	www.les-expressions.com	Les citations	www.lescitations.net

⚠ **Mais sachez que l’idéal est de créer votre propre phrase ;-)** Mon conseil est d’utiliser le niveau 4 de la méthode et d’avoir 8 à 12 caractères pour cette partie fixe avec déjà 2 caractères spéciaux.

Etape n°2

Utilisez une partie fixe facile à retenir en trouvant votre phrase clé idéale !

La partie variable, pour faire la différence

Pour l'instant, vous avez un super mot de passe mais identique pour tous les sites, ce qui est évidemment très déconseillé. Voyons à présent comment le personnaliser en fonction du site où vous êtes.

Ce qui est commun à tous les sites, c'est d'avoir une adresse url du style : www.nomdusite.com ou www.nomdusite.fr ou encore rubrique.nomdusite.fr

Nous allons donc nous intéresser à la partie centrale "nomdusite" qui est le réel point commun avec les 3 adresses internet précédentes.

Par exemple, pour le site de la Redoute : l'url est www.**laredoute**.fr => la partie centrale est : laredoute

C'est à partir de cette partie centrale que vous allez créer la partie variable de votre futur mot de passe.

Voici quelques exemples de stratégie pour extraire un code à partir du nom de site "laredoute". Ces exemples ont pour but de vous inspirer, à vous de créer votre propre stratégie.

La stratégie est de prendre en fonction du nom du site :	Résultat
les 2 premières et 2 dernières lettres	late
les 4 premières voyelles (avec répétition si pas assez de voyelles)	aeou
les 4 premières consonnes (avec répétition si pas assez de consonnes)	lrdt
garder les 4 derniers caractères mais remplacer les consonnes par des étoiles	ou*e
garder les 4 derniers caractères mais remplacer les voyelles par des dièses	##t#
observer la première lettre puis noter les 4 lettres de l'alphabet qui suivent	mnop
observer la dernière lettre puis noter les 4 lettres de l'alphabet qui suivent	fghi
les 2 premières lettres et le nombre de lettre (si <10 mettre un zéro)	la09
les 2 dernières lettres et le nombre de voyelles (si <10 mettre un zéro)	te05
les 2 dernières lettres et le nombre de consonnes (si <10 mettre un zéro)	te04

Voici le même tableau avec les 10 mêmes stratégies mais avec le nom de domaine Amazon.

La stratégie est de prendre :	Résultat
les 2 premières et 2 dernières lettres	amon
les 4 premières voyelles (avec répétition si pas assez de voyelles)	aaoa
les 4 premières consonnes (avec répétition si pas assez de consonnes)	mznm
garder les 4 derniers caractères mais remplacer les consonnes par des étoiles	a*o*
garder les 4 derniers caractères mais remplacer les voyelles par des dièses	#z#n
observer la première lettre puis noter les 4 lettres de l'alphabet qui suivent	bcde
observer la dernière lettre puis noter les 4 lettres de l'alphabet qui suivent	opqr
les 2 premières lettres et le nombre de lettres (si <10 mettre un zéro)	am06
les 2 dernières lettres et le nombre de voyelles (si <10 mettre un zéro)	on03
les 2 dernières lettres et le nombre de consonnes (si <10 mettre un zéro)	on03

⚠ **A vous de créer votre propre stratégie**, peut-être en vous inspirant et mixant des stratégies présentées dans les tableaux ci-dessus. Notre conseil est d'avoir entre 4 à 8 caractères pour cette partie variable. Ce chiffre variant en fonction du nombre de caractères déjà retenu pour la partie fixe. Sachant qu'au final, l'objectif que votre mot de passe comporte entre 12 et 16 caractères.

Etape n°3

Utilisez une partie variable en fonction des sites.

Assemblez les deux parties avec finesse

Vous allez à présent ajouter votre partie fixe et votre partie variable pour constituer votre Mot de Passe.

Alors vous pouvez simplement mettre la partie variable avant ou après la partie fixe mais vous avez une infinité d'autres solutions. Faîtes preuve là encore d'originalité, de créativité, mais pensez à une solution qui permette une utilisation régulière.

Voici 6 exemples de possibilités d'assemblages du plus simple au plus complexe. Pour les exemples suivants nous allons prendre les hypothèses suivantes :

Une partie fixe de 12 caractères, la phrase clé est : "Deux majuscules, cinq minuscules et deux caractères spéciaux construiront mon secret" avec comme règle de mettre les majuscules en début et fin. Cela donne : **2M,5m&2cscmS**

Une partie variable de 4 caractères, trouver à partir de la technique suivante : "les 2 dernières lettres et le nombre de voyelles(si <10 mettre un zéro)".

Sites	Exemple de Méthodes d'assemblage	Résultats
Gmail	Partie fixe puis partie variable	**2M,5m&2cscmSil02**
Gmail	Partie variable puis partie fixe	**il022M,5m&2cscmS**
Microsoft	Début partie fixe sur 4 caractères, partie variable, puis fin partie fixe	**2M,5ft03m&2cscmS**
Microsoft	2 premières lettres de la partie variable + partie fixe + fin partie variable.	**ft2M,5m&2cscmS03**
Leboncoin	Imbriquer les 2 parties en commençant par le début et la partie fixe	**2lMe,054m&2cscmS**
Leboncoin	Imbriquer les 2 parties en commençant par la fin et la partie variable.	**2M,3m&2clsec0m4S**

⚠ Privilégiez un assemblage qui vous soit facile à réaliser au quotidien. Une méthode trop complexe ne sera pas retenue ou difficile à mettre en application et donc pas utilisée.

Quels sont les risques lors de l'assemblage ?

Si l'un de vos mots de passe s'égare, il ne faut pas que le pirate puisse déduire facilement votre technique.

Imaginons que Facebook se fasse pirater et que votre mot de passe était :

y-6jH"Egj*book

Il est facile de se dire que la partie variable est "les 4 dernières lettres du site" et si l'email fait partie du butin pourquoi ne pas tester sur la messagerie.

Votre email est hébergé par Gmail.com ? Le pirate tentera **y-6jH"Egj*mail**

Sur Laposte.net, il essayera avec **y-6jH"Egj*oste**

Vous avez compris que la partie variable ne doit pas être évidente car le risque est accru.

Etape n°4

Assemblez les deux parties, fixe et variable, en mariant mémorisation et complexité.

Comment tester la structure de vos mots de passe ?

A ce stade, vous avez sûrement une idée de votre méthode pour construire vos mots de passe. Félicitation !

Pour vous faire plaisir, vous allez vérifier si votre structure est bien au top !

Prenez un site fictif, imaginons, jetestemonmotdepasse.com, à priori vous avez déjà en tête le mot de passe correspondant.

Il existe plusieurs sites qui vont vous aider à tester votre structure mais attention vous n'allez pas mettre l'un de vos mots de passe directement. Vous pourriez ainsi alimenter une base de donnée dont on ne connaît pas l'objectif. Alors il va falloir changer quelques lettres.

Ce qu'il faut tester, c'est essentiellement votre structure et la taille. Alors gardez la même longueur et changez quelques chiffres par d'autres, idem pour les lettres ou caractères spéciaux.

Ainsi un mot de passe du style

AZé8Y'nyZml5$*)

Pourrait devenir pour faire le test

QSà0O"kjDro4^*&

Vous remarquez que la structure est la même : des lettres en majuscule et minuscule, des chiffres et caractères spéciaux aux mêmes endroit mais différents.

Voici à présent 3 sites qui vous proposent de tester la force de votre mot de passe :

Undernews.fr

[Cliquez ici pour accéder au test]

Password.kaspersky.com

[Cliquez ici pour accéder au test]

Inforisque.info

[Cliquez ici pour accéder au test]

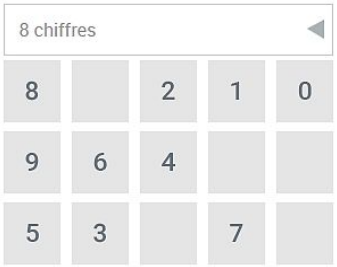
A priori, avec notre exemple, il semble que le résultat soit suffisant. J'espère qu'il en est de même pour vous.

Etape n°5

Testez la structure de votre mot de passe, le résultat devrait être dans les meilleurs scores possible.

Le cas des claviers numériques.

Dans certains cas, vous devrez taper votre code sur un clavier numérique. Nul besoin de majuscules, minuscules ou caractères spéciaux, il vous faudra uniquement des chiffres.



Deux possibilités, soit vous pouvez changer le code, soit vous devez garder celui imposé. Dans les deux cas, vous devrez vous en rappeler.

Voici une méthode pour mieux retenir une série de chiffre.

Le code chiffre-lettre.

Dans ce système, on va **convertir les chiffres en consonnes suivant un code** bien précis. Voici le code « historique » que l'on trouve dans les vieux (et récents) manuels de mnémotechnie.

- **0 : s ou z**
- **1 : t ou d**
- **2 : n**
- **3 : m**
- **4 : r**
- **5 : l**
- **6 : ch ou j**
- **7 : k ou gu**
- **8 : f ou v**
- **9 : p ou b**

En fait on ne va pas utiliser les lettres telles quelles mais plutôt les sons associés. Le 1 par exemple est converti avec les sons « teu » ou « deu ». Pour convertir le nombre 11, je pourrais utiliser les mots : tête, tutu, tâter, etc…

Quelques exemples de conversion :

1237	donnera	“**d**y**n**a**m**i**qu**e”
74212	donnera	“**g**r**e**n**a**d**i**n**e”
7452	donnera	“**c**a**r**o**l**i**n**e”
5321	donnera	“**l**i**m**o**n**a**d**e”

Il est plus facile de retenir un à deux mots que 8 chiffres, alors réfléchissez à quels mots correspond votre code actuel.

Vous manquez d'inspiration pour trouver des correspondances entre les mots et les chiffres ? Il existe un petit logiciel nommé 2Know qui convertit des chiffres en mots, très pratique ! Vous pourrez le télécharger ici.

014167

Mot candidat	Représente
stratégique	014167
stratégiques	014167
stratège	01416
stratèges	01416
stratégie	01416

Etape n°6

Prévoir une méthode également pour les codes numériques.

Glossaire

Cheval de Troie	Un programme malveillant déguisé en un logiciel légitime ou qui y est intégré.
Chiffrement	Substitution d'une information, d'une forme à une autre, afin d'en dissimuler le contenu.
Coupe-feu	Un coupe-feu est un type de barrière de sécurité placée entre différents environnements réseaux.
Cryptographie	Ensemble des procédés visant à crypter des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.
Cyberattaque	Une forme d'attaque informatique, combinée à une attaque physique ou non, qui vise à endommager ou à détruire des systèmes de données informatiques d'un adversaire.
Déchiffrement	Transformation d'un message qui a été encodé.
Détournement de domaine	Rediriger les utilisateurs d'un site Web légitime vers un faux site Web, permettant aux criminels de voler les informations que l'utilisateur dévoile.
Espionnage par-dessus l'épaule	Regarder par-dessus l'épaule de quelqu'un pour voir le contenu de son ordinateur ou de l'écran de l'appareil mobile.
Fouiner	Semblable à « surveiller sans relâche » dans le monde réel, « fouiner » consiste à suivre attentivement quelqu'un en ligne par le biais des mises à jour de statuts, de profils, de photos, etc.
Hachage	Cette fonction algorithme va prendre le texte du mot de passe et le convertir pour obtenir une signature (cette signature est aussi appelée « empreinte »).
Hameçonnage	Tentative d'une tierce partie de solliciter de l'information confidentielle appartenant à un individu, un groupe ou une organisation en imitant ou démystifiant une marque commerciale connue aux fins de gains financiers. Les malfaiteurs désirent amener les utilisateurs à partager leurs renseignements personnels tels que numéro de carte de crédit, informations bancaires ou autres renseignements.
Hameçonnage par message texte	Messages textes frauduleux conçus pour inciter les utilisateurs à révéler leurs renseignements personnels ou financiers par le biais de leur téléphone cellulaire.
Harponnage	Pratique qui cible de façon plus précise un groupe d'internautes

	donné afin de lui soutirer son nom d'utilisateur et son mot de passe. Contrairement à l'hameçonnage, qui cible un plus grand nombre d'utilisateurs, l'harponnage se fait à petite échelle et cible plus spécifiquement les victimes.
Ingénierie sociale	Pratique qui a pour but d'extorquer des informations confidentielles en manipulant les utilisateurs. Un pirate psychologique utilise souvent le téléphone ou l'Internet pour tromper les individus et parvenir à obtenir leurs renseignements personnels.
Logiciel espion	Un logiciel qui permet aux annonceurs ou aux pirates informatiques de recueillir de l'information dans l'ordinateur d'un utilisateur sans son autorisation.
Ordinateur zombie	L'ordinateur personnel est infecté par un programme malveillant qui permet au pirate de le contrôler librement par le biais d'un canal de communication.
Porte dérobée	Porte d'accès à un système informatique qui permet le contournement des mécanismes d'authentification ou de sécurité de l'accès à distance, tout en tentant de rester dissimulée lors d'inspections occasionnelles.
Rançongiciel	Logiciel qui bloque l'accès à vos données et ne les libère qu'une fois que vous avez versé de l'argent pour les récupérer.
Troll	Une personne qui publie des messages méchants dans le seul but de bouleverser les autres.
Ver informatique	Un programme informatique qui se copie par lui-même. Il utilise un réseau pour envoyer des copies de lui-même à d'autres systèmes et il peut le faire sans que l'utilisateur n'intervienne.
Vulnérabilité	Un défaut dans la conception qui pourrait être exploité pour compromettre les biens ou les activités d'une organisation.

Conclusion

Avec cette méthode, vous voilà prêt à affronter le Net avec plus de sérénité, en attendant que les empreintes digitales et reconnaissance faciale prennent le relais…

Notez cependant que quelques sites vous proposent déjà “la validation en deux étapes” qui vous proposera l’envoi d’un code par sms. N’hésitez pas à activer cette option, c’est vraiment une sécurité supplémentaire.

Si vous avez des commentaires sur cet ebook, des améliorations que je pourrais apporter, n’hésitez pas à m’en faire part. L’évolution dans les technologies est rapide. Ce qui est vrai aujourd’hui peut ne plus l’être demain. Je me ferai un plaisir de prendre en compte vos messages.

Contacts

@ : eric.sotoca@gmail.com

Site Pro : www.sotoca-online.com

Tél : 06.51.33.22.09

Diplômé d'un Master en Information et Communication option Gestion de Contenus Numériques