Les mots de passe

Sommaire

1 Choisir un bon mot de passe

Un bon mot de passe doit être :

- Difficile à trouver
  - En le cherchant avec des robots.
- Facile à se rappeler
  - Nécessité d'un moyen simple pour le retrouver.

1.1 Construire le mot de passe

Pour qu'il soit difficile à trouver, la règle élémentaire est de toujours choisir un mot de passe :

1. Utilisant des caractères de tous types et en nombre suffisant.
2. Sécurisé et difficile à deviner par sa construction.

1.1.1 Large gamme de caractères

Les robots seront d'autant plus sollicités si la gamme de caractères est étendue : des lettres (majuscules et minuscules), des chiffres et des caractères spéciaux (point d'exclamation par exemple).
Il est aussi souhaitable (pour la même raison) que le mot de passe soit le plus long possible (8 caractères est un strict minimum, 12 est un minimum plus réaliste).

Des sites dédiés permettent se rendre compte de la solidité d'un mot de passe contenant de nombreux caractères (dont certains spéciaux) et de la faiblesse des mots de passe trop simples :

- https://howsecureismypassword.net/
- http://password-checker.online-domain-tools.com/

La plupart des experts conseillent de choisir ce que l'on appelle une phrase de passe plutôt qu'un mot de passe La longueur est alors privilégiée :
« JeLisMonJournalTousLesJoursEtJaimebiença. »
Un mot de passe voit sa sécurité augmenter lorsqu'on y ajoute des caractères spéciaux, il est donc également vivement recommandé d'agrémenter sa phrase de passe de quelques caractères spéciaux ; un seul (un point, un guillemet ou autre) peut suffire à compliquer la tâche de ceux qui essaieraient de le deviner.

1.1.2 Difficile à imaginer

Il faut éviter que le mot de passe soit facilement accessible à quelqu'un d'extérieur même vous connaissant un peu. Par accessible on entend :

1. Physiquement (post-It sur l'écran, fichier simple, etc.) : l'endroit de stockage, s'il existe, est difficilement accessible par quelqu'un d'autre (l'idéal étant votre mémoire).
2. Sa construction n'est pas triviale (AZERTY, un prénom proche, etc.)

Les mots de passe triviaux sont connus, une publication en est faite tous les ans. En francisant un peu :

1. 123456
2. password
3. 12345678
4. azerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567

Le principal danger menaçant un internaute lambda vient souvent de ses proches : collègues, amis, camarades de classe, famille, compagnon… qui pourraient céder à l'envie de lire ses courriels ou ses messages sur les réseaux sociaux. Il vaut donc mieux choisir un mot de passe qui n'a rien à voir avec soi : pas de date de naissance, pas le prénom du petit dernier, pas le nom de son écrivain préféré, pas le nom de son animal de compagnie, etc. trop faciles à deviner par son entourage.

1.2 Se souvenir du mot de passe

La priorité doit rester à faciliter la mémorisation par l'utilisateur. Un bon mot de passe doit pouvoir être conservé en mémoire sans avoir à être écrit et sans risquer d'être oublié au moment où il doit être utilisé. Le mot de passe doit être le résultat d'un exercice mnémotechnique car les humains mémorisent plus facilement les informations complexes lorsqu'elles suivent une construction logique. On ne se souvient pas de la liste des conjonctions de coordination mais tout le monde connaît la séquence : "mais où est donc Ornicar ?". Il faut donc définir une recette, un algorithme qui, à partir d'une phrase, d'une idée, d'une réécriture aboutira à un bon résultat.

Méthode 1 : retenir la ou les premières lettres de chaque mot composant une phrase. Ensuite, à chacun d'apporter sa petite touche personnelle en y incorporant quelques majuscules (une lettre sur deux, ou sur trois par exemple), et chiffres (remplacer certaines lettres par des chiffres dont la typographie est voisine s'avère très efficace).
Exemple : utilisons la phrase suivante: « L'œil ne voit rien si l'esprit est distrait » : En optant pour l'utilisation de la première lettre de chaque mot, d'une majuscule toutes les deux lettres, et des remplacements des O et des E par des 0 et 3, on obtient: L'0nVrSl'33D.

Méthode 2 : l'utilisation de la phonétique. En prononçant une phrase, chaque son générera l'un des caractères du mot de passe. Naturellement, toutes les phrases ne s'y prêtent pas, mais une fois le choix fait, la mémorisation sera aisée.
Exemple : on se basera sur la phrase suivante « J'ai acheté trois œufs et deux BD ce matin ». Toujours avec une majuscule toutes les deux lettres, ont obtient: gHt3Eé2BdCeMaT1.

Méthode 3 : Choisissez un mot de passe « classique », puis décalez chaque lettre d'une touche vers la droite.
Exemple : en partant du prénom Jean-Claude, on obtient (toujours avec une majuscule pour deux lettres) KrZ,èVmZiFr.

De nombreuses méthodes existent que l'on peut combiner entre-elles. Le tout étant toujours d'obtenir un moyen de retrouver son mot de passe.

2 Dissimuler son mot de passe

Le Post-it sous le clavier ? Les mots de passe cachés dans le lecteur CD de l'ordinateur ? Si le bureau ou la pièce de logement dans lequel se trouve notre ordinateur sont fermés à double tour lorsqu'on n'y est pas, pourquoi pas. Le reste du temps, c'est à proscrire. De la même manière, le mot de passe ne doit pas être stocké dans un endroit facilement accessible : Smartphone, téléphone, tablette numérique, etc.

Il est également déconseillé de faire mémoriser à son navigateur ses mots de passe : oui, certes, c'est du temps perdu, mais cela évite qu'un collègue/ami/ennemi/compagnon, en utilisant notre ordinateur, puisse se connecter sans même avoir à saisir un mot de passe. Et devoir saisir régulièrement (quotidiennement) son mot de passe est le meilleur moyen pour s'en souvenir !
Décochez, au moins, tout simplement l'option "souvenez-vous de moi" et prenez les quelques secondes nécessaires pour écrire votre mot de passe.

De même éviter le fichier Word ou Excel (ou assimilé) sur votre machine : lisible par n'importe qui. De plus, il sera sauvegardé avec le reste des données…

Et, surtout, ne jamais communiquer son mot de passe. Le mot de passe doit être strictement personnel. Même lorsqu'il n'est plus utilisé ou qu'il a été changé il ne doit pas être révélé. Car il trahit la recette de construction de l'utilisateur et peut donc être utilisé pour décrypter un nouveau mot de passe.

3 Utiliser son mot de passe

Le problème se complique lorsqu'il apparait que :

- Le mot de passe doit avoir une utilisation unique.
- Les plus sensibles doivent être renouvelés de temps en temps.

3.1 Un mot de passe par compte

Il y a un endroit où le mot de passe est stocké et qui n'est pas du ressort de l'utilisateur : chez le gestionnaire du service auquel il permet l'accès. Certes il est très bien protégé dans la plupart des cas mais il est aussi une cible privilégié…

Si vous avez le même mot de passe pour toutes vos connexions, une seule brèche peut endommager tous les comptes que vous avez.

Chaque site web/abonnement utilisé par l'internaute doit avoir une clef d'accès différente. On évite ainsi de mettre tous ses œufs dans le même panier. Sinon une fois le mot de passe d'un service connu, ce sont tous les autres qui s'ouvrent : c'est un des angles d'attaque connu.

Pour faciliter la mémorisation des phrases de passe sans (trop) sacrifier à la sécurité, il est possible d'utiliser ce que l'on appelle une « routine » de mot de passe : une structure de mot de passe se répétant pour chaque service ou site que l'on utilise.
Une méthode consiste en l'utilisation d'une structure commune afin de gérer une diversité de mots de passe. Il est possible de créer un tronc commun, complété d'une seconde partie propre à chaque service (Facebook, Twitter etc.). Exemple de tronc commun (fixe) : le titre de son film préféré. Exemple de seconde partie (variable) : pourquoi ne pas ajouter un "FBK" au mot de passe pour se connecter à Facebook.

Exemple : si vous aimez « La Guerre des Etoiles » :

1. *Prendre les deux premières lettres de chaque mot afin d'arriver à une longueur suffisante.*
2. *Une majuscule pour deux lettres.*
3. *Remplacer les E par des 3.*

Le mot de passe sera : LaGuD33t-FBK

Un site pour savoir si votre adresse a été piratée chez un fournisseur de services et donc si elle est connue des pirates :
« Have I Been Pwned ? » (que l'on pourrait traduire par « *est-ce que je me suis fait avoir ?* »). Le principe est simple : **vous renseignez votre adresse mail dans le champ** prévu à cet effet et le site vous indique si votre mail est concerné par une fuite de données personnelles.

3.2 Renouveler son mot de passe

En changer (et ne pas utiliser toujours le même) !

Idéalement, il faut changer ses mots de passe principaux tous les mois (banques, réseaux sociaux et surtout compte courriel, qui est le Graal pour quiconque veut accéder à tous nos services, puisqu'il est possible de se faire envoyer tous ses mots de passe par courriel). Il faut aussi les changer lorsqu'un ou plusieurs sont touchés par une faille ou un vol de mot de passe. Et évitez de revenir à de précédents mots de passe et de passer de l'un à l'autre.

4 Le gestionnaire de mots de passe

Tout ça est très compliqué à gérer. C'est même infaisable sans assistance si on veut tout respecter.

Heureusement il est possible, pour se faciliter la vie, d'utiliser un gestionnaire de mot de passe. Ils permettent de mémoriser les codes d'accès de tous les sites utilisés, au sein d'une même base de données, accessible elle-même à l'aide d'un unique mot de passe. Vous aurez ainsi tout le loisir de créer des combinaisons très sûres, sans avoir à les retenir pour autant. C'est le moyen le plus simple pour vous souvenir et vous sentir en sécurité à propos de vos mots de passe sur les différents sites,

S'il n'existe pas de solution miracle, le logiciel open source KeePass Password Safe (Keepass) semble faire consensus. On peut l'utiliser depuis n'importe quel type d'ordinateur. Côté fonctionnel, il permet de classer les mots de passe et stocker toutes les informations importantes qui leur sont associées.
Le choix d'un logiciel open source n'est pas anodin en matière de sécurité. On ne sait pas ce qui se cache derrière les lignes de code d'un logiciel propriétaire. Et la situation est identique pour un service Internet. L'ouverture du code laisse toute latitude pour vérifier qu'aucune menace ne s'y cache. La sécurité de KeePass a été évaluée par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et est certifié CSPN.

5 Avenir

D’autres moyens d'authentification peuvent être envisagés comme des mécanismes d'authentification reposant sur une clef physique (carte avec ou sans puce, jeton, clef, etc.) ou sur un paramètre biométrique (empreinte digitale, vélocimétrie sanguine, reconnaissance de l'iris, frappe au clavier, etc.).