Gestion des mots de passe

Avec ce tutoriel, vous apprendrez à :
— comprendre l'utilité d'un mot de passe,
— définir un mot de passe très sûr,
— trouver un moyen efficace de les retenir.

1. À quoi servent les mots de passe ?

Le mot de passe est la clé d'entrée dans votre ordinateur, dans votre compte ouvert sur un site internet, dans votre boîte aux lettres électronique... Les mots de passe sont partout et il devient vite compliqué de les retenir.

La tentation est donc grande de mettre le même partout. Ce qu'il faut ABSOLUMENT éviter, car il sert à protéger vos données.

Associé à votre identifiant, il sert à montrer patte blanche avant d'agir en votre nom sur le périphérique ou le site internet. Sa robustesse dépendra des données à protéger. **Le risque d'usurpation de votre identité n'est pas à négliger.**

Nous allons voir comment définir un bon mot de passe, et le retenir.

2. Bien définir un mot de passe

La première règle de sécurité est de tenir votre mot de passe secret, afin qu'aucun tiers non autorisé ne puisse accéder à vos données.

Voici quelques règles énoncées par Wikipédia[1] : *La robustesse d'un mot de passe dépend de plusieurs critères :*

— *Sa simplicité : 123456, 111111, Love, 0000, azerty... sont à proscrire, de même que les dates de naissance, le nom du chien...*
— *Sa longueur. Il est conseillé d'utiliser des mots de passe de plus de dix caractères.*
— *Le nombre de types de caractères différents. Il est conseillé de mélanger des majuscules, des minuscules, des chiffres et des caractères spéciaux.*
— *Sa durée de vie. Un mot de passe est d'autant plus robuste qu'il est changé régulièrement (par exemple, tous les six mois).*

Par ailleurs, notons que le choix d'un mot de passe doit se faire suivant la criticité de ce dernier (par exemple, un mot de passe permettant d'accéder à l'interface d'administration d'une application ou d'un équipement sera considéré comme étant très critique).

2.1. « Les pires mots de passe, à ne pas utiliser »

Une étude portant sur 32 millions de mots de passe du site RockYou.com, obtenus à la suite d'une attaque du site, a montré que 30 % de ces mots de passe comportaient six

1. http://fr.wikipedia.org/wiki/Mot_de_passe

caractères ou moins, et que le plus fréquent (un peu moins d'un sur cent) est « 123456 ».[2] *Tous les ans, SplashData, fournisseur de solutions de sécurité, publie également une liste des mots de passe les plus utilisés, et désignés comme étant « les pires mots de passe, à ne pas utiliser ». Les 5 mots de passe les plus utilisés par les utilisateurs du monde entier en 2012 sont :*

- *123456*
- *password*
- *12345678*
- *qwerty*
- *abc123*

2.2. Comment créer un bon mot de passe et le retenir ?

Avec les capacités techniques actuelles, la taille d'un mot de passe doit être d'au moins 10 caractères non signifiants, composés de lettres majuscules, minuscules, de chiffres et si possible de caractères spéciaux.[3]

Un bon mot de passe est un mot de passe correctement formé, qui sera donc difficile à retrouver même à l'aide d'outils automatisés, mais facile à retenir.

En effet, si un mot de passe est trop compliqué à retenir, l'utilisateur mettra en place des moyens mettant en danger la sécurité du Système d'Information, comme par exemple l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier où l'utilisateur doit s'authentifier.

Il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.[4]

- *Exemple : La méthode phonétique*
  Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple, la phrase « j'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am
- *Exemple : La méthode des premières lettres*
  Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson, ...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tien vaut mieux que deux tu l'auras » deviendra 1TvmQ2tl'@

J'ajouterais à ces méthodes professionnelles celles-ci :

- Le dessin sur le clavier : votre mot de passe représente un certain schéma sur votre clavier. Dans ce cas, on est souvent incapable de dicter son mot de passe : ce sont vos doigts qui l'ont mémorisé. Le mieux est de jouer avec la touche ⇧ pour renforcer la sécurité de ce mot.

2. http://fr.wikipedia.org/wiki/Mot_de_passe
3. http://www.securite-informatique.gouv.fr/autoformations/motdepasse/co/Mots_de_Passe_CH01_SCH02_U02.html
4. http://www.securite-informatique.gouv.fr/autoformations/motdepasse/co/Mots_de_Passe_CH01_SCH02_U02.html

— Dans un mot qui a du sens pour vous, remplacez certaines lettres par les chiffres approchants, insérez quelques majuscules et des symboles de ponctuation. Exemple : « Cormeilles » devient « c0rm3i2Les: ».

3. Des outils de génération de mots de passe

Il existe des outils de génération de mots de passe sécurisés.
Par exemple, le site internet www.generateurdemotdepasse.com (voir Figure 1).

FIGURE 1 – Un site de génération de mot de passe

1. Sélectionnez les options de votre mot de passe, et notamment :
   — les caractères spéciaux qui pourront y figurer (sur certains sites, tous les caractères spéciaux ne sont pas acceptés),
   — le nombre de caractères qui composeront le mot de passe.
2. Cliquez sur Créer le mot de passe.
3. Le mot de passe s'affiche. Il ne vous reste qu'à faire un copier / coller pour l'intégrer dans votre formulaire.

Je n'ai pas trouvé de logiciel qui remporte totalement mon adhésion. Je ne préfère donc pas vous en recommander un. À vous de voir. Attention toutefois à ne pas installer les différents « malwares » qui accompagnent souvent les téléchargements effectués depuis les plateformes www.01net.com, www.softonic.com,...

Sous Linux, le logiciel pwgen vous rendra de merveilleux services et vous évitera bien des maux de tête !

4. Récupération du mot de passe

On peut considérer que certains mots de passe seront « jetables », c'est-à-dire qu'on ne prévoit pas de s'en servir souvent. Dans ce cas on peut ne pas noter le mot de passe et demander à le récupérer si on souhaite se reconnecter sur ce site ultérieurement, grâce au lien de **récupération de mot de passe**, que vous retrouverez partout (voir Figure 2).

FIGURE 2 – Lien de récupération de mot de passe du site sncf.com

Dans la majorité des cas, on vous demandera simplement l'adresse mail qui a servi à créer le compte (voir Figure 3), afin de vous envoyer un mail qui contiendra un lien hypertexte. Ce lien vous permettra de définir un nouveau mot de passe, sans avoir à redonner l'ancien.

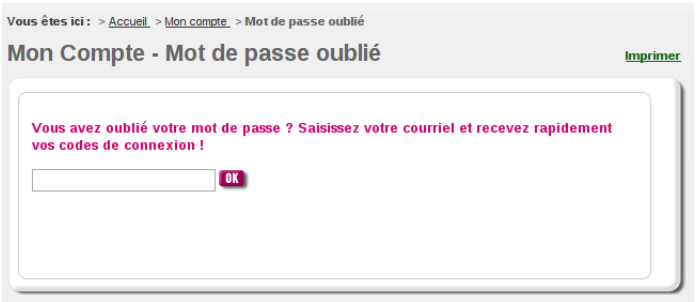

FIGURE 3 – Fenêtre « Mot de passe oublié » du site www.transilien.com

Ce lien peut également être utilisé si vous avez oublié le mot de passe associé à une adresse mail. Dans ce cas précis, on vous demandera généralement de répondre à votre question secrète, choisie à la création du compte.

Voilà une bonne raison de répondre aux questions de sécurité des vos comptes mails ou autre (question secrète, adresse mail de récupération, numéro de mobile,...).

4.1. Ne négligez pas les écrans de sécurité !

Principalement dans le cas des adresses de courrier électronique, votre fournisseur d'accès vous présente cycliquement des pages de sécurité, qui vous demandent de compléter vos informations personnelles, de vérifier si votre numéro de portable est toujours le bon, idem pour une adresse mail de secours,...

Ne négligez pas d'y répondre. Vous le regretteriez si vous aviez besoin de retrouver ce mot de passe ou de le réinitialiser.

5. Stocker les mots de passe

Il faut bien avouer qu'il est tout de même difficile de retenir tous ces mots de passe. D'autant qu'on nous demande de plus en plus souvent de créer des comptes pour accéder à des services numériques.

Voici plusieurs solutions qui pourront vous aider.

5.1. Utiliser un carnet

Cette solution est basique, mais peut convenir pour tous les sites internet, si vous ne risquez rien de vos proches. Un pirate informatique ne viendra pas voler ce bloc note .

Par contre, évitez de le garder dans votre sac à main ou votre sacoche, ou à proximité immédiate de votre ordinateur, justement pour éviter qu'il ne vous soit dérobé.

5.2. Créer un fichier verrouillé

Votre logiciel de bureautique (Libre Office ou Microsoft Office, par exemple), vous permet de créer un fichier qui sera verrouillé par un mot de passe. Vous pourrez ainsi y stocker toutes vos données sensibles, en les protégeant d'individus malveillants. Attention toutefois à ne pas donner à ce fichier un nom trop explicite, tel que « mes-mots-de-passe ».

Par exemple, vous pouvez créer une feuille de calcul contenant les sites internet, les identifiants et les mots de passe associés. Au moment de l'enregistrement de votre document, vous donnez un nom à votre fichier et cochez la case Enregistrer avec un mot de passe (voir Figure 4).

Une nouvelle fenêtre s'ouvre et vous demande de définir le mot de passe qui servira à chiffrer le fichier (voir Figure 5). Saisissez votre mot de passe en employant l'une des méthodes proposées sous-section 2.2.

Remarquez que vous pouvez également définir un mot de passe qui permettra l'édition du fichier. Cela vous garantit que seules les personnes autorisées pourront modifier ce fichier.

NB : Cette méthode fonctionne également avec un fichier créé en traitement de texte.

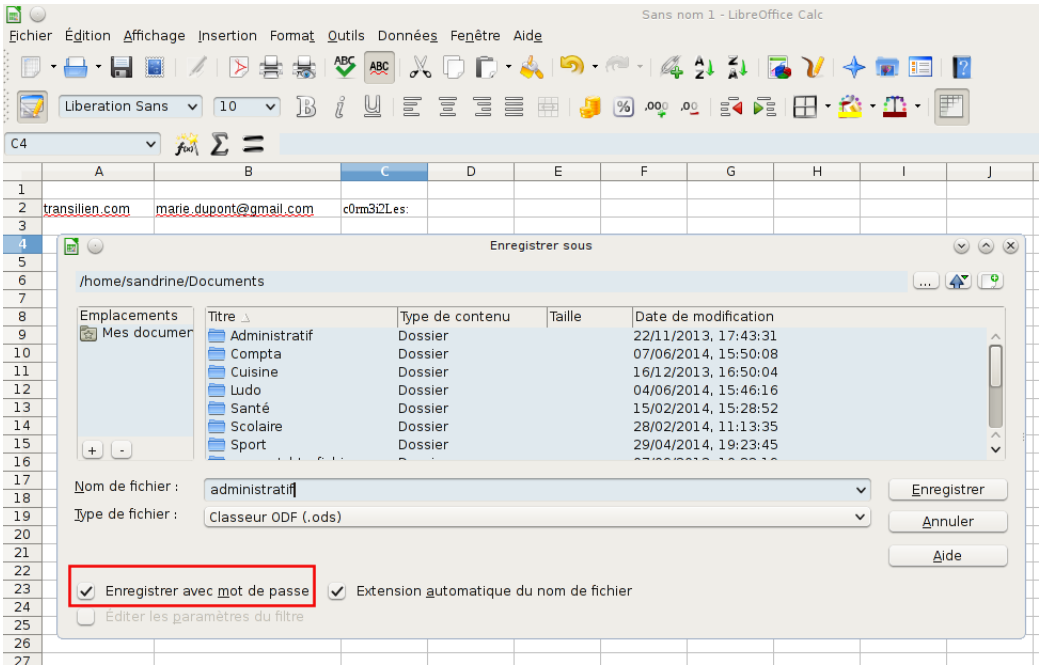

FIGURE 4 – Libre Office Calc : enregistrer avec un mot de passe

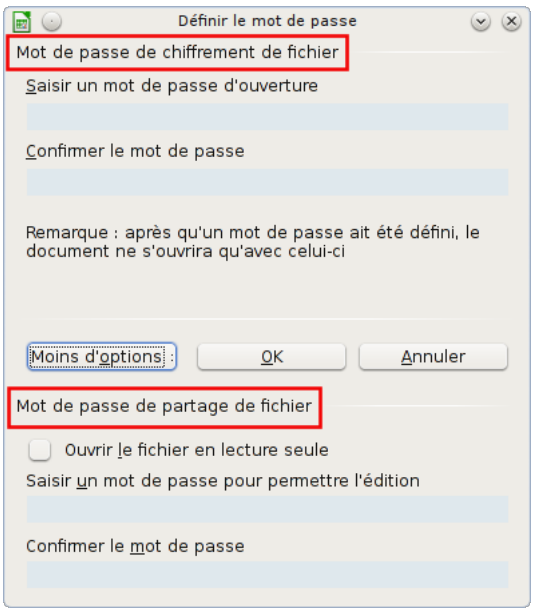

FIGURE 5 – Fenêtre Libre Office Calc de définition d'un mot de passe

5.3. Utiliser les portefeuilles de mot de passe intégrés

Les navigateurs internet sont également capables de vous aider à mémoriser vos mots de passe. On appelle ces outils des **portefeuilles de mots de passe**.

Développons la méthode de Firefox, que je trouve très sûre et efficace.

5.3.1. Firefox

Vous pouvez charger Mozilla Firefox de mémoriser vos mots de passe. Lorsque vous entrez un mot de passe sur un site internet, pour la première fois, le logiciel vous propose de le « retenir » (voir Figure 6).

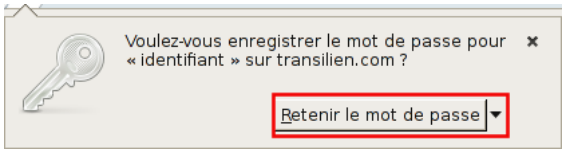

FIGURE 6 – Infobulle proposant d'enregistrer votre mot de passe

Vérifiez qu'il s'agit bien de l'identifiant et du site internet que vous voulez mémoriser. Vous disposez de quelques secondes pour cliquer sur le bouton Retenir le mot de passe.

Si vous ne le faites pas, le mot de passe ne sera pas stocké.

Si vous cliquez sur le bouton, Firefox entrera votre mot de passe dans votre « portefeuille ». La prochaine fois que vous vous connecterez sur ce site, une fois l'identifiant saisi, le mot de passe s'insérera automatiquement dans le champ correspondant. Il ne vous restera plus qu'à cliquez sur le bouton de connexion.

À ce stade, vos mots de passe sont accessibles par toute personne ayant accès à votre ordinateur, simplement en allant dans le menu > Préférences.

Dans la fenêtre qui s'affiche, en cliquant sur l'onglet **Sécurité**, à gauche, vous accédez au menu de gestion des mots de passe (voir Figure 7).

FIGURE 7 – Firefox : menu de gestion des mots de passe

1. Cocher la case Enregistrer les identifiants.
2. Pour sécuriser au maximum votre portefeuille, cochez la case Utiliser un mot de passe principal et définissez un mot de passe fort tel que décrit dans la sous-section 2.2. **Avantage maximal :** vous ne retenez qu'un mot de passe très sécurisé, qui se charge de vous restituer tous les autres mots de passe, aussi sécurisés que possible, sans que vous ayez à vous encombrer l'esprit !

Si vous souhaitez modifier le mot de passe dit « principal », retournez dans le même menu Menu > Préférences > Sécurité et cliquez sur Changer le mot de passe principal (voir Figure 8).

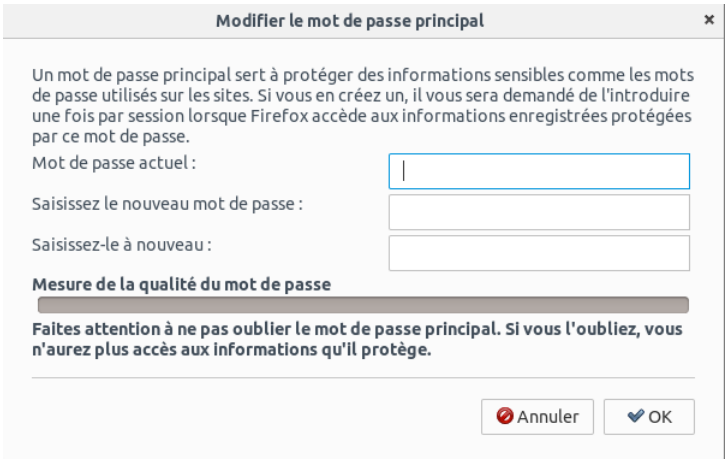

FIGURE 8 – Firefox : modifier le mot de passe principal

Le précédent mot de passe principal vous sera demandé avant la saisie du nouveau. N'espérez donc pas contourner un oubli par ce biais 😉.

5.4. Microsoft

Internet Explorer vous propose également d'enregistrer vos mots de passe, option activée par défaut. Pour en savoir plus sur la façon dont Microsoft gère vos comptes et vos mots de passe, consultez la page http://windows.microsoft.com/fr-fr/internet-explorer/fill-in-forms-remember-passwords-autocomplete#ie=ie-11.

5.5. Quelques autres cas

Sous Linux, les coffre-forts de mots de passe sont présents par défaut, à l'installation du système d'exploitation.

Certains portails internet vous proposent de retenir votre mot de passe, afin de faciliter une connexion future. Cette solution n'est sans doute pas la plus sûre, notamment si l'accès à votre navigateur n'est pas verrouillé...

5.6. Utiliser un logiciel spécifique

5.6.1. Pour vous aider dans votre choix

Le site www.panoptinet.com propose un test de 3 gestionnaires de mots de passe. L'article est un peu ancien, mais peut sans doute vous aider. http://www.panoptinet.com/cybersecurite-decryptee/test-dashlane-lastpass-keepass-quel-logiciel-choisir/.

Voir aussi,
http://www.lesnumeriques.com/telephone-portable/exploiter-gestionnaire-mots-passe-dashlane-a2103.html, en complément sur Dashlane (article plus récent).

5.6.2. Choisir un logiciel libre

Il existe un logiciel libre qui retiendra pour vous vos mots de passe. Il s'agit de PassReminder http://eyecanseeyou.free.fr/passreminder_password_manager. La page d'accueil est en anglais. Mais le logiciel est disponible en version française.

Pour le télécharger, rendez-vous dans la rubrique Download. Vous y trouverez :

— une version pour Windows avec Java intégré : « Windows installer PassReminder with JVM »,
— une sans la machine virtuelle Java « without JVM » ,
— une version sans JVM mais « zippée », c'est-à-dire téléchargeable dans un format compressé (plus légère à télécharger, mais qu'il faudra décompresser ensuite),
— une version Linux,
— et même une version que vous pourrez mettre sur une clé USB.

Grâce à notre tutoriel « Installer un programme », vous devriez pouvoir trouver toutes les informations nécessaires à l'installation de ce logiciel.

Une fois le logiciel installé et lancé, cliquez sur Aide pour choisir la langue française (voir Figure 9).

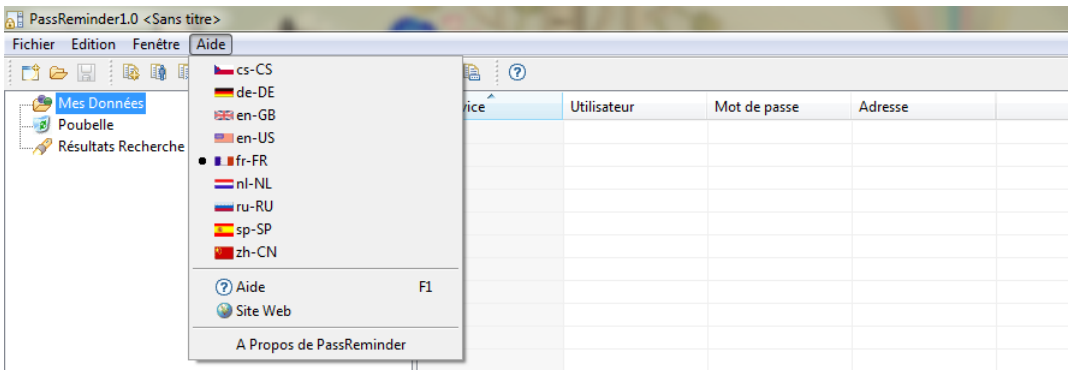

FIGURE 9 – Passer le logiciel libre PassReminder en français

Le fichier de vos mots de passe sera verrouillé par un mot de passe principal, qui vous sera demandé dès la création du premier fichier.

5.6.3. Installer une application sur votre smartphone ou votre tablette Android

Personnellement, j'utilise l'application **aWallet Password Manager**, que vous pourrez télécharger gratuitement depuis le Playstore (voir Figure 10), et qui me permet d'avoir toujours sur moi mes mots de passe importants, sans crainte qu'ils ne me soient dérobés, car j'ai refusé la sauvegarde dans le « cloud » et choisi un mot de passe très sûr pour l'ouverture du fichier.

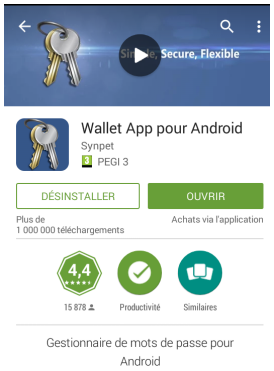

FIGURE 10 – Application aWallet à télécharger sur le PlayStore

5.6.4. Un gestionnaire multi-plateformes

Enfin, voici un logiciel, propriétaire, disponible à la fois sur Apple, Windows, Android, Linux,... **Enpass**.

Je ne l'ai pas testé, mais d'après l'article qu'en fait www.korben.info, site que je suis régulièrement, c'est un bon gestionnaire.

Mais attention, il vous en coûtera 10 € pour l'utiliser sur votre périphérique Android (gratuit pour la version ordinateur).

Source : http://korben.info/enpass-un-nouveau-gestionnaire-de-mots-de-passe.html