# Bien choisir ses mots de passe et ses questions secrêtes

Il est très important de bien choisir ses mots de passe.

Imaginons que vous choisissiez sur un site un mot de passe composé de cinq chiffres. Un programmeur mal intentionné pourrait tester votre mot de passe en moins de temps qu'il n'en faut pour le dire. Car il lui suffirait au maximum de 99999 essais (5 chiffres tous compris entre 0 et 9, il suffit de commencer à 0, puis d'ajouter 1 à chaque fois pour tomber au bout d'un moment sur le mot de passe) pour l'obtenir. A raison de plusieurs centaines d'essais par secondes (prenons 1000), l'ordinateur de ce programmeur peut trouver votre mot de passe en moins d'une minute et quarante secondes. Le chiffre de 1000 était vraiment loin de la vérité.

Supposons maintenant que votre mot de passe ne soit composé que de lettres toutes en minuscules. Pour un ordinateur de la même puissance pour trouver un mot de passe de cinq lettres, il faudrait 11881376 essais au maximum, soit un calcul de trois heures et vingt minutes pour tester toutes les combinaisons possibles.

Ce qui est déjà beaucoup plus long mais pas impossible.

Le truc à savoir, c'est que très souvent, les gens utilisent toujours par exemple le nom de leur chien, ou un mot existant. Du coup, il existe une autre technique permettant de trouver le mot de passe de quelqu'un : la technique du dictionnaire.

Cette technique consiste à tester le mot de passe avec une liste de mots.

Prenons par exemple une liste de deux millions de mots. Il faudra un peu plus d'une demi heure au maximum pour trouver votre mot de passe.

Tout ceci pour vous dire qu'il ne faut absolument pas choisir de mot de passe simple. Et surtout pas de mot de passe composé uniquement de chiffres, ni uniquement de lettres.

Il vaut mieux choisir un mot de passe composé de lettres et de chiffres. Et il vaut même mieux qu'il y ait des lettres en minuscules et en majuscules dans votre mot de passe, voir des symboles autres comme un espace, un point (simple, d'interrogation, d'exclamation), un #, une virgule, ou tout autre symbole accessible sur votre clavier. Une taille minimale à respecter pour un mot de passe serait de huit caractères (d'ailleurs, bon nombre de sites imposent ce nombre minimal de caractères pour des mots de passe maintenant).

## Quelques techniques de création de mots de passe sûrs

Créez un mot de passe sûr et facile à retenir en 6 étapes

Pour créer un mot de passe sûr, procédez comme suit :

1. Imaginez une phrase que vous pourrez mémoriser. Elle servira de point de départ à l'élaboration de votre mot ou phrase de passe. Choisissez une phrase facile à mémoriser, par exemple : « Mon fils Olivier a trois ans ».
2. Vérifiez si votre ordinateur ou votre système en ligne accepte cette phrase. Si vous pouvez effectivement utiliser une phrase de passe (avec des espaces séparant les caractères) sur votre ordinateur ou sur votre système en ligne, n'hésitez pas.
3. Dans le cas contraire, transformez la phrase de passe en mot de passe. Prenez la première lettre de chaque mot de cette phrase pour créer un mot, qui n'aura alors plus aucune signification. Avec l'exemple ci-dessus, vous obtenez : « mfoata ».
4. Brouillez les pistes en utilisant à la fois des minuscules et des majuscules, ainsi que des chiffres. Vous pouvez également inverser certaines lettres ou intégrer des fautes d'orthographe. Par exemple, dans la phrase ci-dessus, vous pouvez faire en sorte que le nom Olivier comporte une faute d'orthographe, ou bien remplacer le mot « trois » par le chiffre 3. De nombreuses possibilités de substitutions s'offrent à

vous ; et n'oubliez pas : plus la phrase de départ est longue, plus le mot de passe pourra être complexe. La phrase peut ainsi devenir « Mon FilS OlivI6R à 3 aNs ». Si votre ordinateur ou votre système en ligne n'accepte pas les phrases de passe, utilisez la même technique sur un mot de passe plus court. Vous pouvez alors obtenir un mot de passe du type « MfOa3a ».

5. Enfin, il est conseillé d'avoir recours à des caractères spéciaux. Vous pouvez utiliser des symboles ressemblant à des lettres, accoler des mots (en supprimant les espaces). Pensez à toute autre méthode permettant d'augmenter la complexité du mot de passe. En appliquant ces astuces, on obtient par exemple une phrase de passe comme « Mon€ilS O10R @ 3 An$ » ou un mot de passe (reprenant la première lettre de chaque mot) tel que « M€Oa3A ».
6. Testez tout nouveau mot de passe à l'aide d'un testeur de mots de passe.

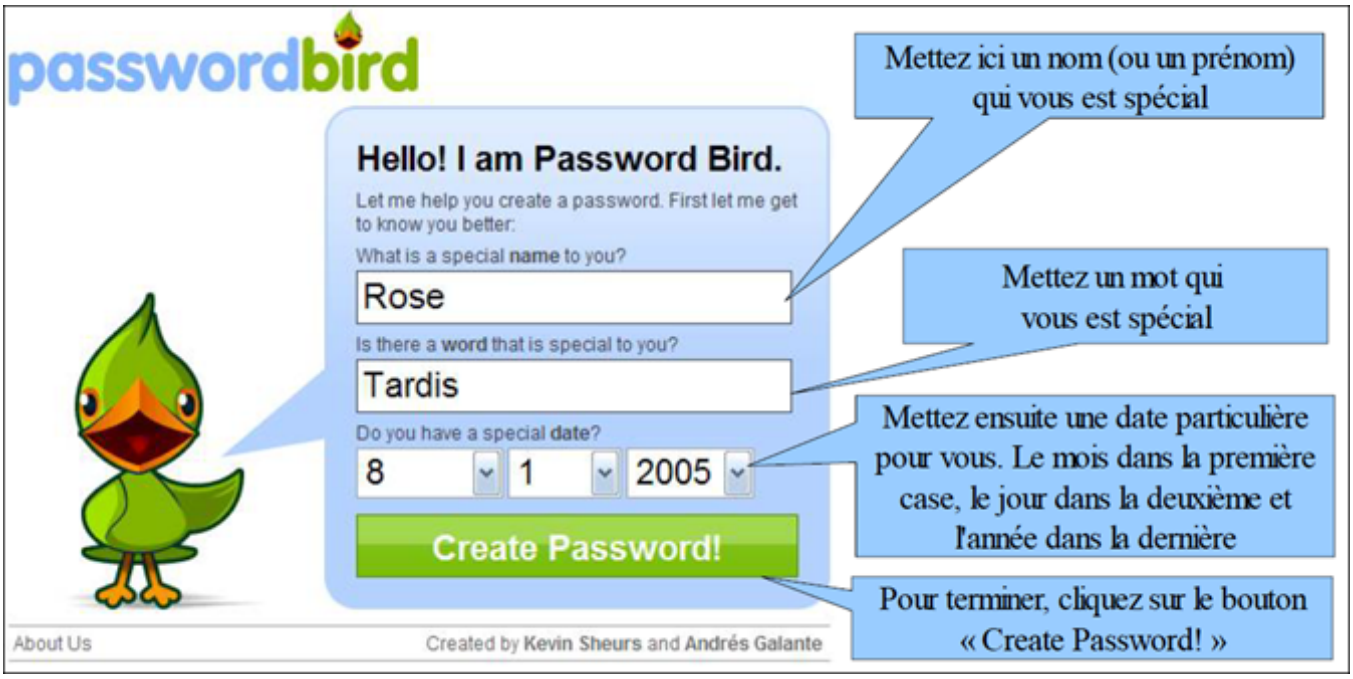
Stratégies à éviter

Les criminels connaissent la plupart des méthodes de création de mots de passe les plus répandues. Pour éviter les mots de passe de faible niveau de sûreté, faciles à deviner :

- N'utilisez pas de suites ou de répétitions de caractères. « 12345678 », « 222222 », « abcdefg » ou une suite de lettres voisines sur le clavier forment des mots de passe relativement inefficaces.
- Évitez de remplacer des lettres uniquement par le chiffre ou le symbole leur ressemblant le plus. Les criminels et autres personnes mal intentionnées assez expérimentés pour essayer de pirater votre mot de passe ne se laisseront pas leurrés par l'emploi du chiffre« 1 » à la place d'un « i » ou du caractère « @ » à la place d'un « a », comme dans « N1nteñd0 » ou « m0tdep@88e ». Cependant, ce type de substitution peut se révéler utile s'il est associé à d'autres astuces permettant d'améliorer la sûreté du mot de passe, comme le fait de privilégier la longueur, l'ajout de fautes d'orthographe ou les changements de casse.
- N'utilisez pas votre identifiant de connexion. Il est fortement déconseillé de former un mot de passe à partir de tout ou partie de votre nom, de votre date de naissance ou de votre numéro de sécurité sociale, ou d'informations du même type relatives à vos proches. C'est souvent par là que les criminels commencent leurs manœuvres de piratage.
- Évitez d'employer des mots se trouvant dans le dictionnaire, même dans une autre langue. Les criminels utilisent des outils sophistiqués pouvant deviner les mots de passe rapidement en se basant sur le contenu de différents dictionnaires et contourner les astuces consistant à écrire les mots à l'envers, à intégrer des fautes d'orthographe courantes ou à avoir recours à des substitutions de caractères. Sont également à exclure tous les types de jurons imaginables et les mots que vous ne dites jamais en présence de vos enfants.
- N'utilisez pas le même mot de passe partout. Si l'un des ordinateurs ou site Internet protégé par ce mot de passe est compromis, vous pouvez considérer que toutes vos informations personnelles protégées par ce mot de passe sont également compromises. Il est extrêmement important de créer un mot de passe différent pour chaque système.
- Évitez de stocker par écrit votre mot de passe dans votre ordinateur (ou un quelconque ordinateur sur Internet), car une personne piratant un site Internet ou même votre ordinateur pourrait retrouver le mot de passe stocké.

## Un générateur de mots de passe simples à retenir

Ce générateur simple s'appelle passwordbird. Vous pouvez soit le rechercher avec votre ami Google, soit en recopiant ce lien dans la barre d'adresses de votre navigateur : http://passwordbird.com/




Une fois sur la page du site, suivez les instructions marquées ci-dessus (j'ai mit un truc assez bidon dans l'image d'exemple).

Ce qui donne :


Si le mot de passe ne vous plait pas, vous pouvez cliquer sur le lien « Click here and I will make a new one! » afin qu'il en génère un nouveau avec les mêmes mots clés. Si vous voulez en générer un autre complètement nouveau, cliquez sur le lien « Click here and tell me different information! » (le deuxième lien).

N’hésitez pas à mettre un caractère spécial (ponctuation ou autre) pour augmenter la sécurité de votre mot de passe.

## Mais aussi bien choisir ses questions secrètes !

De nombreux services Internet (Hotmail, Windows Live Messenger, Gmail, …) vous proposent un moyen de récupérer votre mot de passe. Ce moyen, c’est très souvent la question secrète.

Le concept :

Quand vous vous inscrivez à un service, vous choisissez un mot de passe, et vous choisissez/rédigez une question à laquelle vous donnez la réponse exacte (sinon, ça ne sers à rien).

Trois jours plus tard, vous vous rendez compte que vous ne vous rappelez plus de votre mot de passe car vous avez choisit le mot de passe le plus compliqué au monde. Du coup, vous cliquez sur un lien « Mot de passe oublié », ou tout autre lien ressemblant à ça. Ensuite, une question vous sera posé (la fameuse question secrète que vous avez choisi/rédigé). Vous devrez répondre exactement la même chose que le jour de votre inscription pour pouvoir recréer un mot de passe.

Le problème, c’est que le plus souvent, les gens mettent des réponses évidentes (un personnage de série TV alors que tout le monde sais que la personne est fan de cette série, …).

Quand vous pouvez choisir la question, ne prenez pas quelque chose à quoi tout le monde vous connaissant (voire tout le monde tout court) pourrait répondre.

Prenez un truc qui sois extrêmement personnel, auquel seul vous pourra répondre, mais aussi un truc dont vous serez sûr de vous souvenir (pas votre personnage de fiction préféré par exemple, car ça peut changer).

Autre raison pour ne pas prendre un truc trop facile :

Si vous avez un blog, il est fort probable que vous parliez par exemple de vos animaux de compagnie. Si le nom de votre animal (ou un animal que vous aviez) apparaît dans votre blog, et que c’est la réponse à la question secrète d’un service sur lequel vous êtes inscrit, le risque de vous faire pirater votre compte est grand.

De même pour les mots de passe, c’est aussi une raison pour laquelle il ne faut pas prendre un simple mot ayant un sens pour vos comme mot de passe.