

# Créer des mots de passes efficaces

Date de dernière mise à jour : 27/06/2007 à 19:36

Source : <http://www.vulgarisation-informatique.com/creer-mot-passe.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)

Si une personne parvient à se procurer vos mots de passe, elle peut pratiquement faire ce que bon lui semble. Inutile de dire alors que plusieurs "bons" mots de passe sont indispensables.



**Voici quelques actions que peut faire une personne possédant vos mots de passe :**

- Accéder aux documents protégés de votre ordinateur.
- Recevoir et lire vos mails. Elle peut aussi en envoyer.
- Modifier vos mots de passe. De cette manière, vous ne pourrez plus accéder à vos informations. Cela devient grave.
- Usurper votre identité.
- Retirer de l'argent de votre banque.

Pour être sûr que personne n'utilise vos mots de passe, vérifiez les journaux de connexion (fichiers .log). Inquiétez vous si vous voyez des activités pendant les heures où vous n'êtes pas censé être en ligne.

Pour ce protéger d'un vol de mot de passe, il faut que le mot de passe en lui même soit le plus compliqué possible.

Pour trouver un mot de passe, les pirates font appel à des logiciels qui essayent plusieurs milliers de mots de passe en cherchant dans les combinaisons faciles.

Il vous faut par exemple un évènement que vous pourrez transformer en code secret : prenons cette phrase toute simple : "j'ai acheté un PC". Elle peut devenir : jaupc, ou encore en inversant les lettres : cpuaj. Le mot de passe ainsi produit n'a aucune signification.

Mais ce mot de passe n'est encore pas assez difficile. Il faut le combiner avec des chiffres par exemple. Il peut ainsi se transformer en c1p3u9j4. La signification est encore moins grande mais le mot de passe est bien plus fiable et difficile à trouver. Notez que "c1p3" peut signifier "c'est un pentium 3" !!! Il ne vous reste plus que u9j4 à mémoriser.

**Les points à respecter pour choisir un bon mot de passe :**

- Il faut que sa longueur soit au moins de 7 ou 8 caractères. Plus il est long et plus la combinaison est difficile à trouver. Windows peut gérer les mots de passe jusqu'à 128 caractères.
- Permutez les minuscules et majuscules. Les chances de trouver la combinaison sont encore diminuées.
- Insérez des symboles (comme par exemple &-)
- Ne mettez pas les mêmes caractères
- La séquence du mot de passe ne doit pas signifier un mot. Elle doit être aléatoire.

**Les règles à appliquer pour éviter de se faire voler un mot de passe :**

- Protégez votre connexion internet des pirates en installant un antivirus et un pare-feu (voir dossiers protection du PC)
- N'utilisez pas votre nom de connexion pour vos mots de passe
- N'utilisez pas votre date de naissance, c'est très courant mais bien connu.
- N'utilisez pas de lettres ou chiffres consécutifs comme 123 ou abc, etc.
- N'utilisez pas de touches adjacentes à votre clavier comme par exemple "Azerty" ou encore "uiop^\$".
- Utilisez des mots de passe différents pour les sites ayant une importance moyenne à ceux ayant une importance élevée. Adaptez

naturellement le mot de passe en conséquence, mais ne réutilisez rien de votre ancien mot de passe.

**Conservez vos mots de passe à l'abri :**

- Ne collez pas un Post It sur votre moniteur avec vos mots de passe. Autant ne pas mettre de mot de passe du tout.
- Ne rangez pas vos mots de passe dans un tiroir. Utilisez éventuellement un coffre fort.
- Ne partagez pas votre mot de passe avec quelqu'un. Si vous devez le partager, changez le ensuite.
- Ne cochez pas la case "mémoriser mon mot de passe" lorsque vous consultez un site à partir d'un ordinateur public.
- Changez de mot de passe tous les 6 mois.

Source : <http://www.vulgarisation-informatique.com/creer-mot-passe.php>.

Distribution interdite sans accord écrit d'Anthony ROSSETTO (<http://www.vulgarisation-informatique.com/contact.php>)