Panoptinet

Gardez un oeil sur votre réseau

10 conseils pour un mot de passe solide

admin · Monday, May 2nd, 2011

Le mot de passe est souvent l'unique rempart pour accéder à des données personnelles : compte mail, site web de commerce, forums, clé WPA, accès box, etc. Etant donnée la valeur de nos informations personnelles (messages, coordonnées, documents, numéros bancaires), mieux vaut s'assurer de les protéger correctement !

Pourtant, à l'heure où l'insécurité numérique s'intensifie, de nombreuses personnes utilisent encore des mots de passe faibles tels que "1234", "médor" ou "password", facilement trouvables par des pirates mal intentionnés,. Convaincu ? Alors voici quelques conseils qui vous permettront de choisir des mots de passe solides et fiables.

1. Evitez les grands classiques

Choisissez un mot de passe plus original (et surtout plus fiable) que les traditionnels "motdepasse", "password", "sésame", etc.

2. Oubliez les suites logiques

Les mots de passe tels que "1234", "azerty" ou "abcde" ne sont hélas d'aucune utilité.

3. Bannissez les mots du dictionnaire

Certains logiciels spécialisés et connus des "crackers" testent à grande vitesse tous les mots issus des dictionnaires (français, anglais, espagnol, noms propres, etc.) pour forcer un mot de passe. Même un mot plus savant comme "doryphore" n'a aucune chance.

4. Ne composez pas avec des informations personnelles

Les mots de passe issus de la date de naissance d'un proche, de votre adresse ou de votre immatriculation sont facilement devinables, même par une personne qui vous connait peu.

5. Préférez un mot de passe long

Au moins égal à 8 caractères, vous pouvez même aller jusqu'à 12, 30 ou plus ! Pas trop long non plus si vous devez saisir votre mot de passe plusieurs fois par jour…

6. Mélangez les types de caractères

Plus un mot de passe est complexe, et plus il est difficile à cracker. Mélangez au maximum minuscules, majuscules, chiffres et caractères spéciaux. Un bon mot de passe est aussi un mot de passe que l'on arrive à retenir ! Essayez donc de trouver le bon équilibre entre complexité et mémorisation. Par exemple, préférez "C4raVan3!" à "caravane"

7. Créez différents mots de passe

L'idéal est un mot de passe pour un accès. Mais cela peut devenir rapidement très compliqué. Par contre, il est possible de créer plusieurs mots de passe, 3 par exemple : 1 généraliste pour les sites web, 1 confidentiel pour les mails, et 1 professionnel pour tout ce qui touche à votre travail. Compartimenter ses espaces protégés est très efficace.

8. Ne partagez pas vos mots de passe

Un mot de passe, c'est comme une brosse à dent, ça ne se prête pas ! Même envers une personne bien intentionnée, qui peut par mégarde le perdre ou le transmettre.

9. N'envoyez pas vos mots de passe par mail

Même les messageries sont parfois mal sécurisées… En règle générale, ne laissez pas de trace écrite de vos mots de passe : message, post-it, etc.

10. En cas de doute, changez votre mot de passe

Si vous pensez qu'une personne a trouvé, déduit ou deviné votre mot de passe, changez-le immédiatement : l'opération prend une minute maximum, et garantit votre sécurité. Il est d'ailleurs conseillé de changer régulièrement votre mot de passe, surtout s'il permet d'accéder à des données particulièrement confidentielles…

Banalisé au quotidien, l'usage des mots de passe est pourtant à prendre au sérieux ! Inutile toutefois de devenir complètement parano ou d'utiliser des combinaisons à 250 caractères ! L'application de ces quelques conseils devrait vous permettre de conserver vos données personnelles en toute sécurité. Enfin, méfiez-vous des sites Internet que vous connaissez mal et qui vous proposent la génération automatique de mots de passe : leurs intentions ne sont peut-être pas si louables… A contrario, si vous craignez que vos mots de passe sont trop faibles, passez-les au Panoptipass, il testera leur solidité !

Lien : memoclic

This entry was posted on Monday, May 2nd, 2011 at 4:35 pm and is filed under Actualités pratiques
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.