Newsletter n° 15

OCTOBRE 2018

ÉDITO

Lorsque l'on souhaite accéder à un site Internet protégé, à une ressource informatique ou à un service dont l'accès est limité, un mot de passe est demandé comme moyen d'authentification pour prouver son identité.

Afin de protéger vos informations, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Cette Newsletter vous donne quelques conseils en la matière.

Daniel BAZOT

A LA UNE

Les mots de passe

Internet nous propose un nombre élevé de sites dans lesquels sont stockées des informations publiques et privées.

Il est très vite apparu qu'il était nécessaire d'identifier le correspondant qui souhaitait se connecter et ne lui offrir que les informations auxquelles il peut prétendre, d'où l'apparition des termes d'identifiant et de mot de passe.

Le mot de passe n'est pas nouveau puisque, depuis la nuit des temps, les militaires l'utilisent.

Mais, en informatique, les hackers *(informaticiens qui recherchent les moyens de contourner les protections logicielles et matérielles)* sont capables de pénétrer dans n'importe quel site en brisant les codes, par défi ou esprit malfaisant, voire les deux.

Il est donc important de nous protéger en rendant nos données confidentielles même celles paraissant anodines.

Plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant un mélange de lettres, de symboles et de chiffres.

Il est conseillé de posséder plusieurs mots de passe par catégorie d'usage, en fonction de la confidentialité des données qu'ils protègent.

Alors, ne facilitez pas le travail des hackers et choisissez des mots de passe personnalisés, simples à retenir et différents pour chaque site.

Et n'hésitez pas à en changer régulièrement.

Mots de passe

Quelques conseils

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire.
- Choisissez un mot de passe qui n'a pas de lien avec vous *(pas de mot de passe composé de votre nom, d'un nom de société, d'une date de naissance, etc.)*.
- Ne demandez jamais à un tiers de générer pour vous un mot de passe.
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque *(exemple : en ligne sur Internet)*, encore moins sur un document imprimé facilement accessible.
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
- Pour les sites où vous avez des données sensibles (banque, sites marchands, messageries, etc.), ne permettez pas à votre ordinateur, téléphone portable, tablette de retenir les mots de passe.

Comment choisir un mot de passe ?

- Ne créez pas des mots de passe ultra compliqués que vous oublierez quand vous voudrez les utiliser.
- Mélangez des chiffres, des lettres et quand c'est possible des caractères (*,+,- , »,&). Si vous utilisez un mot, glissez une majuscule, mais pas au début. Exemple : menNecy91cim.
- Un mot de passe aura au minimum entre 10 et 12 caractères.
- Utilisez des moyens mnémotechniques :
  - la citation de Jean de La Fontaine : « *Rien ne sert de courir7, il faut partir à point 8* » deviendra **rnsdC7ifpa.8**.
  - cette phrase de Jacques Brel : « *Dans le port d'Amsterdam1, Y a des marins qui chantent 9* » donnera **dLpdA1yadmqc 9**.
- Vous pouvez aussi inverser les caractères : « mennecy91 » deviendra **19ycennem**.
- Enfin, il existe sur Internet des générateurs de mots de passe sécurisés. Nous déconseillons leur usage pour les raisons suivantes :
  - comme les mots de passe sont générés de façon aléatoire, vous n'aurez aucun moyen simple de les retenir,
  - soyons parano... Imaginons un générateur malveillant qui retienne le mot de passe produit. Il lui sera possible de le retrouver dans le maquis du Web et d'accéder à vos données...

Les pires mots de passe...

SplashData, éditeur d'une solution de gestion de mots de passe, donne son classement annuel des mots de passe les plus utilisés. Et malheureusement, le tandem « 123456 » et « password » fait la course en tête.

Basé sur un échantillon de 3,3 millions de mots de passe diffusés sur le Net, le classement de SplashData indique très clairement quels sont les modèles à ne pas suivre.

Ainsi, si vous utilisez une des suites alphanumériques présentées ci-contre pour un service revêtant une quelconque importance, n'hésitez pas : changez-la. Ces mots de passe sont les premiers qu'un pirate en herbe essaiera de combiner avec votre adresse mail pour accéder à vos différents comptes.

ACTUALITÉ

Calendrier des activités

Le calendrier des activités est disponible sur le site Internet du club.

Ateliers

- Diaporama : jeudi 4 octobre
- Photo : jeudis 18 octobre et 15 novembre à 17 H 00
- Généalogie : jeudis 11 et 25 octobre et 8 et 22 novembre à 14 H 30
- Image créative : tous les lundis à 20 H 30
- Atelier multimédia : tous les mercredis à 9 H 30
- After Effects : tous les vendredis à 14 H 30
- GIMP : un mercredi sur deux à 16 H 30

Merci de vous inscrire aux ateliers auprès de l'animateur concerné.

Thématiques

- 1er octobre : courrier électronique
- 22 octobre : optimiser l'utilisation de vos imprimantes pour économiser vos cartouches d'encre
- 12 novembre : Facebook

Les réunions commencent à 14 H 30. Merci de vous inscrire auprès de l'animateur dès que vous recevrez le mail d'invitation car le nombre de places est limité.

Au CIM, il se passe toujours quelque chose...

Newsletter du CIM - Directeur de la publication : Daniel BAZOT - Rédacteur : Denis GELIN