Sécurité informatique, les mots de passe

2653 Nov 12, 2024 Autre

Afin d'augmenter la sécurité de son informatique, nous énumérons un certain nombre de bonnes pratiques. Cet article contient quelques conseils pour la gestion de ses mots de passe.

La malédiction des mots de passe

Les mots de passe sont souvent un point faible dans la sécurité informatique, car dépendants de la faillibilité humaine. Comme souvent les nombreux mots de passe doivent être mémorisés, les utilisateurs commettent principalement deux erreurs : utiliser des mots de passe courts et faciles à mémoriser ou deviner et réutiliser les mêmes mots de passe pour plusieurs services différents.

Longueur du mot de passe

Un mot de passe devrait être assez long pour éviter d'être trouvé trop facilement par "force brute" (un programme tente toutes les combinaisons de chiffres et lettres possibles : en-dessous de 6 caractères, quelques secondes ou minutes suffisent). Un minimum de 10 caractères combinant des lettres majuscules et minuscules, des chiffres et des symboles spéciaux (&%*+-) devrait être utilisé.

Pour tout mot de passe à saisir sur le web, ne pas craindre les mots de passe longs, car ils peuvent être enregistrés dans le navigateur web, et n'ont donc pas besoin d'être mémorisés.

Différents sites web (dont https://bitwarden.com/password-strength/) vous renseignent sur la force d'un mot de passe.

Mots de passe distincts

Un mot de passe distinct devrait être utilisé pour chaque site web et service. En effet, en cas de fuite de données, un hacker tentera de réutiliser le même mot de passe sur un autre site et pourrait ainsi facilement accéder aux comptes d'un utilisateur négligent.

Utilisez des mots de passe distincts pour votre vie numérique privée et professionnelle.

Pour faciliter l'utilisation de dizaines de mots de passe différents, il existe de nombreux utilitaires tels que 1Password. Les navigateurs web proposent aussi de mémoriser les mots de passe. Prudence cependant avec des applications ou sites web stockant vos mots de passe, à moins qu'ils n'aient une excellente réputation.

Autres précautions

Un mot de passe est personnel et ne doit jamais (sauf rares exceptions) être communiqué à un tiers.

Un mot de passe ne devrait jamais être écrit sur un Post-It collé sur l'écran ni envoyé par e-mail, SMS, chat ou d'autres moyens laissant des traces.

Si le site web ou le service le propose, activer l'identification à 2 facteurs (confirmation par SMS ou mieux, via une application d'authentification).

Online URL: https://om-bm.knowledgebase.co/article-2653.html