Comment choisir et conserver un mot de passe sécurisé

27.12.2022 - Informations générales

Avec les mots de passe, vous avez l'embarras du choix, ils doivent être aussi sûrs que possible et doivent être faciles à mémoriser. Mais les mots de passe les plus sûrs sont cryptiques et très longs et donc peu adaptés à la mémoire humaine. Cependant, vous pouvez simplement suivre quelques règles pour éviter les mots de passe particulièrement faciles à craquer tout en choisissant un mot de passe sûr. Les gestionnaires de mots de passe comme KeePass permettent de conserver de nombreux mots de passe en toute sécurité.

Règles relatives aux mots de passe

Actuellement, les caractères spéciaux suivants sont autorisés dans un mot de passe (y compris l'espace):

```
: ; < > | = . , _ - ~ ! ? & % @ # $ £ € ° ^ * § ( ) + [ ]
```

Et au minimum 8 caractères, mais mieux vaut en utiliser 12 ou jusqu'à 25 (voir le lien ci-dessous), qui contiennent des lettres minuscules et majuscules et des chiffres. En principe, plus c'est long, plus c’est mieux et sécurisé.

Lien des mots de passe sécurisés

Lien avec des instructions pour les gestionnaires de mots de passe

Lien vers un aperçu des gestionnaires de mots de passe actuels

Lien KeePass

Mon login/email a-t-il été piraté?

Des millions de connexions sont piratées chaque jour et des données sont volées ou des mots de passe sont utilisés pour causer des dommages tels que l'usurpation d'identité, des achats illégaux, le téléchargement de données de cartes, etc. Vous pouvez vous protéger contre cela en utilisant un mot de passe long et imprévisible, différent pour chaque service web. Pour vérifier si vos identifiants ont déjà été piratés, vous pouvez utiliser ce service. Si vos identifiants ont été compromis, vous devez immédiatement définir un nouveau mot de passe sécurisé!

Ai-je été piraté? Est-ce que je me suis fait avoir?