

COMMENT UN EXPERT INFORMATIQUE CHOISIT UN MOT DE PASSE SÉCURISÉ

EN CINQ ÉTAPES

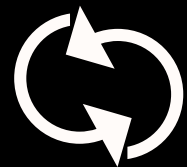
123

TROP SIMPLES

N'utilisez en aucun cas des mots de passe trop simples : prénoms, "azerty", "qwertz", "123456", "motdepasse", etc. Ils font partie des banques de mots de passe testés en priorité. Dans le même ordre d'idées, ne reprenez pas l'intitulé de votre compte:

MÉLANGEZ

Mixez des lettres avec des chiffres et des caractères spéciaux (!#\$%_-_). Les pirates informatiques testent d'abord tous les mots du dictionnaire !



INFORMATIONS CONNUES

Bannissez les informations qui peuvent être découvertes facilement : résidence, deuxième prénom, date de naissance, etc. Ces mots de passe sont faciles à trouver pour quelqu'un de votre entourage ou connecté avec vous sur Facebook.

MOTS DE PASSE LONGS

Utilisez des mots de passe longs, de plus de 10 caractères. Plus votre mot de passe est long, plus il est difficile à craquer. Il vaut mieux un mot de passe en lettres long qu'un court avec des caractères spéciaux.



PR

ALTERNEZ MINUSCULES ET MAJUSCULES

Alternez les lettres minuscules et majuscules, cela ajoute de la complexité et renforce le niveau de sécurité de votre mot de passe.



MAKING IT WORK