5 dicas para manter seguras as suas *passwords*

compilado por

AP2SI

1

Use “frases-passe” longas ao invés de “palavras-passe” complexas

Uma “frase-passe”, apesar de mais longa pode ser mais fácil de fixar que uma “palavra-passe” complexa e igualmente difícil de ser comprometida.

Juntar 4 a 6 palavras numa mnemónica pode apoiar o esforço de memorização e manter a segurança.

compilado por

AP2SI

2

Use *passwords* diferentes em serviços diferentes

Reutilizar a mesma *password* em diversas contas e serviços aumenta a probabilidade que esta possa vir a ser descoberta (por exemplo, numa fuga de informação), colocando em causa a segurança de todos as contas e serviços a que está associada.

compilado por

AP2SI

3

Altere as suas passwords periodicamente

Quanto mais tempo usar a mesma *password* numa conta ou serviço, maiores serão as probabilidades de que esta possa ser comprometida.

compilado por

AP2SI

4

Use um gestor de *passwords*

Um gestor de *passwords* é uma aplicação que armazena as suas palavras-passe ou frases-passe de uma forma segura para que não tenha que as memorizar.

Algumas aplicações também o apoiam a escolher *passwords* robustas, sugerem alterações periódicas e incluem serviços de monitorização de fugas de informação que lhe indicam quando a sua *password* está em risco.

compilado por

AP2SI

5

Use vários factores de autenticação

Qualquer que seja a sua *password*, use também factores adicionais de autenticação, sempre que possível. SMS, geradores de códigos aleatórios de utilização única, chaves de segurança, são mecanismos que ajudam a manter as suas contas seguras mesmo se a informação da password se tornar pública, dando-lhe mais tempo para actuar no caso de esta se tornar pública.

compilado por

APSI

Dicas compiladas por

Conheça melhor a AP2SI
em *https://ap2si.org*