Senhas mais seguras (e fáceis de se lembrar)

Nós fazemos de tudo para deixar o que é nosso em segurança, porém a falsa sensação de segurança, facilita o roubo daquilo que é nosso, uma dessas falsa sensações são as senhas que você acha que são seguras.

Existe várias maneiras de criar senhas seguras, nós mesmos sugerimos o uso de um gerenciador de senhas, como o Bitwarden, que é Open Source, assim, você só precisa de lembrar de uma única senha, e as outras estão bem guardadas no gerenciador; outra forma é usar uma longa combinação de palavras aleatórias; e existe uma forma criada pela Grafenea, confira a seguir nesse passo a passo:

1• Escolha 3 palavras, ex.:

pastel, galinha, osso

2• Deixe elas com letra maiúsculas e as separe com um traço, espaço, números, símbolos, você que escolhe. No caso, usamos traços (-):

Pastel-Galinha-Osso

3• Converta elas em Base64:

UGFzdGVsLUdhbGluaGEtT3Nzbw==

4• Calcule o hash Sha-256 com o resultado da Base64:

687a3e725e0895461a7d369d8d8f617e1b6427f3ecb274f0d4627cd9aff3a540

5• Pegue o Sha-256 e converta em Base64:

Njg3YTNlNzI1ZTA4OTU0NjFhN2QzNjlkOGQ4ZjYxN2UxYjY0MjdmM2VjYjI3NGYwZDQ2MjdjZDlhZmYzYTU0MA==

• **Nunca use a mesma senha para serviços diferentes**, sempre pense em palavras aleatórias que não se completam. Caso queira, use mais palavras.

• **Você pode criar as suas próprias senhas simples fáceis de gravar, não necessariamente precisa seguir esse tutorial**, você por exemplo, pode pular o primeiro Base64, e *caso o serviço/site limite o tamanho máximo da senha* para 40 caracteres, exemplificando, você pode substituir o Sha-256 pelo MD5, e apagar 4 caracteres. E não se esqueça, se puder use a verificação de 2 etapas.

Sites sugeridos (ambos open Source):

Enigmator

Cyberchef (Versão automatizada)

Online Tools