Dicas para

CRIAR PALAVRAS-PASSE

fortes e seguras

1

2

3

4

5

800 219 090 Linha Internet Segura

APAV Apoio à Vítima

Crie Palavras-passe Longas

- Palavras-passe longas são mais seguras.
- Recomenda-se usar pelo menos 12 caracteres.

Use uma Mistura de Caracteres

- Inclua letras maiúsculas e minúsculas, números e símbolos.
- Quanto mais variada for a combinação de caracteres, mais difícil será para um hacker desvendar a palavra-passe

Evite Informações Pessoais

- Não use informações facilmente acessíveis, como o seu nome, data de nascimento, nomes de familiares ou animais de estimação, etc.

Não Utilize Palavras Comuns

- Evite utilizar palavras na integra, uma vez que são mais fáceis de adivinhar.
- Em vez disso, deve combinar letras, números e símbolos de forma pouco óbvia.

Utilize Frases como Palavra-passe

- Considere usar uma frase ou uma sequência de palavras que apenas você possa identificar.
- Por exemplo, a primeira letra de cada palavra numa frase que gosta, misturada com números e símbolos.

Evite Repetir Palavras-passe

- Use palavras-passe diferentes para diferentes contas. Se um serviço for comprometido, as outras contas permanecerão seguras.

Atualize Regularmente

- Mude as palavras-passe regularmente, especialmente para contas importantes como e-mail e bancos.

Use Autenticação de Dois Fatores

- Sempre que possível, ative a autenticação de dois fatores.
- Isto adiciona uma camada extra de segurança.

Poderá instalar um gestor de palavras-passe

- Para gerir as várias palavras-passe, considere usar um gestor de palavras-passe. Ajudará a criar e armazenar as palavras-passe seguras.

Fique atento a *Data Breach*

Mantenha-se informado sobre a partilha não consentida de dados e mude as suas palavras-passe se achar que as suas contas podem ter sido afetadas.