INSTRUÇÃO PARA O TRABALHO

SENHAS

Em tempos de ataques digitais cada vez mais sofisticados, o desafio está em criar senhas fáceis de lembrar, mas difíceis de serem descobertas por outras pessoas ou sistemas automatizados. Para ajudar a resolver esse dilema, apresentamos algumas estratégias criativas e eficazes para criar senhas seguras.

Utilize uma frase e escolha a primeira letra de cada palavra.

Ex.: "Água mole em pedra dura, tanto bate até que fura?", você pode gerar a senha: "Amepdtbaqf?".

Remova as vogais de uma frase simples.

Ex.: "Voe como uma águia" → "Vcmmg", ou mais criativamente em inglês: "Fly like an eagle" → "Flylkngl".

Escolha uma palavra ou nome fácil de lembrar e misture com um número de mesmo comprimento, alternando os caracteres.

Ex.: "DivSeg" com "123456" → "D1i2v3S4e5g6".

Aplique padrões de substituição criativos, adicionando complexidade visuais ou sonoras. Ex.:

- "a" por "@", "e" por "3", "o" por "o", "i" por "1", etc.
- Repita letras como "s" e "r": "password" → "pa$$worrd".

VALIDADOR DE SENHAS

Avalia a complexidade de senhas considerando comprimento, variedade de caracteres e padrões comuns.

Contudo, mesmo uma senha classificada como "muito forte" pode não ser segura se incluir informações pessoais, que podem ser facilmente obtidas por atacantes.

A Divisão de Segurança da Informação disponibiliza em sua página este serviço, acesse aqui.

Fique atento e ALTERE SUAS SENHAS, se:

- **Suspeitar de que a senha foi descoberta ou que o computador foi comprometido.**
- **Perder ou houver furto de dispositivo com senhas armazenadas.**
- **Fazer uso de padrões para senhas e suspeitar de que foram descobertas.**
- **Usar da mesma senha em múltiplos sistemas e suspeitar de comprometimento em algum deles.**
- **Instalar dispositivos de rede com senhas padrão de fábrica, que são facilmente descobertas na Internet.**