

**TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO – 2º ciclo****Cibersegurança****Atividade: “A Minha Palavra-Passe é Segura?”**

O objetivo desta atividade é compreender o que torna uma palavra-passe forte ou fraca e aprender a criar senhas mais seguras.

 Dicas para uma palavra-passe forte:

- ☒ Deve ter **pelo menos 8 caracteres** (quanto mais longa, melhor!)
- ☒ Mistura **letras maiúsculas e minúsculas** (ex.: A e a)
- ☒ Inclui **números e símbolos** (ex.: 3, 7, !, @, #)
- ☒ Evita usar o **teu nome, data de nascimento ou escola**
- ☒ Usa **frases criativas** que só tu entendas
- ☒ Exemplo: “Adoro gelado de morango” → @d0r0G3lad0!
- ☒ **Não partilhes** a tua palavra-passe com ninguém
- ☒ **Muda-a de vez em quando**, especialmente se alguém a descobrir



Palavra passe forte e segura – como criar.

Procedimentos:**Passo 1 – Cria a tua palavra-passe:**

Escreve num papel uma palavra-passe inventada (não deve ser uma que uses na vida real).

Passo 2 – Teste da segurança:

Digita no computador do professor, no site de verificação, a palavra-passe.

<https://www.strongpasswordgenerator.org/pt/password-strength-checker/>

<https://www.uic.edu/apps/strong-password/>

<https://password.kaspersky.com/pt/>

<https://psono.com/pt/password-strength-test?>

Passo 3 – Observa os resultados

O site mostra se a senha é fraca, média ou forte e indica o que falta.

Toma nota dos resultados.

Passo 4 – Melhoria da palavra-passe

Melhorar a tua palavra-passe com base nas dicas aprendidas e volta a testá-la.

Bom trabalho!