Recomendações de segurança - Palavras passe CIFFT

Vitor Marques

Palavras Passe

Em primeiro lugar, é crucial que cada conta ou serviço que usamos tenha uma senha única. Isto evita que, se uma senha for comprometida, todas as nossas contas fiquem em risco.

Além disso, é importante que estas senhas sejam grandes e complexas. Isto torna-as mais difíceis de adivinhar ou de serem descobertas através de ataques de força bruta.

Algumas dicas para gerar uma palavra passe forte são

1. Usar uma mistura de caracteres

Uma boa palavra-passe deve incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais como `!`, `@`, `#`, `$`, `%`, etc.

2. Evitar palavras-passe óbvias

Não usar palavras-passe que possam ser facilmente adivinhadas ou pesquisadas, como o nome da empresa, o nome do dono da empresa, ou datas de aniversário. Estas são as primeiras opções que um hacker irá tentar.

Exemplos de palavras-passe

- Fraca: `empresa123`
- Forte: `S3cur!tYr0cks!`

3. Palavras-passe geradas por computador

Utilizar um gestor de palavras-passe como o KeePass para criar palavras-passe aleatórias, que são muito mais difíceis de decifrar. Estas palavras-passe são uma mistura aleatória de caracteres, como `G5!b8^2hW!pD`.

4. Usar uma passphrase

Se for difícil lembrar de palavras-passe complexas, criar uma passphrase é uma opção. O único problema é que acabam por ser maiores que o normal, então, em alguns serviços que limitam o limite de carateres de senhas, pode não funcionar. Um exemplo para construir uma passphrase é peguar numa frase que seja significativa e transformá-la numa palavra-passe usando a primeira letra de cada palavra, misturada com números e símbolos. Por exemplo, "A vida é bela e cheia de surpresas" pode tornar-se `Av1b&cds`, ou até `A-vida-e-bela-e-cheia-de-surpresas2`

Gestor de Palavras Passe

O KeePassXC, assim como outras alternativas como o BitWarden, são ferramentas de gestão de senhas que podem ser muito úteis num contexto empresarial. Estes sistemas permitem que cada membro da equipa tenha acesso a um número específico de registos na base de dados de senhas, garantindo que cada pessoa só tem acesso às informações de que realmente precisa.

Estas ferramentas estão disponíveis em vários sistemas operativos, desde computadores a telemóveis, o que significa que as suas senhas podem ser acedidas de forma segura, independentemente do dispositivo que estiver a usar.

Num mundo cada vez mais digital, é essencial que as empresas utilizem um sistema robusto de gestão de senhas. Estes sistemas oferecem proteção end-to-end, o que significa que as suas senhas estão seguras, quer estejam em repouso ou em trânsito.

Com o KeePassXC, só precisa de memorizar uma senha mestra forte. Depois de desbloquear a base de dados com esta senha, o programa pode preencher automaticamente as suas senhas quando necessário.

Finalmente, ao contrário de muitas outras alternativas, o KeePassXC é open source e gratuito. Isto não só ajuda a reduzir os custos, mas também permite que qualquer pessoa verifique o código para garantir que não há falhas de segurança ocultas.