Gestão de Palavras-passe

Enquadramento

As palavras-passe que escolhemos e a forma como as gerimos são uma das principais razões de dados comprometidos.

Abaixo deixo estratégia para uso seguro das mesmas.

Gestor

Para gerir todas as credenciais, uso o Proton Pass.

Gero as passwords com 4 tipos de carateres, no mínimo com 17 mas tendo a preferir 21.

OTP

OTP é acrónimo de "*One Time Password*" e são aqueles códigos numéricos (6 algarismos) gerados a cada 30 segundos pelo Google Authenticator, por exemplo.

Para além de usar o Proton Pass para tal, de modo integrado, uso também o Aegis no Android.

Para quem tem iPhone, têm o OTP Auth.

Backup

Tenho backup de todas as contas OTP presentes no Aegis, salvaguardadas no Notesnook e Proton Drive.

A password de acesso ao Aegis está guardada no Proton Drive e no Notesnook.

Em suma, as credenciais centrais estão guardadas em mais de que um local seguro.

Chaves de Hardware

Podemos incrementar a segurança associando chaves Yubico.

Implementamos hardware key em todas as plataformas que o permitirem (Google aceita, por exemplo).

Papel

Como segurança final, é aconselhável termos em casa um caderno, em local seguro, onde registamos as credenciais do Proton Pass, Aegis, Notesnook, etc.

O meu até já

Revision #7
Created 12 May 2023 12:36:10 by MoldedLight
Updated 14 July 2024 18:36:57 by MoldedLight