Protocolo de segurança para armazenamento e gerenciamento de senhas e arquivos sensíveis

Compartilho com todos, o protocolo de armazenamento e gerenciamento de senhas e arquivos sensíveis, que passei a adotar há mais de dez e que nunca me deixou na mão. **Faço a ressalva de que já estou com muita prática nisso e aconselho a quem queira adotar este protocolo, que comece fazendo testes com arquivos sem importância, durante tempo suficiente em que se sinta realmente seguro para fazer uso de arquivos de uso real.**

O coração desse meu protocolo está no software *open source* de gerenciamento de senhas KeePassX. Ele por si só é uma verdadeira mão na roda quando o assunto é cofre de senhas. Basta criar um novo cofre, atribuindo uma senha-mestre para ele, classificar as categorias de login dentro, gerar senhas aleatórias e muito fortes para novos cadastros em sites de serviços e etc.

Eu digo que não sei de cabeça mais de 98% das minhas senhas de login, onde eu costumo gerar uma senha aleatória de força bem alta, deixo armazenada no cofre do KeePass, entro nele e uso a uso função de "Auto-digitação" nos sites que eu preciso. Sei que existem softtwares parecidos e integrados aos navegadores, mas de verdade, eu prefiro usar um software à parte, fora dos navegadores.

Essas funcionalidades no KeePassX (cofre de senhas e gerador de senhas robustas) não tem nada de novidade para muitos que já fazem uso de softwares similares, mas o meu protocolode segurança vai muito mais além. O KeePassX gera um arquivo para o cofre de senhas com a extensão (.kdbx). Então, deixo este arquivo salvo em uma pasta da minha máquina em sincronização com a nuvem, em serviços como Dropbox ou Google Drive. Não vejo problemas em fazer essa sincronização, já que trata-se de arquivo criptografado. Além do mais, existe a possibilidade do "cofre" ser aberto somente com o apontamento de um arquivo-chave, além da senha é claro!

E essa sincronização fica disponível além do meu notebook, também no celular, porque existe o KeePass também para Android, o KeePassDroid. Então, são dois dispositivos diferentes, além da *cloud*, onde ocorre que a alteração que eu fizer em qualquer um desses meios, será replicada imediatamente nos demais. **Esquecer senha de login, nunca mais.**

Juntamente com o KeePass, também faço uso do VeraCrypt, um poderosíssimo software de encriptação de pastas e arquivos. Com ele é possível criar um arquivo "fake" com o tamanho que desejar, no caso eu aconselho nomear como arquivo de vídeo porque é crível ter um tamanho grande, onde na verdade ele é um arquivo secreto que esconde uma partição particular, criptografada, onde podemos colocar todo e qualquer arquivo de natureza mais sensível, tipo fotos originais de documentos pessoais e ainda assim, poder hospedar esse "arquivo de vídeo" sem problemas na *cloud*. E no meu caso, a senha de acesso a ele, como é de se esperar, ficar armazenada dentro do cofre do KeePass.

Espero que eu tenha conseguido me fazer entender por inteiro e que este protocolo possa acrescentar muito para a segurança digital e pessoal de muitas pessoas.