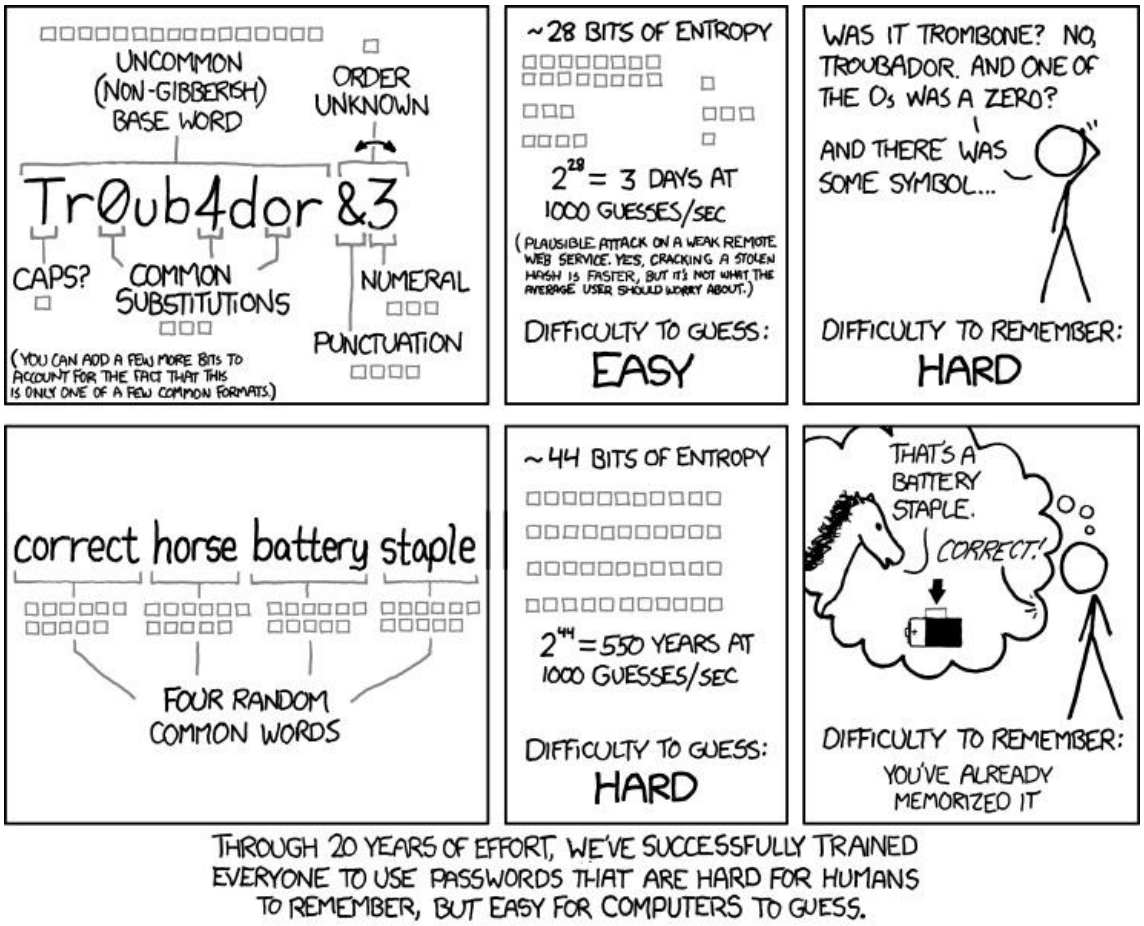
Criador das regras para senhas 'seguras' diz que suas orientações são inúteis

Você já deve saber que uma senha como “123456” não deve ser usada, mas sites estão pegando cada vez mais pesado nos requisitos para palavras-chave. Em alguns casos, é exigida uma senha com ao menos uma letra maiúscula, números e símbolos, forçando o usuário a ter uma memória de aço para lembrar sua senha. Para piorar, o homem que criou essas regras agora diz que elas não servem para nada.

A pessoa arrependida é Bill Burr, ex-gerente do Instituto Nacional de Padrões e Tecnologias dos Estados Unidos. Ao criar um guia de oito páginas sobre como inventar senhas seguras, o documento acabou ditando, na prática, as exigências que você precisa preencher na hora de criar uma senha para um serviço de e-mail novo ou ao se cadastrar em algum aplicativo.

Burr, contudo, **admitiu** em entrevista recente ao Wall Street Journal que não sabia muito sobre senhas em 2003, quando redigiu o manual, e também não era nenhum especialista em cibersegurança. Arrependido, ele diz que o texto se baseou em um documento escrito nos anos 1980, quando simplesmente não existia a web comercial e os computadores não tinham a potência que têm hoje para quebrar senhas.

O que acontece é que este formato de senha, que apenas substitui letras por símbolos, como trocar “Joaozinho” por “J0@0zinh0”, é facilmente superado em um ataque de força-bruta, quando a matemática mostra que seria muito mais difícil quebrar uma senha longa com palavras fáceis de serem lembradas. A tirinha abaixo, do **excelente site xkcd**, dá o exemplo de como a senha “Tr0ub4dor&3” pode ser quebrada em três dias, enquanto uma senha como “correct horse battery staple”, formada por quatro palavras sem uma ordem lógica, só conseguiria ser superada em 550 anos.



O problema, como aponta o autor da tirinha, Randall Munroe, é que, com esse sistema, nós criamos senhas que são difíceis para lembrarmos, mas bastante fáceis de serem quebradas por computadores.

Claro, se você tem a possibilidade de usar um gerenciador para criar e usar uma senha como “QhswSdKG9JpXd=uxMDSQ8gHH9P#xsd+AQ!knFCyc$Y!p$2tH^T97kk#Dqd”, será muito mais difícil quebrar a sua palavra-chave. Para a maioria das pessoas, uma sequência longa e ilógica de palavras é o suficiente. Também vale a pena configurar autenticação em dois passos nos serviços mais importantes para você, se não quiser confiar exclusivamente em uma senha.

Fonte:

Olhar Digital: https://goo.gl/F67TLH