Senha segura precisa ter dez caracteres

22/06/2011 - 15h50

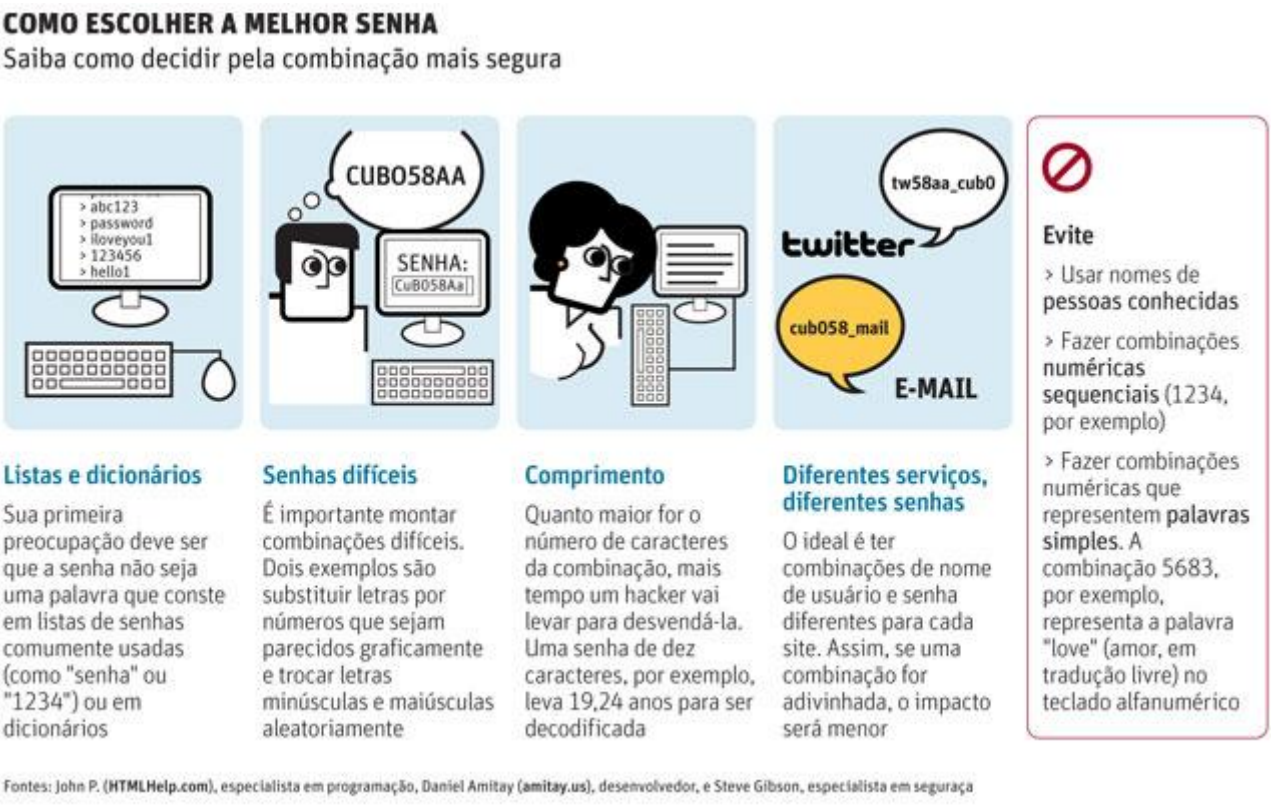
RANDALL STROSS
DO "NEW YORK TIMES"

Para uma senha bem difícil, pense dez. Se a sua senha tiver dez caracteres, você terá condições de dormir bem à noite - talvez por 19 a 24 anos. Esse é o tempo que um hacker levaria para testar todas as combinações de dez caracteres, assumindo que a senha esteja criptografada e que o hacker tenha poderio computacional suficiente para organizar 100 bilhões de combinações por segundo e quebrar a codificação.

Mas, se os seus nomes de usuário e as suas senhas aparecerem em um servidor sem estar criptografado, talvez você não durma nem por um instante, pensando nos efeitos potencialmente devastadores à sua espera.

Hackers adorariam colocar as mãos em uma coleção completa de todas as suas senhas, como as guardadas pela LastPass, um serviço de gerenciamento de senhas.

Editoria de Arte/Folhapress



A partir da instrução de seus clientes, a LastPass armazena nomes de usuário e senhas em seu servidor quando um site é visitado e, em uma próxima visita, preenche todos os formulários automaticamente.

No mês passado, a LastPass afirmou ter notado um comportamento estranho nos registros do tráfego em sua rede e que poderia ter sofrido uma invasão on-line.

Eu sou cliente da LastPass desde o ano passado e senti uma ponta de preocupação ao ouvir a notícia. Mas os meus nervos se acalmaram com o entusiasmo de consultores em segurança que consideram o modelo de segurança da LastPass muito bem elaborado.

A empresa não armazena senhas reais, somente as criptografadas. O serviço não possui a senha para decodificá-las --somente seus usuários a tem. Ela nem sequer armazena a senha LastPass mestre, usada para gerar acesso a todas as outras senhas, que também é criptografada antes de ser enviada à nuvem.

A LastPass tem uma possível vulnerabilidade que Joe Siegrist, seu diretor-executivo, não faz esforço para esconder: o serviço depende de o usuário escolher uma senha mestre difícil e inexistente em qualquer língua.

Se a LastPass ou qualquer outra empresa que armazenou senhas em formato criptografado sofresse um ataque, o risco seria o de ladrões partirem para a força bruta, sem pressa e off-line, tentando todas as combinações possíveis de caracteres. Eles precisariam ter expectativa de vida quase infinitas para esgotar as possibilidades.

Computadores, porém, trabalham em outra velocidade.

COMBINAÇÕES

Steve Gibson, especialista em segurança, publicou uma página na internet que permite ao visitante ver quanto tempo demoraria para um computador testar todas as combinações possíveis de palavras, números e símbolos especiais para quebrar uma senha criptografada.

Eis aqui um teste: qual é a senha mais difícil? "PrXyc.N54" ou "D0g!!!!!!!"?

A primeira, com nove caracteres, é muito boa. O site de Gibson diz que um hacker levaria 2,43 meses para testar off-line todas as combinações envolvendo os nove caracteres, a uma razão de 100 bilhões de conjecturas por segundo. No entanto, a segunda possui dez caracteres. E esse caractere extra torna a senha bem mais difícil. O teste, a uma razão de 100 bilhões de conjeturas por segundo, levaria 19,24 anos.

Não se preocupe com a aparente semelhança do "D0g", com um zero no meio. Isso não faz sentido, "pois o invasor é totalmente incapaz de perceber tais semelhanças", escreveu Gibson.

Gibson afirma que, se a senha não fizer parte de uma lista de senhas comumente usadas e não constar em dicionários, o fator mais importante nela é o comprimento.

Paul C. Van Oorschot, professor de ciências da computação na Universidade Carleton, em Ottawa, tem uma visão cética. "Eu acredito que qualquer sistema irá falhar", afirmou ele. Consequentemente, "não uso um gerenciador de senhas. Escrevo minhas senhas em um papel".

Mesmo isso não lhe oferece tranquilidade: ele não possui conta bancária on-line por causa de sua preocupação em sofrer um ataque hacker.

Uma alternativa a esse risco é usar senhas difíceis, caracteres sem sentido, somando pelo menos dez deles. Claro, é imperativo que os sites armazenem sua senha de forma criptografada. Sempre.

Fonte: Artigo no UOL ... Tradução de **FABIANO FLEURY DE SOUZA CAMPOS**