

Dicas de segurança

Um ataque muito comum a sites é ir conectando várias vezes e testando senhas triviais, que geralmente são as mais usadas. Embora nosso sistema esteja preparado para dificultar ataques desse tipo, seu site **NÃO** vai estar bem protegido se você ignorar as dicas importantes de segurança abaixo:

1 - Não ache que ninguém irá imaginar que sua senha é X e coloque uma senha qualquer. Também não pense "Ah! Ninguém vai querer entrar no meu site!". As tentativas de adivinhar senhas são automatizadas e testam as mais comuns, tendo sucesso muitas das vezes! Seu site é acessível ao mundo inteiro, e tem muita gente querendo alterar suas páginas só para aparecer, e esse é o menor dos estragos possível.

2 - Sua senha deve ser uma mistura de letras maiúsculas, minúsculas, números e símbolos, sem lógica aparente. Exemplo: IW5_9bnk e 9K/0Zndu (não use estas). Não use palavras (veja abaixo), nem que estejam modificadas.

3 - Pense em uma frase e utilize as letras iniciais de cada palavra para formar uma senha. Alterne maiúscula e minúscula e insira números. Exemplo: A verdade fala pela boca dos pequenos -- 4VfpB+P. ("A" virou 4, o "dos" virou "+" e acrescentou-se um "." no final). Isso resulta em uma boa senha e a frase a torna fácil de lembrar.

4 - Não use palavras que estejam no dicionário, da língua que for, para formar sua senha. Programas de quebra de senha têm dicionários de senhas comuns e palavras de várias línguas, meticulosamente testando-as uma por uma e suas variações.

5 - Não use senhas com menos de 6 caracteres. Elas exponencialmente são mais fáceis de quebrar do que as de 6 caracteres ou mais. O ideal mesmo são 8 caracteres no mínimo.

6 - NUNCA, JAMAIS use o nome de sua conta na senha (nem que esteja modificado de alguma forma). Pode parecer óbvio, mas ainda tem muita gente que faz isso.

7 - NUNCA use seqüências de números do tipo 12345, 43210, 24680, 567890, ou seqüências de teclas, asdf, qwerty, etc. Isso também é muito comum, e perigoso!

8 - não use nomes próprios (cônjuge, parente, filho, animal de estimação, time de futebol, personagem de ficção, celebridade, local, etc.), datas de nascimento ou informações acessíveis sobre você (telefone, placa do carro, identidade ou CPF) ou seu ambiente ou de pessoas relacionadas a você.

9 - Não use NENHUMA variação das senhas triviais citadas acima, por mais engenhosa você possa achar que seja. Por exemplo: inverter a ordem dos caracteres, colocar algumas letras maiúsculas e outras minúsculas, colocar um número do começo, meio ou fim, trocar letras por números parecidos (O = 0, I = 1, E = 3, A = 4, etc.), ou qualquer combinação dessas variações. Os programas de quebra de senha testam TODAS as combinações dessas variações e muitas outras.

10 - Use um gerenciador de senhas. Um excelente e gratuito é o [Whisper 32](http://www.ivory.org/whisper.html). (<http://www.ivory.org/whisper.html>) Sua função é produzir um arquivo que contém todas as suas senhas, criptografado. Também gera senhas fortes para você, sem haver a preocupação de ter que memorizá-las.

11 - Não use a mesma senha para propósitos diferentes. Se alguém descobrir uma senha sua e você tem o hábito de usá-la em vários serviços diferentes, a ameaça a sua segurança é maior do que se ela só servir para uma finalidade específica.

12 - Não forneça sua senha para quem peça apenas por se identificar como administrador ou técnico, peça prova de sua identidade.

13 - Não entre sua senha em um computador em que você não confie. Há possibilidade de haver instalado um programa do tipo "cavalo-de-tróia", que grava o que você digita e pode, assim, capturar sua senha.

14 - Troque sua senha periodicamente, de preferência a cada mês. Se alguém estiver usando sua senha sem sua autorização e conhecimento, vai ter um tempo limitado para usá-la em vez de ficar indefinidamente se passando por você.