

CSIRT POP-MG
Grupo de Resposta a Incidentes de Segurança do POP-MG
<http://www.csirt.pop-mg.rnp.br>
csirt@csirt.pop-mg.rnp.br

Como criar boas senhas

Alison Carmo Arantes
alison@csirt.pop-mg.rnp.br

Este documento foi produzido pelo CSIRT POP-MG e pode ser distribuído gratuitamente desde que os créditos de produção sejam exclusivos do CSIRT POP-MG.

Outubro de 2006

Sumário

1	Introdução	2
2	Regras para criar boas senhas	2
3	Técnicas para criar senhas seguras	3
3.1	Senhas Baseadas em Geometria do Teclado	3
3.2	Concatenação de palavras existentes	3
3.3	Letras de Frases	3
3.4	Construções Lógicas	4
4	Conclusão	4

1 Introdução

Com o crescimento da internet nos últimos anos, vários serviços tornaram-se on-line como: bancos, lojas e outros. A SENHA é um dos métodos mais usados hoje em dia para autenticação de usuários nestes tipos de serviços. Ter uma senha segura e difícil de ser quebrada hoje é fundamental para manter confiabilidade e confidencialidade dos dados transmitidos na grande rede.

Este pequeno tutorial tem por objetivo mostrar como construir senhas eficientes e seguras.

2 Regras para criar boas senhas

Para muitos usuários de computador, fica a impressão que senhas são conseguidas utilizando-se de alguma vulnerabilidade ou falha de um sistema computacional. Isso não deixa de ser verdade, mas a maioria das invasões bem sucedidas, estima-se 80% dos casos, ocorrem devido à senhas mal escolhidas.

Mas o que é considerado uma senha segura? Em linhas gerais, uma senha segura é uma senha que não é baseada em palavras de dicionário, possui caracteres especiais e principalmente, que seja de conhecimento apenas do próprio dono da senha.

Para se ter uma senha segura é aconselhável seguir as regras abaixo:

- Nunca use nomes ou números que possam ser descobertos facilmente por um estranho. Iso inclui: login, nome, nome do cachorro, nome de parentes, data de nascimento, data de nascimento de parentes, placa do carro, número de celular, RG, CPF, etc...
- Nunca use palavras como senhas baseadas em palavras de dicionários, incluindo dicionários estrangeiros como alemão, inglês, japonês e outros.
- Não usar variações das senhas mostradas acima como seu nome ao contrário, data de aniversário da sua namorada junto com a sua, palavra conhecida com letras minúsculas e maiúsculas, duplicadas ou palavras com números substituindo algumas letras, exemplo (paSSw2).
- A norma ISO 1779 recomenda senhas com no mínimo 6 caracteres. Senhas com 4 ou menos caracteres podem ser quebradas em poucas horas. Recomendamos senhas com no mínimo 8 caracteres.
- Nunca use a mesma senha em lugares diferentes. Se a sua senha do e-mail é descoberta, apenas seus e-mail estarão vulneráveis por exemplo.
- Nunca guarde senhas em papéis. Guarde suas senhas em sua mente.
- Evite senhas com apenas letras e números. Use caracteres especiais.
- Evite reutilizar ou reciclar senhas antigas
- Altere suas senhas regularmente, como a cada 3 meses, por exemplo;

- Não guarde senhas em arquivos do Word, Excel, TXT, etc. Use programas próprios para isso, de preferência, guarde em sua mente.
- Tome cuidado ao digitar sua senha perto de outras pessoas.
- Se for usar uma senha baseada em palavra conhecida e fizer alteração de letras por outros códigos, evite substituições do tipo a por @ 5 por s, etc.

3 Técnicas para criar senhas seguras

3.1 Senhas Baseadas em Geometria do Teclado

Um dos métodos para senhas muito utilizado. Basicamente, olha-se para o teclado e imagina-se uma figura geométrica e liga-se os pontos apertando os botões correspondentes à figura. Por exemplo, vc pode imaginar um triângulo com as letras SEFD e outro triângulo com as letras FTHG. Deve-se ter cuidado para não criar figuras como linhas retas, por exemplo, pois as ferramentas de quebra de senhas testam estas combinações. Outro cuidado que se deve tomar é que ninguém saiba que sua senha é baseada em figura geométrica pois se alguém quiser descobrir sua senha tentará enxergar o padrão da figura quando você estiver digitando. Sempre que possível, coloque caracteres especiais.

Exemplo:SeFd+FtHg

3.2 Concatenação de palavras existentes

Este método consiste na união de duas ou mais palavras e é interessante pois fica fácil de lembrar. Por exemplo, palavras como: **carro** e **envenenado** são palavras de dicionário mas juntando as duas, teremos **carroenvenenado**, uma palavra totalmente nova. Se colocarmos um caracter especial entre as duas palavras, como: **carro+envenenado** ou **carro\$envenenado** fica melhor ainda. Palavras como **!carro** ou **=envenenado** não são interessantes como senha, pois os programas de teste de senha podem facilmente fazer o teste de um caracter qualquer com uma palavra de dicionário. Variação deste método inclui colocar uma palavra dentro da outra, exemplo: ?envecarronenado?. Deve-se notar que neste método, é imprescindível que a senha tenha o maior número de caracteres possível, uma vez que decorá-la não é uma tarefa difícil. Recomendamos pelo menos 10 caracteres. Misturar letras maiúsculas e minúsculas e substituir letras por números ajuda muito a manter sua senha mais forte.

Exemplo:Carro+Envenenado

3.3 Letras de Frases

Este é um método muito eficiente e relativamente fácil de decorar e é o método preferido pois é fácil de lembrar e gera senhas muito eficientes. A idéia é a seguinte. Imagine um trecho de uma música, poesia, frase marcante, ditado popular. Pegue as primeiras letras de cada palavra da frase e está formada sua senha. Para melhorar,

pode-se alterar algumas letras por números ou caracteres especiais. Imagine a frase: E Deus disse: faça-se a luz. A senha poderia ser: `EDd:fal.`

3.4 Construções Lógicas

Este método basicamente é a criação de um algoritmo que gera a senha de acordo com uma palavra relativa ao local onde a senha está sendo criada. A vantagem deste método é que você pode decorar somente o algoritmo e aplicá-lo a todo lugar onde for criar sua senha. Imagine que vc está criando sua senha na loja ?submarino? e seu algoritmo é o que se segue: Pegue a primeira letra e transforme-a em maiúscula. As vogais viram caracteres especiais correspondentes no teclado: a é !, e é , i é #, o é \$ e u é %, as consoantes, serão sempre uma consoante a frente no alfabeto alternadas ora maiúscula, ora minúscula. Assim, nossa senha seria: `T%cN!s#O$` A desvantagem deste método é que se alguém descobrir seu algoritmo, descobre TODAS as suas senhas. Outra desvantagem é que você pode criar um algoritmo complexo e por isso, ficar pensando toda hora quando for digitar sua senha. `Exemplo:T%cN!s#O$`

4 Conclusão

A escolha de senhas fáceis e simples é um dos maiores problemas em segurança atualmente. De acordo com o SANS, a segunda maior vulnerabilidade em uma lista de 20.

Criar senhas eficientes é o princípio para manter seus dados seguros. Senhas complexas garantem que o invasor não tenha tempo disponível para quebrá-las.

Para finalizar, existe uma página da microsoft para testar a qualidade da sua senha:

http://www.microsoft.com/brasil/athome/security/privacy/password_checker.msp