

# Guia de como criar e manter uma boa senha

Por mais incômodo que possa ser a utilização de senhas, essa é ainda a forma mais utilizada de autenticação, para garantir que apenas pessoas autorizadas possam acessar serviços tais como os oferecidos por bancos, lojas, acessar suas contas de e-mail, o Portal da Ufrgs, etc. Escolher uma senha forte e manter ela segura é fundamental nesse processo.

## Riscos envolvidos em uma conta comprometida

*"Tá, mas a minha conta não tem nada de importante mesmo!"*

A frase parece familiar ? Ok, mas talvez isso não seja bem verdade...

- **Roubo de identidade** - Que tal alguém usar a sua conta para passar e-mails em seu nome, enviar spam, entrar em sites de relacionamento e se passar por você na rede?
- **Divulgação de dados pessoais** - E se seus e-mails pessoais se tornassem públicos? Ou mesmo as suas fotos ?
- **Divulgação/alteração de dados institucionais** - Não haveria problema se os seus e-mails, relatórios e dados do seu setor ou departamento acabasse nas mãos de terceiros ? E as notas dos alunos, questões de provas, etc ?
- **Envolvimento em atos ilícitos** - E se a sua conta "sem importância" for usada em ataques a outras instituições ? Ou mesmo no suporte a uma rede de pedofilia ? Lembre-se que se for feito um rastreamento, ele invariavelmente irá chegar até a sua conta.

Uma conta comprometida é sempre problema, para o seu responsável e/ou para a instituição que a hospeda, podendo acarretar grandes prejuízos e incomodação, até que o problema seja resolvido.

Já que temos mesmo que utilizar senhas de qualquer jeito, então é melhor escolher logo uma boa, certo ? Abaixo, estão algumas dicas do que fazer (e não fazer) para obter uma boa senha.

## O que não fazer ao se criar uma senha

É sempre bom conhecer as **péssimas idéias**, para poder evitá-las. O uso delas é bastante comum e levam sempre a senhas frágeis, expondo as respectivas contas ao risco de serem invadidas ou utilizadas de forma imprópria.

- **NÃO use o nome da sua conta**, duplicado, invertido, ou qualquer variação do mesmo.
- **NÃO use nada relacionado a quaisquer dados pessoais**, seja invertido, acrescido de um número, ou qualquer outra forma. Estão incluídos aí partes do próprio nome, endereço, data de nascimento, placa do carro, carteira de identidade, nome da namorada(o), do cachorro, do Timão, etc. Por que ? É barbada alguém levantar esses dados e acabar adivinhando a senha por tentativa e erro.
- **NÃO use nomes próprios**, seja de que forma for. Nomes de pessoas, cidades e países, por exemplo, já estão em listas ou dicionários eletrônicos, prontos para serem usados por programas próprios para isso.
- **NÃO use seqüências de caracteres triviais de serem decifradas**, como por exemplo

"12345", "qazwsx", etc. Essa última segue um padrão físico do teclado.

- **NÃO use nenhum nome ou termo que esteja em algum dicionário**, seja de que língua for. Estão incluídos aí termos usados em áreas específicas, tais como Star Wars, Lord of the Rings, e por aí vai. Também já existem listas ou dicionários eletrônicos com esses dados.
- **EVITE modificar palavras apenas substituindo "i" por "1", "o" por "0", "e" por "3", etc.** Essa técnica pode ser utilizada em combinação com outras, mas deve ser evitado usar apenas ela. Esse truque já é velho e tem programas que também levam isso em conta.

## Boas estratégias para se criar uma senha

Agora que sabemos o que não fazer para criar uma senha, aí vão algumas dicas do que pode (e deve) ser feito para obter uma boa senha. Geralmente uma combinação dessas dicas dão os melhores resultados.

---> **A palavra chave aqui é "CRIATIVIDADE" - Use e abuse dela!**

- **USE, como regra geral, no mínimo oito caracteres.** Quanto maior a senha, mais difícil é de adivinhar.
- **USE letras maiúsculas e minúsculas, números e, pelo menos, um caracter especial** (!@#\$%^\*()\_+=, etc). Evite repetição de caracteres. Isso complica mais ainda a vida de quem quer quebrar a senha.
- **USE as iniciais de uma frase** de tamanho adequado, contendo maiúsculas, minúsculas e mais algum caracter especial. Exemplo:

"Até que isso não é tão difícil assim" ---> &AQinetDA!

- **USE palavras curtas, modificadas**, contendo também números, ligadas por sinais de pontuação. Exemplos:

"me perdi" ---> Mi%Perd1?

"te acho demais" ---> Te-axoD+

"po de mico" ---> po'deMic0

- **INVENTE uma palavra sem significado, mas que seja sonora e fácil de lembrar**, aplicando também alguns modificadores. Exemplo:

faringel ---> faR!Ingel

**ATENÇÃO: É claro que nenhuma das senhas dos exemplos acima devem ser utilizadas !**

## Boas práticas no uso de senhas

Não basta criar uma boa senha. É preciso também saber cuidar delas e usá-las corretamente para que possam cumprir a sua função.

- **Use o bom senso na escolha da senha.** Não vai adiantar muito se a sua senha for grande e complicada, se você tiver que anotar ela por perto, porque nem você consegue se lembrar.
- **Não dê a sua senha para ninguém.** E isso significa também não compartilhar as suas

contas, seja com quem for. Lembre-se sempre que é você quem vai responder por ela, em caso de problemas.

- **Troque a sua senha periodicamente.** Novamente, use o bom senso quanto à periodicidade. "Senhas de estimação" geralmente dão encrenca, mais cedo ou mais tarde.
- **Troque a senha imediatamente** se, por qualquer motivo, desconfiar que outras pessoas podem ter tomado conhecimento dela. *Na dúvida, troque!*
- **Nunca use a mesma senha em outras contas.** Use senhas completamente diferentes e não apenas a mesma senha com uma pequena modificação. Assim, as suas outras contas não correrão risco, se uma delas for comprometida.
- **Não reutilize as suas senhas anteriores.**
- **Use programas de gerenciamento de senhas.** Você tem 25 senhas ?? Ok, talvez seja mesmo preciso anotá-las em algum lugar. Existem programas específicos que fazem isso. Nesses programas, uma senha "mestra" permite o acesso às demais, que ficam criptografadas em arquivo. O "**keepass**", por exemplo, é um dos programas desse tipo, disponíveis tanto para Windows quanto para Linux. Ele tem versão "portável" (não é preciso ser instalado no sistema), podendo ser usado a partir de um pendrive. *É bom redobrar os cuidados com a senha "mestra", já que a segurança das demais depende dela !!*
- **Mantenha seu computador livre de malware (vírus, spyware e outros bichos)!** Muitos deles monitoram o teclado e podem capturar as suas senhas, tornando inúteis todos os cuidados que você teve até agora, colocando em risco *todas* as suas contas.