Como criar senhas difíceis e memorizá-las.

Você consegue criar **senhas difíceis** para proteger seus dados na Internet? A grande rede trouxe para nós muitas soluções, mas também criou algumas novas dificuldades. Uma delas é a **segurança das informações** que disponibilizamos em diversos sites, e até hoje a maneira mais fácil de se obter acesso a esses dados é por meio de **logins e senhas**.

As senhas são chatas, mas extremamente necessárias. Bancos, cartões de crédito, e-mails, redes sociais e lojas *on-line* estão entre as principais aplicações que dependem delas, e não adianta utilizar senhas se elas podem ser **facilmente descobertas**.

A criação de senhas para serviços da internet exige cuidado e atenção do internauta, pois, por incrível que pareça, muitos ataques ainda acontecem porque usuários não criam **senhas seguras** o suficiente, e é exatamente por isso que este texto foi criado. Aqui você encontrará dicas para criar **senhas difíceis e seguras**, conhecerá **macetes para protegê-las**, orientações sobre **o que fazer** e **o que não fazer** além de algumas **dicas extras** muito interessantes.

Como NÃO criar senhas

1. Não crie senhas baseadas em sequências

Evite combinações como **12345678**, **abcdefgh**, **1020304050**, **abc123** e etc. Pode parecer uma dica meio óbvia, mas muitos problemas de segurança em empresas e serviços *on-line* ocorrem pelo uso de senhas assim, pois, quando um indivíduo mal-intencionado quer descobrir a senha de alguém, estes tipos de combinações **são as primeiras a serem testadas**.

2. Não use datas especiais, nomes e afins

Evite armadilhas comuns como suas iniciais, nomes de parentes, placa do seu carro, número de seu telefone, data de nascimento, cidade de nascimento, nome dos filhos ou qualquer outra **referência pessoal**, pois são informações facilmente conseguidas através da internet, usando as redes sociais por exemplo.

3. Evite utilizar senhas relacionadas aos seus gostos

As chances de uma pessoa criar uma senha com base em seus próprios gostos são grandes, pois quando alguém gosta muito de alguma coisa, normalmente deixa isso claro para todos ao seu redor. Portanto, evite usar o nome do seu time de coração, o nome da banda que você curte ou de seus músicos ou ainda utilizar nomes de livros que você goste como senha.

Como criar senhas difíceis e seguras

1. Misture letras, números e símbolos especiais

É importante que a senha seja alfanumérica: misturando letras, números e **caracteres ou símbolos especiais** como **asterisco (*)**, **exclamação (!)** e **interrogação (?)**. Os caracteres especiais dificultam a vida do usuário mal intencionado, pois ajuda a formar **combinações**

estranhas para dicionários de caracteres. Uma dica para ajudar a decorar este tipo de senha é utilizar uma palavra como base e substituir alguns de seus caracteres. Por exemplo, em vez de usar a palavra **internet** como senha, utilize **!nt3rn3+**. Desta forma, a palavra continua fazendo sentido para você e os caracteres substituídos podem ser decorados facilmente.

2. Utilize letras maiúsculas e minúsculas

Vários mecanismos de autenticação são **"*case sensitive*"**, ou seja, tratam letras maiúsculas e minúsculas como **caracteres diferentes**, e senhas que envolvem estas duas características são **mais seguras**. Esta dica pode ser explorada de várias maneiras: você pode definir que todas as consoantes em uma senha sejam maiúsculas e as vogais minúsculas; ou, então, em vez de colocar a primeira letra em maiúscula, como fazemos com nomes, coloque a segunda ou a terceira. Combinando esta orientação com a dica anterior (misturar letras, números e símbolos especiais), você criará uma senha muito mais segura.

3. Use uma quantidade de caracteres superior ao recomendado

Ao criar uma senha, utilize sempre uma quantidade de caracteres superior ao mínimo exigido, por exemplo, se o site em que você está criando uma senha informa que o mínimo de caracteres é 8 (oito), utilize 9 (nove) ou mais caracteres, pois, cada caractere que você adiciona em sua senha torna a sua **descoberta mais difícil**, até mesmo para **programas** criados especialmente para essa finalidade.

4. Crie senhas que utilize as duas mãos para digitar

Não é uma dica muito importante, mas tem sua utilidade em algumas situações. Por exemplo, se você estiver em um **computador público**, alguém pode tentar decorar a sua senha apenas observando suas mãos enquanto você digita. Não é fácil ter sucesso com esta prática mas não é impossível, e por isso, procure criar senhas com **letras bem distribuídas**, de forma que você tenha que utilizar as duas mãos.

Por exemplo, na combinação **14catarata**, você poderá digitá-la apenas com a mão esquerda. Já na combinação **20cogumelo**, terá que digitar usando as duas mãos. Com isso, a pessoa que estiver tentando olhar sua senha enquanto você digita terá mais dificuldade para identificá-la.

5. Use métodos para criar suas senhas e não esquecê-las

Essa dica talvez seja a mais interessante e importante deste texto: **é recomendável que você crie uma senha diferente para cada serviço**, isto é, sua senha do **Facebook** não pode ser igual a do **Twitter**. O grande problema é que você será obrigado a decorar uma grande variedade de combinações. Mas há como fazer isso de maneira **simples e muito eficiente**: criando senhas com base em métodos.

Veja alguns métodos:

Método 1:

- Escolha uma frase
- Retire a primeira letra de cada palavra
- Adicione alguns números e símbolos.

Exemplo:

- **T**enho **v**ários **a**migos **n**o **F**acebook
- O que dá: **TvanF**
- Adicione números e símbolo: Tvan329F&

Desta forma, a senha é longa e praticamente inacessível aos ataques de "dicionário" e você pode lembrá-la facilmente a partir da frase.

Método 2:

Você pode pegar o refrão de uma música que gosta muito e usar a primeira letra ou sílaba de cada palavra e alternar entre maiúsculas, minúsculas e caracteres especiais.

Exemplo:

Somos **o** **f**uturo **d**a **n**ação, **g**eração **C**oca-**C**ola

Pegamos como exemplo o trecho da música "Geração Coca-Cola", do Legião Urbana. Com as letras iniciais, destacadas em negrito, foi possível criar: **SoFdNgCc@**

Para dificultar um pouco mais, pode-se trocar letras por números. A letra "o" pelo número "0" ou "S" pelo número "5", por exemplo.

Método 3:

- Escolha duas palavras que você é capaz de lembrar facilmente. Exemplo "**computador**" e "**internet**".
- Depois, "**numerize**" essas palavras, trocando as vogais pelos respectivos números semelhantes: "c0mput4d0r" e "1nt3rn3t".
- Agora vamos colocar a segunda palavra toda em maiúsculas. Teremos: "1NT3RN3T".
- Vamos unir as palavras colocando-as intercaladas letra por letra. Colocaremos a primeira palavra em azul e a segunda em vermelho para um melhor entendimento: "c 0 m p u t 4 d 0 r" + "1 N T 3 R N 3 T" = "c10NmTp3uRtN43dT0r".

Os métodos apresentados são apenas exemplos. A ideia é que você explore a sua criatividade e monte seus próprios métodos.

Como proteger as suas senhas

1. **Guarde suas senhas na mente**. Evite escrever suas senhas em pedaços de papel ou arquivos eletrônicos desprotegidos. Se for realmente necessário escrever, apenas escreva a senha, não informe o que aquela combinação significa.
2. Não use a opção de "**lembrar senha**" em computadores públicos.
3. Sempre clique em Sair, *Logoff* ou equivalente.
4. Se possível, não utilize suas senhas mais importantes (como de sua conta bancária) em computadores públicos ou redes desconhecidas. Também evite usar suas senhas em redes *WiFi* que você desconhece.
5. **Verifique se você está digitando a senha no campo correto**. Tome cuidado para não digitar sua senha no lugar errado, por exemplo, no campo "Login". Se isso acontecer, uma pessoa próxima a você conseguirá ler o que você escreveu, já que somente o campo de senha é protegido.
6. **Mude sua senha periodicamente**, pelo menos a cada três meses.
7. Não use a mesma senha para vários serviços.
8. Não use perguntas com respostas óbvias. A ideia é fornecer uma pergunta que **somente você** saiba a resposta.
9. **Jamais compartilhe as suas senhas**, mesmo com gente íntima.
10. Cuidado com e-mails ou sites falsos que pedem sua senha.

Dicas Extras

Separamos 3 **dicas** extras **maravilhosas** para ajudar você com suas senhas e principalmente com a segurança de suas informações.

Dica Extra 1: Wireless Key Generator

É um programa capaz de criar senhas usando diferentes forças e números de caracteres. Fácil de usar, possui várias opções de criação e possui uma interface intuitiva. Com ele é possível escolher entre os métodos de criptografia WEP e WPA para criar senhas que variam entre 8 e 63 caracteres. Além disso, também é possível salvar as sequências desenvolvidas em **arquivo TXT** na Área de trabalho.

Wireless Key Generator

Dica Extra 2: Passpack

É um serviço de gerenciamento de senhas que permite criar *logins* descartáveis, ideias para acessar e-mails e outros serviços em redes públicas como *lan house* e *cibercafés*. Basta criar uma conta no *Passpack* e cadastrar os serviços desejados. Depois, na aba *Security*, clique em *Disposable Login*. Pressione o botão *Generate* e escolha o número de *logins* que serão criados e o prazo de expiração de cada um. O resultado final é uma lista de senhas com expiração definida. Usando essas senhas, acesse o endereço **www.passpack.com** e faça o *login* seguro nos serviços cadastrados.

Passpack

Dica Extra 3: LastPass

É um gerenciador de senhas, onde você cria senhas complexas e as armazena (sem precisar decorá-las) e, no momento de usá-las, ative um recurso de autopreenchimento. Desse modo, na maioria das vezes você precisa apenas decorar a senha do gerenciador.

LastPass ⬇

Note que, os **gerenciadores de senhas** são ferramentas computacionais, ou seja, **não estão isentos a falhas**. As chances de algum problema de segurança ocorrer são pequenas, mas exitem.