OUCH! | Maio de 2013

A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO..

Senhas

Contexto

A senha é uma das maneiras mais utilizadas para provarmos quem nós somos. É através dela que você acessa seu e-mail, banco on-line, compra bens e também obtém acesso à dispositivos, tais como seu notebook ou smartphone. De muitas maneiras, as senhas são as chaves para o seu reino. Como resultado, se alguém souber a sua senha, eles podem roubar sua identidade, transferir o seu dinheiro ou acessar todas as suas informações pessoais. Senhas fortes são essenciais para proteger a sua identidade e informações. Vamos aprender o que torna uma senha forte e como usá-las de forma segura.

Editor Convidado

Raul Siles é o editor convidado para esta edição de OUCH! Raul é o fundador e analista sênior de segurança da Taddong e também um dos autores do SANS, instrutor de segurança e um apaixonado pelo tema. Você pode seguir o Raul no Twitter em **@taddong** e em seu blog na **blog.taddong.com**.

Senhas Fortes: Frases como senhas

O problema é que os criminosos virtuais têm desenvolvido programas sofisticados que podem adivinhar ou encontrar a sua senha por "força bruta". E eles estão ficando cada vez melhores nisso. Significa dizer, que eles podem roubar suas senhas, se elas forem fracas ou fáceis de se adivinhar. Nunca use informações fáceis ou óbvias para suas senhas, como sua data de nascimento, nome do seu animal de estimação ou de qualquer outra coisa que pode ser facilmente determinada a partir de suas mensagens nas redes sociais ou pelo Google. Em vez disso, a melhor maneira de criar uma senha forte é a utilização de uma senha longa. E quanto mais caracteres, melhor. Na verdade, em vez de usar uma única palavra, use várias palavras - ou mesmo uma frase completa. Este tipo de senha é chamada de "passphrase" (algo como "senha por frase") e é uma das senhas mais fortes que você pode usar. Vamos ver um exemplo de uma:

pausa para o cafe

É isso, isto é tudo que você precisa. Se necessário, você pode fazer a sua senha ainda mais forte adicionando símbolos, letras maiúsculas e números, como aqueles que você vê no exemplo abaixo. Isto é especialmente importante se você estiver usando um site que não permite que várias palavras ou uma frase completa seja sua senha. Veja o exemplo a seguir:

P@us@ p@r@ 0 c@fe!

Senhas

Observe como este exemplo anterior usa uma letra maiúscula e também substitui letras por números ou símbolos. Você pode por exemplo substituir em suas senhas a letra ‘a’ com o símbolo ‘@’ e a letra ‘o’ com o número zero, ou usar sinais de pontuação comuns, como um ponto de interrogação, exclamação, vírgula ou mesmo espaços. Se um site ou programa limita o número de caracteres que você pode usar em uma senha, utilize o número máximo de caracteres permitidos.

Use senhas fortes, de preferência senhas compostas de várias palavras, e não se esqueça de utilizá-las de forma segura.

Usando Senhas com Segurança

Além de usar senhas fortes, você deve ter cuidado como você as usa. Ter uma senha forte não adianta muito se elas puderem ser facilmente roubadas ou copiadas.

1. Certifique-se de usar senhas diferentes para contas diferentes. Por exemplo, nunca use as senhas do seu trabalho ou contas bancárias como senhas de suas contas pessoais, como o Facebook, YouTube ou Twitter. Dessa forma, se uma de suas senhas é descoberta, as outras contas ainda são seguras. Se você tem muitas senhas para lembrar, considere o uso de um gerenciador de senhas, que nada mais é do que um programa especial que você executa em seu computador ou dispositivo móvel e que armazena para você com segurança todas as suas senhas. As senhas que você precisará lembrar são as senhas para acessar o seu computador ou dispositivo móvel e para acessar o programa gerenciador de senhas. Se as senhas são para o trabalho, então verifique com seu supervisor ou com a equipe de suporte se a utilização de um programa gerenciador de senhas é permitida dentro de sua organização;

2. Nunca compartilhe sua senha com ninguém, incluindo colegas de trabalho. Lembre-se que sua senha é um segredo, se alguém souber a senha ela não é mais segura. Se você acidentalmente compartilhar sua senha com alguém ou acreditar que ela pode ter sido comprometida ou roubada, não se esqueça de mudá-la imediatamente;

3. Não use computadores públicos, como os de hotéis ou bibliotecas, para entrar em uma conta de trabalho ou do banco. Como qualquer pessoa pode usar esses computadores, eles podem estar infectados com algum código malicioso que captura tudo o que é digitado. Somente faça login para o seu trabalho ou em contas bancárias em computadores confiáveis ou dispositivos móveis que você controla;

4. Tenha cuidado com sites que exijem que você responda perguntas pessoais. Estas perguntas são usadas se você esquecer sua senha e precisar redefini-la. O problema é que as respostas a estas perguntas muitas vezes podem ser encontrados na Internet, ou mesmo na sua página do Facebook. Tenha certeza de que se você responder a

Senhas

perguntas pessoais, esteja usando somente informação que não é disponível públicamente ou que seja fictícia, que você inventou. Gerenciadores de senhas podem ajudar com isso também, pois muitos permitem que você armazene estas informações adicionais;

5. Muitas contas on-line oferecem algo chamado autenticação de dois fatores, ou verificação em duas etapas. Este é o lugar onde você precisa de mais do que apenas a sua senha para efetuar o login, uma informação adicional como códigos enviados para o seu smartphone é necessária. Esta opção é muito mais segura do que apenas uma senha, por si só. Sempre que possível, use esses métodos mais fortes de autenticação;

6. Dispositivos móveis geralmente exigem um PIN para proteger o acesso a eles. Lembre-se que um PIN nada mais é do que uma outra senha. Quanto maior o seu PIN, mais seguro ele é. De fato, muitos dispositivos móveis permitem alterar o seu número PIN para uma senha propriamente dita.

7. Finalmente, se você não estiver mais usando uma conta, certifique-se de fechá-la, excluí-la ou desativá-la;

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Verificação em duas etapas:	http://www.google.com/landing/2step
Gerenciadores de senhas (em Inglês):	http://www.freepasswordmanager.com
Senhas Fortes:	http://cartilha.cert.br/senhas/
Glossário de segurança:	http://cartilha.cert.br/glossario/
SANS - Dicas de Segurança do Dia (em Inglês):	http://preview.tinyurl.com/6s2wrkp

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser