A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Frases Secretas

Contexto

As senhas são algo que você usa quase todos os dias, para acessar seu e-mail e serviços bancários on-line, para aquisição de bens ou acessar seu smartphone. No entanto as senhas são também um dos seus pontos mais fracos, pois se alguém as descobre poderá roubar sua identidade, transferir seu dinheiro ou acessar suas informações pessoais. Senhas fortes são essenciais para proteger a si mesmo. Neste boletim, você vai aprender como criar senhas fortes que são fáceis de lembrar, usando um tipo de senha chamado Frases Secretas.

Editor Convidado

Guy Bruneau é consultor de segurança sênior da IPSS Inc., instrutor do SANS e analista do ISC. Guy é certificado SANS GSE e completou o programa SANS Cyber Guardian. Você pode acompanhar Guy no Twitter em**GuyBruneau** e em **handlers.sans.org/gbruneau**.

Frases secretas

O desafio que todos nós enfrentamos é que os atacantes cibernéticos desenvolveram métodos sofisticados de adivinhar nossas senhas, os chamados ataques de “força bruta”, e eles estão constantemente melhorando o que fazem. Isto significa que eles podem comprometer suas senhas se elas forem fracas ou faceis de adivinhar. Um passo importante para se proteger é usar senhas fortes. Quanto mais caracteres sua senha tiver, mais forte ela é e mais difícil será para um atacante adivinhar. No entanto senhas longas e complexas podem ser difíceis de lembrar. Então, em vez disso, recomendamos que você use frases secretas, que são frases simples ou expressões fáceis de lembrar, mas difícil de descobrir. Veja um exemplo:

Onde está o rei Julian?

O que torna essa frase tão forte não é só ter 21 caracteres de comprimento, mas usar letras maiúsculas e símbolos (lembre-se que espaços e pontuação são símbolos). Você pode tornar a sua senha ainda mais forte se você trocar letras por números ou símbolos, como substituir a letra ‘a’ com o símbolo “@” ou a letra “o” com o número zero. Se um site ou programa limita a quantidade de caracteres que você pode usar em uma senha, utilize o número máximo de caracteres permitidos.

Usando frases secretas de forma segura

Você também deve proteger suas Frases Secretas. Usar uma Frase Secreta não vai ajudar se os bandidos puderem roubá-la ou copiá-la facilmente.

Frases Secretas

1. Certifique-se de usar uma Frase Secreta diferente para cada conta ou dispositivo que você tem. Por exemplo, nunca use a Frase Secreta do seu trabalho ou conta bancária nas suas contas pessoais, como o Facebook, YouTube ou Twitter. Dessa forma, se uma de suas contas é invadida, as outras contas ainda estarão seguras. Se você tem muitas Frases Secretas para lembrar (o que é muito comum), considere o uso de um Gerenciador de Senhas (Password Manager). O Gerenciador de Senhas é um programa especial que armazena de forma segura todas as suas Frases Secretas para você. Assim, as únicas Frases Secretas que você precisará lembrar são as do seu computador e do Gerenciador de Senhas;

2. Nunca compartilhe uma Frase Secreta ou a sua estratégia de criação de frases secretas com outra pessoa, incluindo colegas de trabalho. Lembre-se, uma Frase Secreta é um segredo; se alguém sabe sua Frase Secreta, ela não é mais segura. Se você compartilhar acidentalmente a frase-senha com outra pessoa, ou acreditar que ela possa ter sido comprometida ou roubada, mude-a imediatamente;

Usar Frase Secretas é uma das medidas mais eficazes que você pode tomar para proteger sua identidade e informações.

3. Assim como na criação de senhas, evite usar frases secretas fáceis de adivinhar ou comumente usadas. Por exemplo, a frase “essa é minha senha” não é uma boa frase secreta, pois é fácil de adivinhar;

4. Não use computadores públicos, como os que estão em hotéis ou bibliotecas, para fazer login em uma conta de trabalho ou banco. Como qualquer pessoa pode usar esses computadores, eles podem estar infectados com código malicioso que captura todas as teclas digitadas, como um “grampo de teclado”. Apenas faça o login para o seu trabalho ou contas bancárias em computadores confiáveis ou dispositivos móveis;

5. Tenha cuidado com sites que exigem que você responda a perguntas pessoais. Estas perguntas são usadas se você esquecer a senha e precisar redefini-la. O problema é que as respostas a estas perguntas podem ser encontradas na Internet, ou até mesmo em sua página no Facebook. Certifique-se de responder perguntas pessoais apenas com informações que não estão disponíveis publicamente ou informações fictícias que você tenha inventado. Gerenciadores de Senha podem ajudar com isso, pois muitos permitem armazenar também estas informações adicionais;

6. Muitas contas on-line oferecem algo chamado de autenticação de dois fatores, também conhecida como a verificação em duas etapas. Significa que você precisa de mais uma etapa além de fornecer a frase secreta, para fazer o login (se autenticar), como digitar um código secreto enviado ao seu smartphone. Esta opção é muito mais segura do que a utilização da frase secreta sozinha. Sempre que possível use esses métodos mais fortes de autenticação;

Frases Secretas

7. Os dispositivos móveis (smartphones, tablets) muitas vezes são configurados para exigir um PIN para acessá-los. Lembre-se que um PIN não é nada mais que uma outra senha. Quanto maior for o número PIN, mais seguro ele é. Muitos dispositivos móveis permitem que você mude o seu número PIN para uma Frase Secreta;

8. Finalmente, se você já não estiver usando uma conta, não se esqueça de fechar, excluir 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
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

Verificação em duas etapas:	http://www.securingthehuman.org/ouch/2013#august2013
Gerenciadores de Senha s:	http://www.securingthehuman.org/ouch/2013#october2013
Engenharia Social:	http://www.securingthehuman.org/ouch/2014#november2014
Termos comuns de Segurança:	http://www.securingthehuman.org/resources/security-terms

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