OUCH! | Abril de 2017

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Frases de Acesso

Conhecimento/Experiência

Senhas são algo que você usa quase todos os dias, seja para acessar seu e-mail ou banco on-line ou para comprar bens ou acessar seu smartphone. No entanto, as senhas também são um de seus pontos mais fracos. Se alguém obtém ou descobre sua senha, ele pode acessar suas contas como você, permitindo-lhe transferir seu dinheiro, ler seus e-mails ou roubar sua identidade. É por isso que senhas fortes são essenciais para se proteger. No entanto, as senhas costumam ser confusas, difíceis de lembrar e difíceis de digitar. Neste boletim você aprenderá como criar senhas fortes que são fáceis de lembrar e simples de digitar - chamadas frases de acesso.

Editor Convidado

My-Ngoc Nguyen (se pronuncia Me-Nop Wynn) é instrutora Certificada SANS e CEO / Consultora Principal para Soluções de Segurança de TI. Ela traz experiência com certificações top/superiores e mais de 14 anos de desenvolvimento, amadurecimento e gerenciamento de programas de segurança cibernética para várias indústrias e setores. Twitter: **@MenopN** LinkedIn: My-Ngoc ”Menop” Nguyen.

Frases de Acesso

O desafio que todos enfrentamos é que os invasores cibernéticos desenvolveram métodos sofisticados e eficazes de adivinhação automática de senhas, conhecidos como força bruta. Significa que os bandidos podem comprometer suas senhas se elas forem fracas ou fáceis de adivinhar. Um passo importante para se proteger é usar senhas fortes. Normalmente isso é feito através da criação de senhas complexas, no entanto, estas podem ser difíceis de lembrar, confusas e difíceis de digitar. Em vez disso, recomendamos que você use frases de acesso, que pode ser uma série de palavras aleatórias ou uma frase. Quanto mais caracteres tiver sua senha, mais forte ela será. A vantagem é que são muito mais fáceis de lembrar e digitar, mas ainda difícil para os atacantes cibernéticos descobrirem. Aqui estão dois exemplos diferentes:

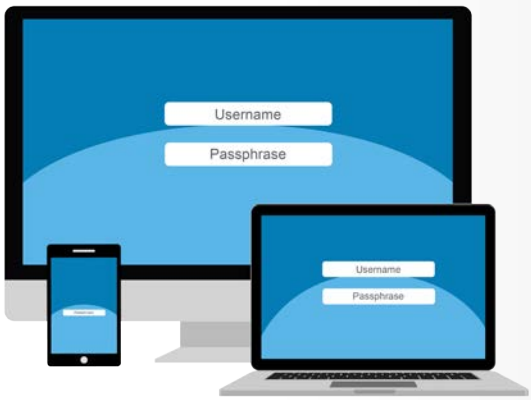
Sustentar-Facilmente-Detenção
Hora-do-chá 1:23

O que torna essas frases de acesso tão fortes não é só o fato de serem longas, mas usarem também letras maiúsculas e símbolos (lembre-se: espaços e pontuação são símbolos). Ao mesmo tempo, essas frases de acesso também são fáceis de lembrar e digitar. Você pode tornar sua senha ainda mais forte se substituir letras por números ou símbolos, como substituir a letra ‘a’ pelo símbolo ‘@’. Ou a letra ‘o’ pelo número zero. Se um site ou programa limitar o número de caracteres que você pode usar em uma senha, use o número máximo de caracteres permitido.

Frases de Acesso

Use sua frase de acesso com segurança

Você também deve ter cuidado ao usar frases de acesso. Usar uma frase de acesso não ajudará se os invasores cibernéticos puderem facilmente roubá-la ou copiá-la.



Frase de acesso é uma maneira simples de lembrar e criar senhas fortes.

1. Use uma senha diferente para cada conta ou dispositivo que você tem. Por exemplo, nunca use a mesma frase de acesso do seu trabalho ou conta bancária para suas contas pessoais, como Facebook, YouTube ou Twitter. Desta forma, se uma das suas contas for invadida, as outras contas continuarão seguras. Se você tem muitas frases de acesso para lembrar (o que é muito comum), considere o uso de um gerenciador de senhas. O gerenciador de senhas é um programa especial que armazena com segurança todas as frases de acesso para você. Dessa forma, as únicas frases de acesso que você precisa lembrar são aquelas para o seu computador ou dispositivo e para o programa gerenciador de senhas;
2. Nunca compartilhe uma frase de acesso ou sua estratégia de criação de frases secretas com outra pessoa, incluindo colegas de trabalho ou seu supervisor. Lembre-se: uma frase de acesso é um segredo. Se alguém conhece sua senha, ela não é mais segura. Se você compartilha acidentalmente uma frase de acesso com outra pessoa ou acredita que sua frase de acesso pode ter sido comprometida ou roubada, altere-a imediatamente. A única exceção é se você quiser compartilhar suas frases de acesso pessoal com um membro da família altamente confiável em caso de emergência. Uma abordagem é anotar suas frases de acesso pessoais (certifique-se de que elas não estão relacionadas ao trabalho), armazene-as em um local seguro e compartilhe esse local com um membro da família altamente confiável. Dessa forma, se algo acontecer com você e você precisar de ajuda, seus entes queridos podem acessar suas contas importantes;
3. Não use computadores públicos, como aqueles em hotéis ou cafés, para fazer login em suas contas. Uma vez que qualquer pessoa pode usar esses computadores, eles podem ser infectados e capturar todas as suas teclas digitadas. Faça login em suas contas utilizando apenas computadores ou dispositivos móveis confiáveis;
4. Tenha cuidado com sites que exigem que você responda a perguntas pessoais. Essas perguntas são usadas se você esquecer sua senha e precisar redefini-la. O problema é que as respostas a essas perguntas podem frequentemente ser encontradas na Internet, ou mesmo na sua página do Facebook. Certifique-se de que, se responder às perguntas pessoais, utilize apenas informações que não são publicamente disponíveis ou informações fictícias criadas por você. Não consegue se lembrar de todas as respostas para as perguntas de segurança? Selecione um tema como um

Frases de Acesso

personagem de filme e baseie suas respostas nesse personagem. Outra opção é mais uma vez usar um gerenciador de senhas, a maioria deles permite que você também armazene com segurança esta informação adicional;

5. Muitas contas on-line oferecem algo chamado autenticação de dois fatores, também conhecida como verificação em duas etapas. É aqui que você precisa de mais do que apenas sua senha para efetuar login, como um código de acesso enviado para seu smartphone. Esta opção é muito mais segura do que apenas uma frase de acesso por si só. Sempre que possível, habilite e use esses métodos mais fortes de autenticação;
6. Os dispositivos móveis geralmente exigem um PIN para proteger seu acesso. Lembre-se de que um PIN não é nada mais do que outra senha. Quanto mais longo for o PIN, mais seguro será. Muitos dispositivos móveis permitem que você altere o seu número PIN para uma frase de acesso ou use um meio biométrico, como sua impressão digital;
7. 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 securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop

Marta Visser – Tradutora autônoma

Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Gerenciadores de Senhas:	https://securingthehuman.sans.org/ouch/2015#october2015
Verificação em Duas etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Bloqueie seu login (em Inglês):	https://lockdownyourlogin.com
SANS SEC301 - Curso de cinco dias sobre segurança cibernética:	https://sans.org/sec301

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser