A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Cinco Passos para Ficar Seguro

Visão Geral

A medida que a tecnologia ganha um papel mais importante em nossas vidas, ela também cresce em complexidade. Dada a rapidez com que a tecnologia muda, manter-se atualizado com as recomendações de segurança pode ser confuso. Parece que há sempre novas orientações sobre o que você deve ou não fazer. No entanto, embora os detalhes de como se manter seguro possam mudar ao longo do tempo, há coisas fundamentais que você sempre pode fazer para ajudar a proteger-se. Independentemente da tecnologia que você está usando ou onde estiver usando, recomendamos as seguintes cinco etapas fundamentais.

Editor Convidado

Lenny Zeltser se concentra em proteger as operações de TI dos clientes da NCR Corp e ensina a combater malware no Instituto SANS. Lenny está ativo no Twitter como **@lennyzeltser** e escreve um blog sobre segurança no **blog.zeltser.com**.

Cinco etapas fundamentais

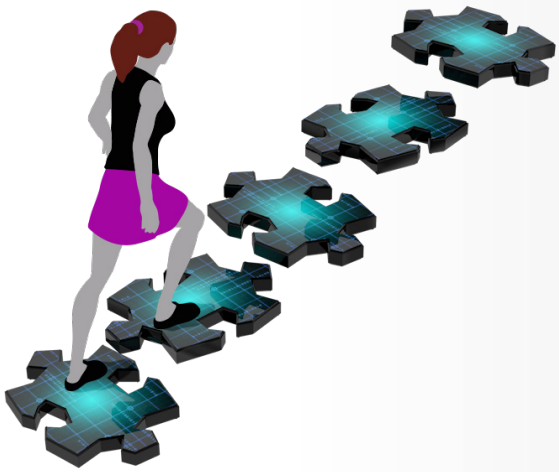
Cada um dos cinco passos a seguir é uma descrição simples. Para saber mais sobre cada passo, consulte a seção Recursos ao final deste boletim.

1. **Você**: Em primeiro lugar, tenha em mente que a tecnologia por si só não pode protegê-lo. Os agressores descobriram que a maneira mais fácil para contornar a tecnologia de segurança é atacar você. Se eles querem a sua senha ou seu cartão de crédito a coisa mais fácil para eles é induzi-lo a dar-lhes esta informação. Por exemplo, eles podem chamá-lo fingindo ser o suporte técnico da Microsoft alegando que seu computador está infectado, quando na realidade eles são apenas cyber criminosos que querem que você dê acesso a eles. Ou talvez eles possam enviar-lhe um e-mail explicando que sua encomenda não pôde ser entregue e pedir para você clicar em um link para confirmar seu endereço, quando na realidade eles querem que você visite um site malicioso que irá invadir seu computador. Em última análise, a maior defesa contra os invasores é você. Desconfie usando o bom senso, assim você pode detectar e impedir a maioria dos ataques;

2. **Atualização**: Certifique-se de que seus computadores, dispositivos móveis, aplicativos e tudo mais que estiver conectado a uma rede esteja executando a versão mais recente de software. Cyber criminosos estão constantemente à procura de vulnerabilidades nas tecnologias que você usa. Quando descobrem essas fraquezas, eles usam programas especiais para explorar a vulnerabilidade e invadir qualquer tecnologia que você esteja usando, incluindo sua rede, o seu computador e dispositivos móveis. Enquanto isso, as empresas que criaram a tecnologia que você está usando trabalham duro para mantê-la atualizada. Uma vez que uma vulnerabilidade é conhecida, eles criam uma atualização

Cinco Passos para Ficar Seguro

para corrigi-la e a liberam para o público. Ao assegurar que os seus computadores e dispositivos móveis tenham essas atualizações, você reduz o número de vulnerabilidades conhecidas, o que torna muito mais difícil alguém hackear você. Para ficar atualizado, ative a atualização automática sempre que possível. Esta regra aplica-se a quase todas as tecnologias ligadas a uma rede, incluindo Televisores conectados à Internet, babá eletrônica, roteadores domésticos, consoles de jogos ou um dia, talvez, até mesmo o seu carro. Se o sistema operacional do seu computador, dispositivo móvel ou qualquer outra tecnologia que você está usando não é mais suportado e não receberá mais nenhuma atualização, recomendamos que você mude para uma nova versão que seja suportada;



Ao seguir estes cinco passos-chave, você terá um longo caminho de segurança, aproveitando a tecnologia mais recente.

3. **Senhas**: O próximo passo para se proteger envolve o uso de uma senha forte, única para cada um dos seus dispositivos, contas e aplicações online. As palavras-chave são forte e única. Uma senha forte significa que não pode ser facilmente descoberta por hackers ou por seus programas de quebra de senha. Em vez de uma palavra única, use uma frase longa com várias palavras com alguns símbolos e números de forma balanceada. Única significa usar uma senha diferente para cada dispositivo e conta on-line. Dessa forma, se uma senha for comprometida, todas as suas outras contas e dispositivos ainda estarão seguros. Não consigo me lembrar de todas essas senhas fortes e únicas? Não se preocupe, nós também não. É por isso que recomendamos que você use um gerenciador de senhas, que é uma aplicação especializada para seu smartphone ou computador que pode armazenar de forma segura todas as suas senhas em um formato criptografado. Finalmente, se qualquer de suas contas suportar a verificação em duas etapas, recomendamos sempre habilitá-la, pois esta é uma das formas mais seguras de proteger a sua conta;

4. **Criptografia**: A terceira etapa que recomendamos é o uso de criptografia. A criptografia garante que somente você ou as pessoas que você confia possam acessar suas informações. Os dados podem ser criptografados em dois lugares: em repouso e em movimento. A criptografia de dados em repouso significa protegê-los quando eles são armazenados como arquivos, como no seu disco rígido ou de um dispositivo USB. A maioria dos sistemas operacionais permite que você criptografe automaticamente todos os seus dados usando recursos como Criptografia completa do disco. Recomendamos que você a habilite sempre que possível. A criptografia de dados em movimento significa a criptografia de dados quando é transmitida a partir do seu computador ou dispositivo para outros computadores, tais como quando você está acessando seu banco online. Uma maneira simples de verificar se a criptografia está ativada quando você está navegando é certificar-se de que o endereço do site que você está visitando começa com “https:” e tem a imagem de um cadeado fechado ao lado dele;

Cinco Passos para Ficar Seguro

5. **Backups**: Às vezes, não importa o quão cuidadoso você seja, um dos seus dispositivos ou contas pode ser comprometida. Se for esse o caso, muitas vezes a única opção para garantir que o seu computador ou dispositivo móvel esteja livre de malware é para limpá-lo completamente e reconstruí-lo a partir do zero. O atacante pode até mesmo impedir que você acesse seus arquivos pessoais, fotos e outras informações armazenadas no sistema comprometido. Sua única opção pode ser restaurar todas as suas informações pessoais a partir do backup. Certifique-se de que você está fazendo backups regulares de todas as informações importantes e faça testes regulares para verificar se é possível restaurar seus dados a partir desses backups. A maioria dos sistemas operacionais e dispositivos móveis suportam backups automáticos.

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

Ataques phishing e-mail:	http://www.securingthehuman.org/ouch/2013#february2013
Mantendo seu tablet seguro:	http://www.securingthehuman.org/ouch/2013#december2013
Senhas fortes:	http://www.securingthehuman.org/ouch/2013#may2013
Gerenciadores de senhas:	http://www.securingthehuman.org/ouch/2013#october2013
Verificação em duas etapas:	http://www.securingthehuman.org/ouch/2013#august2013
Criptografia:	http://www.securingthehuman.org/ouch/2014#august2014
Backups:	http://www.securingthehuman.org/ouch/2013#september2013

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