SANS SECURITY AWARENESS

OUCH! | Janeiro de 2018

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- Senhas
- O que é Autenticação de Dois Fatores
- Como ela funciona

Criando um Lar Ciberneticamente Seguro

Visão Geral

Vários anos atrás, criar uma casa ciberneticamente segura era simples. A maioria das casas consistia em nada mais do que uma rede sem fio e vários computadores. Hoje, a tecnologia tornou-se muito mais complexa e está integrada em todas as partes de nossas vidas, desde dispositivos móveis e consoles de jogos até seu termostato doméstico, e até talvez sua geladeira. Aqui estão quatro passos simples para criar um lar ciberneticamente seguro.

Editor Convidado

Matt Bromiley é um analista de incidentes durante o dia, onde ajuda clientes de todos os tipos a lidar com violações de dados. Ele também é instrutor do SANS e ensina FOR508, o curso de Forense Digital Avançada e Resposta a Incidentes. Siga Matt em **@mbromileyDFIR**.

Sua rede sem fio

Quase todas as redes domésticas começam com uma rede sem fio (ou Wi-Fi). Ela é que permite que todos os seus dispositivos se conectem à Internet. A maioria das redes sem fio em casa são controladas pelo seu roteador de Internet ou de um ponto de acesso sem fio separado. Ambos funcionam da mesma forma através da transmissão de sinais sem fio, utilizados pelos dispositivos em sua casa para se conectarem. Isso significa que proteger sua rede sem fio é uma parte fundamental da proteção de sua casa. Recomendamos as seguintes etapas para protegê-la:

- Mude a senha padrão de administrador do seu roteador de Internet ou ponto de acesso sem fio, seja qual for o equipamento que controle sua rede sem fio. A conta de administrador é que permite que você defina as configurações para sua rede sem fio;
- Certifique-se de que apenas pessoas que você confia podem se conectar à sua rede sem fio. Faça isso habilitando uma segurança forte. Atualmente, a melhor opção é usar o mecanismo de segurança chamado WPA2. Ao habilitá-lo, torna-se necessária uma senha para que as pessoas se conectem à sua rede doméstica e, uma vez conectadas, suas atividades on-line são criptografadas;
- Certifique-se de que a senha usada para se conectar à sua rede sem fio é uma senha forte e que é diferente da senha do administrador. Lembre-se de que você só precisa inserir a senha uma vez para cada um de seus dispositivos, pois eles armazenam e lembram a senha;
- Muitas redes sem fio suportam o que é chamado de Rede de Convidados. Isso permite que os visitantes se conectem à Internet, mas protege sua rede doméstica porque não permite que se conectem a nenhum outro dispositivo de

Criando um Lar Ciberneticamente Seguro

sua rede doméstica. Se você adicionar uma rede de convidados, certifique-se de habilitar o WPA2, bem como uma senha exclusiva para esta rede;

Está em dúvida de como fazer essas etapas? Pergunte ao seu provedor de serviços de Internet ou verifique seu site, verifique a documentação que acompanha seu roteador de Internet ou ponto de acesso sem fio ou consulte o respectivo site.

siga estas quatro etapas simples para criar um lar ciberneticamente seguro; proteja sua rede Wi-Fi, habilite a atualização automática, use frases de acesso únicas e ative backups.

Seus dispositivos

O próximo passo é saber quais dispositivos estão conectados à sua rede doméstica sem fio e garantir que todos esses dispositivos estejam seguros. Isso costumava ser simples quando você tinha apenas um computador ou dois. No entanto, hoje quase qualquer coisa pode se conectar à sua rede doméstica, incluindo seus smartphones, TVs, consoles de jogos, babá eletrônica, alto-falantes ou talvez até seu carro. Depois de ter identificado todos os dispositivos em sua rede doméstica, verifique se cada um deles está seguro. A melhor maneira de fazer isso é garantir que você tenha atualização automática ativada sempre que possível. Os hackers estão constantemente encontrando novas fraquezas em diferentes dispositivos e sistemas operacionais. Ao permitir atualizações automáticas, o computador e os dispositivos estão sempre rodando o software mais atual, o que os torna muito mais difícil de serem invadidos.

Senhas

O próximo passo é usar uma senha forte e exclusiva para cada um de seus dispositivos e contas on-line. As palavras-chave aqui são forte e única. Cansado de senhas complexas que são difíceis de lembrar e difíceis de digitar? Nós também. Use uma Frase de Acesso em vez disso. Este é um tipo de senha que utiliza uma série de palavras para torná-la fácil de lembrar, como “Onde está meu café?” ou “sol-donuts-feliz-perdida”. Quanto maior for a sua senha, mais forte. Senha única significa usar uma senha diferente para cada dispositivo e conta online. Desta forma, se uma senha estiver comprometida, todas as suas outras contas e dispositivos ainda estarão seguros. Não se lembra 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 um programa de segurança especial que armazena de forma segura todas as suas senhas, utilizando criptografia.

Finalmente, habilite a verificação em duas etapas sempre que disponível, especialmente para suas contas on-line. A verificação em duas etapas é muito mais forte. Ele usa sua senha, mas também adiciona um segundo passo, como um

Criando um Lar Ciberneticamente Seguro

código enviado para o seu smartphone ou um aplicativo em seu smartphone que gera o código para você. A verificação em duas etapas é, provavelmente, o passo único e mais importante que você pode tomar para proteger-se on-line e é muito mais fácil do que você pensa.

Backups

Às vezes, não importa quão cuidadoso você seja, você poderá ser invadido. Se isso acontecer, muitas vezes a única maneira de recuperar suas informações pessoais é restaurando um backup. Verifique se você está fazendo backups regulares de qualquer informação importante e verifique se você pode restaurá-las. A maioria dos dispositivos móveis suporta backups automáticos para a Nuvem. Para os computadores, na maior parte deles, você pode ter que comprar algum tipo de software ou serviço de backup, que é relativamente barato e simples de usar.

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

Frases de Acesso:	https://securingthehuman.sans.org/ouch/2017#april2017
Gerenciador de Senhas:	https://securingthehuman.sans.org/ouch/2017#september2017
Autenticação de dois fatores:	https://securingthehuman.sans.org/ouch/2017#december2017
Backups:	https://securingthehuman.sans.org/ouch/2017#august2017

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