A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- A Sua Rede Sem Fio
- Os Seus Dispositivos

Protegendo sua Rede Doméstica

Visão Geral

Anos atrás, as redes domésticas eram relativamente simples, geralmente nada mais do que um ponto de acesso sem fio e um ou dois computadores usados para navegar na Internet, fazer compras on-line ou para jogos. No entanto as redes domésticas tornaram-se cada vez mais complexas. Agora nos conectamos com muito mais dispositivos e usamos mais do que apenas para navegação na web ou compras. Neste boletim vamos descrever como criar uma rede segura em casa para você e sua família.

Editor Convidado

Cheryl Conley lidera a equipe de Educação e Conscientização em Segurança na Lockheed Martin, empresa americada de produtos aeroespaciais, levando a campanha "The I Campaign™" a mais de 100.000 funcionários. Isto inclui grupos focais de aliança e defesa por toda a empresa, além de um programa global para phishing. Siga Cheryl em **@conleychera**.

A Sua Rede Sem Fio

Quase todas as redes domésticas começam com uma rede sem fio (às vezes chamada de Wi-Fi). Isto é o que permite conectar qualquer dos seus dispositivos, sem cabos de rede, à Internet, desde notebooks e tablets até consoles de jogos e televisões. A maioria das redes sem fio é controlada pelo roteador de Internet, que é o dispositivo instalado pelo seu provedor de serviço de Internet. No entanto, em alguns casos, a sua rede sem fio pode ser controlada por um sistema separado chamado de ponto de acesso sem fio (Wireless Access Point) que se conecta ao seu roteador de Internet. Independente de qual forma use, ambas funcionam da mesma maneira por transmissão de sinais sem fio. Os diferentes dispositivos em sua casa se conectam à sua rede sem fio através destes sinais. A partir daí estes dispositivos podem conectar-se à Internet, bem como quaisquer outros dispositivos em sua rede doméstica. Isto significa que proteger sua rede sem fio é fundamental para proteger sua rede doméstica. Recomendamos as seguintes medidas de segurança:

- Altere a senha padrão de administrador do seu roteador ou ponto de acesso à Internet sem fio, que controla sua rede sem fio. A conta de administrador é o que permite que você configure as definições da sua rede sem fio. O problema é que muitos roteadores de Internet ou pontos de acesso são fornecidos com um login de administrador e a senha padrão que são bem conhecidos e divulgados na Internet. Então, não se esqueça de alterar a senha de administrador para uma senha forte, única, que só você sabe;
- Altere o nome padrão da rede sem fio (às vezes chamado de SSID). Este é o nome que seus dispositivos irão ver quando buscarem uma rede sem fio. Dê um nome único que você possa identificar facilmente, mas certifique-se de não conter nenhuma informação pessoal. Há pouco valor em configurar sua rede como oculta (ou sem broadcast) pois a maioria

Protegendo sua Rede Doméstica

das ferramentas de scan (procura) de redes sem fio, ou qualquer atacante hábil, pode facilmente descobrir redes ocultas;

- Certifique-se de que apenas as pessoas em quem você confia podem se conectar e usar sua rede sem fio e que essas conexões estejam encriptadas. Faça isso habilitando uma configuração de segurança forte. Atualmente, a melhor opção é usar o mecanismo de segurança chamado WPA2. Ao habilitar isso, é necessária uma senha para as pessoas se conectem à sua rede doméstica e uma vez conectadas, suas atividades online são criptografadas. Certifique-se de não utilizar métodos de segurança antigos ou desatualizados como WEP, ou nenhuma segurança, chamada de rede aberta. As redes abertas permitem que qualquer um se conecte à sua rede sem fio sem qualquer autenticação;
- Certifique-se de que a senha que as pessoas usarão para se conectar à sua rede sem fio é uma senha forte e que é diferente da senha de administrador. Lembre-se que você provavelmente só vai digitá-la uma vez para cada um dos seus dispositivos, já que eles podem armazená-la para uso automático posteriormente;
- Muitas redes sem fio suportam o que é chamado de Rede de Convidado (Guest Network). Isso permite aos visitantes se conectarem à Internet e protege sua rede doméstica, pois impede que eles se conectem a qualquer um dos dispositivos em sua rede doméstica. Se você adicionar uma rede de convidado, não se esqueça de ativar WPA2, bem como uma senha exclusiva para esta rede;
- Desabilite a opção “Wi-Fi Protected Setup” ou outros mecanismos que permitam a um novo dispositivo se conectar à rede sem fio sem conhecer as opções de senha e configuração;
- Se tiver dificuldade em lembrar todas essas senhas, recomendamos fortemente que use um gerenciador de senhas para armazená-las de forma segura.

Para proteger sua rede doméstica, torne segura sua rede sem fio e mantenha todos os seus computadores e dispositivos atualizados e protegidos por senha.

Não tem certeza como fazer estes passos? Pergunte ao seu provedor de serviços de Internet, verifique a documentação que acompanha o roteador ou ponto de acesso à Internet sem fio, ou consulte o respectivo website.

Os Seus Dispositivos

O próximo passo é saber o que está conectado à sua rede doméstica e certificar-se de que todos esses dispositivos estão seguros. Isto costumava ser simples, quando havia apenas alguns dispositivos conectados. Entretanto, no mundo atual “sempre conectado” quase qualquer coisa pode se conectar à sua rede doméstica, incluindo televisões, consoles de jogos, os monitores

Protegendo sua Rede Doméstica

do bebê, alto-falantes, seu termostato ou talvez até o seu carro. Uma maneira simples de descobrir o que está conectado em sua rede doméstica é usar um scanner de rede simples, como o Fing. Esses aplicativos, que você pode instalar no seu computador ou dispositivo móvel, fazem uma varredura em sua rede sem fio e relatam todos os dispositivos conectados a ele. Depois de identificar todos os dispositivos em sua rede doméstica, você precisa garantir que cada um dos dispositivos esteja seguro. A melhor maneira de fazer isso é garantir que eles estejam sempre rodando a última versão de seu sistema operacional / firmware. Sempre que possível, habilite a atualização automática. Se qualquer um dos seus dispositivos exigir uma senha, utilize sempre uma senha exclusiva e forte. Finalmente, não deixe de visitar o site do seu provedor de serviços de Internet, uma vez que ele pode fornecer ferramentas gratuitas para ajudá-lo a proteger sua rede doméstica.

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

Frases secretas:	https://securingthehuman.sans.org/ouch/2015#april2015
Gerenciador de Senhas:	https://securingthehuman.sans.org/ouch/2015#october2015
Como proteger o seu novo tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Mapeamento de sua Rede Doméstica:	http://l.rud.is/home-network-mapping

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