OUCH! I Junho de

SANS SECURITY AWARENESS

O boletim mensal de conscientização de segurança para você

Criando um lar Ciberneticamente

Visão geral

No passado, construir uma rede doméstica era apenas instalar um roteador sem fio e vários computadores. Hoje, como muitos de nós estamos trabalhando, conectando ou aprendendo em casa, temos que prestar mais atenção à criação de um lar forte ciberneticamente. Confira estes quatro passos para fazer isso.

Sua rede sem fio

Praticamente todas as redes domésticas começam com uma rede sem fio (ou Wi-Fi). É o que permite que seus dispositivos se conectem à Internet. A maioria das redes sem fio domésticas é controlada pelo roteador de Internet ou por um ponto de acesso sem fio dedicado e separado. Ambos funcionam do mesmo modo: ao transmitir sinais sem fio que permitem que os dispositivos em sua casa se conectem à Internet. Isso significa que proteger a sua rede sem fio é uma parte fundamental da proteção da sua casa. Recomendamos as seguintes etapas para protegê-lo.

- Altere a senha padrão do administrador em seu roteador de Internet ou ponto de acesso sem fio, o que estiver controlando sua rede sem fio. A conta do administrador é o que permite definir as configurações de sua rede sem fio.
- Verifique se apenas os dispositivos confiáveis podem se conectar à sua rede sem fio. Faça isso ativando uma segurança forte. Para isso, é necessário uma senha para conectar-se à sua rede doméstica e criptografar as atividades online depois de conectadas.
- Certifique-se que a senha utilizada para se conectar a sua rede doméstica seja uma senha forte diferente da senha do administrador. Lembre-se de que seus dispositivos armazenam senhas; portanto, basta digitar a senha uma vez em cada dispositivo.

Se você não tiver certeza de como executar essas etapas, acesse o site do seu provedor de Internet ou o fornecedor do seu roteador ou ponto de acesso sem fio.

Senhas

Use uma senha forte e exclusiva para cada um dos seus dispositivos e contas online. As palavras-chave aqui são *forte* e *única*. Quanto maior for sua senha, mais forte será. Tente usar uma série de palavras fáceis de lembrar, como ***sol-rosquinhas-feliz***.

Uma senha única significa usar uma diferente para cada dispositivo ou conta online. Use um gerenciador de senhas para lembrar todas essas senhas fortes, que é um programa de segurança que armazena com segurança todas suas senhas em um cofre virtual e criptografado.

Além disso, ative a verificação em duas etapas sempre que estiver disponível, especialmente para suas contas online. Usa sua senha, mas também adiciona uma segunda etapa, como inserir um código enviado ao seu smartphone ou a partir de um aplicativo que gera o código para você. Este é provavelmente o passo mais importante que você pode dar e é muito mais fácil do que pensa.

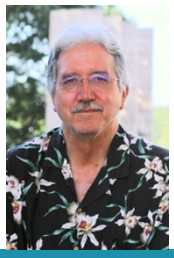
Seus dispositivos

O próximo passo é saber quais dispositivos estão conectados à sua rede doméstica sem fio e certificar-se que todos sejam confiáveis e seguros. Isso costumava ser simples quando você tinha apenas um computador. No entanto, atualmente, quase tudo pode ser conectado à sua rede doméstica, incluindo smartphones, TVs, consoles de videogame, babás eletrônicas, impressoras, alto-falantes ou inclusive o seu carro. Depois de identificar todos os dispositivos em sua rede doméstica, verifique se cada um deles está seguro. A melhor maneira de fazer isso é alterar as senhas padrão e ativar a atualização automática sempre que possível.

Backups

Às vezes, por mais cuidadoso que seja, você ainda pode ser invadido. Se for esse o caso, normalmente a única maneira de restaurar todas as suas informações pessoais é por meio do backup. Certifique-se de fazer backups periódicos de qualquer informação importante e verifique se é possível restaurar seus dados a partir deles. A maioria dos dispositivos móveis oferece suporte para backups automáticos em nuvem. Para a maioria dos computadores, pode ser necessário adquirir algum tipo de software ou serviço de backup, que é relativamente barato e fácil de usar.

Editor convidado



Randy Marchany é o Diretor de Segurança da Informação da Virginia Tech. Ele também é instrutor sênior do SANS e ensina os cursos SEC566, SEC440, Implementando e Auditando os Controles Críticos de Segurança. Siga o Randy @randymarchany

Recursos

Simplificando as senhas: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Gerenciadores de Senhas: https://www.sans.org/security-awareness-training/resources/password-managers-0
Atualização: https://www.sans.org/security-awareness-training/resources/power-updating
Tem Backups?: https://www.sans.org/security-awareness-training/resources/got-backups
Senhas padrão do dispositivos: https://www.routerpasswords.com/

Traduzido para a Comunidade por: David Boldrin