A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Mantendo a Segurança nas Viagens

Visão Geral

Queremos que você aproveite o máximo da tecnologia, mesmo durante as viagens. Nesta edição mostraremos como se conectar à Internet e usar seus dispositivos de forma segura enquanto estiver viajando.

Editor Convidado

Mark Williams é Arquiteto de Segurança Empresarial na BlueCross Blueshield, no Tennessee/EUA. É também instrutor SANS e presidente do capítulo Chattanooga do ISSA. Ele viaja constantemente e entende os problemas encontrados ao levar seus brinquedos tecnológicos com ele.

Verificação Prévia

Enquanto suas redes domésticas ou de trabalho podem ser seguras, ao viajar você deve assumir que qualquer rede à qual se conecte não é confiável. Você nunca sabe quem está conectado nela e o que está fazendo. Aqui vão alguns passos simples que ajudarão a proteger você e seus dados, antes de viajar.

- A informação mais segura é aquela que não está com você. Identifique os dados que não precisa nos dispositivos que levará na viagem e remova essas informações. Isso pode reduzir significativamente o impacto nos casos de perda, roubo/furto ou apreensão por serviço aduaneiro ou de segurança de fronteira entre países. Se sua viagem é de trabalho, pergunte ao seu supervisor se sua empresa disponibiliza equipamentos de uso específico para viagens de trabalho;
- Proteja seus dispositivos móveis e/ou laptop com uma senha forte ou código de acesso. Assim, se ele for roubado/furtado ou perdido, as pessoas não poderão acessar as informações nele contidas. Além disso, habilite a encriptação de disco inteiro nos dispositivos móveis e laptops. Na maioria dos dispositivos móveis ela é automaticamente habilitada quando você usa o bloqueio de tela;
- Instale ou habilite o recurso de rastreamento remoto no seu dispositivo, para que possa localizá-lo e até mesmo apagá-lo remotamente, em caso de perda ou roubo/furto;
- Atualize seus dispositivos, aplicativos e software antivírus antes de viajar, para que esteja rodando as últimas versões existentes. Muitos ataques focam em sistemas com software desatualizado;
- Faça um backup completo dos seus dispositivos. Assim se algo acontecer com eles durante a viagem você ainda terá seus dados originais em um local seguro;
- Para viagens internacionais, verifique com sua operadora o plano de dados que utiliza no seu celular. Muitas

Mantendo a Segurança nas Viagens

vezes elas cobram altas taxas para uso de dados em viagem e você pode querer desabilitar a transferência de dados durante uma viagem internacional ou comprar um cartão SIM pré-pago.

Perda / Roubo de Dispositivos

Uma vez iniciada a viagem, garanta a segurança física dos seus dispositivos. Por exemplo, nunca os deixe no carro onde as pessoas possam vê-los, pois criminosos podem simplesmente quebrar a janela do carro e levar tudo de valor que esteja à vista. Mesmo isto sendo um risco, de acordo com um estudo recente da empresa Verizon, as pessoas estão 100 vezes mais sujeitas à perda do seu dispositivo do que a um roubo/furto. Significa que você deve sempre verificar se ainda está com seus dispositivos durante a viagem, como quando passar na segurança do aeroporto, deixar o táxi ou o restaurante, fazer o check out do hotel ou depois de desembarcar do avião. Lembre-se de verificar aquele bolso traseiro da poltrona à sua frente.

Para manter a segurança durante a viagem, proteja seus dispositivos antes de sair de casa, mantenha-os protegidos fisicamente e criptografe duas comunicações online.

Acesso Wi-Fi

Acessar a Internet durante a viagem significa muitas vezes utilizar redes Wi-Fi públicas como as encontradas em hotéis, cafeterias e aeroportos. Dois problemas com redes Wi-Fi são: você nunca sabe quem as configurou e você nunca sabe quem está conectado nelas. Por isso elas devem ser consideradas não confiáveis. De fato, é por isso que você segue todos esses passos para proteger seus dispositivos antes de viajar. Adicionalmente, redes Wi-Fi usam ondas de rádio, que significa que qualquer pessoa fisicamente próxima de você pode potencialmente interceptar e monitorar essas comunicações. Por essas razões, se você utilizar uma rede Wi-Fi pública, certifique-se de que todas as suas atividades online estejam criptografadas. Por exemplo, quando conectar-se a um site de Internet com seu navegador, certifique-se de que o acesso ao site é criptografado. Você pode confirmar observando o texto 'HTTPS://' e/ou a imagem de um cadeado no endereço do site ou na barra de endereços do navegador. Adicionalmente você pode ter um serviço chamado VPN (Virtual Private Network ou Rede Privada Virtual), que criptografa todas as suas atividades online quando estabelecidas. Ela pode ser configurada para você pela sua empresa ou você pode comprar este serviço para uso pessoal. Se estiver preocupado em não haver um serviço Wi-Fi em que possa confiar, considere a possibilidade de conectar-se utilizando seu smartphone como âncora. Aviso: como mencionado anteriormente, isso pode custar caro em viagens internacionais, portanto verifique primeiramente com seu provedor de serviço.

Mantendo a Segurança nas Viagens

Computadores Públicos

Não utilize computadores públicos como aqueles disponíveis em hotéis ou cyber café, para entrar em nenhuma de suas contas ou acessar dados sensíveis. Você não sabe quem utilizou esses computadores antes de você, se eles foram infectados acidentalmente ou deliberadamente. Sempre que possível utilize dispositivos que você controle e confie. Na melhor das hipóteses, um computador público pode ser utilizado para acessar informações públicas, como previsão do tempo ou sites de notícias. Entrar em quaisquer contas, como suas contas do Google, pode ser um convite para os hackers que podem estar em vigilância.

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 Secretas:	https://securingthehuman.sans.org/ouch/2015#april2015
Cópias de Segurança:	https://securingthehuman.sans.org/ouch/2015#august2015
Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Criptografia:	https://securingthehuman.sans.org/ouch/2016#june2016
Arquivo / Traduções OUCH!:	https://securingthehuman.sans.org/ouch/archives

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

