A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- **Pré-Verificação**
- **Aparelhos perdidos / roubados**
- **Acesso Wi-Fi**
- **Computadores públicos**

Permanecendo seguro em Viagem

Visão geral

Neste boletim vamos abordar como você pode se conectar com segurança à Internet e fazer suas coisas durante viagem.

Editor Convidado

Steve Armstrong é o Diretor Técnico da CyberCPR em Logically Secure, é um instrutor certificado SANS e autor antigo do curso SANS. Ele participa ativamente no Twitter como **@Nebulator** e no Google Plus: **+SteveArmstrongSecurity**.

Pré-verificação

Enquanto a sua rede de casa ou do trabalho podem ser consideradas seguras, quando você viaja você deve sempre presumir que qualquer rede em que você se conecte não é confiável. Você nunca sabe quem mais está nela e as ameaças que eles podem representar. Algumas medidas simples de pré-viagem podem proteger seus dados enquanto você viaja. Uma ou duas semanas antes de sua viagem:

- Identificar quais os dados que você não precisa nos aparelhos que você está levando com você e, em seguida, remover qualquer informação desnecessária. Isso pode ajudar a reduzir significativamente o impacto caso seus aparelhos sejam perdidos, roubados ou apreendidos pela alfândega ou por pessoal de segurança de fronteiras. Se sua viagem é relacionada com o trabalho pergunte ao seu supervisor se sua empresa fornece aparelhos alternativos que são utilizados especificamente para trabalhar durante viagem;
- Em viagens internacionais, verifique qual o tipo de conector de energia o país usa, pode ser necessário obter um adaptador para carregar seus aparelhos. Além disso, verifique as condições do seu plano de dados com a sua operadora de telefone móvel. Muitas vezes, os prestadores de serviços cobram taxas elevadas para o uso de dados internacional. Você pode querer desativar ou modificá-lo para a viagem internacional;
- Instale um software no seu aparelho para que possa acompanhar remotamente onde o aparelho está e até mesmo limpar seus dados remotamente, em caso de perda ou roubo. Muitos aparelhos móveis já têm essa funcionalidade incorporada, você só tem que habilitá-la (lembre-se que precisa estar conectado à Internet para funcionar);

Um ou dois dias antes de viajar:

- Atualize seus aparelhos, aplicativos e anti-vírus para que rodem as versões mais recentes;
- Habilite todas as configurações de segurança do seu aparelho, tais como firewalls;
- Bloqueie todos os seus aparelhos móveis com uma senha forte ou código de acesso. Dessa forma, se você perder seu telefone ou ele for roubado, as pessoas não poderão acessar suas informações nele;
- Criptografe todos os seus aparelhos para que, em caso de perda ou roubo, seus dados não possam ser

Permanecendo seguro em Viagem

acessados. Alguns aparelhos, como iPhones fazem isso automaticamente se você definir uma senha ou código de acesso no dispositivo;

- Faça um backup completo de todos os seus aparelhos. Dessa forma, se algo acontecer a eles enquanto viaja, ainda terá todos os seus dados em um local seguro.

A chave para permanecer seguro durante uma viagem é proteger seus aparelhos antes de sair de casa, mantê-los fisicamente seguros, saber onde eles estão a todo momento e criptografar todas as suas atividades on-line.

Aparelhos Perdidos / roubados

Ao iniciar sua viagem esteja atento à segurança física de seus aparelhos. Por exemplo, nunca deixe seus aparelhos no carro onde as pessoas podem vê-los facilmente, pois os criminosos simplesmente quebram a janela do seu carro e pegam qualquer coisa de valor que eles veem. Uma opção é levar um cabo de segurança de modo que você possa bloquear fisicamente seus aparelhos, como o seu laptop, quando precisar se afastar dele. Mesmo que o roubo seja definitivamente um risco, o que você pode não perceber é que você está, na verdade, muito mais propenso a perder o seu aparelho do que tê-lo roubado. De acordo com um estudo de dez anos da Verizon, as pessoas são 15 vezes mais propensas a perder um aparelho do que tê-lo roubado. Isso significa que você sempre deve verificar que ainda está com seus aparelhos quando você viaja, como quando passa pela segurança no aeroporto, sai de num táxi ou restaurante, quando faz um check out de um quarto de hotel ou antes de desembarcar de seu avião.

Acesso Wi-Fi

Acessar a Internet enquanto viaja muitas vezes significa o uso de pontos de acesso Wi-Fi públicos, como os encontrados em um hotel, na sua loja de café local ou no aeroporto. O problema com pontos de acesso Wi-Fi públicos não é somente você nunca ter certeza de quem os configurou, mas você nunca sabe quem está conectado a eles. Então ele deve ser considerado não confiável. E na verdade foi por isso que você tomou todas as medidas para proteger seus aparelhos antes de sair. Além disso, Wi-Fi usa ondas de rádio para se comunicar a partir do seu aparelho para o ponto de acesso Wi-Fi. Isto significa que qualquer pessoa fisicamente perto de você pode, potencialmente, interceptar e monitorar suas comunicações.

É por isso que se você usar Wi-Fi público, você precisa garantir que todas as suas atividades on-line são encriptadas. Por exemplo, ao se conectar à Internet e utilizar o seu navegador (Internet Explorer ou equivalente), certifique-se de que os sites que você está visitando são criptografados (eles terão 'https://' na URL e uma imagem de um cadeado fechado). Além disso, você pode ter o que é chamado de uma conta VPN (Virtual Private Network), que irá encriptar toda a sua atividade online. Isso pode ser disponibilizado para você pela sua empresa, ou você pode adquirir uma VPN para o seu uso pessoal. Se você está preocupado em não encontrar pontos de acesso Wi-Fi em que possa confiar, considere usar o do seu smartphone. (Aviso: Como mencionamos anteriormente, o serviço de dados pode ser caro em viagens ao estrangeiro, consulte a sua operadora antes de utilizá-lo).

Permanecendo seguro em Viagem

Recursos Públicos

Não utilize computadores públicos, tais como computadores em lobbies de hotel, bibliotecas ou em cyber cafés. Você não tem idéia de quem usou esse computador antes de você, eles podem ter infectado esse computador público acidentalmente ou deliberadamente. Sempre que possível, use apenas os aparelhos que você tem controle e confiança para qualquer atividade online. Se você precisa usar um computador público, não utilize qualquer serviço que exija seu login ou senha.

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

Senhas:	http://www.securingthehuman.org/ouch/2013#may2013
Verificação em dois passos:	http://www.securingthehuman.org/ouch/2013#august2013
Criptografia:	http://www.securingthehuman.org/ouch/2014#august2014
Como proteger o seu novo tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014 (em Inglês):	http://www.verizonenterprise.com/DBIR/2014/

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