OUCH! | Janeiro de 2015

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Usando Aplicativos Móveis de Forma Segura

Visão Geral

Dispositivos móveis, como tablets e smartphones tornaram-se uma das principais tecnologias que usamos em nossas vidas pessoais e profissionais. O que torna os dispositivos móveis tão versáteis são os milhões de aplicativos (Apps) que podemos escolher. Estas aplicações nos permitem ser mais produtivos, nos comunicar e compartilhar conteúdo instantaneamente, ensinar e educar, ou apenas nos divertir mais. No entanto, com o poder de todos estes aplicativos móveis vêm também os riscos. Aqui veremos alguns passos que você pode seguir para usar e manter seus aplicativos móveis com segurança.

Editor Convidado

Chris Crowley é um consultor independente, autor de cursos e instrutor certificado do SANS. Ele está no Twitter em **@CCrowMontance** e no Google plus em **+ChrisCrowley**.

Baixando Apps

O primeiro passo é ter certeza que você sempre irá baixá-los a partir de uma fonte confiável e segura. Lembre-se, qualquer um pode criar um aplicativo móvel, então você tem que ter cuidado com a escolha da fonte de onde irá baixá-los. Cyber criminosos aprimoraram suas habilidades em criar e distribuir aplicativos móveis infectados que parecem ser legítimos. Se você instalar um desses aplicativos infectados, esses criminosos podem assumir o controle do seu dispositivo móvel para ler seus e-mails, ouvir as suas conversas e copiar os seus contatos. Ao fazer o download de aplicativos utilizando apenas fontes conhecidas e confiáveis você reduz a possibilidade de instalar um aplicativo infectado. O que você pode não perceber é que a marca do dispositivo móvel que você usa determina as suas opções.

Para os dispositivos da Apple como o iPad ou iPhone, você só pode fazer download de aplicativos móveis a partir de um ambiente gerenciado, a loja de aplicativos da Apple. A vantagem disso é que a Apple faz uma verificação de segurança dos aplicativos móveis e de seus autores. Mesmo a Apple não consegue pegar todos os bandidos ou todos os aplicativos móveis infectados, mas este ambiente gerenciado ajuda a reduzir drasticamente o risco de você instalar um aplicativo infectado. Além disso, se a Apple encontrar um aplicativo em sua loja que acredita estar infectado ela vai rapidamente remover o aplicativo móvel. O Windows Phone usa uma abordagem semelhante para gerir suas aplicações.

Dispositivos móveis Android são diferentes. O Android dá mais flexibilidade por ser capaz de fazer o download de um aplicativo móvel de qualquer lugar na Internet. No entanto, com essa flexibilidade vem mais responsabilidade. Você tem que ser mais cuidadoso para decidir quais aplicativos móveis irá baixar e instalar porque nem todos serão revisados. A Google mantém uma loja de aplicativos móveis, semelhante à da Apple, chamada de Google Play. Os aplicativos móveis baixados da Google Play tiveram algumas verificações básicas. Por isso, recomendamos que você baixe seus aplicativos móveis para dispositivos

© The SANS Institute 2015

Usando Aplicativos Móveis de Forma Segura

Android apenas da Google Play. Evite o download de aplicativos móveis Android de outros sites, já que qualquer pessoa, incluindo os criminosos podem facilmente criar e distribuir aplicativos móveis maliciosos, e induzi-lo a infectar o seu dispositivo móvel. Como proteção adicional, considere a instalação de um antivírus no seu dispositivo móvel.

Para reduzir ainda mais o risco, evite aplicativos que são muito novos, que tiveram poucos downloads, ou que têm poucos comentários positivos. Quanto mais tempo um aplicativo está disponível ou quanto mais comentários positivos ele tem, mais provável que o mesmo seja confiável. Além disso, instale apenas os aplicativos que você precisa e usa. Pergunte a si mesmo, eu realmente preciso deste app? Não só cada app, potencialmente, pode trazer novas vulnerabilidades, mas também novas questões de privacidade. Se você parar de usar um aplicativo, remova-o do seu dispositivo móvel (você sempre pode adicioná-lo novamente mais tarde, se achar que precisa).

O segredo para usar aplicativos móveis com segurança é instalar somente aplicativos de fontes confiáveis e certificar-se de que seus aplicativos estão atualizados e que você verificou as permissões utilizadas.

Finalmente, você pode ser tentado a usar o “jailbreak” ou “root” de seu dispositivo móvel. Este é o processo de burlar o sistema interno e instalar aplicativos não aprovados ou alterar existentes. Recomendamos fortemente a não realizar o “jailbreaking” ou “rooting”, pois não só ignora ou elimina muitos dos controles de segurança incorporados no seu dispositivo móvel, mas muitas vezes também anula garantias e contratos de suporte.

Permissões

Depois de ter instalado um aplicativo móvel de uma fonte confiável, o próximo passo é ter certeza que ele está configurado com segurança e protegendo a sua privacidade. Instalar e/ou configurar aplicativos móveis, muitas vezes requer que você conceda certas permissões. Sempre pense antes de autorizar qualquer acesso: o aplicativo realmente precisa dessas permissões para fazer o seu trabalho declarado? Por exemplo, alguns aplicativos utilizam os serviços de localização geográfica (GPS). Se você permitir que um aplicativo sempre saiba a sua localização, você pode estar permitindo que o criador desse aplicativo rastreie seus movimentos, talvez ele possa até mesmo vender essas informações para terceiros. Se você não quiser conceder as permissões que um aplicativo está solicitando, busque outro aplicativo que atenda às suas necessidades. Lembre-se, você tem muitas opções lá fora. Dispositivos da Apple permitem que algumas permissões sejam alteradas nas configurações ou quando em uso, tais como o acesso a informações de geo-localização. Dispositivos Windows Mobile e Android são diferentes, eles apresentam uma abordagem de tudo ou nada. Se você não conceder todas as permissões especificadas, você não consegue instalar o app.

Atualizando Apps

Aplicativos móveis, assim como o seu computador e o sistema operacional do dispositivo móvel, devem ser atualizados, a fim de manterem-se atualizados. Os criminosos estão constantemente procurando e encontrando os pontos fracos dos

© The SANS Institute 2015

Usando Aplicativos Móveis de Forma Segura

aplicativos. Eles, então, desenvolvem ataques para explorar essas fraquezas. Os desenvolvedores que criaram o seu app também criam e lançam atualizações para corrigir estas deficiências e proteger seus dispositivos. Quanto mais vezes você procurar e instalar atualizações, melhor. A maioria das plataformas permite que você configure o sistema para atualizar aplicativos móveis automaticamente. Recomendamos esta configuração. Se isso não for possível, então nós recomendamos que você verifique, pelo menos, a cada duas semanas as atualizações disponíveis para seus aplicativos móveis. No entanto, quando seus aplicativos são atualizados, sempre verifique quaisquer novas permissões que eles talvez possam exigir.

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

Engenharia Social:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_pt.pdf
Descarte de seus Dispositivos Móveis:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201406_pt.pdf
Protegendo seu novo Tablet:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_pt.pdf
Termos de Segurança Frequentes(Inglês):	http://www.securingthehuman.org/resources/security-terms
SEC575: Curso de Segurança para Dispositivos Móveis(Inglês):	http://www.sans.org/sec575

OUCH! é publicado pelo “SANS Securing the Human” e distribuído sob o licenciamento Creative Commons BY-NC-ND 4.0 license. A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

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