OUCH! | Março de 2017

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Utilizando Apps Móveis com Segurança

Visão Geral

Dispositivos móveis como tablets, smartphones e relógios 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 que podemos escolher. Esses aplicativos nos permitem ser mais produtivos, comunicar e compartilhar instantaneamente com os outros, treinar e educar, ou simplesmente se divertir mais. No entanto, com o poder de todos esses aplicativos móveis vem os riscos. Aqui veremos alguns passos que você pode seguir para utilizar e aproveitar ao máximo os seus aplicativos para dispositivos móveis.

Editor Convidado

Joshua Wright é o diretor técnico do Counter Hack e instrutor sênior do SANS Institute. É também autor do curso “SEC575: Mobile Device Security and Ethical Hacking, and Hacking Exposed: Wireless”. Siga Josh no Twitter **@joswr1ght**.

Baixando Aplicativos

O primeiro passo é garantir que você sempre faça o download de aplicativos para dispositivos móveis de uma fonte segura e confiável. Cyber criminosos têm utilizado suas habilidades na criação e distribuição de aplicativos móveis infectados que parecem legítimos. Se você instalar um desses aplicativos infectados, os criminosos podem assumir o controle completo do seu dispositivo móvel. Ao fazer o download de aplicativos apenas de fontes conhecidas e confiáveis, você reduz a chance de instalar um aplicativo infectado. O que você pode não perceber é que a marca do dispositivo móvel que você usa determina suas opções para baixar aplicativos.

Para dispositivos da Apple, como o iPad ou iPhone, a transferência dos aplicativos para dispositivos móveis se dá apenas na App Store da Apple. A vantagem disso é que a Apple faz uma verificação de segurança de todos os aplicativos móveis antes que eles sejam disponibilizados. Embora a Apple não possa capturar todos os aplicativos móveis infectados, esse ambiente gerenciado ajuda a reduzir drasticamente o risco de instalar um aplicativo infectado. Além disso, se a Apple encontrar um aplicativo em sua loja que acredite estar infectado, ela removerá rapidamente o aplicativo da loja. O Windows Phone usa uma abordagem semelhante para gerenciar aplicativos.

Os dispositivos móveis Android são diferentes. O Android oferece mais flexibilidade por ser possível fazer o download de um aplicativo para celular de qualquer lugar da Internet. No entanto, com esta flexibilidade vem mais responsabilidade. Você precisa ter mais cuidado com os aplicativos para dispositivos móveis que você baixar e instalar, pois nem todos

Utilizando Apps Móveis com Segurança

são revisados. O Google mantém uma loja de aplicativos móveis gerenciados semelhante à da Apple, chamada Google Play. Os aplicativos para celular que você baixou da Google Play passaram por algumas verificações básicas de segurança. Como tal, recomendamos que obtenha seus aplicativos Android apenas a partir do Google Play. Evite fazer o download de outros sites, já que qualquer pessoa, incluindo criminosos virtuais, pode facilmente criar e distribuir aplicativos móveis maliciosos e enganá-lo para infectar seu dispositivo móvel. Como uma proteção adicional, quando possível, instale um antivírus em seu dispositivo móvel.

A chave para usar aplicativos móveis de forma segura é instalar aplicativos somente de fontes confiáveis, instalar atualizações quando disponíveis e conceder apenas as permissões necessárias.

Independentemente do dispositivo que você está usando, uma etapa adicional que você pode tomar é evitar aplicativos que são novos, que poucas pessoas baixaram ou que têm poucos comentários positivos. Quanto mais tempo de existência um aplicativo tiver, mais pessoas tiverem usado e mais comentários positivos tiver, maior será a probabilidade do aplicativo ser confiável. Além disso, instale apenas os aplicativos que você precisa e usa. Pergunte a si mesmo: eu realmente preciso deste aplicativo? Cada aplicativo traz, potencialmente, não apenas 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 dele). Finalmente, nunca realize o jailbreak ou root de seu dispositivo móvel (técnica que desbloqueia o seu aparelho e permite ter controle total do dispositivo). Este é um processo de hacking do dispositivo para a instalação de aplicativos não aprovados ou alteração de funcionalidades pré-existentes de fábrica. Isso não só ignora ou elimina muitos dos controles de segurança incorporados em seu dispositivo móvel, mas muitas vezes também anula garantias e contratos de suporte.

Permissões

Depois de instalar um aplicativo para celular de uma fonte confiável, verifique se ele está configurado com segurança e protegendo sua privacidade. Sempre reflita antes de conceder acesso a um aplicativo: você deseja conceder a permissão solicitada pelo aplicativo, ele realmente precisa dela ? Por exemplo, alguns aplicativos usam serviços de geolocalização. Se você permitir que um aplicativo sempre saiba sua localização, talvez você esteja permitindo que o criador desse aplicativo acompanhe seus movimentos ou até mesmo venda essa informação a outras pessoas. Se você não deseja conceder as permissões, negue a solicitação de permissão ou baixe outro aplicativo que atenda aos seus requisitos. Lembre-se, você tem muitas opções de aplicativos.

Utilizando Apps Móveis com Segurança

Atualizando Aplicativos

Os aplicativos e o sistema operacional para dispositivos móveis, assim como o computador, devem ser atualizados para se manterem na versão mais atual. Os criminosos estão constantemente procurando e encontrando brechas nos aplicativos. Eles então desenvolvem ataques para explorar essas fraquezas. Os desenvolvedores que criaram o aplicativo também criam e lançam atualizações para corrigir esses pontos fracos e proteger seus dispositivos. Quanto mais você verificar e instalar atualizações, melhor. A maioria dos dispositivos permite que você configure seu sistema para atualizar aplicativos para dispositivos móveis automaticamente. Recomendamos esta definição. Se isso não for possível, recomendamos que você verifique pelo menos a cada duas semanas as atualizações de seus aplicativos para dispositivos móveis. Finalmente, quando seus aplicativos são atualizados, certifique-se sempre de verificar as novas permissões que eles 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 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

Engenharia Social:	https://securingthehuman.sans.org/ouch/2017#january2017
Descarte seguro do seu dispositivo móvel:	https://securingthehuman.sans.org/ouch/2016#december2016
Tornando Seguro seu Novo Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Arquivos & Traduções:	https://securingthehuman.sans.org/ouch/archives
Curso de Segurança para Dispositivo Móvel (Inglês):	https://sans.org/sec575

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

