OUCH! | Dezembro de 2016

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Descarte seguro do seu dispositivo móvel

Visão geral

Dispositivos móveis como smartphones, smart watches e tablets continuam avançando e inovando de forma surpreendente. Com isso algumas pessoas trocam seus aparelhos quase que anualmente. Infelizmente muitas pessoas descartam seus aparelhos sem pensar muito sobre a quantidade de dados pessoais que permanece nele. Nesta edição vamos falar sobre os tipos de informação pessoal que podem existir no seu aparelho e como limpá-lo de forma segura antes de descarta-lo ou devolvê-lo. Se o seu dispositivo móvel tiver sido entregue a você por sua empresa ou tiver alguma informação de sua empresa nele, certifique-se de verificar com ela o processo de backup e descarte apropriado antes de seguir os passos abaixo.

Editor Convidado

Heather Mahalik (**@HeatherMahalik**; +HMahalik) é Cientista Forense Principal liderando o esforço forense para ManTech CARD. Ela é a líder de curso e coautora do curso "Advanced Smartphone Forensics (FOR585)" do SANS Institute e instrutora no curso "Windows Forensic Analysis (FOR408)". Ela mantém seu blog em **smarterforensics.com**.

Suas informações

Dispositivos móveis armazenam muito mais dados sensíveis do que você pode imaginar, às vezes até mais do que seu computador. Informações típicas incluem:

- Onde você mora, trabalha e lugares que visita frequentemente
- Detalhes sobre todos os seus contatos pessoais na sua agenda e aplicações, incluindo família, amigos e colegas de trabalho
- Histórico de chamadas recebidas, efetuadas e perdidas
- Mensagens de texto (SMS ou "torpedos"), voz e de vídeo
- Histórico de conversas em aplicações como Chat seguro, jogos e redes sociais
- Histórico de localização baseado em coordenadas GPS ou torres de comunicação celular da operadora
- Histórico de navegação Web, de buscas, páginas armazenadas no aparelho (cache) e cookies (pedaços de código armazenados por páginas que visitou)
- Fotos pessoais, vídeos, gravações de voz e emails
- Senhas armazenadas e acesso às contas pessoais como email ou banco
- Acesso a fotos, arquivos ou informações armazenadas na Nuvem
- Qualquer informação relacionada à sua saúde, incluindo sua idade, frequência cardíaca, pressão sanguínea ou dieta

Limpando seu dispositivo

Como pode ver, provavelmente há uma quantidade tremenda de informações sensíveis no seu dispositivo móvel. Independente de como você descarta seu aparelho, seja por doação, troca por um novo, dando para um membro da família,

Descarte seguro do seu dispositivo móvel

revendendo ou até jogando fora, você precisa certificar-se de primeiro apagar todas essas informações. Você pode não perceber, mas simplesmente apagar os arquivos não é suficiente, pois eles podem ser recuperados facilmente com a utilização de ferramentas grátis encontradas na Internet. Ao invés disso você precisa apagá-los de forma segura, o que é chamado de limpeza (wipe). Isso na verdade sobrescreve as informações garantindo que elas não poderão ser recuperadas ou reconstruídas. Lembre-se que provavelmente você vai querer fazer uma cópia de segurança (backup) antes de limpar todos os dados, assim você poderá recuperá-las no seu novo aparelho.

A forma mais segura de limpar seu dispositivo é usar a função "Restaurar Padrões de Fábrica". Ela retorna o aparelho para as condições originais de quando você o comprou na loja. Nós percebemos que a redefinição de fábrica é o método mais simples e seguro para limpar os dados do seu dispositivo móvel. Essa função varia de aparelho para aparelho, então listamos abaixo o passo a passo de como executá-la em dois dos dispositivos mais populares:

Quando descartar seu dispositivo móvel, certifique-se de fazer a restauração aos padrões de fábrica e remover o cartão SIM e qualquer cartão de memória existente.

- Aparelhos com Apple iOS: Ajustes | Geral | Redefinir | Apagar Todo o Conteúdo e Ajustes
- Aparelhos com Android: Configurações | Privacidade | Restaurar Padrões de Fábrica

Infelizmente, remover dados pessoais de dispositivos Windows não é tão simples como restaurar os padrões de fábrica. Mais pesquisas estão sendo conduzidas sobre os métodos que garantam a limpeza de seus dados do aparelho. Se ainda tiver dúvidas sobre como efetuar uma restauração dos padrões de fábrica, verifique o manual do usuário ou a página de Internet do fabricante. Lembre-se: simplesmente apagar seus dados pessoais não é suficiente pois eles podem ser restaurados facilmente.

Cartões SIM / de armazenamento

Além dos dados armazenados no seu dispositivo, você deve considerar o que fazer com seu cartão SIM (Subscriber Identity Module ou Módulo de Identidade do Assinante, que é o cartão da operadora de celular). O cartão SIM é utilizado pelo aparelho para fazer a conexão celular ou de dados. Quando você executa a restauração aos padrões de fábrica no seu aparelho, o cartão SIM mantém informações sobre sua conta e está vinculado a você, o usuário. Se você está mantendo seu número telefônico e movendo para um aparelho novo, fale com sua operadora sobre como transferir o cartão SIM. Se não for possível, por exemplo se o novo aparelho utilizar um cartão SIM de tamanho diferente, guarde seu cartão antigo e destrua-o fisicamente picotando ou cortando para prevenir que alguém o reutilize.

Finalmente, alguns dispositivos móveis utilizam um cartão SD (Secure Digital) separado para armazenamento adicional. Esses cartões de armazenamento muitas vezes contêm fotos, aplicações de smartphone e outros conteúdos sensíveis.

Descarte seguro do seu dispositivo móvel

Lembre-se de remover quaisquer cartões de armazenamento externo do seu aparelho antes de descarta-lo (para alguns dispositivos, seu cartão SD pode estar escondido no compartimento de bateria do seu dispositivo, possivelmente embaixo da bateria). Esses cartões podem frequentemente ser reutilizados nos aparelhos novos, ou podem ser utilizados como um armazenamento genérico no seu computador com um adaptador USB. Se não for possível reutilizar seu cartão SD, então, assim como seu velho cartão SIM, recomendamos destruí-lo fisicamente.

Se não tiver certeza sobre os passos explicados nesta edição, leve seu aparelho para a loja onde o comprou e obtenha ajuda de um técnico. Finalmente, se for jogar fora seu aparelho, pedimos que, ao invés disso, considere a possibilidade de fazer uma doação. Há inúmeras instituições de caridade que podem aceitar dispositivos móveis usados.

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
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

Recursos

Tornando seguro seu novo Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Cópia de Segurança (Backup) e Restauração:	https://securingthehuman.sans.org/ouch/2015#august2015
Curso “Advanced Smartphone Forensics”, em inglês:	https://sans.org/for585
Arquivos da publicação 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

