OUCH! | Junho de 2014

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Descarte de seus Dispositivos Móveis

Visão Global

Os dispositivos móveis, como smartphones e tablets, continuam avançando e inovando em um ritmo surpreendente. Como resultado, muitos de nós substituímos nossos dispositivos móveis regularmente, como a cada 18 meses. Infelizmente, muitas pessoas simplesmente descartam seus dispositivos móveis antigos sem pensar sobre a quantidade de dados pessoais têm acumulado neles. Neste informativo vamos abordar quais tipos de informação pessoal podem estar no seu dispositivo móvel e como você pode limpá-lo de forma segura antes de descartar ou devolvê-lo. Se o seu dispositivo móvel foi concedido pela sua empresa ou tem quaisquer dados organizacionais armazenados nele, não se esqueça de verifique com o seu empregador os procedimentos de backup e descarte adequado antes de seguir os passos abaixo.

Editor Convidado

Christopher Crowley (**@CCrowMontance**; **+Chriscrowley**) é consultor e trabalha em Washington, DC. Ele é o principal instrutor para o curso do Instituto SANS “Mobile Device Security and Ethical Hacking” (SEC575) e autor de “Incident Response Team Management” (MGT535).

Suas Informações Pessoais

Os dispositivos móveis armazenam mais dados confidenciais do que você pode perceber, provavelmente até mais do que seu computador. As informações normalmente armazenadas por um dispositivo móvel podem incluir:

- Locais onde você vive, trabalha e visita com frequência;
- Informações detalhadas de todos os contatos da sua agenda, incluindo família, amigos e colegas de trabalho;
- Histórico de chamadas, incluindo chamadas recebidas, discadas e não atendidas;
- Mensagens de texto e de voz;
- Conteúdo de conversas (chat) dentro de aplicações como jogos e mídias sociais;
- Histórico de localização com base em coordenadas de GPS ou de celular;
- Histórico de navegação, cookies (arquivos com informações sobre suas escolhas pessoais durante a navegação web) e páginas em cache (armazenadas previamente para consulta posterior mais rápida);
- Fotos, vídeos, gravações de áudio e e-mails pessoais;
- Senhas armazenadas e acesso a contas pessoais, como a do seu banco ou e-mail;
- Acesso a fotos, arquivos ou informações armazenadas em Nuvem (Cloud);
- Informações relacionadas à saúde, incluindo a sua frequência cardíaca, pressão arterial ou dieta.

Limpando seu Dispositivo

Como explicado, pode haver uma enorme quantidade de informações confidenciais em seu dispositivo móvel. Independentemente de como você vai se desfazer dele, como doá-lo, dar a outro membro da família, revendê-

Descarte de seus Dispositivos Móveis

lo ou até mesmo jogá-lo fora, você precisa ter certeza de que apagou primeiro todas as suas informações confidenciais. Além disso, você precisa apagar suas informações se você estiver devolvendo seu dispositivo móvel ou trocando por um novo. Se não o fizer, quem ficar com o dispositivo móvel poderá ser capaz de acessá-las facilmente. No entanto, antes de começar a limpá-lo, você provavelmente precisará fazer backup de todos os dados, incluindo fotos, vídeos ou qualquer outra informação. Depois de limpá-lo você não será capaz de recuperar qualquer um desses dados.

Quando descartar o seu dispositivo móvel, certifique-se de fazer uma redefinição de fábrica e remover os cartões SIM ou SD instalados nele.

Depois de fazer o backup de seus dados, você precisa apagá-los de forma segura. Excluir simplesmente os arquivos, fotos ou dados não é suficiente. Os dados que foram apagados podem ser facilmente recuperados usando ferramentas gratuitas encontradas na Internet. Por isso você precisa apagar com segurança todos esses dados, o que é chamado de limpeza. Esse processo, na verdade substitui as informações garantindo que não possam ser recuperadas. A maneira mais fácil de fazer isso é usar a função “restaurar a configuração de fábrica” do dispositivo. Isto irá devolvê-lo à condição em que estava quando você o comprou. Descobrimos que restaurar a configuração de fábrica irá fornecer o método mais seguro e mais simples para a remoção de dados do seu dispositivo móvel. A função de restaurar a configuração de fábrica varia entre os dispositivos. Listamos abaixo os passos para os três dispositivos mais populares.

- Dispositivos iOS da Apple: Ajustes / Geral / Redefinir / Apagar Todo o Conteúdo e Ajustes
- Dispositivos Android: Configurações / Privacidade / Restaurar padrão de fábrica;
- Windows Phones: Configurações / Sobre / Restaurar seu telefone.

Se você ainda tiver dúvidas sobre como restaurar a configuração de fábrica, consulte o manual do proprietário ou o site do fabricante. Lembre-se que simplesmente apagar seus dados pessoais não é suficiente, uma vez que eles podem ser facilmente recuperados.

SIM / Cartões de Armazenamento Externo

Além dos dados armazenados no seu dispositivo, você também precisa considerar o que fazer com o seu cartão SIM (Subscriber Identity Module). Um cartão SIM é o que um dispositivo móvel usa para fazer uma conexão celular de voz ou dados. Quando você restaura a configuração de fábrica no seu aparelho, o cartão SIM mantém as informações sobre sua conta. Se você vai manter o seu número de telefone e mudar para um dispositivo novo, fale com o vendedor de telefone sobre a transferência de seu cartão SIM. Se isso não for possível, por exemplo, se o seu novo telefone usa um cartão SIM de tamanho diferente, guarde seu cartão SIM antigo e o destrua fisicamente para evitar que outra pessoa use.

Descarte de seus Dispositivos Móveis

Finalmente, alguns dispositivos móveis utilizam um cartão SD (Secure Digital) separado para armazenamento adicional. Estes cartões de memória, muitas vezes contêm fotos, aplicativos do smartphones e outros conteúdos confidenciais. Lembre-se de remover todos os cartões de armazenamento externo do seu dispositivo móvel antes de descartá-los (em alguns dispositivos, os cartões SD podem estar escondidos no compartimento da bateria do seu dispositivo, possivelmente, embaixo da bateria). Estes cartões podem muitas vezes ser reutilizados em novos dispositivos móveis, ou podem ser usados como armazenamento genérico no seu computador, com um adaptador USB. Caso não seja possível reutilizar o cartão SD, recomendamos que você o destrua fisicamente, assim como o seu cartão SIM antigo.

Se você não tem certeza sobre qualquer uma das etapas abordadas neste informativo, leve o seu dispositivo móvel para a loja onde o comprou e obtenha ajuda de um técnico treinado. Finalmente, se você estiver jogando o seu dispositivo móvel fora, pedimos que você considere a possibilidade de doá-lo, ao invés disso. Há muitas organizações de caridade que aceitam 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 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

Diretrizes Americanas para limpeza de mídias de armazenamento - NIST SP800-88 Rev. 1 (em inglês):
http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
OUCH! Backups:
http://www.securingthehuman.org/ouch/2013#september2013
What Is Cloud Backup?:
http://open-tube.com/what-is-cloud-backup-a-beginners-guide-to-cloud-backup/

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