Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- **Информацията ви**
- **Изтриване на устройството**
- **SIM / Карти с памет**

Безопасна раздяла с мобилно устройство

Преглед

Мобилните устройства, като смартфони, умни часовници и таблети, продължават да се развиват с удивителна бързина. В резултат на това има хора, които сменят мобилните си устройства често – някои от тях всяка година. За съжаление твърде много хора изхвърлят устройствата си без да се замислят за личните данни, които са съхранени в тях. В този бюлетин ще обхванем какви видове лична информация би могла да се намери на мобилното ви устройство, и как сигурно да я изтриете преди да рециклирате или върнете устройството. Ако устройството ви е предоставено от работодател, или има съхранени работни данни, обърнете се към прекия си началник относно процедурите по архивиране и рециклиране преди да продължите със следващите стъпки.

Гост-редактор

Хедър Махалик (**@HeatherMahalik**; **+HMahalik**) е Главен Научен Следовател начело на разследващия екип на ManTech CARD. Тя води и е съавтор на курса на SANS Institute Advanced Smartphone Forensics (FOR585) и е инструктор по Windows Forensic Analysis (FOR408). Има блог на **smarterforensics.com**.

Вашата информация

Мобилните устройства съхраняват много повече лични данни отколкото може би си представяте, често повече отколкото дори компютъра ви. Типично това може да включва:

- Къде живеете, работите и често посещавани от вас места
- Подробности за всичките ви контакти в адресната книга и приложенията, включително семейство, приятели и колеги
- История на обажданията – входящи, изходящи и пропуснати обаждания
- Текстови (SMS), гласови и мултимедийни съобщения
- История на разговорите в приложения като чатове, игри и социални мрежи
- История на местоположенията ви, базирана на GPS координати или клетки на мобилните мрежи
- История на уеб сърфирането, история на търсенията, бисквитки и временно съхранени страници
- Лични снимки, видео и аудио записи, имейли
- Съхранени пароли и достъп до лични сметки, като например онлайн банкиране или имейл
- Достъп до снимки, файлове или информация съхранена в Облака
- Здравна информация, включително възрастта ви, сърдечен ритъм, кръвно налягане или диети

Изтриване на данните на устройството

Както е видно, най-вероятно има огромно количество лична информация на мобилното ви устройство. Независимо от това какво ще направите с устройството, било то даряване, замяна с ново, даване на друг член от семейството,

Безопасна раздяла с мобилно устройство

продажба или дори просто изхвърляне на боклука, трябва първо да се уверите, че всичката тази лична информация е напълно изтрита. Вероятно не знаете, че простото изтриване на данни не е достатъчно – данните могат да бъдат възстановени с прости програми налични в Интернет. Вместо това е нужно данните да се изтрият по сигурен начин, наречен пълно изтриване (wiping). Това всъщност представлява записване на данни върху вече съществуващите, така че предишните вече да не могат да бъдат възстановени. Напомняме, че преди пълното изтриване на всички данни най-вероятно бихте искали да им направите архивно копие, за да можете лесно да ги използвате на новото си устройство.

Когато се разделяте с мобилното си устройство, не забравяйте да направите фабрично нулиране и да махнете SIM картата, както и всички SD карти, ако вашето устройство има такива.

Най-лесният начин да направите сигурно пълно изтриване на данните на устройството си е да използвате функцията за „фабрично нулиране“ (“factory reset”). Това ще върне устройството в състоянието, в което е било веднага след покупката му. Нашето заключение е, че фабричното нулиране е най-сигурният и лесен начин за премахване на данни от мобилни устройства. Функцията за фабрично нулиране е различна при различните устройства; тук са изброени стъпките за две от най-често срещаните устройства.

- Apple iOS устройства: Settings | General | Reset | Erase All Content and Settings
- Android устройства: Settings | Privacy | Factory Data Reset

За съжаление, премахването на лични данни от устройства с Windows Phone не е толкова лесно като просто фабрично нулиране. В ход са допълнителни проучвания за начини за пълно изтриване на данните ви от устройството. Ако все още имате въпроси относно как да направите фабрично нулиране, проверете ръководството на потребителя или уебсайта на производителя. Запомнете, че простото изтриване на личните ви данни не е достатъчно, тъй като те могат лесно да бъдат възстановени.

SIM & Карти с памет

В допълнение към данните съхранени на вашето устройство, вие трябва да обмислите и какво да правите със своята SIM (Subscriber Identity Module) карта. SIM картата е онова, което вашето мобилно устройство използва, за да осъществи клетъчно свързване или свързване за пренос на данни. Когато извършите фабрично нулиране на устройството, SIM картата запазва информация за акаунта ви и е свързана с вас - потребителя. Ако запазвате телефонния си номер и само сменяте устройството, говорете със своя доставчик на услуги относно прехвърляне на картатата ви. Ако това не е възможно, ако например новият ви телефон използва SIM карта с различен размер, задръжте старата си SIM карта и физически я нарежете или унищожете, за да предотвратите възможността някой друг да я използва.

Безопасна раздяла с мобилно устройство

И накрая, някои мобилни устройства използват отделна SD (Secure Digital) карта за допълнително място за съхранение. Тези карти за съхранение често съдържат снимки, приложения за смартфони и друго съдържание с поверителен характер. Не забравяйте да свалите всички карти за съхранение от мобилното си устройство преди да го изхвърлите (за някои устройства SD картите могат да са скрити в отделението за батерията на устройството, възможно е и под батерията). Тези карти могат често да бъдат използвани отново в нови мобилни устройства или да бъдат използвани като общо допълнително съхранение на компютъра ви чрез USB адаптер. Ако не е възможно да използвате SD картата отново, тогава, точно както и със старата SIM карта, препоръчваме ви физически да я унищожите.

АКо не сте сигурни за някоя от стъпките, които се описани в този бюлетин, занесете мобилното си устройство в магазина от който сте го купили и поискайте помощ от обучен техник. И накрая, ако ще изхвърляте мобилното устройство на боклука, молим ви вместо това да обмислите да го дарите за благотворителност. Има много отлични благотворителни организации, които приемат използвани мобилни устройства.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Обезопасяване на новия таблет:	https://securingthehuman.sans.org/ouch/2016#january2016
Архивиране и възстановяване:	https://securingthehuman.sans.org/ouch/2015#august2015
Курс по Advanced Smartphone Forensics:	https://sans.org/for585
Архиви на бюлетина OUCH:	https://securingthehuman.sans.org/ouch/archives

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова

