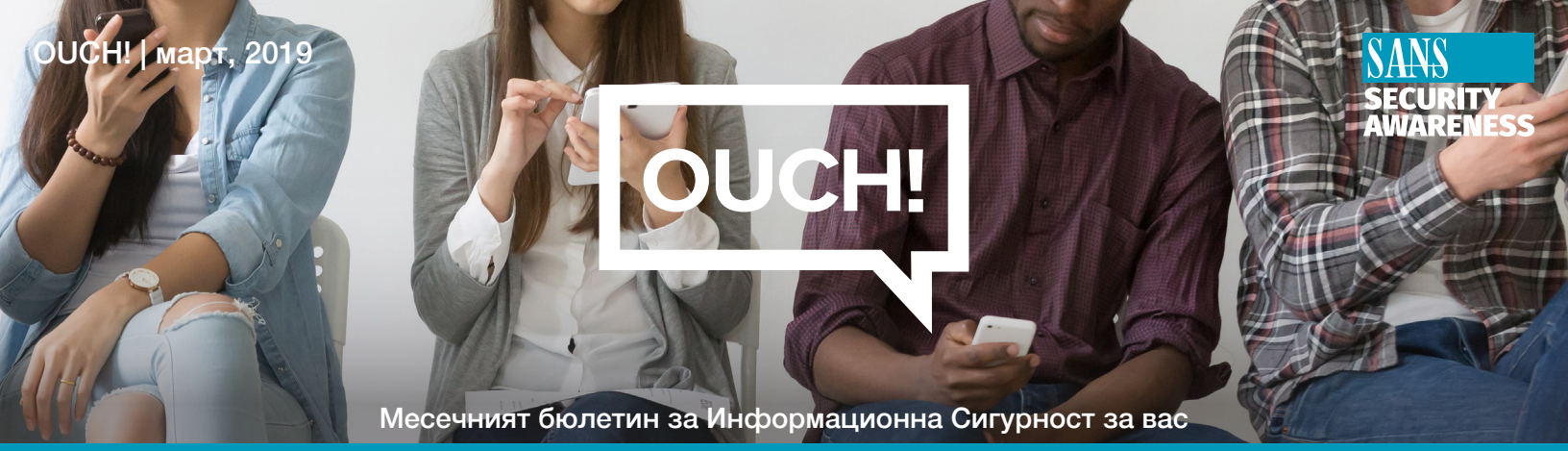

Месечният бюлетин за Информационна Сигурност за вас

Изхвърляне на мобилно устройство

Преглед

Мобилните устройства, като смартфони, смарт часовници и таблети, продължават да се развиват с главозамайваща скорост. В резултат на това много хора сменят мобилните си устройства често – понякога всяка година. За съжаление хората често не осъзнават колко лична информация се намира в тези устройства. По-надолу ще разгледаме какво може да се намери на мобилното ви устройство и как сигурно да го изтриете преди да се разделите с него. Ако мобилното устройство ви е дадено от работодател, или има каквато и да е служебна информация на него, допитайте се до мениджър относно правилните процедури по архивиране и изхвърляне.

Вашата информация

Мобилните устройства съхраняват повече лична информация отколкото много хора осъзнават, далеч повече от компютъра ви.

⚠

- **Къде живеете, работите и кои места посещавате;**
- **Контактите на всеки в адресната ви книга, включително семейство, приятели и колеги;**
- **История на обажданията, включително изходящи и входящи разговори, гласова поща и пропуснати обаждания;**
- **Съобщения или чат сесии в приложения, игри и социални мрежи;**
- **История на сърфиране, търсене, бисквитки и кеширани страници;**
- **Лични снимки, видеа и звукови записи;**
- **Запазени пароли и достъп до ваши акаунти, като например такива за банкиране, социални мрежи или имейл;**
- **Здравна информация, включително възраст, пулс, история на тренировки, кръвно налягане.**

Нулиране на устройството

Независимо как ще се отървете от мобилното си устройство – даряване, размяна за ново, даване на близък, продажба или дори изхвърляне, първо трябва да сте сигурни, че всичката тази лична информация е изтрита. Обикновеното изтриване на данни не е достатъчно; вместо това трябва да изтриете всички данни на устройството. Най-лесният начин за това е да го нулирате. Тази функция е различна при различните устройства; по-долу са изброени стъпките за двата най-често срещани вида устройства. Още по-сигурен начин е да включите криптиране на устройството преди да му върнете фабричните настройки. На повечето съвременни устройства това просто изисква да е активирано заключването на

екрана (което трябва да сте включили така или иначе). И накрая, препоръчваме да архивирате данните от устройството преди да ги изтриете.

- **Apple iOS Устройства: Settings | General | Reset | Erase All Content and Settings**
- **Android Devices: Настройки | Поверителност | Възстановяване на фабрични настройки**

СИМ & външни карти

Освен самото устройство, трябва да вземете предвид и СИМ (SIM, Subscriber Identity Module) картата. СИМ картата е това, което позволява на мобилно устройство да се свързва към мобилна мрежа. Когато изтриете данните в устройството, в СИМ картата остава информация относно акаунта ви, която е свързана с вас. Ако запазвате мобилния си номер и просто искате ново устройство, говорете с мобилния си оператор за трансфер на СИМ картата. Ако това не е възможно, задръжте СИМ картата и я унищожете физически, за да сте сигурни, че никой няма да може да я използва отново и да получи достъп до ваша информация или акаунти. И накрая, някои Андроид базирани телефони използват допълнителна карта с памет - SD (Secure Digital) карта за съхранение. Извадете тези външни карти за съхранение от мобилното устройство преди да се разделите с него. Тези карти често могат да бъдат използвани отново в други мобилни устройства, или за обикновено съхранение на компютър чрез USB адаптер. Ако не е възможно да използвате отново SD карта, също както СИМ картата, ви препоръчваме да я унищожите физически.

Ако не сте сигурни за някоя от стъпките по-горе, или ако опциите за нулиране на устройството ви са различни, занесете устройството в магазина откъдето е купено и поискайте помощ от обучен техник. И накрая, ако просто ще изхвърлите устройството, помислете дали да не го дарите. Има много благотворителни организации, на които може да се помогне по този начин, и много мобилни оператори имат кутии за оставяне на дарени устройства в магазините си.

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

Гост-редактор

Кристофър Кроули *(@CCrowMontance) е независим консултант в района на Вашингон, специализиращ в оперативната сигурност. Активен е в Туитър и в личния си блог. Скоро ще бъде публикувана негова книга на тема Центрове по Оперативна сигурност. Той е също така старши инструктор в SANS Institute.*

Ресурси

SANS курс: Pen Testing Mobile Devices:	https://sans.org/sec575
SANS курс: Advanced Smartphone Forensics Course:	https://sans.org/for585
FTC Advice on Disposing Your Mobile Device:	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device