Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Какую информацию содержит мобильное устройство**
- **Стирание данных с вашего устройства**
- **SIM / Карта памяти**

Безопасная утилизация мобильного устройства

Обзор

Мобильные устройства, такие как смартфоны, умные часы и планшеты, продолжают совершенствоваться с удивительной скоростью. Как результат, некоторые люди меняют свои мобильные устройства каждый год. К сожалению, далеко не все люди заботятся об удалении персональных данных с устройств при их утилизации. В этом выпуске мы поговорим о том, какого рода персональная информация может содержаться на мобильных устройствах, как вы можете правильно её удалить перед утилизацией или возвратом устройства. Если вы используете служебное устройство или на вашем устройстве есть рабочая информация, обсудите с вашим руководителем процедуру надлежащего резервного копирования перед тем, как выполнить следующие шаги.

Об авторе

Хизер Махалик (**@HeatherMahalik**; **+HMahalik**) – ведущий учёный-криминалист, возглавляющая направление криминальных расследований компании ManTech CARD. Она - соавтор и преподаватель курсов Института SANS: «Криминалистический анализ смартфонов – Продвинутый уровень» (FOR585) и «Криминалистический анализ Windows (FOR 408)». Она ведёт блог **smarterforensics.com**.

Какую информацию содержит мобильное устройство

На мобильном устройстве содержится гораздо больше личной информации, чем вы думаете, и иногда даже больше, чем на компьютере. Информация может быть следующая:

- Где вы живёте, работаете и какие места часто посещаете
- Детальная информация о всех контактах из вашей адресной книги и приложений, включая членов семьи, друзей и коллег
- История звонков, включая входящие, исходящие и даже пропущенные
- Текстовые (SMS), голосовые и мультимедиа сообщения
- Переписка через защищённый чат, игры и социальные сети
- История всех перемещений, основанная на данных GPS или использования мобильного роуминга
- История просмотра интернет сайтов, запросы поисковика, кэшированные страницы и куки страниц
- Личные фото, видео, аудио записи и электронная почта
- Пароли и доступы к личным учётным записям, например, онлайн банкинга или электронной почты
- Доступ к фото и файлам, хранящимся на «Облаке»
- Информация о здоровье, включая возраст, частоту пульса, давление или диету

Безопасная утилизация мобильного устройства

Стирание данных с вашего устройства (wiping)

Как вы видите, на мобильном устройстве содержится огромное количество личной информации. Независимо от способа утилизации вашего устройства: пожертвования, обмена на новый, передачу другому члену семьи, продажу или даже отправки в мусор, вы прежде всего должны убрать всю личную информацию с него. Вы должны знать, что простого удаления недостаточно, так как данные можно легко восстановить с помощью бесплатных инструментов из Интернета. Вот почему необходимо безопасно удалить все данные с устройства (wiping). Безопасное удаление данных представляет собой перезапись информации, после которой её нельзя восстановить. Помните, что перед стиранием данных необходимо сделать резервную копию всех данных для переноса на новое устройство.

когда вы утилизуете ваше мобильное устройство, обязательно сделайте «возврат к настройкам производителя» и удалите все SIM и SD карты из него.

Самый простой способ стереть данные с вашего устройства – это воспользоваться функцией «возврат к настройкам производителя». Это вернёт устройство к его состоянию на момент покупки. Этот способ сброса настроек считается самым простым и безопасным методом удаления данных с мобильного устройства. Функция возврата к настройкам производителя варьируется в зависимости от устройства; ниже приведены шаги для двух самых популярных типов устройств:

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

К сожалению, удаление данных с устройств Windows Phone несколько сложней, чем «возврат к настройкам производителя». Сейчас изучаются более надёжные способы удаления данных с этого устройства. Если вам требуется дополнительная информация по функции «сброс к настройкам производителя», советуем изучить «Руководство Пользователя» устройства или поискать информацию об этой процедуре на сайте производителя. Но помните, простого удаления данных недостаточно, так как их легко можно восстановить.

SIM / Карта памяти

Давайте ещё поговорим об информации, которая хранится на SIM Карте (Subscriber Identity Module - Модуль Идентификации Абонента). Такие карты дают возможность мобильным устройствам использовать сотовое соединение. Вы можете вернуть устройство к настройкам производителя, но на SIM карте останется информация

Безопасная утилизация мобильного устройства

о вас, как абоненте. Если вы хотите сохранить номер телефона, то попросите вашего провайдера перенести SIM карту на новое устройство. Если это невозможно, например, в новом телефоне другой размер SIM карты, просто физически уничтожьте старую SIM карту, чтобы ей больше никто не мог воспользоваться.

Некоторые мобильные устройства используют карту SD (Secure Digital) как дополнительный носитель информации. Эти карты часто содержат фотографии, мобильные приложения и другую частную информацию. Не забудьте перед утилизацией вашего устройства удалить из него все карты – носители данных (в некоторых устройствах ваши SD карты могут находиться в батарейном отсеке устройства, иногда под батареей). Эти карты часто могут быть использованы в ваших новых мобильных устройствах; их также возможно использовать как обычную флешку на вашем компьютере (через адаптер USB). Если ваша карта SD не может быть использована, тогда, как и в случае со старой SIM картой, просто физически уничтожьте её.

Если вы не вполне уверены в выполнении рекомендаций, приведённых в этом выпуске, отнесите ваше мобильное устройство в магазин, где вы его купили, и попросите помощи опытного техника. Наконец, если вы собираетесь выбросить ваше мобильное устройство, рассмотрите возможность передачи его в одну из благотворительных организаций.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Безопасность планшета: https://securingthehuman.sans.org/ouch/2016#january2016

Резервное копирование и восстановление данных: https://securingthehuman.sans.org/ouch/2015#august2015

Криминалистический анализ смартфонов – Продвинутый уровень» (FOR585): https://sans.org/for585

Архив OUCH!: https://securingthehuman.sans.org/ouch/archives

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова

