OUCH! Декабрь 2022

Ежемесячный информационный бюллетень по безопасности

Утилизация вашего мобильного устройства

Обзор

Мобильные устройства, такие как смартфоны, смарт-часы и планшеты, продолжают развиваться и внедрять инновации с поразительной скоростью. В результате вы можете менять новое устройство не реже одного раза в год. К сожалению, вы можете не осознавать, сколько личных данных хранится на ваших устройствах — гораздо больше, чем на вашем компьютере. Ниже мы расскажем о типах данных на ваших мобильных устройствах и о том, как вы можете безопасно стереть данные с устройства перед его утилизацией или заменой. Если ваше мобильное устройство было выдано вам по работе, сначала уточните у своего руководителя порядок утилизации.

Ваша информация

Ваши мобильные устройства хранят больше конфиденциальных данных, чем вы думаете, включая файлы . . .

Место, где вы живете и работаете, и ваши ежедневные привычки в поездках.
Контактные данные каждого в адресной книге, в том числе семьи, друзей и коллег.
История телефонных звонков, включая входящие, исходящие, голосовую почту и пропущенные вызовы.
Текстовые сообщения или сеансы чата в приложениях, таких как безопасный чат, игры и социальные сети.
Личные фото, видео и аудиозаписи.
Сохраненные пароли и доступ к вашим счетам, таким как ваш банк, социальные сети или электронная почта.
Информация о здоровье, включая ваш возраст, частоту сердечных сокращений, историю тренировок или кровяное давление.
Финансовая информация, включая кредитные карты, способы оплаты и транзакции.

Удаление данных с вашего устройства

Независимо от того, как вы утилизируете свое мобильное устройство, например, отдаете его в дар, обмениваете на новое, отдаете кому-то, перепродаете или сдаете на переработку, сначала удалите всю конфиденциальную информацию. Не думайте, что следующий владелец «поступит правильно». Первым шагом является резервное копирование вашего устройства, чтобы вы могли восстановить и перенести все свои данные и настройки на новое устройство. После резервного копирования вы захотите сбросить настройки устройства, так как это стирает ваши данные и сбрасывает их до заводских значений по умолчанию. Во время процесса сброса вам может быть предложено ввести свой облачный пароль, чтобы разорвать любые связи с этим устройством в облаке; обязательно сделайте это. Приведенные ниже шаги сброса предназначены для двух наиболее распространенных устройств — Apple и Android.

Устройства Apple iOS: Настройки | Общие | Сброс | Удалить содержимое и настройки.

Android-устройства: Настройки | Система | Сбросить параметры | Стереть все данные (эти параметры различаются в зависимости от производителя вашего устройства).

SIM-карта и внешние карты

В дополнение к вашему устройству вам также нужно подумать, что делать с вашей SIM-картой (Модуль идентификации абонента). Это маленькая карточка в вашем телефоне, выданная вам оператором мобильной связи; это то, что идентифицирует ваше устройство и позволяет ему установить сотовую связь или подключение для передачи данных. Когда вы удаляете информацию с устройства, SIM-карта сохраняет информацию о вашей учетной записи и привязана к вам. Если вы сохраняете свой номер телефона и переходите на новое устройство, поговорите с поставщиком услуг телефонной связи о передаче SIM-карты. Если это невозможно, сохраните старую SIM-карту и физически уничтожьте ее. Многие из современных смартфонов имеют так называемую eSIM, которая представляет собой виртуальную SIM-карту, а не физическую SIM-карту. eSIM стирается в процессе сброса.

Наконец, некоторые мобильные устройства Android используют съемную SD-карту для дополнительного хранения. Удалите внешнюю карту памяти из вашего мобильного устройства перед утилизацией. Внешниии карты памяти часто могут быть повторно использованы в новых мобильных устройствах или могут использоваться в качестве универсального хранилища на вашем компьютере с USB-адаптером. Если повторное использование SD-карты невозможно, то, как и вашу старую SIM-карту, мы рекомендуем вам её физически уничтожить.

Если вы не уверены в каком-либо из шагов, описанных выше, или если у вас другие параметры сброса устройства, отнесите свое мобильное устройство в магазин, в котором вы его купили, и обратитесь за помощью к квалифицированному специалисту. Наконец, если вы решили выбросить устройство, рассмотрите возможность пожертвовать его. Есть много прекрасных благотворительных организаций, которые принимают использованные мобильные устройства, и у многих мобильных провайдеров есть в магазинах специальные для этого ящики.

Приглашенный редактор

Хитер Махалик (@HeatherMahalik) Is the Sr. Директор отдела цифрового интеллекта в Cellebrite и SANS, руководитель учебной программы DFIR, автор FOR585и научный сотрудник факультета SANS. Карьера Хитер была основана на криминалистических исследованиях и 20-летнем опыте работы с конкретными делами. Она ведет блог на www.smarterforensics.com/blog.

Ресурсы

Безопасное использование мобильных приложений: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Защита ваших мобильных устройств: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Пожертвование мобильного телефона: https://www.makeuseof.com/best-places-to-donate-your-old-phone/
Курс SANS: расширенный курс по криминалистике для смартфонов: https://sans.org/for585

Роман Полаков