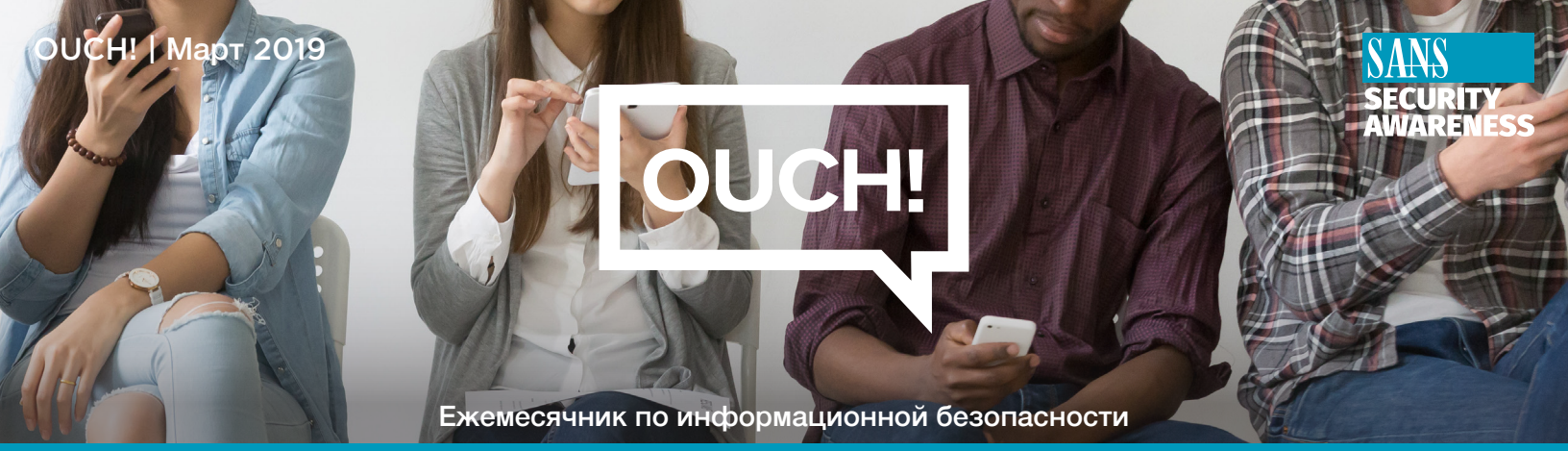

Ежемесячник по информационной безопасности

Утилизация вашего мобильного устройства

Обзор

Мобильные устройства, такие как смартфоны, умные часы и планшеты, продолжают развиваться и внедрять инновации с удивительной скоростью. В результате некоторые люди каждый год меняют свои мобильные устройства. К сожалению, люди часто не понимают, сколько личных данных на этих устройствах. Ниже мы расскажем о том, что может быть на вашем мобильном устройстве, и о том, как вы должны безопасно с него всё стереть, прежде чем утилизировать. Если ваше мобильное устройство было выдано вам вашим работодателем или на нем хранятся какие-либо рабочие данные, обязательно сначала проконсультируйтесь с вашим руководителем о правильных процедурах резервного копирования и утилизации.

Ваша информация

Мобильные устройства хранят более конфиденциальные данные, чем многие думают, зачастую гораздо больше, чем ваш компьютер.

⚠

- **Где вы живете, работаете и какие места посещаете**
- **Контактные данные для 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**
- **История веб-браузера, история поиска, куки-файлы и кэшированные страницы**
- **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**

Удаление информации с вашего устройства

Независимо от того, как вы распоряжаетесь своим мобильным устройством, например, пожертвуете его, меняете на новое, отдаете другому члену семьи, перепродаете или даже выбрасываете его, вы должны быть уверены, что сначала удалили всю конфиденциальную информацию. Простое удаление данных не достаточно, вместо этого вы должны надежно стереть все данные на устройстве. Самый простой способ сделать это - перезагрузить ваше устройство. Функция сброса зависит от устройства; Ниже перечислены шаги для двух наиболее распространенных устройств.

Еще более безопасный шаг - убедиться, что на вашем устройстве включено шифрование перед его сбросом. На большинстве современных мобильных устройств самый простой способ сделать это - просто включить блокировку экрана (которую, надеюсь, вы уже включили). Наконец, мы настоятельно рекомендуем сделать резервную копию с вашего устройства перед его перезагрузкой.

- **Устройства Apple iOS: Настройки | Общие | Сброс | Удалить содержимое и настройки**
- **Устройства Android: Настройки | Конфиденциальность | Сброс настроек**

SIM-карта и внешние карты

В дополнение к вашему устройству вам также нужно подумать, что делать с вашей SIM-картой (Модуль идентификации абонента). SIM-карта - это то, что мобильное устройство использует для сотовой связи или 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 свою старую SIM-карту и физически уничтожьте ее, чтобы предотвратить повторное использование ее кем-либо другим, чтобы выдать себя за вас и получить доступ к вашей информации или учетным записям. 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

Кристофер Кроули *(@CCrowMontance) является независимым консультантом в Вашингтоне, округ Колумбия, специализирующийся на операциях безопасности. Он иногда пишет в Твиттере и блогах. Следите за его предстоящей книгой по операционным центрам безопасности. Он старший преподаватель в институте SANS.*

Ресурсы

Курс SANS:	https://sans.org/sec575
Курс SANS:	https://sans.org/for585
FTC Советы по утилизации вашего мобильного устройства:	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device

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:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Алэн Вэггонер, Шерил Конли*