Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Меры предосторожности
- Что делать, если вы потеряли мобильное устройство или его украли

Потеря мобильного устройства

ОБ АВТОРЕ

Автор данной статьи - Хизер Махалик. Хизер - сертифицированный инструктор SANS. Хизер возглавляет лабораторию экспертизы мобильных устройств компании Basis Technology в Вашингтоне, США. Она ведёт записи в Twitter как @heathermahalik.

ОБЗОР

Мы используем мобильные устройства для связи, для получения и передачи информации. Поэтому часто эти устройства содержат конфиденциальную информацию, например, электронную почту, текстовые сообщения, голосовую почту, календарь событий, места нахождения, фото и видео. Если вы потеряете мобильное устройство или его украдут, то любой, имея физический доступ к вашему устройству, может получить доступ к этой информации и создать серьёзную угрозу для вас, ваших знакомых и вашей компании. В этом выпуске мы обсудим способы защиты информации на устройстве в случае его утери или кражи.

ВНИМАНИЕ:

Большинство советов в статье применимы для личных мобильных устройств. Если вам выдали служебное мобильное устройство, и оно содержит конфиденциальную информацию вашей компании, то необходимо следовать политикам вашей организации по обеспечению безопасности мобильных устройств.

МЕРЫ ПРЕДОСТОРОЖНОСТИ

Пожалуй, есть только один наиболее надёжный способ защиты ваших устройств. Защиту следует начать с использования ПИН-кода, пароля или шаблона блокировки доступа к устройствам. Эти меры гарантируют доступ к информации только авторизованных пользователей.

ПИН. ПИН (Персональный Идентификационный Номер) – это номер, который нужно ввести для доступа к мобильному устройству.

Пароль. Использование пароля для мобильных устройств аналогично использованию пароля для компьютера и онлайн аккаунтов. Сложный пароль обеспечивает более надёжную защиту, чем ПИН.

Шаблон блокировки (Pattern Lock). Шаблон или уникальный рисунок, который вы рисуете на экране устройства.

Настоятельно рекомендуем включить опцию удаления информации с устройства в случае нескольких неудачных попыток доступа – это поможет защитить устройство от несанкционированного использования. Если включите данную опцию, будьте осторожны: дети

Потеря мобильного устройства

могут из любопытства попытаться получить доступ к устройству. Независимо от способа аутентификации, используйте сложный ПИН-код, пароль или шаблон блокировки и никому его не сообщайте.

- Дистанционное отслеживание устройства и удаление информации: большинство мобильных устройств поддерживает программное обеспечение, которое может дистанционно найти устройство и/или стереть информацию с пропавшего устройства. На некоторые устройства нужно установить это программное обеспечение. В устройства iPhone и iPad встроена специальная функция «Найти мой iPhone», которая активируется с помощью Apple ID. Устройства BlackBerry обладают аналогичной возможностью; функция подключается через сервер BES. Устройства на базе Android требуют установки специальной программы для удаленного обнаружения и удаления данных.
- Шифрование: если кто-то получит физический доступ к вашему устройству, то он может с помощью современных технологий обойти ваш ПИН-код или пароль и завладеть информацией. Шифрование помогает защитить от таких сложных видов атак. Некоторые мобильные устройства автоматически шифруют данные, для других нужно установить специальную программу для шифрования. Например, iPhone и iPad автоматически шифруют данные аппаратными способами. Ваши данные защищены и без пароля. В устройствах на базе Android эту функцию нужно активировать в меню конфигурации безопасности.
- Резервное копирование: резервное копирование дает возможность быстро восстановить информацию с потерянного или украденного устройства. Резервное копирование нужно проводить регулярно с помощью следующих методов:

с помощью простых действий вы можете защитить себя в случае потери мобильного устройства.

- Резервное копирование непосредственно на компьютер
- iCloud - бесплатная услуга для всех владельцев iPhone, iPad и iPod. Пользователь может выбрать контакты, письма электронной почты, календарь, фотографии, музыку и другие файлы для сохранения в своей защищенной области iCloud

Потеря мобильного устройства

- Google Cloud – бесплатный сервис резервного копирования для устройств на базе Android. Функционально Google Cloud похож на iCloud.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ПОТЕРЯЛИ МОБИЛЬНОЕ УСТРОЙСТВО ИЛИ ЕГО УКРАЛИ

Если вы потеряли мобильное устройство или его украли, выполните следующие действия:

- Если пропавшее устройство выдано вашей организацией или на нём хранится служебная информация, то немедленно свяжитесь со Службой Безопасности вашей компании и следуйте их указаниям.
- Если установлено специальное программное обеспечение, то дистанционно удалите все данные. Это исключит риски в случае доступа к устройству. Если устройство украли, то необходимо сначала обратиться в правоохранительные органы и сообщить о возможности отследить устройство перед тем, как удалить данные. В этом случае не пытайтесь найти устройство самостоятельно.
- Сообщите поставщику услуг связи о потере или краже мобильного устройства. Компания заблокирует номер телефона; это исключит возможность звонить с вашего номера до тех пор, пока вы его не смените.
- После того, как смените устройство, восстановите информацию с резервной копии.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

20 приложений безопасности для Android:
http://preview.tinyurl.com/27qbb6w

10 приложений безопасности для iOS:
http://preview.tinyurl.com/bumb8vv

Google Cloud:
http://preview.tinyurl.com/cy49ntb

iCloud:
https://www.icloud.com/#find

Термины по информационной безопасности:
http://preview.tinyurl.com/6wkpae5

Ежедневные советы по безопасности SANS:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков