корпорация Российский учебник

Безопасность мобильных устройств

Галяев Владимир Сергеевич, Галяев Владимир Сергеевич
к.ф.-м.н., старший научный сотрудник
Лаборатории математического моделирования и информационных технологий
ФГАОУ ДПО ЦРГОП и ИТ

Дрофа
Вентана-Граф
Астрель
LECTA
Дрофа

О чем будем говорить

- основные угрозы мобильным устройствам;
- последствия "взлома" мобильного устройства;
- меры по защите мобильных устройств.

Что будем понимать под мобильными устройствами

Мобильные устройства – ряд устройств, который включает в себя смартфоны, планшеты, электронные книги, телефоны, КПК, главной особенностью которых является размер, выполняемые функции и специальная операционная система.

Мобильные операционные системы

Мировое распределение ОС на декабрь 2017

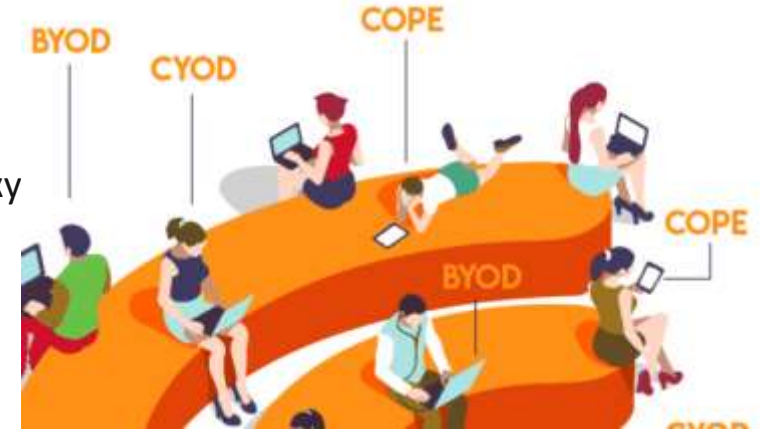
- Android – 71,58%
- iOS – 19,73%
- Windows 10 for mobile / Windows Phone – 1,13%
- Иные – 7,56%

Распределение ОС в России на декабрь 2017

- Android – 68,87%
- iOS – 26,56%
- Windows 10 for mobile – 2,54%
- Иные – 2,03%

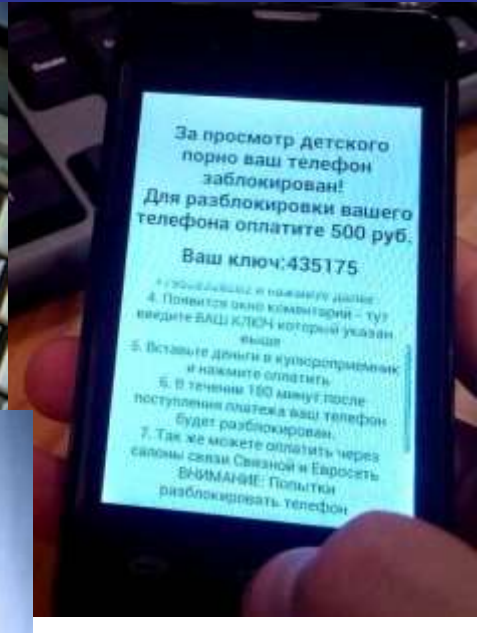
Модели использования мобильных устройств

- BYOD: Bring Your Own Device — «принеси свое устройство» — сотрудник предприятия использует свое личное мобильное устройство, в том числе и для рабочих задач, с ведома работодателя (возможно с компенсацией).
- CYOD: Choose Your Own Device — «выбери свое устройство» — предприятие предоставляет своим сотрудникам те устройства, которые оно само приобрело, с оформленным договором на оказание услуг связи и настроенными приложениями.
- COPE: Corporate-Owned, Personally Enabled — «корпоративные устройства, самостоятельное обслуживание») — предприятие предоставляет сотруднику смартфон или планшет, обычно с разрешением на использование этого устройства в личных целях тоже. Сотрудник (до определенной степени) самостоятельно отвечает за его настройку и текущее техническое обслуживание



Кроме денег …

- Потеря личных и корпоративных данных
- Отсутствие доступа к устройству и данным
- Репутационные потери



Основные угрозы мобильным устройствам

- Вредоносное программное обеспечение

- Социальная инженерия

- Физический доступ к устройству

Социальная инженерия

Киберпреступники используют методы социальной инженерии для проникновения в инфраструктуру организации или получения доступа к ресурсам и данным пользователя.

Социальная инженерия — совокупность приёмов и методов (из области социологии и психологии) и информационных технологий, которые позволяют создавать такие обстоятельства, которые приводят к конкретному действию со стороны пользователя, с использованием методов.

Фишинг

Фишинг — это метод социальной инженерии, целью которого является получение доступа к конфиденциальным данным пользователей, чаще всего логинам и паролям.

- Сообщение в электронной почте;
- Фальшивые обновления программ;
- Вшитые в документ исполняемые файлы (скрипты);
- Ссылки на поддельные сайты;
- Фишинговые сообщения в социальных сетях;
- Сообщения в мессенджерах или SMS;
- Фишинговое сообщение в push-уведомлении

Физический доступ к устройству – это не просто потеря смартфона?

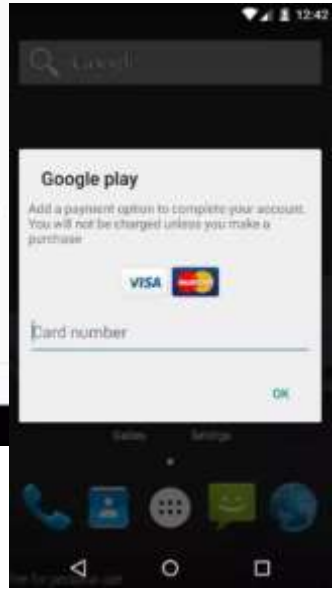
- Доступ к хранимым данным
- Доступ к информации в приложениях
- Управление онлайн-банкингом
- Генерация одноразовых паролей

Корпорация Российский учебник

Бесконтактные платежи – удобно … злоумышленникам

- Большинство современных Android-смартфонов оснащены модулем NFC. Android-троянец, который превращает смартфон жертвы в аналог ретранслятора NFC-сигнала.
- Через NFC можно украсть не «саму транзакцию», а информацию о банковской карте.
- Исследователи из британского Университета Суррей продемонстрировали возможность считывания по NFC данных на расстоянии около 80 см от смартфона с помощью компактного сканера.

Виды вредоносного программного обеспечения



Самое страшное в 2019

По оценкам экспертов "Positive Technology"

- Криптоджекинг
- Нарушение данных
- Небезопасные сети
- Социальная инженерия

Меры предосторожности

- Не храните критичные данные на устройстве.
- Установите программу по удаленному управлению смартфоном, чтобы стереть все данные и заблокировать доступ в случае его утери.
- Сделайте надежную резервную копию данных.
- Используйте надежные способы блокировки. Регулярно меняйте пароль.
- Не используйте мобильный банкинг с того же устройства, которое генерирует пароли для двухфакторной авторизации.
- С осторожностью используйте электронную почту – большинство злоумышленников по-прежнему использует этот канал.
- Устанавливайте только проверенное программное обеспечение из доверенных источников.
- Используйте проверенные Wi-Fi-каналы.
- Установите антивирусное программное обеспечение.
- Не получайте на своем устройстве права суперпользователя (режим разработчика).

Корпорация Российский учебник | Дрофа | Вентана-Граф

Какие симптомы?

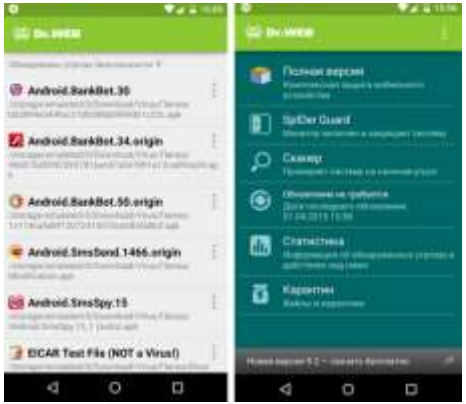
- Если на устройстве установлен шпион, возможно периодическое самостоятельное включение геопозиции.
- Установка программ без ведома пользователя – возможно, какое-то приложение получило административный доступ.
- Самопроизвольно загорающийся экран – неадекватная активность, не обязательно вредоносная.
- Гораздо более быстрая разрядка устройства.

Если смартфон утерян …

- Отключите мобильный банкинг, деактивируйте сеансы, а лучше смените пароли во всех социальных сетях и мессенджерах (особенно это касается учетных записей gmail и iCloud).
- Если смартфон использовался для генерации кодов, в срочном порядке выберите новое устройство в качестве генератора одноразовых паролей, а старое отвяжите от всех аккаунтов.
- Ознакомьтесь с официальным руководством от производителей смартфонов в случае кражи или утери и выполните все указанные там действия.

Если произошло заражение …

- Если есть подозрения, какое приложение было заражено, - удалите его.
- Установите антивирус, выполните полную проверку. Можно удалить текущий антивирус, установить другой и также проверить.
- Если все критически важные данные сохранены, и ничего не помогает вылечить телефон – выполните сброс до заводских настроек.



Спасибо за внимание!