Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Безопасное использование мобильных приложений

Обзор

Мобильные устройства, такие, как планшеты, смартфоны и часы, стали основными технологиями, которые мы используем каждый день не только для личных, но и для служебных целей. Огромный выбор из миллионов приложений делает мобильные устройства поистине универсальными. Приложения позволяют нам быть более продуктивными, всегда оставаться на связи и обмениваться информацией или просто приятно проводить время. Но помимо огромных возможностей, приложения таят в себе и большую опасность. Вот некоторые шаги, которые помогут вам безопасно использовать мобильные приложения и извлекать из них максимальную пользу.

Об авторе

Джошуа Райт – технический директор фирмы Counter Hack и старший инструктор Института SANS. Он является автором курса SEC575: Безопасность Мобильных Устройств и Этический Взлом, и книги Секреты хакеров: Беспроводные сети. Джош ведёт блог в Twitter **@joswr1ght**.

Установка мобильных приложений

Первый шаг - убедиться, что вы загружаете мобильные приложения из надёжных и проверенных источников. Кибер преступники совершенствуют свои навыки по созданию и распространению инфицированных мобильных приложений, которые выглядят вполне правдоподобно. Если вы установите подобное приложение, кибер преступники получат полный контроль над вашим устройством. Поэтому следует загружать мобильные приложения только с известных, проверенных сайтов. Для каждого бренда устройств есть свой надёжный источник мобильных приложений.

Для устройств Apple, таких, как iPad и iPhone, следует загружать приложения только из магазина приложений Apple App Store. Преимущество данного источника в том, что компания Apple проверяет все приложения перед тем, как опубликовать. Компания Apple не всегда может обнаружить инфицированные мобильные приложения, но эта контролируемая среда помогает максимально снизить вероятность установки зараженных мобильных приложений. Если компания Apple обнаруживает вирус в уже опубликованном приложении, то она очень оперативно его удаляет. Система Windows Phone использует подобный подход к управлению приложениями.

Безопасное использование мобильных приложений

С устройствами на базе Android ситуация другая. Пользователи могут загружать приложения из любых источников в Интернете. Но такая свобода выбора несет и большую ответственность. Следует быть предельно осторожным при выборе источника мобильных приложений, особенно при отсутствии отзывов пользователей. У Google есть ресурс, похожий на магазин приложений Apple, так называемый Google Play. Мобильные приложения с данного ресурса тоже проходят базовую проверку безопасности. Поэтому мы рекомендуем пользователям Android загружать мобильные приложения только с Google Play. Следует избегать другие источники, так как злоумышленники легко могут подделать приложения и распространять вирусы через них. И, по возможности, следует установить антивирус на мобильное устройство.

Устанавливайте мобильные приложения только из проверенных и надёжных источников, регулярно их обновляйте и разрешайте доступ только к реально необходимой информации.

Вне зависимости от того, устройство какого бренда вы используете, избегайте новых приложений, приложений с небольшим количеством загрузок и незначительным количеством отзывов пользователей. Чем дольше приложение доступно, и чем больше людей оставило о нём отзывы, тем больше доверия оно вызывает. Устанавливайте только те приложения, которые вам действительно нужны. Спросите себя: мне действительно нужно это приложение? Ведь каждое мобильное приложение – потенциальная опасность и новая уязвимость. Если вы не используете приложение, удалите его с устройства (вы всегда сможете его загрузить снова, в случае необходимости). Ни в коем случае не взламывайте стандартные системы защиты с целью получения прав суперпользователя (jailbreak или rooting). Этот процесс предназначен для взлома и установки нелегальных приложений или изменения стандартных функций устройства. Это нарушает не только встроенный контроль безопасности, но и лишает вас гарантии и поддержки мобильного устройства со стороны производителя.

Настройки безопасности

После того, как вы загрузили мобильное приложение из надёжного источника, убедитесь, что оно безопасно сконфигурировано и не представляет угрозы вашей безопасности. Всегда подумайте, перед тем, как дать мобильному приложению доступ к чему-либо, действительно ли это необходимо? Например, функция геолокации.

Безопасное использование мобильных приложений

Если вы разрешаете данному приложению доступ к вашим перемещениям, то оно может передавать эти данные автору приложения, и он сможет вас отследить и даже продать эти данные другим лицам. Если вы не хотите давать приложению доступ к вашей информации, отклоните запрос или установите другое приложение. Помните, у вас всегда есть выбор.

Обновление мобильных приложений

Мобильные приложения, как и ваш компьютер, мобильное устройство, базируются на операционной системе, которой нужны регулярные обновления. Злоумышленники всё время ищут слабые места и чаще всего находят их в мобильных приложениях. Затем они атакуют через это слабое место. Разработчики это знают и выпускают регулярные обновления, чтобы защитить устройство. Чем чаще вы будете проверять и делать обновления, тем лучше. В большинстве устройств можно настроить автоматическое обновление мобильных приложений. Мы рекомендуем этим воспользоваться. Если нет такой возможности, то следует проверять каждые две недели обновления для мобильных приложений. При установке обновлений обязательно проверяйте, не запрашивает ли приложение нового доступа к вашим данным.

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

Социальная Инженерия:	https://securingthehuman.sans.org/ouch/2017#january2017
Безопасная утилизация мобильного устройства:	https://securingthehuman.sans.org/ouch/2016#december2016
Безопасность планшета:	https://securingthehuman.sans.org/ouch/2016#january2016
Архив и переводы выпусков OUCH:	https://securingthehuman.sans.org/ouch/archives
Институт SANS – Mobile Device Security Course:	https://sans.org/sec575

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

