Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Безопасное использование мобильных приложений

Обзор

Мобильные устройства, например, смартфоны и планшеты, становятся незаменимыми в личной и профессиональной сфере. Возможность выбора из огромного количества приложений делает мобильные устройства невероятно универсальными. Приложения повышают продуктивность работы, позволяют мгновенно обмениваться информацией, учиться новому и просто развлекаться. Но вместе с безграничными возможностями приходят и риски. Стоит предпринять следующие шаги, чтобы безопасно использовать и поддерживать мобильные приложения.

Автор выпуска

Крис Кроули – независимый консультант, сертифицированный инструктор и автор курсов Института SANS. Он ведёт записи в Twitter **@CCrowMontance** и блог в Google+ **ChrisCrowley**.

Установка мобильных приложений

Прежде всего, следует загружать приложения только из надёжного, проверенного источника. Помните, любой желающий может создать приложение; поэтому очень тщательно проверяйте происхождение приложений. Киберпреступники совершенствуют свои навыки, и их вредоносное приложение может выглядеть вполне правдоподобно. Если вы установите подобное приложение на ваше устройство, оно заразит устройство, и киберпреступники получат полный доступ к вашим разговорам, переписке и контактам. Поэтому приложения следует загружать только из проверенных и надёжных источников: это существенно уменьшает вероятность установки инфицированного приложения. Обратите внимание на модель вашего устройства, это поможет с выбором источников.

Для продуктов Apple, таких iPad или iPhone, вы можете приобретать приложения исключительно в фирменном магазине приложений Apple – Apple Store. Преимущество заключается в том, что Apple проверяет как безопасность самих приложений, так и надёжность их авторов. Но даже Apple не в состоянии поймать всех «плохих парней» или выявить все инфицированные приложения. Тем не менее, это позволяет значительно снизить риск получить вирус. Если Apple находит заражённое приложение в Apple Store, то оно оперативно удаляется. Для управления приложениями Windows Phone используется аналогичный подход.

© The SANS Institute 2015

Безопасное использование мобильных приложений

Для устройств Android ситуация немного отличается. Пользователи могут сами выбирать в Интернете источник загрузки приложений. Однако, с этой гибкостью появляется больше рисков. Вы должны относиться с большой осторожностью к выбору и установке мобильных приложений, так как не все из них проверяются. У Google есть сервис Google Play, подобный Apple Store. Приложения с данного сервиса проходят базовую проверку. Мы рекомендуем пользователям устройств на базе Android загружать приложения исключительно с Google Play. Не загружайте приложения для Android с других сайтов, так как они могут содержать вирусы и заразить ваше устройство. В качестве дополнительной защиты можно установить антивирус.

ключевые правила использования мобильных приложений – загрузка из надёжных источников, регулярные обновления и правильные настройки прав доступа.

Чтобы снизить риск инфицирования, следует избегать совсем новых приложений, тех, которыми ещё мало кто пользовался или о них мало положительных отзывов. Чем дольше приложение существует или чем больше о нём хороших отзывов, тем больше ему можно доверять. Устанавливайте только необходимые приложения. Всегда спрашивайте себя, действительно ли вам нужно это приложение? Ведь каждое новое приложение не только повышает риск инфицирования, но и может нарушить личную жизнь. Если вы перестали использовать приложение, удалите его (если это приложение вновь понадобится, вы сможете его установить его снова).

Ну и, наконец, вы можете сделать jailbreak или root вашего устройства. Это процесс отключения штатных средств защиты для установки несанкционированных приложений или изменения существующих, встроенных функций. Мы настоятельно не рекомендуем этот метод, так как это не только устраняет многие элементы безопасности, но и аннулирует гарантийное обслуживание устройства.

Права доступа

После загрузки приложения из достоверного источника следует убедиться, что оно правильно сконфигурировано и обеспечивает вам конфиденциальность. Установки и/или настройка мобильных приложений часто запрашивает определённые права. Всегда задумайтесь, насколько приложению действительно необходимы для работы некоторые права доступа. Например, многие приложения запрашивают геолокацию. Если вы разрешите приложению всегда знать ваше местонахождение, производитель приложения всегда сможет

© The SANS Institute 2015

Безопасное использование мобильных приложений

узнать, где вы находитесь и даже сможет продавать эту информацию другим. Если вы не хотите давать приложению определённые права, поищите в магазине другое приложение, соответствующее вашим пожеланиям. Помните, у вас всегда есть большой выбор. Пользователи Apple могут вносить изменения в настройки приложений или в процессе их использования регулировать доступ, например, к функционалу геолокации. Пользователи Windows или Android этого делать не могут: подход «всё или ничего». Если они не предоставят запрашиваемые права, они не смогут установить приложение.

Обновление приложений

Мобильные приложения, так же как и ваш компьютер или операционная система мобильных устройств, должна регулярно обновляться. Преступники постоянно ищут и находят слабые места в приложениях. Затем они готовят атаки на эти слабые места. Разработчики приложений тоже создают и выпускают обновления для исправления этих недостатков и защиты устройств. Чем чаще вы обновляете систему, тем лучше. Большинство систем позволяют настроить автоматическое обновление приложений. Мы рекомендуем этим воспользоваться. Если автоматическое обновление нельзя настроить, то следует обновлять систему и приложения как минимум раз в две недели. Не забудьте проверить настройки приложений после каждого обновления.

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 http://www.securingthehuman.org.

Ресурсы

Социальная инженерия:	http://www.securingthehuman.org/ouch/2014#november2014
Утилизация мобильного устройства:	http://www.securingthehuman.org/ouch/2014#june2014
Как защитить новый планшет:	http://www.securingthehuman.org/ouch/2013#december2013
Термины по информационной безопасности:	http://www.securingthehuman.org/resources/security-terms
Институт SANS: Программа курса обучения SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

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: ouch@securingthehuman.org

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

© The SANS Institute 2015