Dr.WEB®
с 1992 года

DWCERT-070-7

Общие принципы защиты мобильных Android-устройств

Первый
российский антивирус
для Android

Более 130 миллионов
скачиваний только
с Google Play

Бесплатный
для пользователей домашних
продуктов Dr.Web*

*Кроме Dr.Web KATANA

План курса

1. Экосистема Android

Чтобы понять, почему для Android существует так много вредоносных программ, нужно знать особенности операционной системы Android.

1. **В ОС Android, как и в каждом программном обеспечении, есть уязвимости** — «дыры» в безопасности. Одним из направлений развития вирусописательства является поиск возможностей проникновения вредоносных программ в системы через уязвимости. Некоторые из них широко распространены.

   По статистике Dr.Web (а это данные с более чем 100 миллионов устройств):
   - на 56,4% устройств присутствует уязвимость ObjectInputStream Serialization;
   - на 41,85% устройств присутствует уязвимость Fake ID;
   - на 37,7% устройств присутствует уязвимость PendingIntent.

   А еще уязвимости есть в мобильных приложениях для устройств на базе ОС Android. Их разработчики могут поддерживать только устройства наиболее популярных производителей и физически не способны протестировать работу своего ПО на всех смартфонах и планшетах.

   Программы для мобильных устройств пишут программисты, которым, как и людям любых других профессий, свойственно ошибаться. По статистике каждая пятая программа для ОС Android — с уязвимостью (или, иными словами, — с «дырой»), что позволяет злоумышленникам успешно внедрять мобильных троянцев на устройства и выполнять нужные им действия

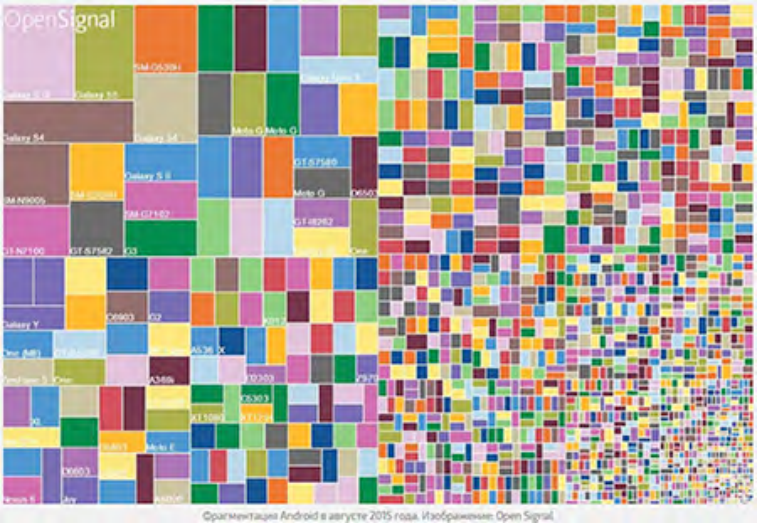
   Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом. Не существует ПО, в котором не было бы уязвимостей. Разработчики программного обеспечения прилагают усилия по закрытию уязвимостей, особенно критических, но вирусописатели часто узнают об уязвимостях раньше, чем разработчики этого ПО (это так называемые уязвимости нулевого дня — 0day exploits, уязвимости, о которых пока известно только вирусописателю или для исправления которых производитель ПО пока еще не выпустил «заплатки»).

Подавляющее большинство современных «успешных» мобильных троянцев проникают в системы преимущественно через уязвимости, в том числе через уязвимости нулевого дня. Антивирус пытается закрывать таким троянцам пути проникновения через уязвимости, но это чаще всего борьба с последствиями — об уязвимости раньше узнают вирусописатели.

Dr.Web рекомендует

Чтобы устранять уязвимости (закрывать бреши безопасности), пользователю надо своевременно обновлять установленное на мобильном устройстве ПО — все без исключения программы, а не только антивирус.

2. В Android **отсутствует централизованная система выпуска и распространения обновлений безопасности** для Android.



Доли рынка различных устройств под управлением Android

Компания Google разрабатывает новые версии платформы Android OS и предоставляет ее своим партнерам, которые дорабатывают ее под свои нужды. В результате не существует единой операционной системы, и любая программа поддерживает не конкретные версии Android, а версии определенных производителей устройств.

Внимание!

- *По причине фрагментарности Android невозможно реализовать единую для всех устройств систему распространения обновлений безопасности, закрывающих уязвимости: каждый производитель выпускает их самостоятельно.*
- *К сожалению, нельзя рассчитывать, что купленное устройство будет поддерживаться его производителем бесконечно. Как правило, обновления выпускаются только для последних версий ОС, а пользователи старых (относительно!) устройств остаются с незакрытыми уязвимостями — возможность перехода на новые версии ОС для них зависит от производителя их устройства.*
- *Google доставляет обновления только для пользователей собственных устройств.*

Результат печален: не получая уведомлений о необходимости установки обновлений безопасности, пользователи полагают, что и уязвимостей у них нет. А это совершенно не так! Также считается, что осторожность нужна только при установке самого приложения, а установка обновлений к нему вполне безопасна.

Важно! *Одним из способов внедрения вредоносной программы на устройство пользователя стал момент обновления приложения! Уже зафиксированы случаи, когда программа может помещаться в магазин приложений без вредоносного функционала — и получать его вместе с обновлениями.*

3. **Для ОС Android существуют тысячи приложений**. Открытая экосистема платформы Android дала возможность любому разработчику создавать для нее приложения. Процедура размещения приложений в специализированных магазинах максимально упрощена, и в результате количество программ для «андроидов» исчисляется сотнями тысяч.

Почти четверть вредоносных программ создается именно для платформы Android.

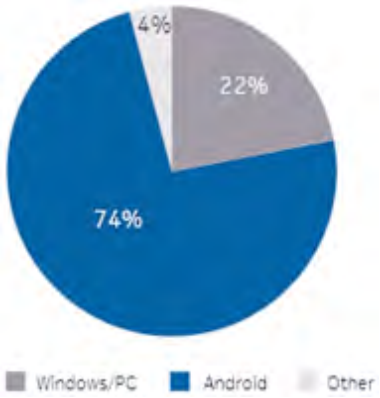
Особенностью вредоносных программ для Android является то, что, загрузив вредоносное ПО на свое устройство, вы отдаете его в полное распоряжение злоумышленнику.

Три из пяти троянцев — загрузчики иных вредоносных программ. То есть злоумышленники, попав на ваше устройство, могут проанализировать открывшиеся перед ними возможности и использовать их максимально

Попавшие на Android-устройство вредоносные программы могут отсылать платные СМС, открывать удаленный доступ, красть денежные средства, шифровать данные на устройстве и так далее.

Полезно знать

В обыденной речи все вредоносные программы называются вирусами. Но вирусы — это еще и определенный тип вредоносных программ, отличающийся тем, что его представители (наряду с червями) могут сами распространяться. ***Для Android вирусов — вредоносных программ, которые распространяются сами, — НЕТ.*** *Основной тип вредоносных программ для Android — троянцы, программы, устанавливаемые в результате действий самих пользователей.*



Из доклада Nokiainfo-icon об угрозах за первое полугодие 2016 года

http://resources.alcatel-lucent.com/asset/200492

Думаете, это повод расслабиться?

Более 1 000 000 владельцев Android-смартфонов и планшетов загрузили из Google Play приложение с именем «Multiple Accounts: 2 Accounts», которое на самом деле является трояном Android.MulDrop.924

Новость

2. Не стройте иллюзий: их цель — воровство

В «Доктор Веб» проанализировали, какой функционал закладывают злоумышленники в троянские программы для Android, достижению каких целей служат эти опасные приложения. И вот что мы увидели.

Большинство вредоносных программ для Android создаются с целью незаконного завладения чужим имуществом и получения информации — попросту воровства.

Распространители Android-троянцев крадут все, что можно украсть с мобильного устройства:

- Деньги — это наиболее важный вектор атак вирусописателей. Для этого злоумышленники создают так называемых троянцев-банкеров — о них подробнее расскажем дальше.
- Логины и пароли.
- Исходящие СМС — троянцы списывают деньги с мобильного счета в пользу преступников путем отправки дорогостоящих СМС с телефона жертвы втайне от нее.
- Входящие СМС — например, подтверждающие или спрашивающие разрешения на подключение к мобильным премиум-сервисам и контент-услугам. Троянцы скрывают их от владельца и также скрытно направляют поддельные ответы для того, чтобы жертва как можно дольше не узнала о подписке на такие сервисы и не предприняла действий к прекращению деятельности троянца. Также в зоне риска — СМС с сообщениями от систем «банк-клиент», содержащие проверочные mTAN-коды.
- Звонки — пользователь платит за звонки на дорогостоящие премиум-номера, которые совершаются без его ведома.
- Сообщения электронной почты.
- Фотографии.
- Записи переговоров.
- Контакты.
- Координаты устройства.
- Техническая информация об устройстве.

Распространенный среди пользователей устройств на основе Android миф гласит, что при определенной осторожности можно избежать заражения. Увы, это не так — статистика скачивания вредоносных программ из магазинов приложений полностью опровергает миф. При этом действие наиболее успешных троянцев, направленных на кражу, в большинстве случаев можно обнаружить только тогда, когда всё уже украдено. Иногда спустя месяцы после заражения, когда поделать уже ничего нельзя.

Полезно знать

Авторы троянских программ, а также все, кто задействован в их распространении и дележе доходов от такой преступной деятельности (т. е. каждый участник преступных группировок), в той или иной мере могут подпадать под действие таких статей Уголовного кодекса РФ, как ст. 272 (Неправомерный доступ к компьютерной информации), ст. 273 (Создание, использование и распространение вредоносных компьютерных программ), ст. 158 (Кража), ст. 159 (Мошенничество в сфере компьютерной информации), ст. 163 (Вымогательство), ст. 165 (Причинение имущественного ущерба путем обмана или злоупотребления доверием). Причем уголовная ответственность, при наличии соответствующих признаков, может наступать и по совокупности преступлений с частичным или полным сложением сроков лишения свободы (не более 25 лет).

Узнайте больше!

О возможностях троянских программ для Android рассказывает информационный проект «Мобильное воровство».

3. Банкеры

Каждый уважающий себя банк имеет в своем арсенале специальное мобильное приложение онлайн-банкинга и стимулирует своих клиентов пользоваться его сервисами. Услуги мобильного банкинга, доступные владельцам Android-устройств через специальные клиентские приложения, для многих пользователей давно стали привычной и удобной формой управления персональными финансами. Действительно, контролируя свои счета и совершая платежи в программе, вместо того чтобы каждый раз идти в отделение банка или искать ближайший банкомат, можно сэкономить уйму времени и потратить его с гораздо большей пользой. Развитие мобильных технологий банками будет только нарастать!

Понимают это и киберпреступники. Смартфоны и планшеты, используемые для проведения денежных операций, давно являются одной из излюбленных целей злоумышленников, которые они атакуют с помощью так называемых банковских троянцев (банкеров).

Банковские троянцы для мобильных устройств — семейства (т. е. множества вредоносных программ, имеющих одинаковые признаки) компьютерных вредоносных программ, основной целью которых является хищение данных для доступа к мобильным банковским приложениям с целью последующей кражи средств их владельцев с банковских счетов, в том числе через эти же мобильные банковские приложения.

Первые банкеры для Android появились еще в 2011 году. В вирусной базе Dr.Web сегодня насчитывается более 270 записей о представителях различных **семейств** банкеров, но еще большее их количество выявляется с помощью технологии Origins Tracing™.

Только факты

- **Банковский троянец Android.SpyEye.1.** При обращении к различным банковским сайтам, адреса которых присутствуют в конфигурационном файле троянца, в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого (текст или веб-формы для ввода данных). Ничего не подозревающая жертва загружает в браузере веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «банк-клиент», с предложением загрузить на мобильный телефон специальное приложение, содержащее троянскую программу.
- **Программа для перехвата СМС–сообщений Android.Pincer.** Вредоносная программа распространяется под видом сертификата безопасности, который якобы требуется установить на Android-устройство. В случае если неосторожный пользователь выполнит установку и попытается запустить троянца, Android.Pincer.2.origin продемонстрирует ложное сообщение об успешной установке сертификата. При очередном включении мобильного устройства Android.Pincer.2.origin подключается к удаленному серверу злоумышленников и загружает на него ряд сведений о мобильном устройстве. Android.Pincer.2 дает возможность использовать вредоносную программу как инструмент для проведения целевых атак, в том числе красть специфические СМС-сообщения с указанных номеров, например сообщения от систем «банк-клиент», содержащие проверочные mTAN-коды.
- С каждым днем появляется все больше «умных» Android-троянцев, которые после заражения мобильных устройств проверяют, какое банковское ПО установлено в системе, и ждут момента, когда жертва запустит соответствующее приложение. Как только одна из таких программ начинает работу (а троянцы могут контролировать приложения десятков и даже сотен кредитных организаций!), вредоносная программа выводит на экран фальшивое окно ввода логина и пароля для доступа к учетной записи пользователя мобильного банкинга. После того как обманутый владелец устройства добровольно предоставляет троянцу свои конфиденциальные данные, они тут же отправляются злоумышленникам. В результате киберпреступники получают полный контроль над всеми счетами жертвы и могут беспрепятственно переводить деньги себе – до тех пор, пока жертва не заметит это и не обратится в банк за блокировкой счета или карты.

Описанным функционалом обладают, например, многочисленные представители семейств **Android.ZBot**, **Android.Banker** и ряд троянцев семейства **Android.SmsSpy**.

- А вот создатели троянца **Android.BankBot.65.origin** пошли еще дальше. Они взяли одно из официальных банковских приложений крупной кредитной организации и уже непосредственно в него внедрили вредоносную надстройку. При этом сама программа полностью сохранила свою работоспособность! После такой хитроумной модификации злоумышленники загрузили этот банковский клиент на один из популярных интернет-ресурсов, где распространяли программу под видом ее обновленной версии с расширенным функционалом, услужливо советуя потенциальным жертвам удалить «старую» версию ПО перед установкой «новинки». Попав на мобильное устройство, **Android.BankBot.65.origin** похищал информацию из телефонной книги пользователя, а также мог перехватывать СМС с одноразовыми паролями, которые поступали жертве, и автоматически отправлять ответные СМС, чтобы подтвердить мошеннические переводы денег.

4. Мобильные бот-сети

Одно из направлений развития вирусописательства – заражение мобильных Android-устройств троянцами с целью вовлечения их без ведома владельца устройства в преступную деятельность бот-сети.

После того как злоумышленники получают контроль над мобильными устройствами, они могут «приказать» им выполнить любое действие.

Самыми популярными вредоносными функциями «мобильных» ботнетов являются:

- рассылка СМС-спама,
- кража конфиденциальной информации,
- кибершпионаж,
- показ нежелательной рекламы,
- осуществление DDoS-атак на веб-сайты.

> ***Dr.Web предупреждает***
> *Все перечисленные выше действия являются уголовно наказуемыми во многих странах, и ответственность за них несет в том числе и владелец зараженного устройства.*

В некоторых случаях число зараженных устройств, входящих в «мобильные» ботнеты, может составлять десятки тысяч.

Только факты

- Троянец **Android.SmsBot.120.origin** в июне 2014 года был обнаружен специалистами Dr.Web на более чем 670 000 устройств. Эта вредоносная программа могла отправлять, перехватывать и удалять СМС-сообщения, открывать в браузере заданные веб-страницы, получать координаты зараженного Android-устройства и даже производить удаление определенных приложений!

Все более распространенными становятся «мобильные» бот-сети, которые строятся на основе Android-смартфонов и планшетов, зараженных банковскими троянцами.

Только факты

- В ноябре 2014 года вирусные аналитики «Доктор Веб» обнаружили многофункционального банковского трояна **Android.Wormle.1.origin**, который заразил более 15 000 смартфонов и планшетов пользователей из многих стран. По команде киберпреступников троянец мог не только незаметно перевести им деньги с принадлежащих жертвам банковских счетов, но также был способен выполнять множество других нежелательных действий.
- С использованием различных модификаций другого банковского трояна, **Android.SmsSpy.88.origin**, злоумышленники с конца 2015 года сформировали десятки бот-сетей, общая численность которых превысила 40 000 устройств. Главное предназначение этого вредоносного приложения — похищение логинов и паролей для доступа к учетным записям мобильного банкинга и кража данных о кредитных картах. Однако троянец также может красть все СМС-сообщения, рассылать спам по номерам из телефонной книги и даже блокировать экран зараженных устройств, вымогая у пользователей деньги за разблокировку.

5. Вымогатели

Блокировщики экрана и шифровальщики также представлены среди вредоносных программ для Android. Надо признать, что в отличие от аналогичных троянцев для Windows они пока еще не так сильно распространены. Вполне возможно, что описанный ниже пример — лишь первая ласточка.

Троянец-вымогатель Android.Locker.387.origin, обнаруженный в каталоге Google Play и распространявшийся под видом программы Energy Rescue, которая якобы оптимизировала работу аккумулятора, блокировал зараженный смартфон или планшет, требуя выкуп за его разблокировку.

Интересно, что разработчики вымогателя попытались защитить его от обнаружения специальным упаковщиком. Несмотря на это он успешно обнаруживается антивирусными продуктами Dr.Web для Android как Android.Packed.15893.

Помимо блокировки Android-устройств, Android.Locker.387.origin крал информацию об имеющихся в телефонной книге контактах и все доступные СМС-сообщения.

Новость

Поможет Dr.Web

Dr.Web Security Space для Android разблокирует устройство, инфицированное троянцами-блокировщиками.

- *Даже при полной блокировке телефона*
- *Даже если блокировщика еще нет в вирусной базе Dr.Web*
- *Без необходимости выплаты выкупа злоумышленникам*

Смотрите видео о том, как легко избавиться от троянца-блокировщика с помощью Dr.Web

6. Троянцы в прошивках

Как правило, троянцев для Android пользователи получают на свои устройства совершенно бесплатно. Но есть способ, когда пользователь реально платит (т. е. фактически покупает) троянца. Причем продавцом выступает ... производитель устройства, а невольным «соучастником» этого преступления — торговая сеть. В открывшемся окне Настройки выберите пункт Компоненты защиты и далее Превентивная защита.

Только факты

- Январь 2016 года — специалисты компании «Доктор Веб» обнаружили руткит Android.Cooee.1 в прошивке Android-смартфона известного производителя. Новость
- Март 2016 года — на более чем 40 моделях смартфонов был найден троянец Android.Gmobi.1, который шпионил за пользователями, воруя адреса их электронной почты и другую приватную информацию, показывал рекламу и без разрешения устанавливал различное ПО. Новость

Поможет Dr.Web

Dr.Web Security Space для Android выявит предустановленные в системе вредоносные программы. Для этого надо запустить полное сканирование и дождаться результатов проверки. Если будет найден какой-либо троянец, Dr.Web сможет его удалить, однако для этого потребуется наличие root-доступа.

- ***На рутованных устройствах*** *Dr.Web удалит такого троянца — но только если запись о нем в базе помечена вирусными аналитиками «Доктор Веб» как безопасная для удаления. То есть после этой процедуры телефон не превратится в бесполезный кирпич.*
- ***На нерутованных устройствах*** *(т. е. на подавляющем большинстве устройств) Dr.Web для Android работает с правами обычного приложения. В таком режиме он может обнаруживать вредоносные программы, попавшие в системный каталог Android, но не имеет прав на их удаление.*

Иногда Android-троянцы в прошивках «окапываются» так глубоко, что удалять их становится очень опасно. При заражении троянцем нерутованного устройства у пользователя выбор невелик: или дать повышенные права своему защитнику (рутовать устройство самостоятельно), или обратиться к производителю устройства и потребовать выпустить новую прошивку, очищенную от троянца.

Один из способов получить root-права — установить специальное приложение для рутования устройства. **С точки зрения антивируса Dr.Web такие утилиты — потенциально опасные или хакерские программы.** При этом Dr.Web не блокирует такие приложения по умолчанию, просто демонстрирует предупреждение. Поэтому в местах распространения таких программ пишут, что перед скачиванием и установкой утилиты рутования необходимо отключить антивирус, чтобы он не мешал. **Выполнившие эту рекомендацию пользователи нередко скачивают на устройство троянца вместо утилиты рутования.**

Внимание! *В системе координат Android получение root-прав в операционной системе открывает почти неограниченный доступ к использованию всех ее возможностей* — **в том числе без ведома владельца устройства**.

А еще получение root-прав может означать потерю прав на техническую поддержку производителя.

Dr.Web рекомендует

- *Если root-полномочий на устройстве нет, необходимо связаться с производителем или авторизованным сервисным центром и запросить у них чистую версию прошивки без вредоносной программы.*
- *Сделайте резервную копию всех пользовательских данных, затем выполните операцию сброса настроек до заводских и установите новую прошивку устройства, полученную от производителя, откуда троянец был удален самим производителем устройства.*

Если прошивка не будет предоставлена, лучшим решением будет вернуть купленное устройство продавцу. Пользоваться таким устройством НЕЛЬЗЯ.

Внимание, ограничение! *Бесплатная версия Антивируса Dr.Web для Android Light — с ограниченным функционалом. Она позволяет только обнаружить вредоносное ПО, установившееся в системных каталогах или внедряющееся в системные процессы, но обезвредить и удалить такое ПО можно только с помощью Dr.Web Security Space для Android.*

Расскажет Dr.Web

О причинах попадания троянцев в прошивки написано в выпуске «Вшито-скрыто» просветительского проекта «Антивирусная правДА!».

7. Троянцы в магазинах приложений для Android

Для удобства покупки и установки программ на Android-устройства действуют официальные магазины приложений — так называемые маркеты. Самый известный среди них — Google Play.

По сравнению с другими источниками скачивания маркеты считаются наиболее безопасными. Они стараются не допускать появления вредоносных программ на своих «витринах», для чего проверяют получаемые от разработчиков дистрибутивы.

Однако сегодня даже на Google Play можно вместе с приложением скачать троянца. «Доктор Веб» все чаще выявляет такие вредоносные программы — некоторые из них пользователи успевают скачать сотни тысяч раз.

Троянец	**Количество скачиваний с Google Play**	**Ссылки**
Android.Spy.277.origin	3 200 000	Новость
Android.Spy.305.origin	2 800 000	Новость
Android.MulDrop.924	1 000 000	Новость

Как программы с троянцами попадают на маркеты?
Любой человек или компания может зарегистрировать в Google Play аккаунт разработчика и загружать в магазин любые приложения. Все загружаемые программы проходят некую проверку, но вирусописатели изобретают все новые уловки, и отсев время от времени не срабатывает. В случае блокировки администрацией Google Play аккаунта, с которого было загружено вредоносное приложение, злоумышленники просто создают новую учетную запись.

Как и почему пользователи скачивают троянцев с Google Play?
Вводя пользователей в заблуждение, злоумышленники применяют несколько методов, чтобы троянца скачали как можно больше пользователей.

- **Манипуляция мнением — через накрученный рейтинг приложения**

Выбирая, что скачать, многие пользователи ориентируются в том числе на рейтинг и отзывы пользователей. Киберпреступники научились продвигать свои изделия на маркетах, накручивая их рейтинги.

В январе 2017 года вирусные аналитики компании «Доктор Веб» обнаружили троянца Android.Skyfin.1.origin, который внедряется в активный процесс программы Play Маркет и незаметно накручивает счетчик установок определенных приложений в каталоге Google Play.
Новость

Троянца в «топе» рейтинга гарантированно скачают сотни тысячи раз всего за пару-тройку дней.

- **Маскировка — под полезные утилиты**

Для маскировки троянцы могут снабжаться и полезным функционалом. Самым ярким во всех отношениях примером стал Android.Toorch.1.origin, притворившийся «фонариком». Кроме официально заявленного функционала он мог незаметно выполнять установку и удаление приложений, дополнительно скачивать необходимые компоненты, передавать киберпреступникам различную конфиденциальную информацию, включая GPS-координаты зараженного устройства.

Банковский троянец **Android.BankBot.80.origin** маскировался под «банк-клиент» одной из крупнейших в России кредитных организаций. После запуска он требовал права администратора на устройстве до тех пор, пока пользователь на соглашался с требованием, а после этого приступал к своей вредоносной деятельности.
Новость

- **Мимикрия — под приложения других разработчиков**

Приложения злоумышленников могут визуально напоминать известные программы — утилиты, фоторедакторы, графические оболочки, анимированные обои рабочего стола и другие приложения. Пользователи думают, что скачивают знакомое им известное приложение, но на деле это не так.

Большинство программ, в составе которых распространяется **Android.Spy.277.origin**, представляют собой поддельные версии популярного ПО, название и внешний вид которого злоумышленники позаимствовали для привлечения внимания пользователей и увеличения количества загрузок троянца.
Новость

- **Перепаковка приложений других разработчиков**

Другой мошеннический метод — «перепаковка» уже существующих программ с добавлением в них вредоносного кода. Легитимное приложение заворачивается в «обертку», содержащую вредоносный код, и размещается в магазине.

Типичным представителем таких упакованных троянцев можно считать **Android.Packed.8677**. Такой упаковщик может содержать множество различных троянцев, отличающихся по функциональности, которые запакованы для защиты от анализа и обнаружения и как раз по упаковщику и обнаруживаются.

- **Бомбы замедленного действия**

С Google Play можно скачать программу без вредоносного функционала, но с потенциально опасными особенностями. Через некоторое время после активации такая изначально безобидная программа докачает на устройство троянские компоненты и начнет вредоносную деятельность.

Троянец **Android.Cooee.1** был разработан так, чтобы начинать вредоносную деятельность не сразу после первого включения инфицированной системы, а лишь по прошествии определенного периода, заданного злоумышленниками. Владельцы устройства полагали, что причиной появления рекламы стали программы, которые они успели установить за время использования смартфона, и настоящий источник навязчивых уведомлений оставался необнаруженным до попадания в вирусную лабораторию «Доктор Веб».

Dr.Web рекомендует

Даже скачивая игру из магазина приложений Google Play, вы не можете быть уверенными, что вместе с ней вы не скачали троянца. Просто помните об этом и внимательно читайте, на что именно запрашивает права очередная игрушка. Если вы не понимаете, зачем игре в карты доступ к системным областям устройства или ваша геолокация, лучше откажитесь от ее установки.

К сожалению, тот факт, что маркеты тоже небезопасны, мало кому известен.

8. Для чего покупают Android-устройства?

- Чтобы и дома, и за рабочим столом, и за рулем машины, и на встрече в командировке быть на связи.
- Чтобы мгновенно оплачивать товары и услуги.
- Чтобы в любой момент контролировать свои расходы.
- Чтобы всегда под рукой была нужная информация.
- Чтобы, попав в незнакомый город, можно было быстро найти себя на карте и проложить маршрут к нужному месту.
- Чтобы общаться в режиме онлайн с целым миром в социальных сетях и чатах.
- Чтобы в любой момент в списке контактов были все нужные телефоны — скорая, полиция, спасатели.
- Чтобы следить — за новостями, женой/сыном/…*
- Чтобы фотографировать все дорогие сердцу моменты жизни — и носить фотографии при себе.
- Чтобы рисовать — используя графические планшеты — и хранить на них свои работы.
- Чтобы контролировать в любой момент времени устройства «умного дома».
- Для имиджа.

И это не исчерпывающий список.

* Компания «Доктор Веб» не поддерживает идею слежки за кем-либо. Не собирает данные, позволяющие идентифицировать своих пользователей, и не помогает кому-либо в сборе подобных данных.

Мобильные устройства используются людьми и для работы. Сотрудники работают в дороге и дома, хранят корпоративные данные на личных устройствах, заходят на корпоративные ресурсы с личных устройств, сохраняя пароли доступа к ним на мобильных устройствах.

А вот для чего не покупают Android-устройства

- Чтобы хакер грелся на заморских курортах с моделями после кражи ваших денег.
- Чтобы внезапно остаться без устройства в чужом городе или стране.
- Чтобы установить мошенническое приложение якобы для оплаты парковки в Москве со скидкой, а потом получать счета на штрафы за неоплату стоянки от настоящих владельцев парковки.
- Чтобы спецслужбы и хакеры читали переписку.
- Чтобы воры следили за перемещениями по городу и знали, когда вас точно нет дома, чтобы ограбить квартиру.
- Чтобы не платить за перерасход трафика в роуминге по возвращении домой или не оказаться с отключенным телефоном по той же причине.
- Чтобы оказаться частью бот-сети и участвовать в DOS-атаке на сайт президента / ЦРУ / Пентагона / NASA / ваш вариант.

Случаи разные бывают.

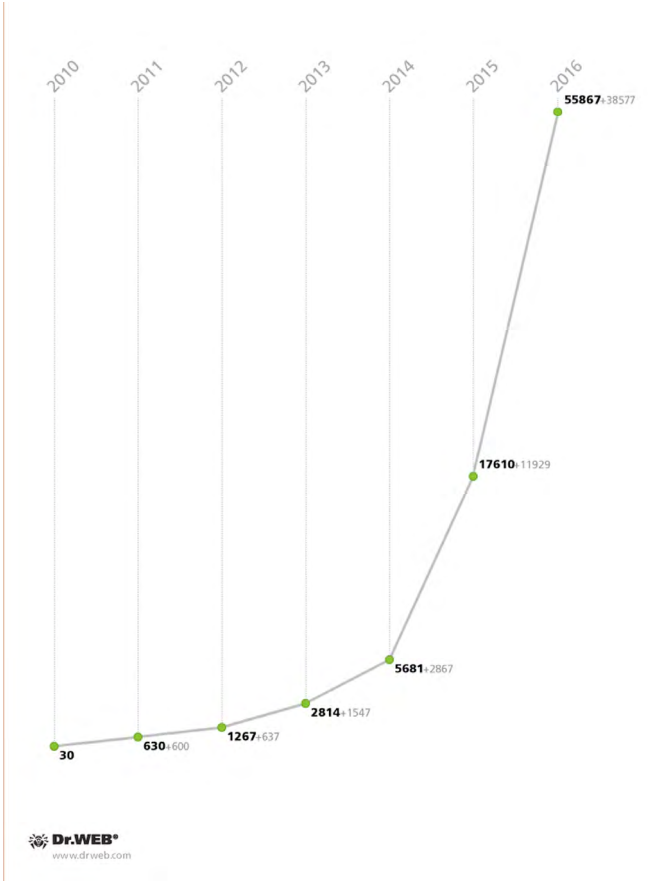
9. История Dr.Web для Android

Когда в 2007 году компания «Доктор Веб» выпустила первый антивирус для мобильных устройств, вирусов для мобильных было так мало, что мы твердо решили не брать за этот продукт деньги с пользователей — потому что было неэтично брать плату за защиту от возможных будущих угроз, почти не существовавших тогда. При этом в том, что угрозы для мобильных будут, и что их будет немало, — мы не сомневались — иначе мы бы не стали вкладывать средства в разработку этого продукта. За нами последовали (позднее) производители некоторых других антивирусов.

С 2007 года и до сих пор компания «Доктор Веб» предоставляет покупателям продуктов Dr.Web для защиты домашних ПК право бесплатного использования Dr.Web Mobile Security и не собирается менять эту политику.

Количество бесплатно предоставляемых лицензий на Dr.Web Mobile Security равно количеству ПК в купленной лицензии на продукт для защиты личного компьютера.

Платные лицензии на Dr.Web для Android
График роста количества записей вредоносных программ для ОС Android в вирусной базе Dr.Web:



В июле 2012 года, когда количество угроз для мобильных ОС достигло огромной цифры и стало ясно, что коммерчески ориентированные вирусописатели считают этот сегмент серьезным, компания «Доктор Веб» начала продажи отдельных лицензий на Dr.Web Mobile Security.

Полезно знать

*Dr.Web Mobile Security — это название **коммерческого** продукта для защиты мобильных устройств, который включает в себя несколько **программных** продуктов Dr.Web: для защиты Android и BlackBerry.*

Покупая одну лицензию на Dr.Web Mobile Security, пользователь может использовать ее только на одном устройстве на свой выбор: под управлением Android или Blackberry. Если в течение срока действия лицензии пользователь сначала установил Dr.Web на Android-устройство, а затем приобрел устройство под BlackBerry, ему не надо покупать новую лицензию — достаточно перенести ее на другое устройство, удалив с первого.

Только факты

- Антивирус Dr.Web для Android Light появился в августе 2010 года.
- Dr.Web Security Space для Android был выпущен в 2011 году.
- Dr.Web для BlackBerry вышел в свет в ноябре 2016 года.

Виды лицензий

	Рекомендуем!	
Антивирус Dr.Web для Android Light	**Dr.Web Security Space для Android (shareware)**	**Dr.Web Security Space для Android (life license)**
Скачивание только в Google Play	Скачивание с сайта «Доктор Веб» и официальных маркетов	Покупка и скачивание только в Google Play
Для работы серийный номер не требуется	Для работы требуется серийный номер – коммерческий или демо	Для работы требуется коммерческий серийный номер
Без возможности переноса на другое устройство	Возможность переноса на другое устройство	Возможность переноса на другое устройство
Бесплатно	Доступная цена	Дорогая лицензия
Бессрочная лицензия	Демо 14 дней. Возможность покупки лицензии на 1 или 2 года	Бессрочная лицензия
Только антивирус	Все компоненты защиты	Все компоненты защиты
Этой лицензии недостаточно для защиты от всех угроз для мобильных устройств!*		**Только в Google Play!**

* Она подойдет для того, чтобы проверить устройство на вирусы и понаблюдать, как Dr.Web находит новые угрозы, но для постоянной защиты устройства, особенно если с него пользуются интернет-банкингом, эту лицензию использовать мы не рекомендуем.

Виды поставки

Лицензии на Dr.Web для Android поставляются в электронном виде (серийные номера), в составе всех коробочных продуктов и на скретч-картах в виде OEM-лицензий в рознице, в тарифах услуги «Антивирус Dr.Web» Dr.Web Премиум и Dr.Web Мобильный.

Продление

Продлить срок действия лицензии на Dr.Web Mobile Security можно двумя способами: приобрести электронную лицензию или коробочный продукт Dr.Web.

- **Платное продление защиты для мобильного**

Чтобы продлить срок действия Dr.Web, купите новую лицензию или коробку Dr.Web Mobile Security Suite. Для этого продукта скидок на продление нет.

- **Бесплатное продление защиты для мобильного**

Вы также может приобрести для продления Dr.Web Security Space. В его состав входит бесплатный Dr.Web для Android. Таким образом, вы сможете не только бесплатно продлить срок действия защиты для мобильного, но еще и обеспечить защиту ПК/Mac. Впоследствии вы сможете продлевать эту лицензию со скидкой от 40% на год и более.

- **Самое выгодное продление — коробкой**

Если в магазине продаются коробочные продукты Dr.Web Security Space, покупка такого продукта будет самой выгодной для пользователя.

- При покупке коробки в комплектации 2 ПК на 2 года и последовательной регистрации обоих серийных номеров из коробки на 1 ПК, срок действия лицензии для нового покупателя составит 4 года и 300 бонусных дней. И все это время защита мобильного будет бесплатной – для двух(!) устройств.
- Если коробка в комплектации 2 ПК на 1 год, при последовательной регистрации обоих серийных номеров из коробки на 1 ПК срок действия лицензии для нового покупателя составит 2 года и 150 бонусных дней. Защита 1 мобильного устройства будет бесплатной на этот же период.

А если покупатель ранее пользовался Dr.Web Security Space, к сроку этих лицензий будут добавлены еще 150 дней.

Напоминания о продлении

В стандарт обслуживания клиентов Dr.Web входит система сервисных e-mail-сообщений, отправляемых на e-mail пользователя в течение срока действия лицензии. В том числе отправляются напоминания о продлении лицензии.

Напоминания о продлении коммерческих лицензий Dr.Web Mobile Security отправляются за 30 дней до окончания лицензии, а также в день ее окончания и через 20 и 40 дней после окончания лицензии. Тексты этих сообщений также хранятся в сервисе «Сообщения» личного кабинета пользователя «Мой Dr.Web».

Напоминания о продлении демолицензий отправляются в день запроса демо, а также через 10 и 13 дней после выдачи демо.

Дозакупка

Если покупатель сначала приобрел одну лицензию Dr.Web, а затем захотел защитить еще другие устройства, ему необходимо приобрести новую лицензию без скидки. На этот продукт нет никаких скидок, в том числе за количество лицензий.

10. Как скачать Dr.Web для Android

Мы рекомендуем устанавливать Dr.Web только с нашего сайта или из Google Play — это гарантия того, что вместе с Dr.Web на мобильное устройство не попадет троянец. Официальный маркет разработчика ОС Android — Google Play.

Dr.Web рекомендует
Скачивать Android-приложения либо из Google Play, либо с сайта разработчика приложения — самая безопасная практика в отношении любых программ для Android.

Dr.Web рекомендует
Перед скачиванием и установкой приложения Dr.Web ознакомьтесь с текстом лицензионного соглашения — его можно скачать в Центре лицензирования Dr.Web. Также этот текст демонстрируется в приложении во время установки. В случае несогласия с его положениями установка будет прервана.

Как скачать Dr.Web из Google Play

В маркете доступны следующие лицензии Dr.Web:

- Dr.Web Security Space для Android (shareware)
- Dr.Web Security Space для Android (life license)
- Антивирус Dr.Web для Android Light (freeware) — бесплатная с ограниченным функционалом бессрочная лицензия. В ее состав включен только антивирус (и отсутствуют все остальные компоненты защиты полной версии).

Покажет Dr.Web

Обо всех способах скачивания и установки Dr.Web расскажут обучающие видеоролики.

Полезно знать
Помимо Dr.Web для Android в Google Play есть программа Dr.Web для системных администраторов компаний — Мобильный центр управления Dr.Web для администрирования антивирусной сети, построенной на основе Dr.Web Enterprise Security Suite или Dr.Web AV-Desk, — и специальное приложение для партнеров, реализующих коробочные продукты Dr.Web, — Сканер КОД Dr.Web.

Как скачать Dr.Web с сайта компании «Доктор Веб»

- Если у вас нет серийного номера Dr.Web — на странице скачивания приложения http://download.drweb.com/android выберите удобный для вас способ скачивания — через apk-файл или QR-код. Во время установки можно будет запросить демо на 14 дней.
- Если у вас есть действующий серийный номер — укажите его в Мастере скачиваний и скачайте Dr.Web в удобной для себя форме. Или скачайте Dr.Web с http://download.drweb.com/android и введите серийный номер при установке.

Внимание! *На сайте «Доктор Веб» бесплатной Light-версии нет.*

Dr.Web рекомендует

Страницу скачивания на сайте «Доктор Веб» найти очень просто: откройте главную страницу https://drweb.ru → наведите мышку на раздел ***Скачать*** *→ кликните по ссылке возле иконки Android.*

Если вы зашли на сайт с мобильного устройства — перейдите в раздел ***Скачать*** *и через левое меню Демо для дома → Для мобильных → Dr.Web для Android откройте станицу скачивания продукта (адаптирована под мобильные устройства).*

Полезно знать

Чтобы программа работала, ей необходим серийный номер — коммерческий или демо. Срок действия лицензии начинается с момента активации серийного номера — покупателем или сотрудником магазина, производящим установку Dr.Web на устройство покупателя.

Запрещено регистрировать серийные номера Dr.Web на e-mail-адреса, не принадлежащие владельцу лицензии. В случае обращения в техническую поддержку им может быть отказано в обслуживании.
Кто является владельцем лицензии Dr.Web?

11. Как получить демо

Сделать это можно с сайта разработчика программы — компании «Доктор Веб» или с официальной страницы приложения в Google Play.
Срок действия демо 14 дней.

Полезно знать
Срок действия демолицензии начинается с момента запроса демо.

12. Компоненты защиты Dr.Web Security Space для Android

Представьте дом, в котором, например, три двери. Хозяин поставил замок только на одну из них (установил антивирус на мобильное устройство), а две другие остались незапертыми (например, не используется антиспам и брандмауэр). Станет ли вор ломать замок (антивирус)? Конечно, нет — он войдет в незапертую дверь.

Бесплатный Антивирус Dr.Web для Android Light — это дом только с одной закрытой дверью.

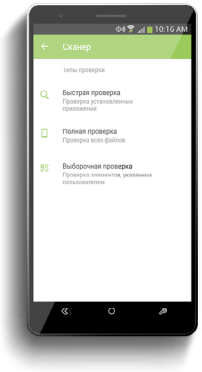
Он защитит от вирусов и вредоносных программ, в частности троянцев. Но сегодня этого уже недостаточно для защиты от всех способов проникнуть на устройство в арсенале вредоносных программ для Android.

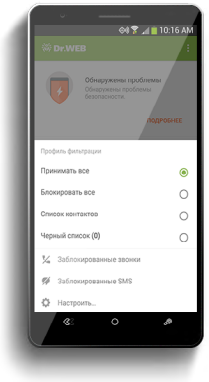
Разумный хозяин запрёт все двери и не оставит ворам ни одного шанса беспрепятственно проникнуть внутрь дома.

Защита Android-устройств должна строиться по такому же принципу: необходимо защитить (закрыть) любые лазейки (открытая дверь — это лазейка, брешь, дыра) для киберпреступников.

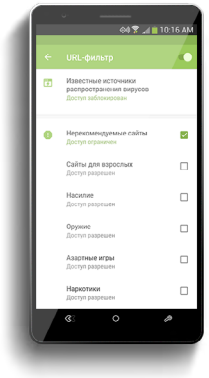
Какие прорехи в защите мобильных устройств использует киберкриминал и какой компонент полной версии Dr.Web Security Space для Android от чего защищает?

- Антивирус — защитит от вредоносных программ, созданных для инфицирования мобильных устройств.

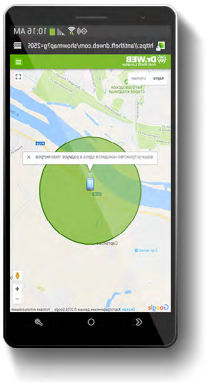




- Фильтр звонков и СМС — защитит от нежелательных звонков и СМС-сообщений с фишинговыми ссылками. А значит, пользователь не перейдет по такой ссылке на фишинговый или вредоносный сайт. Работа антиспама возможна и на устройствах с двумя SIM-картами.



- Облачный URL-фильтр Dr.Web ограничит доступ к нежелательным и потенциально опасным сайтам. Он особенно полезен, если устройством пользуется ребенок, который еще пока не осознает опасности посещения тех или иных ресурсов. Контроль доступа к ресурсам в сети Интернет обеспечивается через встроенный браузер Android, а также наиболее популярные браузеры: Google Chrome, Google Chrome Beta, Firefox, Opera, Opera mini, Next, Amazon Silk, Яндекс.Браузер, Boat Browser и Boat Browser Mini, Adblock Browser, Dolphin Browser, Спутник, UME браузер.



- Антивор Dr.Web — поможет найти мобильное устройство в случае его утери или кражи, заблокировать устройство и при необходимости удаленно стереть с него конфиденциальную информацию. Мобильные устройства подвержены огромному риску потери или кражи. Информация (включая пароли и логины доступа) может попасть в не всегда дружелюбные руки. Для этого надо включить и настроить этот компонент.

Настрой-ка Dr.Web!

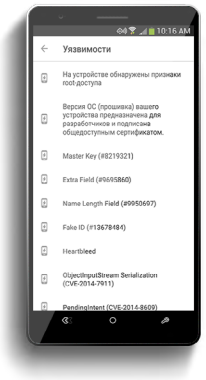
Обо всех настройках Антивора Dr.Web и его возможностях расскажут обучающие видеоролики.

«Как подготовить Антивор к часу икс» — полезная статья проекта «Антивирусная правДА!».

Полезно знать

Если вы забыли код разблокировки Антивора Dr.Web, вы можете самостоятельно восстановить его на странице https://antifraud.drweb.ru/android_theft

- Брандмауэр — проконтролирует сетевую активность приложений и поможет избежать расходования средств на ненужный трафик. Он проверяет любой трафик, откуда бы тот ни передавался. Все попытки внедрения вредоносных программ с недоверенных сетей будут пресечены. Этот компонент надо включить и настроить. Брандмауэр работает на Android 4.0 и выше. Для его использования требуется включение VPN для Android (подробнее). Для работы брандмауэра Dr.Web не требуется получение прав суперпользователя (root) на устройстве.



Настрой-ка Dr.Web!
Обо всех настройках Брандмауэра Dr.Web расскажут обучающие видеоролики.

«Укрощение пожирателей трафика» — полезная статья проекта «Антивирусная правДА!»

- Аудитор безопасности — произведет диагностику устройства, выявит проблемы безопасности и предложит решения для их устранения.

Только комплексное антивирусное решение **Dr.Web Security Space для Android** позволит защищаться от всех типов вредоносного ПО, используемого мошенниками для совершения киберпреступлений на Android-устройствах.

А также
- Автоматические обновления
- Единое окно событий безопасности устройства
- Резервная копия настроек
- Статистика работы компонентов защиты
- Карантин
- Менеджер лицензий
- Личный кабинет «Мой Dr.Web»

Таблица функционала продуктов Dr.Web для защиты мобильных устройств

Сравните продукты Dr.Web для Android

	Dr.Web Security Space для Android	Антивирус Dr.Web для Android Light
Поддерживаемые ОС	Android 4.0–7.1 Android TV 5.0+	Android 4.0–6.0
Номер версии	11	10
Компоненты защиты		
Антивирус	+	+
Антисам*	+	
Антивор*	+	
URL-фильтр	+	
Брандумаэур	+	
Аудитор безопасности	+	
Разблокировка от вредоносных троянцев-блокировщиков	+	

* Использование Антиспама и Антивора на планшетных компьютерах без SIM-карт невозможно.

13. Dr.Web для «умных» телевизоров Android TV

для Android TV 5.0+

Первый антивирус для Android TV

Антивирус — защитит от троянцев и других вредоносных программ

- Постоянная проверка файловой системы для защиты от вредоносных программ в режиме реального времени.
- Быстрое, полное и выборочное сканирование по требованию.

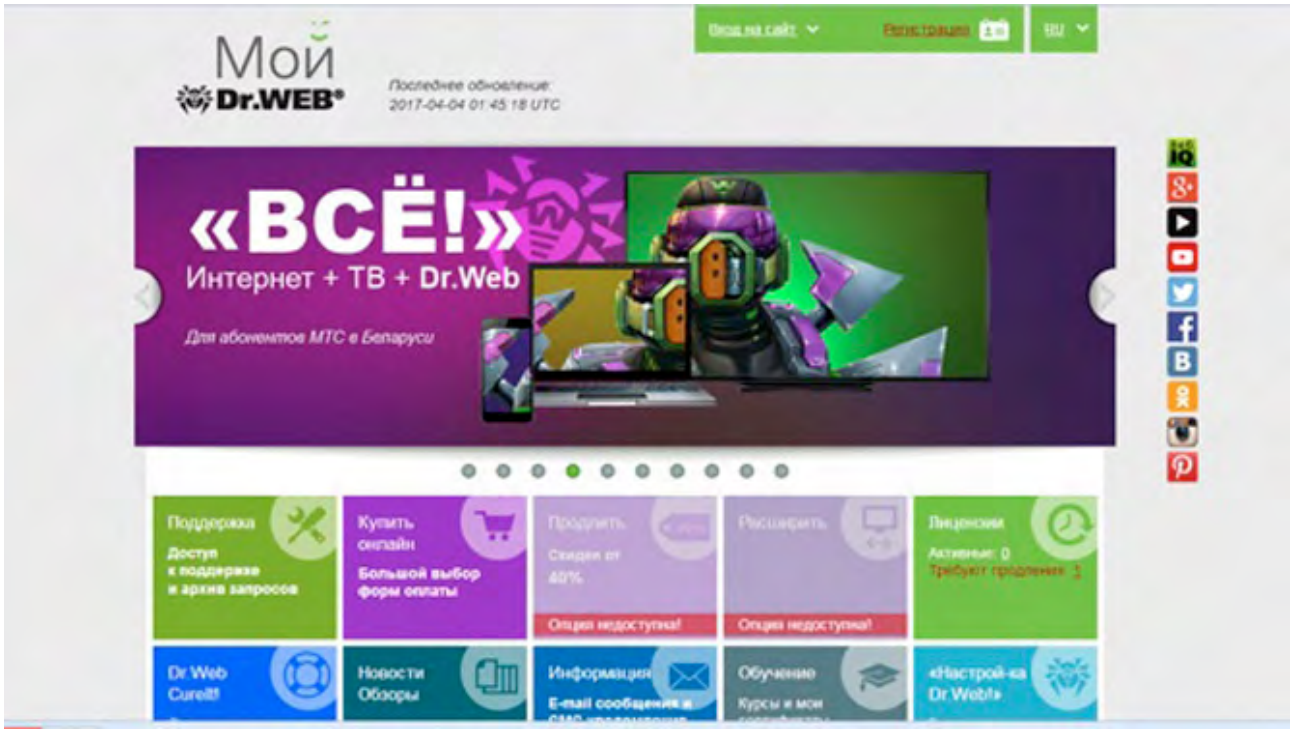
Брандмауэр — проконтролирует сетевую активность приложений.

- Защитит от несанкционированного доступа извне.
- Предотвратит утечки важных данных по сети.
- Проконтролирует подключения и передачу данных по сети Интернет.
- Заблокирует подозрительные соединения.

Аудитор безопасности — произведет диагностику, выявит проблемы безопасности и предложит решения для их устранения.

14. Личный кабинет «Мой Dr.Web»

Это персональный помощник и путеводитель по сервисам для пользователей, персональный доступ к услугам техподдержки и архив всех запросов, которые хранятся в течение действия лицензии и 60 дней после ее окончания. Доступ к кабинету производится из приложения или со страницы http://support.drweb.com/get+cabinet+link



15. Правила гигиены при использовании Android-устройств

Антивирус — не панацея, а эффективный инструмент защиты от интернет-угроз в умелых руках грамотного и внимательного пользователя.

1. Загружайте и устанавливайте приложения только из надежных источников, таких как каталог Google Play или официальные веб-сайты разработчиков установленных на вашем устройстве программ.
2. Регулярно проводите антивирусные сканирования устройства — не реже 1 раза в неделю. Даже если на вашем компьютере не происходит ничего подозрительного, это не означает, что он не заражен.
3. Не отключайте антивирусную защиту (полностью или некоторые ее компоненты).
4. Если Аудитор безопасности диагностировал на устройстве опасную уязвимость, откажитесь от покупки такого устройства. А если вы уже приобрели его — прекратите использование этого устройства и верните его в торговую организацию. Если возврат невозможен, хотя бы не используйте его для онлайн-платежей.
5. Если вы используете мобильное устройство для совершения платежей, антивирус должен быть установлен на такое устройство до установки приложения мобильного банкинга. По возможности используйте мобильные банковские приложения на отдельном устройстве, которое не используется повседневно (например, для посещения социальных сетей, поиска информации в Интернете, просмотра видео и т. п.).
6. Проводите обновление антивируса перед каждой сессией онлайн-банкинга. Актуальные обновления позволят избежать проникновения новейших угроз.
7. Никогда не используйте мобильное приложение онлайн-банкинга через Wi-Fi в общественных местах. Именно там преступники чаще всего совершают хищения аутентификационных данных.
8. Меняйте пароль к онлайн-банкингу не реже чем раз в месяц.
9. Не переходите по непроверенным ссылкам якобы от «друзей» из социальных сетей во избежание заражения мобильного устройства троянцем. Чтобы избежать попадания на устройство СМС с такими ссылками, используйте Фильтр звонков и СМС. Чтобы не попасть на вредоносный сайт, используйте URI-фильтр.

10. Устанавливайте банковское ПО, которое было загружено только из каталога Google Play или непосредственно с веб-сайта кредитного учреждения. Не скачивайте и не устанавливайте банковские приложения со сторонних ресурсов лишь потому, что описание на них сулит вам невероятный функционал и удобство. Используйте только официальные каналы распространения таких программ!
11. Следите за тем, чтобы любое установленное на устройстве ПО (включая банковское) всегда имело самую свежую версию. Своевременно устанавливайте обновления, как только они будут доступны.
12. В настройках банковской учетной записи обязательно включите двухфакторную аутентификацию, если она не была активирована по умолчанию. В случае если злоумышленники получат доступ к вашей учетной записи и попытаются украсть деньги, вам предварительно придет СМС с кодом подтверждения операции, и вы будете в курсе взлома. Подробнее о двухфакторной идентификации рассказано в выпуске «Человеческий двухфактор».
13. Установите лимит на денежные операции, совершаемые с использованием услуг мобильного банкинга. Даже если ваша учетная запись будет скомпрометирована, вы сможете сохранить большую часть денег и в дальнейшем будете решать с банком вопрос о возврате не всех утраченных средств, а лишь небольшой суммы. Сэкономьте себе нервы.

16. Памятка ответственного сотрудника

при использовании личного мобильного устройства/компьютера для работы (так называемая практика BYOD = Bring Your Own Device)

1. Изучите и соблюдайте установленные вашей компанией правила использования личных устройств для работы.
2. Если вы используете ПК или ноутбук, заведите на устройстве 2 администраторские учетные записи: для личных и рабочих нужд; отключите учетную запись Гость и возможность автозапуска программ.
3. Используйте сложные пароли для входа в учетные записи и регулярно меняйте их.
4. Своевременно устанавливайте все обновления и новые версии ВСЕГО установленного ПО, включая банковское (которое должно быть только лицензионным) из официальных источников. При использовании корпоративной системы безопасности должна действовать централизованная установка обновлений установленного ПО.
5. Доверьте выбор антивируса для защиты вашего ПК/ноутбука или смартфона системному администратору вашей компании.
6. Используемый антивирус должен обладать возможностью включения в корпоративную систему безопасности для централизованного управления.
7. Антивирусная защита должна быть комплексной, только антивируса уже недостаточно.

Компоненты защиты для ПК									URL	
Компоненты защиты для мобильного устройства										

На смартфонах и планшетах с SIM-картами Антивор позволит удаленно заблокировать устройство и стереть на нем всю информацию, чтобы она не попала в руки злоумышленников.

Эти компоненты защиты нельзя отключать ни при каких условиях (а при централизованном управлении защитой это сделать невозможно)!

8. Безвозвратно удаляйте корпоративную информацию с помощью специальных средств, если:
   - вы увольняетесь;
   - ваше устройство меняет владельца.
     Рекомендуем доверить это системному администратору вашей компании и задокументировать этот факт — если произойдет утечка данных, вас не смогут обвинить в ней даже после вашего увольнения.
9. Запишите и храните в надежном месте серийный номер устройства — это необходимо на случай его пропажи.

Нельзя!

- Использовать устройства с модифицированной заводской прошивкой или версией ОС, созданной третьими лицами.
- Использовать бывшие в употреблении (б/у) неизвестным вам лицом устройства.
- Скачивать и устанавливать программы из других источников, кроме каталога Google Play или официальных сайтов разработчиков.
- Разрешать другим пользоваться вашим устройством.
- Заходить в Интернет по личным делам с рабочего аккаунта.
- Отключать автоматические обновления антивируса.
- Требовать от системного администратора компании отключать обновления и регулярные сканирования (если используется корпоративная система безопасности).
- Если вы используете устройство для проведения платежей через систему дистанционного банковского обслуживания — на нем **нельзя** проводить **никакие другие** операции.

- Памятка с СМС-командами к Антивору Dr.Web
- Видео о работе продукта
- Частые вопросы
- Рубрика «Туманность Андроида» проекта «Антивирусная правДА!», а также выпуски других рубрик с хештегами #Андроид и #мобильный
- Информационный проект «Мобильное воровство»

Dr.WEB®
с 1992 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Обучение
Кабинет заочника Dr.Web (требуется регистрация)
Курсы для инженеров | Курсы для пользователей | Брошюры

Просвещение
«Антивирусная правДА!» | ВебIQметр | Брошюры

Контакты
Центральный офис ООО «Доктор Веб»
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а

Телефоны

Схема проезда

Контакты для прессы

Офисы за пределами России

антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru | curenet.drweb.ru

© ООО «Доктор Веб»,
2003-2017

Присоединяйтесь к нам в социальных сетях