# Что такое зловредные приложения и как от них избавиться.

К зловредным приложениям относятся следующие вредоносные программы


**Вирус и его виды**

Под вирусом принято понимать разновидность зловреда, копирующего себя. С его помощью происходит заражение других файлов (подобно вирусам в реальной жизни, которые заражают биологические клетки с целью размножения).

С помощью вируса можно проделывать большое количество различных действий: получить доступ к компьютеру в фоновом режиме, украсть пароль и сделать так, что зависнет компьютер (заполняется ОЗУ и загружается ЦП различными процессами).

Однако основной функцией malware-вируса является возможность к размножению. Когда он активизируется, заражаются программы на компьютере.

Запуская софт на другом компьютере, вирус и здесь заражает файлы, к примеру, флешка с зараженного ПК вставленная в здоровый, тут же передаст ему вирус.

**Червь**

Поведение червя напоминает поведение вируса. Отличие только в распространении. Когда вирус заражает программы, запускаемые человеком (если программы не использовать на зараженном компьютере, вирус туда не проникнет), распространение червя происходит с помощью компьютерных сетей, по личной инициативе.

Например, Blaster за быстрый период времени распространился в Windows XP, так как данная операционная система не отличалась надежной защитой веб-служб.

Таким образом, червь использовал доступ к ОС с помощью Интернета.

После этого зловред переходил на новую зараженную машину, чтобы продолжить дальнейшее размножение.

Данных червей увидишь редко, так как сегодня Windows отличается качественной защитой: брандмауэр используется по умолчанию.

Однако черви имеют возможность распространяться другими методами — например, через электронный почтовый ящик инфицируют компьютер и рассылают собственные копии всем, кто сохранен в списке контактов.

Червь и вирус способны совершать множество других опасных действий при заражении компьютера. Основное, что дает зловреду признаки червя — способ распространения собственных копий.

**Троян**

Под троянскими программами принято понимать вид зловредов, которые имеют вид нормальных файлов.

Если вы запустите «троянского коня», он начнет функционировать в фоне совместно с обычной утилитой. Таким образом, разработчики трояна могут получить доступ к компьютеру своей жертвы.

Еще трояны позволяют мониторить активность на компьютере, соединять компьютер с бот-сетью. Трояны используются для открытия шлюзов и скачивания различных видов вредоносных приложений на компьютер.

Рассмотрим основные отличительные моменты.

1. Зловред скрывается в виде полезных приложений и во время запуска функционирует в фоне, открывает доступ к собственному компьютеру. Можно провести сравнение с троянским конем, который стал главным персонажем произведения Гомера.
2. Этот зловред не копирует себя в различные файлы и не способен к самостоятельному распространению по Интернету, подобно червям и вирусам.
3. Пиратский программный софт может быть инфицирован трояном.

**Spyware**


Spyware — еще одна разновидность вредоносного ПО. Простыми словами, это приложение является шпионом.

С его помощью происходит сбор информации. Различные виды зловредов часто содержат внутри себя Spyware.

Таким образом, происходит кража финансовой информации, к например у.

Spyware часто используется с полностью бесплатным софтом и собирает информацию о посещаемых интернет-страницах, загрузках файлов и так далее.

Разработчики программного обеспечения зарабатывают, продавая собственные знания.

**Adware**


Adware можно считать союзником Spyware.

Речь идет о любом виде программного обеспечения для показа рекламных сообщений на компьютере.

Софт показа рекламы внутри самого приложения, как правило, не называют зловредом. Adware получает доступ к системе пользователя, чтобы показывать различные объявления.

Например, может показывать всплывающие рекламные сообщения на компьютере, если вы не устанавливали ничего.

Также часто происходит такое, что Adware использует дополнительную рекламу на сайтах во время их просмотра. В данной ситуации сложно что-либо заподозрить.

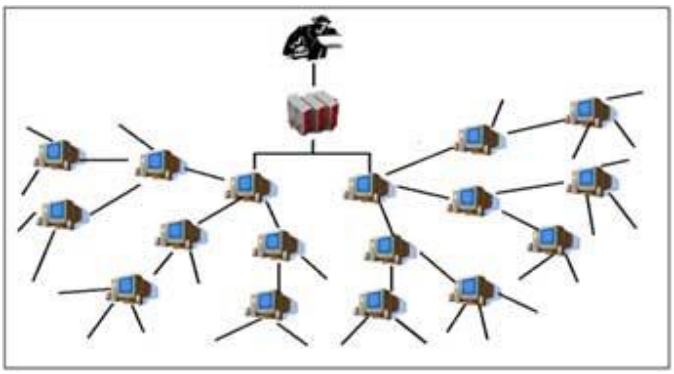
**Keylogger**


Кейлоггер является вредоносной утилитой.

Запускается в фоновом режиме и фиксирует нажатия всех кнопок. Эта информация может содержать пароли, имена пользователей, реквизиты кредитных карт и другие конфиденциальные данные.

Кейлоггер, вероятнее всего, сохраняет нажатия кнопок на собственном сервере, где их анализирует человек или специальное программное обеспечение.

**Ботнет**



Ботнет представляет собой огромную компьютерную сеть, которой управляет разработчик.

В этом случае компьютер работает в качестве «бота», так как устройство инфицировано определенным зловредом.

Если компьютер заражен «ботом», то связывается с каким-нибудь сервером управления и ожидает инструкций от ботнета разработчика.

Например, бот-сети способны создавать атаки DDoS. Все компьютеры в бот-сети могут использоваться для атаки определенного сервера и веб-сайта различными запросами.

Эти частые запросы могут стать причиной выхода из строя сервера.

Разработчики ботнетов продают доступ к собственной бот-сети. Мошенники могут использовать большие бот-сети для реализации своих коварных идей.

**Руткит**

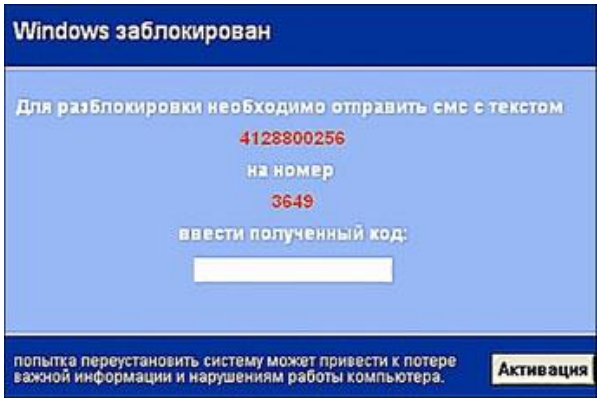

Под руткитом принято понимать вредоносное программное обеспечение, которое находится где-нибудь в глубинке персонального компьютера.

Скрывается различными способами от пользователей и программ безопасности.

К примеру, руткит загружается перед стартом Windows и редактирует системный функционал операционной системы.

Руткит можно замаскировать. Но основное, что превращает вредоносную утилиту в руткит, он скрывается в «недрах» операционной системы.

**Баннеры вымогатели**




Речь идет о достаточно коварном виде вредоносных программных продуктов.

Кажется, с этим видом злоредов встречалось не малое количество людей.

Таким образом, компьютер или отдельные файлы окажутся в заложниках. За них нужно будет заплатить выкуп.

Наиболее популярной разновидностью считаются порно – баннеры, которые требуют отправить денежные средства и указать код. Стать жертвой данного программного обеспечения можно, не только заходя на порно-сайты.

Есть вредоносное программное обеспечение наподобие CryptoLocker.

Оно в прямом смысле этого слова шифрует какие-нибудь объекты и требует оплату за открытие доступа к ним. Данная разновидность злворедов является самой опасной.

Поэтому, важно создавать резервные копии.

**Фишинг**

Фи́шинг (англ. phishing, от fishing – рыбная ловля, выуживание – вид интернет – мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри соц. сетей.


В письме обычно содержится прямая ссылка на сайт, внешне неотличимый от настоящего.

После того, как пользователь попадет на поддельный сайт, мошенники пытаются разными психологическими приемами вынудить пользователя ввести на поддельной странице свои данные, логин  пароль, которые он использует для доступа к сайту, это дает возможность мошенникам получить доступ к аккаунтам и банковским счетам.

**Спам**

Спам (англ. spam) – почтовая рассылка коммерческой или иной рекламы  лицам, не выражавшим желания на получение.


В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.

Не запрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM (англ.) русск. (англ. Spam over IM).

Доля спама в мировом почтовом трафике составляет от 60% до 80% (выдержка взята из Википедии).

Вот практически все наиболее «популярные» виды вредоносных программ вирусов.

Надеюсь вы сможете минимизировать ваши встречи с ними, а с некоторыми никогда не повстречаетесь.

**Итоги**

Почему антивирусное программное обеспечение так называется? Пожалуй, из-за того, что большое количество людей убеждено, что «вирус» — это синоним вредоносного программного обеспечения.

Антивирусы, как известно, защищают не только от вирусов, а и от других нежелательных программ, а еще для профилактики – предупреждения от заражения. На этом пока все, будьте внимательны это одна из главных составляющих зашиты вашего компьютера.

Зловреды поражают не только компьютеры, но и смартфоны. Как сделать так, чтобы защитить свой смартфон от вредоносных приложений

Для того не подвергнуть свой компьютер угрозе и защитить свои персональные данные, нужно как минимум установить хотя бы одну антивирусную программу. Представляем вашему вниманию семь лучших бесплатных антивирусных программ.

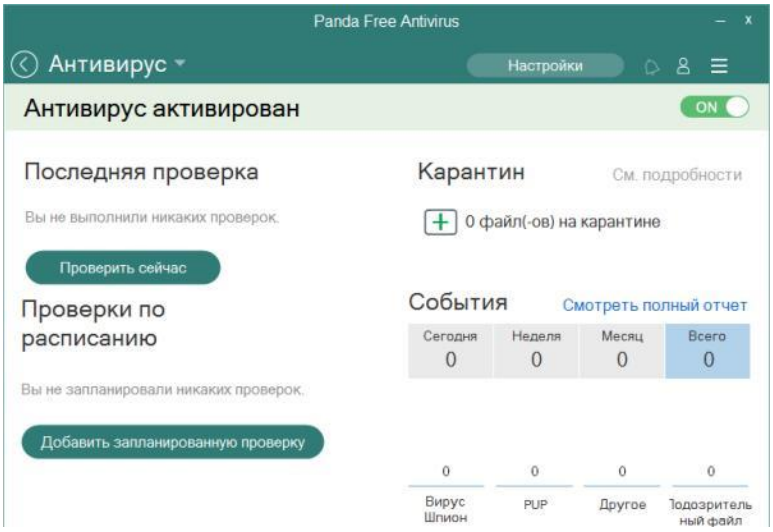
Сегодня без антивируса не обойтись. Конечно, полностью от вирусов они не защитят, но в большинстве случаев помогут вовремя найти и удалить эту заразу. Какой лучше выбрать антивирус? Здесь каждый определяет для себя сам. При этом вовсе не обязательно пользоваться платными версиями. Ведь сегодня существует масса бесплатных продуктов, которые справляются со своей задачей ничуть не хуже. А если нет разницы, зачем платить?

В Виндовс 8 и 10 по умолчанию уже имеется встроенный «Защитник Windows». В принципе, можно пользоваться и ним. Но, как показывает практика, со своей задачей он справляется не всегда.

**Рассмотрим возможности некоторых антивирусных программ.**

**Panda Free Antivirus**

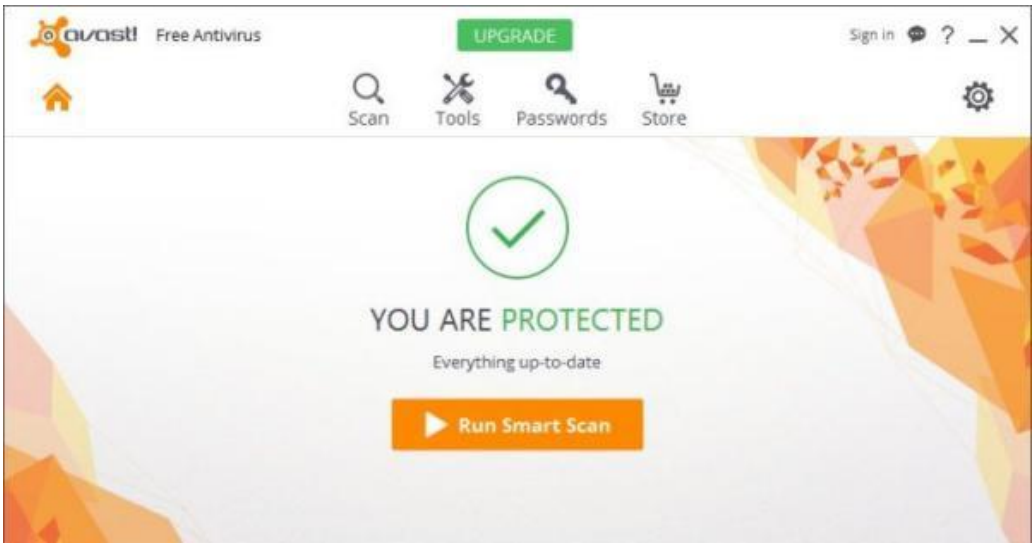
Одним из лучших бесплатных антивирусов считается Panda Free Antivirus. Он прочно застолбил за собой первую строчку в различных рейтингах и показывается практически идеальные результаты (близкие к 100%) на Windows 7, 8 и 10. Этот антивирус включает в себя: облачный антивирус; anti-шпион; anti-руткит; эвристическую проверку.




Также он способен блокировать файлы при автозапуске с флешки (или других USB-устройств). Кроме того, с недавних пор этот бесплатный антивирус приобрел «коллективный интеллект» – новую технологию, благодаря которой проверка вирусов выполняется на удаленных серверах.

Это позволяет не обновлять программу, но в то же время требует наличие быстрого и постоянного интернета. А вот в случае его отсутствия качество защиты несколько снижается. Ссылка на оф. сайт Panda. http://www.pandasecurity.com

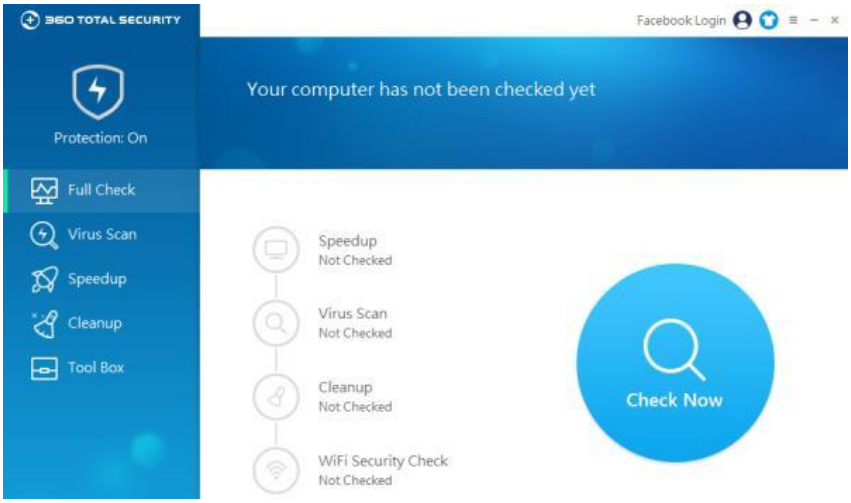
**Avast Free Antivirus Avast** – один из наиболее распространенных бесплатных антивирусов, о котором знают многие пользователи. Если верить тестам, то на Windows 7 и 8 Аваст показывает практически идентичные с платными продуктами результаты. А на Windows 10 оценка составляет 97% (против 99% в «семерке» и «восьмерке»).




Да, некоторым пользователям не нравятся регулярные напоминания о покупке платной версии, но это личное дело разработчиков. Что касается эффективности, то со своей основной задачей Avast справляется превосходно. Основные функции этого бесплатного антивируса: стандартный антишпион; сетевой и интернет-мониторинг (анализ трафика, поиск потенциальных уязвимостей в программах); анализ софта на ПК или ноутбуке (поиск старых программ, которые могут служить источником заражения). Также Avast Free умеет сканировать браузеры и их расширения (плагины), из-за которых очень часто появляется ненужная реклама. Плюс он может создавать аварийный диск (пригодится в том случае, если компьютер или ноутбук даже не включается из-за вирусов). Антивирус полностью на русском языке, интерфейс – простой и понятный. Словом, пользоваться им очень просто. Ссылка на оф. сайт Аваста. https://www.avast.ru/

## 360 Total Security

На самом деле лучшим бесплатным антивирусом считался 360 Total Security. До недавних пор. Согласно тестам, он обогнал многие аналоги и даже был представлен на сайте Microsoft в списке рекомендованных.

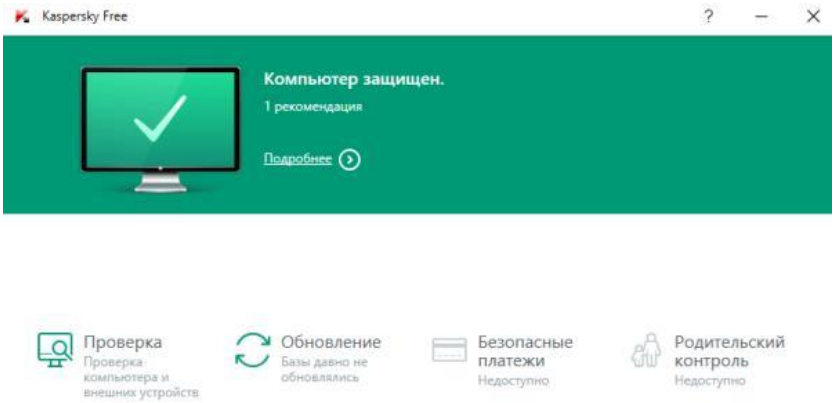



Основные его функции: защита от подозрительных сайтов (можно создать черный и белый список); добавление подозрительного софта в «песочницу» (с целью исключить его влияние на работу Windows); защита документов от вирусов-вымогателей, которые шифруют файлы; защита браузеров, web-камеры, флешек и иных USB-устройств. Но вскоре его дисквалифицировали и исключили из всех возможных рейтингов. За что его «выгнали» – точно неизвестно. В связи с этим событием пользователи разделились на 2 лагеря: первые обходят его стороной, а вторые – спокойно ним пользуются.

## Kaspersky Free

Сегодня существуют также бесплатные версии платных продуктов.

Одна из них – Kaspersky Free.




В Kaspersky Free нет многих доп. защитных модулей, которые имеются в KIS 2017. Тем не менее, он отлично справляется с защитой ПК (как для

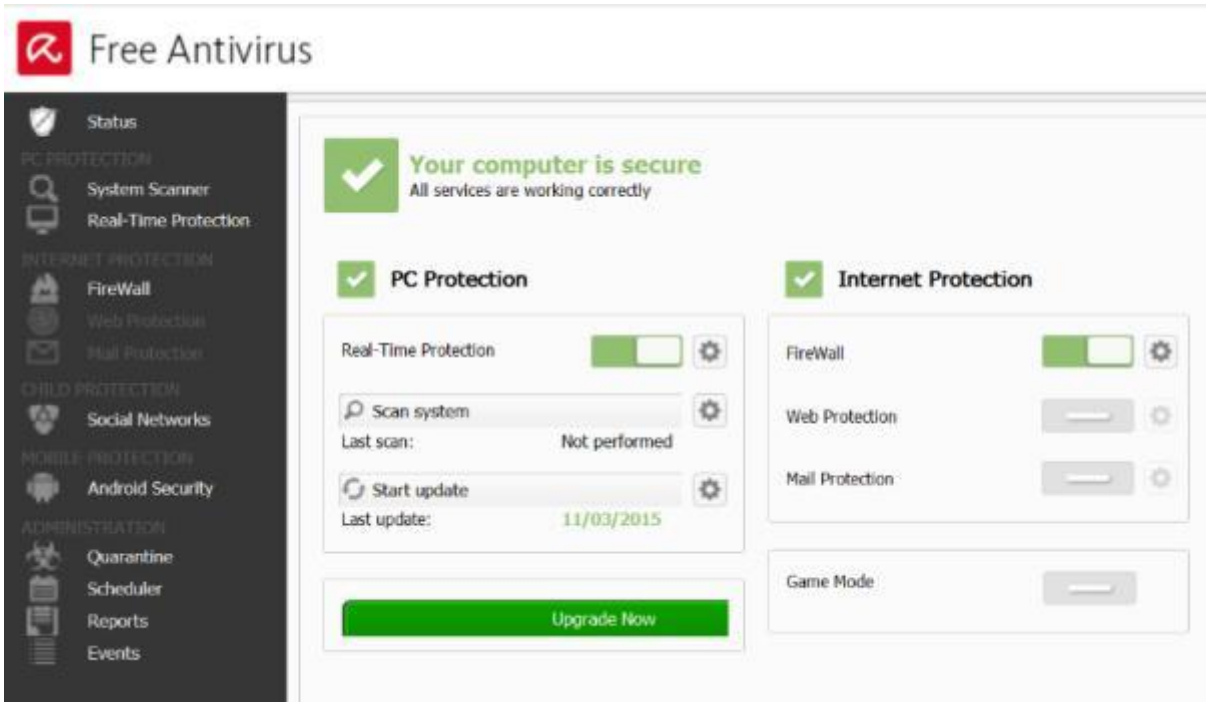
бесплатного софта). И вы можете в этом лично убедиться (ссылка на оф. сайт Kaspersky). https://free.kaspersky.com/ru

**Bitdefender Antivirus Free Edition** еще один отличный бесплатный антивирус, являющийся «урезанной» версией одноименного платного продукта. Единственный в этом списке, который имеет английский интерфейс. С ноября 2016 вышла новая версия с поддержкой Windows 10. Также был немного изменен интерфейс.


Данный антивирус считается одним из лучших бесплатных продуктов, даже несмотря на минимальное количество настроек. А все потому, что он: обеспечивает надежную защиту; не нагружает ПК или ноутбук; не надоедает постоянными всплывающими сообщениями. Ссылка на оф. сайт BitDefender. https://www.bitdefender.com

**AVG Antivirus Free**

И последний среди лучших бесплатных антивирусов – Avira Free. Тоже представляет «урезанную» версию собрата PRO, который получает высокие оценки в тестах.



Среди имеющихся здесь функций: защита ПК; проверка на вредоносные вирусы; возможность создания загрузочного диска. К доп. возможностям относятся поиск руткитов и настройка параметров брандмауэра.

Кстати, Avira показывает практически идентичные результаты с AVG Free. Поэтому, если последний антивирус по определенным причинам вам не подошел, можете попробовать Авиру. С недавних пор Avira помимо Windows 7 и 8 поддерживает также Windows 10. Ссылка на оф. сайт Авиры.

**Помните,** что ставить на ПК или ноутбук можно только один антивирус. Иначе они будут конфликтовать.

«Защитник Windows», имеющийся на Виндовс 8 и 10 является исключением, его данное правило не касается. Также сегодня очень часто в браузерах появляются всплывающие баннеры, окна с рекламой и пр. Бесплатные антивирусы (впрочем, и платные тоже) с ними справляются не всегда. Для этого лучше использовать специальный софт – к примеру, AdwCleaner и подобные ему аналоги. Они не конфликтуют с бесплатными антивирусами, зато хорошо подчищают вирусы и рекламные баннеры, которые они не видят.

## Как НЕ скачать зловредное приложение для Android

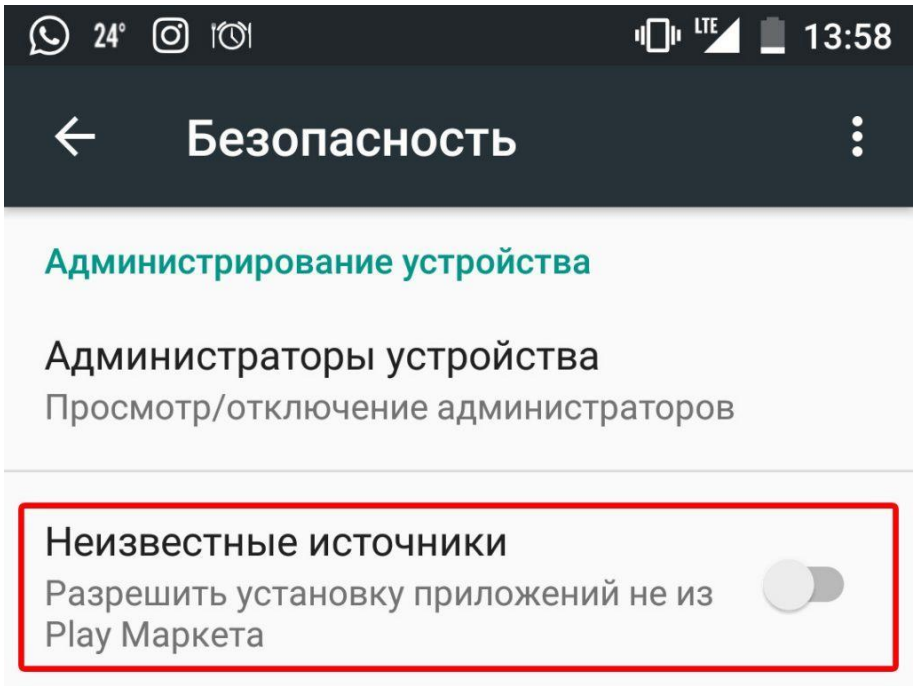
Среди существующих мобильных операционных систем Android — самая распространенная, а потому и зловредного ПО для нее больше всего. На это есть и еще одна причина: Android позволяет устанавливать приложения из любого источника, а не только из единственного официального магазина, как это сделано, например, в iOS.

С одной стороны, это дает пользователю Android больше возможностей выбора, с другой снижает уровень безопасности, поскольку каждый может написать приложение и распространять его через какие угодно каналы — будь то магазины приложений, реклама, форумы и так далее. Подхватить какую-нибудь заразу на Android проще простого, однако есть способы значительно снизить риски — вот 5 основных правил, которых стоит придерживаться, чтобы избежать проблем.

*1. Скачивайте приложения только из Google Play*

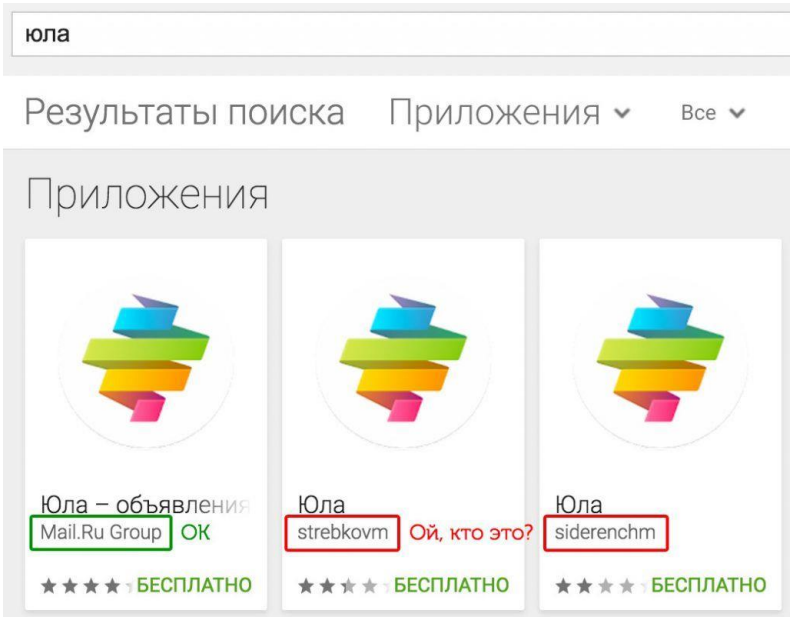
В Google есть целое подразделение, которое занимается именно проверкой приложений, попадающих в Google Play. Да, туда все равно иногда просачиваются зловредные программы, но шанс скачать вредоносное приложение из официального магазина Google намного меньше, чем из какого-то открытого источника — большую часть всякой гадости специалисты Google успевают отфильтровать.
Теоретически можно довериться и другим магазинам — но тоже только большим и известным, не принимающим от разработчиков сомнительные программы. Возможность установки приложений из сторонних источников лучше вообще отключить в настройках — так вы исключите попадание на устройство большой части троянцев, распространяющихся через рекламу и сторонние площадки.

Чтобы это сделать, снимите галочку напротив пункта Настройки -> Безопасность -> Неизвестные источники.



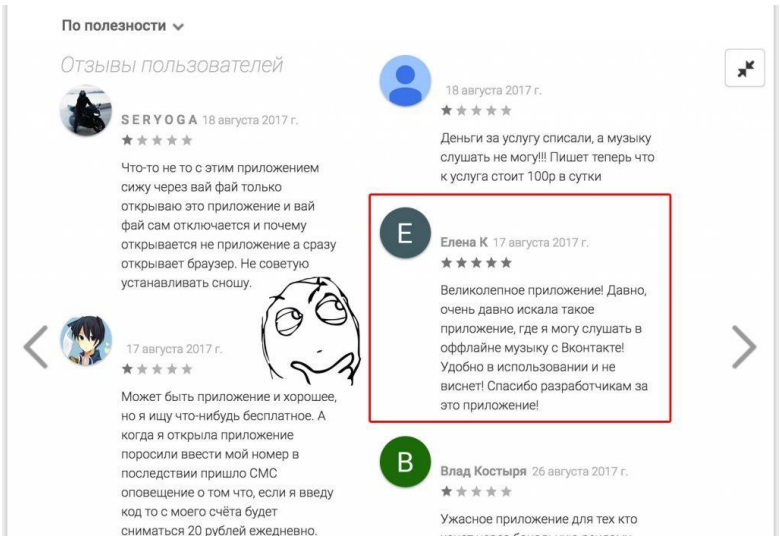
*2. Выбирайте приложения от проверенного разработчика.*

Большой компании с известным именем не резон подсовывать вам зловредов и портить свое честное имя, так что скачивать приложения от известных разработчиков безопаснее. Полное название разработчика, список опубликованных им приложений и его контактные данные можно посмотреть в расширенном описании приложения в том же Google Play Store.




3. *Смотрите на рейтинг и читайте отзывы*

Чаще всего высокий рейтинг приложения в магазине говорит о том, что оно действительно хорошее, полезное и безопасное. Тем не менее и здесь нужно быть бдительным: бывает так, что злоумышленники с помощью троянов накручивают приложениям рейтинги и подделывают отзывы.



Поэтому просто высокого рейтинга мало — стоит посмотреть в отзывы и понять, написаны они в основном людьми или все-таки ботами. Сгенерированные зловредами отзывы чаще всего положительны и односложны, или же несколько одинаковых отзывов могут идти один за другим — это тоже довольно очевидный тревожный звоночек. К тому же в случае проверенных и действительно популярных приложений рейтинги далеко не всегда достигают оценки в пять звезд, а отзывы чаще всего развернутые, в том числе и негативные — пользователи пишут их для связи с разработчиком и решения проблем, с которыми сталкиваются.

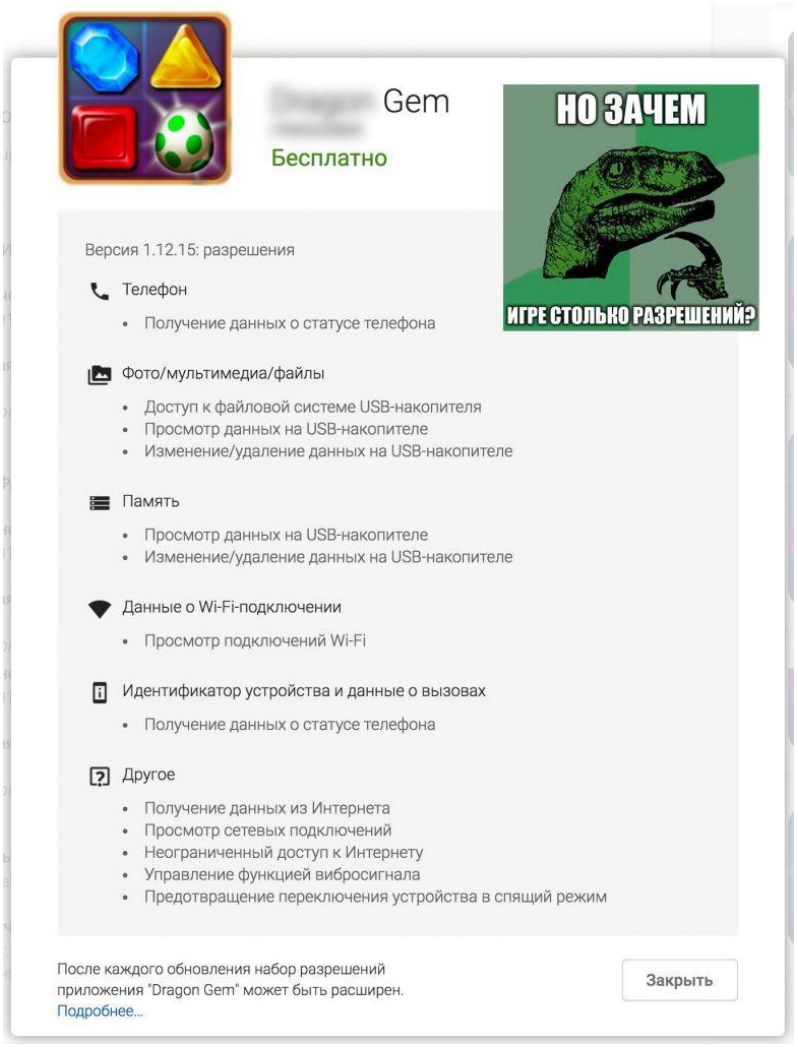
*4. Обращайте внимание на разрешения, которые приложение запрашивает при установке*

Система разрешений — это защитный механизм Android, регулирующий «свободу действий» приложения. Именно с их помощью программа может получить доступ к тем или иным функциям и данным (по умолчанию, если разрешение не выдано, приложениям очень мало что дозволено).

Какие разрешения могут быть опасными и какую именно опасность они представляют.

В основном опасность связана с возможностью сбора данных о вас — местоположения, контактов, личных файлов — и совершения определенных действий — записи при помощи камеры или микрофона, отправки сообщений и так далее.

Поэтому перед установкой приложения важно внимательно посмотреть, какие именно разрешения оно запрашивает, и здраво оценить эти запросы: действительно ли ему нужны эти разрешения и для чего, не выглядит ли это подозрительно. В Android от 6.0 и выше после установки приложения разрешения также можно посмотреть и дать или отозвать в настройках устройства.




5. *Пользуйтесь надежным защитным решением*

В любом случае, что бы вы ни собирались скачать — убедитесь, что на вашем устройстве установлено надежное защитное решение. Существует две версии Kaspersky Internet Security для Android: в базовой бесплатной версии вы можете провести проверку приложений вручную — а в расширенной, платной версии такая проверка проводится автоматически.
Осознанный подход — то, что объединяет все эти правила. Перед установкой приложения стоит задаться вопросом: действительно ли оно вам необходимо? Доверяете ли вы источнику? Не кажутся ли вам подозрительными запросы на разрешения? Если уделять этому достаточно внимания — за удобство использования и собственную безопасность можно не переживать.

В обзоре использованы материалы размещенные на блоге лаборатории Касперского https://www.kaspersky.ru/blog/privacy-ten-tips-2018/20898/