Ложные антивирусы (лже-антивирусы).

Сегодня наша беседа посвящена ложным (фальшивым антивирусам).

Киберпреступники постоянно ищут новые способы манипуляции своими жертвами в Интернете. Один из самых значительных барьеров на пути кибератаки — это осведомленность и бдительность. Именно поэтому стоит знать о фальшивых антивирусах. Они обычно очень похожи на настоящие, только не защищают от вирусов и приносят много проблем.

Этот способ мошенничества с каждым днем набирает обороты и является большой проблемой для многих начинающих пользователей, поэтому цель этой статьи объяснить смысл работы таких программ, чтобы уберечь вас от обмана.

**Что такое ложные антивирусы?**

Ложные, поддельные, фальшивые антивирусы — один из популярных вариантов интернет-мошенничества. Суть его заключается в том, чтобы заставить пользователя заплатить деньги за программу, которая якобы удалит с компьютера или смартфона очень опасные вирусы и защитит в дальнейшем устройство пользователя от различных угроз.

В действительности такое приложение является «пустышкой», т.е. не содержит никакой функциональности, кроме отображения пугающих уведомлений. В зарубежной практике их называют "rogueanti-virus" или "rogueware" — от слова "rogue", означающего «жулик, мошенник».

Поверив злоумышленнику и заплатив деньги, пользователь в лучшем случае получает абсолютно бесполезное приложение, а в худшем — самую настоящую вредоносную программу, которая будет, например, красть данные кредитных карт и прочую конфиденциальную информацию.

**Как программа попадает в ваше устройство?**

Все, наверное, видели, как время от времени при серфинге в Интернете внезапно появляются всплывающее окно или баннер с рекламой антивируса для вас?

Иногда он выглядит как результаты уже проведенного сканирования вашего компьютера, в котором обнаружен десяток страшных вирусов.

После скачивания мы естественно устанавливаем эту программу и запускаем проверку системы. При этом мы абсолютно не замечаем никакого подвоха, т.к. скачивается такая программа как обычно, устанавливается как обычно, и во время сканирования всё выглядит стандартно, красиво и качественно.

По сути, установка «лже-антивируса» является добровольным заражением компьютера.

Всё вроде бы хорошо, если бы не было так плохо! Такая программа только выдает себя за надежную и эффективную, а на самом деле является ложным антивирусом – хитроумной программой для обмана наивных пользователей.

В ходе проверки такая программа обязательно находит в любом компьютере вирусы или вредоносные коды и всячески пытается убедить нас, что они очень опасны.

А далее может следовать предложение отправить платное SMS или приобрести лицензионную копию этой программы, чтобы с её помощью избавить компьютер от найденных вирусов. Такие сообщения могут появляться на рабочем столе, в системном трее либо во всплывающих окнах любого браузера.

Иногда такие всплывающие уведомления вообще не удаётся закрыть каким-либо образом.

Перепуганный пользователь отправляет свои деньги мошенникам, не подозревая, что никаких вирусов в его компьютере возможно и не было. Заплатив деньги, мы в лучшем случае приобретем абсолютно бесполезную программу, которая фактически ничего не делает, а в худшем – получим в свой компьютер троян, который крадет конфиденциальную информацию.

Очень важно понимать, что попасть под такое влияние не так уж и сложно, т.к. очень часто названия и внешний вид «лже-антивирусов» совпадают с официальными лицензионными антивирусами, а некоторые из них имеют даже свою службу поддержки, в которой оператор с помощью чата отвечает на вопросы будущих жертв обмана.

Мы думаем, что работаем с настоящим серьезным сервисом и покупаем надежный антивирус, а на самом деле это просто клон настоящего антивируса, чаще всего представляющий из себя троянскую программу.

Ярким примером «лже-антивируса» служит программа «Security Essentials 2010», которая выдает себя за «Microsoft Security Essentials».

Эта программа вместо обещанного поиска и устранения вирусов контролирует запущенные процессы и пытается завершить те, которые считает ненужными. Кроме того она может изменять реестр, контролирует интернет-трафик, а также совершает массу других действий мешающих нормальной работе компьютера.

Помимо описанного способа распространения таких программ существуют также и другие. Например, тот же «Security Essentials 2010» может распространяться под видом обновления «Flash» проигрывателя, необходимого для просмотра видео в Интернете.

И это не смотря на то, что «Adobe Flash Player» прекратило разработку и поддержку своего программного обеспечения в начале 2021 года в пользу более современного для использования медиа и 3D, которое уже давно встроено во все современные браузеры.

Многие сайты и бесплатного, и платного программного обеспечения практически всегда во все установочные версии любых программ, обязательно встраивают окошко с вопросом о согласии на установку дополнительных утилит для защиты вашего ПК, дополнительных программ, которые вам так необходимы. Некоторые установочные версии настоящих программ могут содержать в себе окно с таким вопросом. Естественно вы должны нажать кнопку: не согласен, отказываюсь, не принимать, снять галочку с установки.

В качестве примера можно привести удобную офисную программу «Стикеры», в установке, которой имеется подобное окно с вопросом о дополнительных утилитах и программах.

Можно также получить предложение проверить ваш компьютер на вирусы онлайн, естественно с помощью ложных онлайн-антивирусов.

Однако, это не говорит о том, что не существует настоящих онлайн антивирусов и что настоящими не стоит пользоваться. Напротив, вам стоит всегда быть внимательными в данном отношении.

Кроме этого мы можем просто попасть на незнакомый сайт, который сразу же выдаст сообщение о том, что наш компьютер заражен вирусами, и тут же предложит скачать «самый надежный антивирус».

Получить такой ложный антивирус можно не только на сайте мошенников, но и на множестве других «партнерских» сайтах, владельцы которых получают процент за каждого обманутого пользователя.

А самое печальное, что попасть на сайт мошенников можно даже с настоящего сайта, если такой сайт содержит стороннюю рекламу. И ключевое слово здесь «Если».

Устанавливая такой «лже-антивирус», мы добровольно заражаем свой компьютер, а удалить его бывает очень сложно, т.к. обычно такие программы защищают себя от удаления. Если мы попытаемся запустить какую-нибудь программу, которая как-то может повлиять на работу лже-антивируса, то сразу же получим предупреждение о том, что эта программа заражена и поэтому будет закрыта.

**Вред от ложных антивирусов.**

Если какая-нибудь программа хоть как-то может повлиять на работу «лже-антивируса», то последний находит любые вирусы под именами: Trojan, Worms и другие. Настоящие программы антивирусы и анти-шпионы обнаруживают подобные программы под именами: Trojan.Fakealert... – от англ. fake (обман).

Встречаются случаи, когда поддельная программа сама устанавливает в систему несколько вредоносных объектов, чтобы придать убедительность своим заявлениям, или занимается шпионажем, передавая разработчику пользовательские данные. Соответственно, есть вероятность, что ущерб от «лже-антивируса» не ограничится его «стоимостью» и выразится, например, в краже паролей от важных онлайн-сервисов.

Фальшивый антивирус может причинить вам немало вреда. Меры, которые он предлагает, сами по себе правильные: сканирование на вирусы, обновление программ. Беда в том, что под видом обновлений в данном случае могут быть скачаны вредоносные программы. Основной задачей фальшивого антивируса является не поиск и уничтожение вирусов, а принуждение жертвы к оплате нескольких тысяч рублей за «защиту», которая не работает. Возможны и другие варианты: поиск и похищение личной информации, в том числе банковской, списание денег с кредитной карты, а также порча файлов на компьютере.

Однако, не только на компьютере. Уже много лет существуют аналогичные поддельные антивирусы для Android (смартфон).

**Как удалить ложный антивирус?**

Удалять такие «лже-антивирусы» можно вручную, но для этого надо знать его расположение, точное название и уметь работать с реестром. Можно использовать специальные программы типа «Anti-Malware» или «Spyware Doctor». Можно сразу воспользоваться специальной утилитой для глубокого сканирования системы и реестра - «Uninstall tool 2» или похожей утилитой. После удаления программы, во всплывающем окошке необходимо подтвердить необходимость глубокого сканирования системы.

Можно также найти в интернете специальные утилиты или сервисы для автоматического удаления «фальшивых антивируса» с конкретным названием.

В качестве дополнительной защиты автозагрузки вашего компьютера можно воспользоваться утилитой под названием «AnVir Task Manager».Это Бесплатная системная утилита, которая позволяет контролировать всё, что запущено на компьютере, а также предоставляет удобные инструменты для расширенной настройки. «AnVir Task Manager» позволяет управлять автозагрузкой, запущенными процессами, сервисами и драйверами и заменяет Диспетчера Задач.

Однако, это утилита предназначена только для управления автозагрузкой и запущенными процессами в вашей системе. Она на защищает ваш компьютер от вирусов и угроз, не смотря на то, что вы вручную можете завершить любой запущенный процесс. «Anvir» только позволяет следить за вашей автозагрузкой и держать её в чистоте и порядке. Это просто расширенный набор инструментов встроенного в Windows «Диспетчера задач», который позволяет, помимо основных функций, управлять автозагрузкой системы и предоставляет набор инструментов для более тонкой настройки вашего компьютера.

**Как не попадаться на предложение установки ложного антивируса?**

Список известных фальшивых антивирусов очень большой, по некоторым данным он уже доходит до 300 названий. Надеемся, что вы понимаете, что запомнить их все просто невозможно, тем более что каждый день появляются новые названия подобных программ. Вполне вероятно, что уже появились и русскоязычные или онлайн-сервисы для такой «лже-проверки».

Лучше знать названия официальных настоящих антивирусов и анти-шпионов, чтобы не попадаться на подобные уловки мошенников.

Умные мошенники это всегда хорошие психологи, поэтому будьте предельно внимательны и следуйте хотя бы элементарной логике, чтобы не прибегать к мучительным поискам по удалению таких программ. Приучите себя не попадаться на уловки мошенников и не скачивать подозрительные бесплатные антивирусы из Интернета.

• Настоящая антивирусная программа никогда не требует платить за то, чтобы удалить вирусы.

• У настоящих антивирусов есть возможность скачивания демо-версии, в которой так же бесплатно удаляются найденные при сканировании компьютера вредоносные коды.

Серьёзные разработчики антивирусов никогда не просят деньги за удаление вирусов. Прежде чем предлагать оплатить лицензию они предлагают скачать демо-версию, которая обязательно позволяет бесплатно удалять обнаруженные вирусы. Лицензионная версия чаще всего отличается от демо-версии возможностью ежедневно обновлять антивирусные базы и дополнительными функциями.

• Серьёзные разработчики антивирусов никогда не будут обещать 100% защиты от всех вирусов, потому что это просто невозможно. Если вам обещают такое, то, скорее всего это обман.

• На сайте серьезного антивируса должны быть контактные сведения. Если информации об обратной связи нет, значит это ложная программа.

Например, на сайте Касперского в разделе «Связаться с нами» по меньше мере пять номеров телефонов для связи, один номер факса и два e-mail адреса для писем. Кроме того там есть служба поддержки, жалобная книга, пресс-центр и целая куча адресов и телефонов региональных представителей, в то время как некоторые сайты не содержат даже e-mail для связи.

Лицензионные антивирусы имеют гораздо меньше недостатков (например, минимальный процент ложных срабатываний) и большие антивирусные базы, базы подозрительных сайтов, фишинговых ссылок и вредоносных программ.

Особенно важна установка антивирусной защиты для тех, кто использует компьютер для совершения интернет-платежей или пользуется услугами интернет-банкинга.

Однако, далеко не все могут пользоваться лицензионными антивирусами.

Некоторые стараются найти бесплатные ключи для платных программ. Вот здесь необходимо предупредить (особенно начинающих пользователей). Такой поиск не всегда заканчивается удачно, а зачастую это даже небезопасно, т.к. сайты, предлагающие такие ключи, часто сами распространяют вирусы. Поиск ключей всегда подразумевает скачивание в компьютер подозрительных файлов и поэтому естественно, что в этом случае риск скачать вирус или троян гораздо выше шанса найти бесплатный ключ. К тому же такие ключи скорее всего будут временные, т.е. будут действовать не более месяца или года. И вам повторно придётся искать новый действующий ключ.

Всегда необходимо избегать малоизвестные программы и пользоваться только проверенными и известными разработчиками.

У всех таких разработчиков всегда имеются бесплатные версии лицензионных антивирусов для бюджетного сегмента пользователей, помимо «Демо-Версий». Они имеют множество ограничений, по сравнению с платной версией. Но вот что совершенно точно – это то, что они добросовестно выполняют заявленный функционал. И это намного лучше, чем просто отсутствие всяческого антивируса на вашем компьютере.

Стоит ещё обратить внимание на то, что у бесплатных версий антивирусные базы намного меньше, чем у платных версий. Поэтому если вам нужен антивирус не для дома, а для офиса, стоит подумать о приобретении платной лицензии.

Вот несколько примеров известных (проверенных) разработчиков антивирусов:

• Касперский

• Dr.Web

• ESET NOD32

• Norton Internet Security

• Avira

• AVG

• Avast

• Panda

• Trend Micro Internet Security

В заключении мы надеемся, что вооружившись нашей информацией, вы станете более осмотрительны, внимательные и не станете устанавливать сомнительные программы неизвестных разработчиков.