ИНСТРУКЦИЯ

ПО УДАЛЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ С УСТРОЙСТВА КЛИЕНТА

Если ваша учетная запись в Интернет-Банке и мобильном приложении Банка была заблокирована по причине кражи или попытки кражи денежных средств, **во избежание повторного несанкционированного доступа мошенников** необходимо осуществить поиск и удаление со своего устройства вредоносных программ. Если под воздействием мошенников вы установили на свой смартфон или компьютер какую-либо программу, вероятнее всего это программа удаленного доступа к вашему устройству. Пока вы не удалите вредоносную программу, мошенникам будет доступно управление вашим телефоном или компьютером (в том числе просмотр логина и пароля для входа в Интернет-Банк и мобильное приложение Банка).

Наиболее популярные программы удаленного доступа – AnyDesk, AirDroid, AirMore, TeamViewer и пр.

Если вы планируете использовать телефон или компьютер, на который была установлена вредоносная программа, для входа в Интернет-Банк и мобильное приложение Банка, то необходимо осуществить поиск и удаление со своего устройства вредоносных программ **до момента восстановления доступа к Интернет-Банку и мобильному приложению Банка**.

Данная инструкция актуальна для последних версий операционных систем компьютеров и смартфонов, наиболее используемых в повседневной жизни. Если у вас на устройстве (компьютере или смартфоне) установлено программное обеспечение более ранних версий, требуется обратиться на сайт разработчика программного обеспечения для получения подробных инструкций или в сервисный центр обслуживания компьютеров, смартфонов.

КАК УДАЛИТЬ ВРЕДОНОСНЫЕ ПРОГРАММЫ С ТЕЛЕФОНА

Шаг 1: Переведите ваш телефон в безопасный режим

Этот шаг позволяет остановить запуск всех сторонних приложений. Если ваш телефон перестает вести себя странно в безопасном режиме, можно предположить, что проблема вызвана вредоносным или неисправным приложением.

Для Android: Нажмите и удерживайте кнопку питания на включенном телефоне. Во всплывающем меню коснитесь кнопки питания. Коснитесь опции «Выключить» и удерживайте на ней палец до появления сообщения «Перезагрузить в безопасном режиме». Нажмите «ОК», чтобы перезапустить устройство в безопасном режиме.

Для iOS: Выключите свой телефон, как обычно. Подождите не менее 15 секунд, а затем снова включите телефон. Как только экран загорится, продолжайте нажимать кнопку уменьшения громкости, пока не увидите логотип Apple.

Шаг 2: Найдите и удалите вредоносные приложения

Для Android: Выберите «Управление приложениями» в настройках и просмотрите приложения, которые вы загрузили. Если какие-либо из них кажутся подозрительными или вы не помните, что их скачивали, это могут быть вредоносные приложения. Выберите приложение, которое вам кажется вредоносным, нажмите «Удалить». Если кнопка неактивна, для удаления приложения отмените доступ администратора устройства в разделе «Администраторы устройства» в разделе «Безопасность».

Также, если на вашем компьютере установлены и включены антивирусные программы, они чаще всего сильнее и более продвинуты, чем мобильные версии. Телефон можно проверить на вирусы через компьютер. Для этого нужно подключить телефон к компьютеру или ноутбуку в режиме «Отладка через USB». Для этого зайти в меню «Настройки», найти подпункт «Для разработчиков» и включите эту функцию. Затем выберите эту же команду в появившемся меню при подключении телефона USB-кабелем. Телефон откроется, как дополнительный диск или флешка. Далее просканируйте его антивирусом. Удалите найденные угрозы.

Для iOS: Удалите приложения, которые вам не известны или те, которые вы скачали приблизительно в то время, когда начались проблемы на вашем телефоне.

Шаг 3: Очистите данные браузера

В настройках вашего браузера выберите «История» либо «Журнал» (в зависимости от производителя и версии браузера) и выполните очистку всех данных за все время.

Шаг 4: Перезагрузите телефон

Зажмите клавишу питания (либо питания и увеличения громкости) на несколько секунд, появится панель «Выключить». Нажмите на «Выключить» (либо проведите пальцем по панели в нужном направлении), чтобы выключить устройство. Затем снова нажмите и удерживайте кнопку питания, чтобы перезапустить устройство. Это может решить проблему. Если проблема остается, перейдите к следующему шагу.

Шаг 5: Если вредоносная программа не дает зайти в меню телефона, сделайте сброс через компьютер

Для Android: С официального сайта скачайте программу Android System Development Kit (официальное приложение от разработчика Google). Распакуйте архив, нажмите кнопку «Обзор» и укажите путь «C:\Program Files». Зайдите в папку с извлеченными файлами и нажмите F2, чтобы дать ей простое название, какое вам нравится. Кликните правой кнопкой мыши по значку «Мой компьютер» или на соответствующем разделе в меню «Пуск», чтобы попасть в «Свойства». Вам понадобится раздел «Дополнительные параметры системы», где во вкладке «Дополнительно» следует щелкнуть по кнопке «Переменные среды». В окне «Системные переменные» выберите поле «Path», а после — «Изменить». Откроется другое окно. Опуститесь вниз и задайте путь к распакованному архиву с точкой с запятой в самом начале. Например, C:\Program Files\ADTsdkplatform-tools. Вызовите командную строку. Для этого либо зайдите в «Поиск» и впишите «cmd», либо зажмите клавиши Win + R. Подсоедините мобильное устройство к компьютеру через USB. В строку запишите «adb shell». Щелкните по клавише «Enter». Когда ADB свяжется с телефоном, допишите «—wipe_data». Дале снова нажмите «Enter». Телефон перезагрузится и вернет стандартные параметры.
Для iOS: Обязательно включите на компьютере антивирус, присоединяя телефон к компьютеру. После подключения USB-кабеля, включите телефон и выберите пункт «Сброс настроек». В этом случае баннер, закрывший экран, не помешает это сделать.

Шаг 6: Восстановите заводские настройки

Для Android: Если ничего из вышеуказанного не помогло, верните телефон к заводским настройкам, предварительно сделав резервные копии файлов. Для этого перейдите в «Настройки»> «Система»> «Сброс настроек»> «Восстановление до заводских настроек» или «Стереть все данные». Помните, что эта процедура сотрет всю информацию с вашего телефона, удалит все контакты, фотографии, приложения и другие данные. Затем восстановить их можно будет только из резервной копии.
Для iOS: Если ничего из вышеуказанного не помогло, верните телефон к заводским настройкам, предварительно сделав резервные копии всех файлов. Для этого перейдите в «Настройки»> «Основные»> «Сбросить»> «Стереть контент и настройки». Помните, что эта процедура сотрет всю информацию с вашего телефона, удалит все контакты, фотографии, приложения и другие данные. Затем восстановить их можно будет из резервной копии.
Пробуйте более ранние версии резервных копий, пока не найдете ту, с которой не возникает проблем и в которой нет вредоносных программ.

КАК УДАЛИТЬ ВРЕДОНОСНЫЕ ПРОГРАММЫ С КОМПЬЮТЕРА

Шаг 1. Отключите доступ к интернету

При отключении от интернета прекращается передача данных с компьютера на сервер вредоносных программ, что позволяет защитить от заражения другие устройства, подключенные к вашей локальной сети. Если требуется подключение к интернету для загрузки какого-либо инструмента, отключитесь сразу после его загрузки. Избегайте повторного подключения к интернету после получения требуемого инструмента. Перед отключением может оказаться полезным распечатать данные инструкции.

Шаг 2: Перейдите в безопасный режим

Переход в безопасный режим позволит изолировать проблемы на устройстве.
Для Windows:

Перезагрузите компьютер. При появлении экрана входа в систему удерживайте нажатой клавишу Shift и выберите «Питание», а затем «Перезагрузить». После перезагрузки компьютера выберите «Поиск и устранение неисправностей», затем «Дополнительные параметры», затем на экране «Выбор действия» нажмите «Параметры загрузки». В следующем окне нажмите «Перезагрузить» и дождитесь появления следующего экрана. При отображении меню с нумерованными параметрами запуска, выберите номер 4 или F4, чтобы запустить компьютер в безопасном режиме.
Для macOS: Перезагрузите компьютер. При запуске компьютера сразу же нажмите и удерживайте клавишу Shift. Отпустите клавишу Shift, как только появится окно входа в систему.

Шаг 3. Не входите в учетные записи

Цель многих вредоносных программ – получение доступа к конфиденциальной информации посредством кражи ваших учетных данных, например, в результате отслеживания нажатий клавиш или считывания пароля с экрана или из буфера обмена. Избегайте входа в учетные записи не только на вашем компьютере, но и в любых используемых вами приложениях, чтобы предотвратить потерю ваших учетных данных.

Шаг 4. Удалите временные файлы

Вредоносные программы могут устанавливать на устройства временные файлы, которые необходимо удалить.
Для Windows: Закройте все активные приложения. Откройте «Параметры», выберите «Система»> «Память»> «Локальный диск»> «Временные файлы». Выберите временные файлы, которые требуется удалить и нажмите «Удалить файлы».
Для macOS: Закройте все активные приложения. Откройте Finder, в меню нажмите «Перейти»> «Перейти к папке», затем введите «~/Library/Caches/». Выделите временные файлы, которые требуется удалить, переместите выбранные файлы в корзину. Очистите корзину.

Шаг 5. Проверьте монитор активности

Если есть подозрение, что было установлено подозрительное обновление или приложение, закройте это приложение, если оно запущено. Монитор активности показывает запущенные на компьютере процессы и позволяет отслеживать их влияние на активность и производительность компьютера.
Для Windows: В поле «Введите данные для поиска» в нижней части экрана введите «Монитор ресурсов». Откроется экран, показывающий действия, выполняемые на вашем устройстве. Чтобы завершить задачу, щелкните по ней правой клавишей мыши и выберите «Завершить процесс».
Для macOS: Перейдите в Finder и выберите пункт «Приложения»> «Утилиты». Перейдите к монитору активности. Данные, отображаемые монитором активности, позволяют выявить подозрительные приложения в области процессов. На закладке ЦП можно также выяснить, какие приложения используют большую вычислительную мощность. При обнаружении подозрительных приложений закройте их с помощью монитора, а затем удалите из меню Finder.

Шаг 6. Запустите поиск вредоносных программ

Антивирусы позволяют удалить многие распространенные вредоносные программы. Однако, если на компьютере уже установлен и используется антивирус, рекомендуется использовать другое средство поиска вредоносных программ, поскольку текущее антивирусное решение может не обнаруживать эти вредоносные программы. Загрузите средство поиска вредоносных программ из надежного источника, запустите его и установите программное решение безопасности, постоянно работающее в фоновом режиме и обеспечивающее защиту от существующих и возникающих угроз безопасности.

Шаг 7. Проверьте браузер

Вредоносные программы часто изменяют домашнюю страницу браузера, чтобы заразить компьютер повторно, а также устанавливают различные расширения. Проверьте домашнюю страницу браузера, параметры подключения и установленные расширения, выполнив следующие действия.

Чтобы проверить домашнюю страницу в Яндекс Браузер, в правом верхнем углу браузера нажмите на три горизонтальные линии. Выберите пункт «Настройки» в раскрывающемся меню. Далее перейдите в пункт «Интерфейс» и включите опции «При запуске восстанавливать вкладки и группы» и «Если нет вкладок, открывать ya.ru».

Для проверки расширений в правом верхнем углу браузера нажмите на три горизонтальные линии. Выберите пункт «Настройки» в раскрывающемся меню. Далее перейдите в пункт «Дополнения». В списке перечислены предустановленные расширения (например, Антишок) и дополнительные функции Браузера (например, синхронизация). Удалите подозрительные расширения. Перезагрузите систему, чтобы изменения вступили в силу.

Чтобы проверить домашнюю страницу в Microsoft Edge, в правом верхнем углу браузера нажмите на три вертикальные точки. Выберите пункт «Настройки» в раскрывающемся меню. Далее перейдите в пункт «Пуск, главная и новые вкладки». Проверьте и подтвердите указанную по умолчанию домашнюю страницу.
Для проверки расширений в правом верхнем углу браузера нажмите на три вертикальные точки. Выберите пункт «Расширения» в раскрывающемся меню. Нажмите «Управление расширениями». Удалите подозрительные расширения. Перезагрузите систему, чтобы изменения вступили в силу.

Чтобы проверить домашнюю страницу в Chrome, в правом верхнем углу браузера Chrome нажмите на три вертикальные точки и выберите пункт «Настройки» в раскрывающемся меню. В меню выберите раздел «Внешний вид». Проверьте и подтвердите указанную по умолчанию домашнюю страницу в пункте «Показывать кнопку "Главная страница"».
Для проверки расширений в правом верхнем углу браузера нажмите на три вертикальные точки. Выберите пункт «Настройки» в раскрывающемся меню. Нажмите «Расширения». Удалите подозрительные расширения. Перезагрузите систему, чтобы изменения вступили в силу.

Чтобы проверить домашнюю страницу в Safari, выберите значок «Инструменты». Нажмите «Свойства браузера». На закладке «Общие» перейдите в раздел «Поиск». Нажмите «Настройки». Проверьте и подтвердите указанную по умолчанию домашнюю страницу.
Для проверки расширений выберите Safari> «Настройки», а затем перейдите на вкладку «Расширения». Удалите подозрительные расширения. Перезагрузите систему, чтобы изменения вступили в силу.

Шаг 8. Проверьте наличие вредоносных программ в элементах входа в систему

Элементы входа в систему включают приложения, которые запускаются при каждом запуске операционной системы. Иногда эти приложения необходимы для запуска операционной системы, а иногда они являются бесполезными и могут содержать вирусы и вредоносные программы. Важно проверить элементы входа в систему и отключить те, которые могут скрывать вредоносные программы.
Для Windows: Откройте «Параметры», выберите «Приложения»> «Автозагрузка. Отключите неиспользуемые элементы.
Для macOS: Для этого нажмите на логотип Apple в строке меню. Выберите «Системные настройки», затем «Пользователи и группы». Нажмите на значок замка в левом нижнем углу. Откройте «Элементы входа». Отключите неиспользуемые элементы.

Шаг 9. Удалите подозрительные приложения

Изучите все установленные приложения и выясните, есть ли среди них те, которые вы никогда не используете. Проанализируйте каждое приложение, чтобы узнать, как оно используется. В большинстве случаев поиском сети интернет удается выяснить, является ли приложение полезным или скрывает вредоносные программы.
Для Windows: Если приложение доступно в официальном магазине приложений Microsoft Store, оно должно быть надежным. В противном случае, если приложение трудно найти либо у него плохие отзывы, оно может являться источником вредоносных программ.
Для macOS: Если приложение доступно в официальном магазине приложений App Store, оно должно быть надежным. В противном случае, если приложение трудно найти либо у него плохие отзывы, оно может являться источником вредоносных программ.