Вредоносные программы

Узнайте, как выявлять вредоносные программы на различных устройствах, избегать их и противостоять им.

1. Что такое вредоносные программы?

Вредоносные программы — это обобщающее понятие, охватывающее различные виды программного обеспечения, которое может заразить устройство вирусом, нарушить его работу или получить несанкционированный доступ.

Вредоносные программы могут заражать компьютеры, телефоны и планшеты. Вот некоторые виды вредоносных программ, о которых вы могли слышать:

- **Программы-вымогатели.** Вредоносные программы, которые могут зашифровывать файлы и блокировать доступ пользователя к его устройству.
- **Шпионские программы.** Вредоносные программы, собирающие информацию о пользователе.
- **Программы для показа рекламы.** Часто проявляются в виде неконтролируемых всплывающих окон.
- **Программы-черви.** Разновидность вируса, который фактически копирует сам себя и рассылает свои копии другим пользователям.
- **Вирус.** Форма вредоносной программы, которая может заразить устройства и повредить данные и программное обеспечение. Вирусы распространяются с помощью кода.

Какие бывают вирусы?

- **Вирус-троян.** Известная разновидность компьютерных вирусов, которые проникают в устройство под видом подлинной программы. Пользователей обманным путем вынуждают установить или загрузить что-то, что содержит вирус-троян.

- **Вирус-угонщик.** Вирусы, которые могут заразить браузер и изменить его настройки или перенаправлять пользователей на вредоносные сайты.
- **Макровирус.** Вирусы, которые могут заражать макросы в Microsoft Word.
- **Файловый вирус.** Вирус, который может заражать критически важные компьютерные файлы и распространяться среди них.

2. Как определить присутствие вредоносных программ?

К сожалению, вредоносную программу выявить непросто. Однако по некоторым признакам вы можете определить, есть ли на вашем устройстве вредоносные программы.

Вы можете установить защитное программное обеспечение, которое просканирует ваше устройство на наличие вредоносных программ. Только сначала хорошо изучите вопрос и убедитесь в том, что вы загружаете подлинное ПО! Некоторые вредоносные программы имитируют защитное программное обеспечение, чтобы вы их установили.

Помните, что некоторое защитное программное обеспечение может быть платным. Однако существуют различные варианты, отличающиеся по стоимости, а на многие устройства защитное программное обеспечение устанавливается производителем, поэтому вы можете выбрать оптимальный вариант в зависимости от ваших потребностей.

Вот несколько признаков, которые помогут вам выявить потенциальные вредоносные программы:

- Ваше устройство работает очень медленно или подвержено частым сбоям.
- Вы не можете выключить или перезагрузить устройство.
- У вас пропадают файлы.
- Вы получаете неожиданные сообщения об ошибках.
- Вы видите странные многочисленные электронные письма, рассылаемые с вашей учетной записи.
- Ваш браузер перенаправляет вас, или его работа замедляется.

- Вы постоянно сталкиваетесь со всплывающими окнами или чрезмерной и назойливой рекламой.
- Ваш аккумулятор быстро разряжается.
- [Для ноутбуков] Вентилятор охлаждения работает непрерывно и шумно.
- Вы видите приложения, открытые вкладки и другие элементы, которые вы не открывали и не устанавливали на свое устройство.

3. Что делать при обнаружении вредоносных программ?

Если вы подозреваете, что загрузили вредоносную программу или ваш компьютер заражен, убедитесь в наличии вредоносной программы и затем приступайте к ее удалению.

Лучше сначала убедиться в обоснованности подозрений, поскольку некоторые признаки наличия вредоносной программы могут быть признаками других проблем. Например, быстро разряжающийся аккумулятор может означать, что устройство устарело!

Но если вы удостоверитесь в наличии серьезной проблемы, можно сделать следующее:

- Воздержитесь от таких действий, как покупки в Интернете или ввод паролей к учетным записям, пока проблема не будет решена. После решения проблемы смените пароли.
- Если ваше устройство подключено к локальной сети, отключите его, чтобы вредоносная программа не распространилась.
- Перезагрузите устройство в безопасном режиме, чтобы упростить работу защитного программного обеспечения и устранить заражение вредоносной программой.
    - **Windows.** Нажмите и удерживайте клавишу «F8», как только начнется перезагрузка, затем выберите в меню Safe Mode («Безопасный режим»). После этого выполните проверку с помощью защитного программного обеспечения.
    - **Mac.** Удерживайте клавишу «Shift» во время перезагрузи, затем выполните проверку с помощью защитного программного обеспечения.

- Убедитесь в актуальности версии вашего защитного программного обеспечения.
- Если у вас не установлено защитное программное обеспечение, установите заслуживающую доверия программу, подходящую для вашего устройства. Вы можете ознакомиться с рекомендациями и списками из надежных источников, например сайтов и блогов, посвященных обзору технологий, в том числе *The New York Times' Wirecutter* (https://www.nytimes.com/wirecutter/).
- Установив защитное программное обеспечение, выполните проверку на вашем устройстве, чтобы выявить вредоносную программу.
- Удалите ее с помощью вашего защитного программного обеспечения.
- В случае более серьезного заражения может понадобиться переустановить операционную систему. Посетите официальный веб-сайт производителя вашего устройства, чтобы узнать, как это сделать.
- Если вам все же требуется помощь, обратитесь в службу технической поддержки для вашего устройства (это может быть предусмотрено гарантией).
- Смените пароли и проверьте ваши учетные записи на наличие признаков мошенничества после заражения вредоносной программой.

4. Как избежать вредоносных программ?

Для защиты ваших устройств от вредоносных программ вы можете сделать следующее:

- **Соблюдайте осторожность при установке программ, приложений и расширений для браузеров.**
  В них могут быть скрыты вредоносные программы, поэтому убедитесь, что вы устанавливаете на свое устройство заслуживающие доверия подлинные программы.

- **Своевременно обновляйте настройки безопасности на ваших устройствах и в браузерах.**
  Своевременно устанавливайте обновления для операционной системы, исправления и обновления для системы безопасности.

- **Будьте бдительны.**

Помните о фишинге, не нажимайте на ссылки и не скачивайте файлы из подозрительных или неизвестных источников.

- **Следите за тем, какие веб-сайты вы посещаете.**

Не игнорируйте предупреждения вашего браузера о небезопасных сайтах.

- **Регулярно делайте резервные копии данных.**

Так вы сможете их защитить и восстановить в случае проблем с вредоносной программой.

- **Установите защитное программное обеспечение.**

Используйте его для контроля вашего устройства и блокирования, выявления и удаления вредоносных программ.

5. Составьте план

Запишите здесь ваш план и идеи насчет того, что вы можете сделать, чтобы избежать вредоносных программ