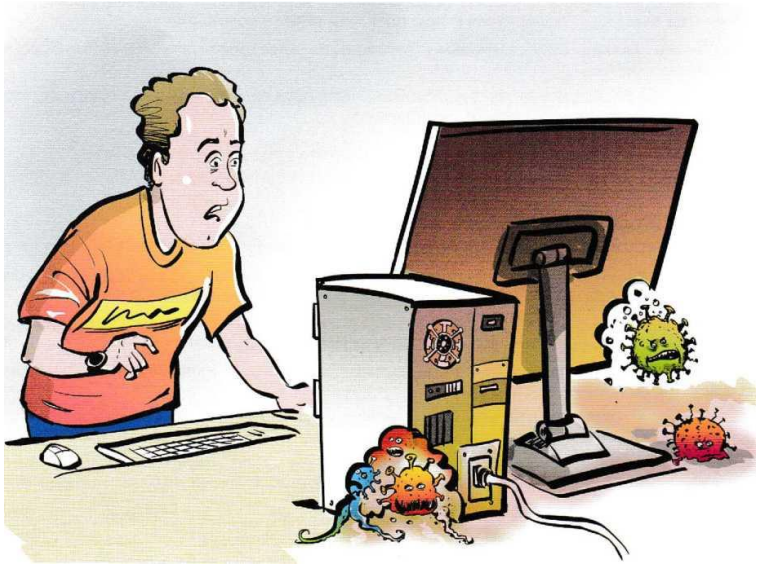
Меры предосторожности, которые помогут избежать заражения устройства вирусами надежный пароль

1.Установите Антивирус. Даже бесплатные программы способны отслеживать работу вашего устройства и вовремя удалять вирусные программы в случае их появления.
2.Не скачивайте файлы из ненадежных источников или сомнительных веб-сайтов. Это может привести к установке вредоносного программного обеспечения на ваше устройство.
3.Регулярно делайте резервное копирование всех своих важных данных, чтобы в случае вирусной атаки вы их не потеряли.
4.Не открывайте письма, присланные с незнакомых адресов. Не скачивайте и не открывайте файлы из таких писем или из сообщений, которые прислали вам незнакомые пользователи.
5.Вовремя устанавливайте обновления системы на компьютере или телефоне, обновления антивирусной программы, если она у вас установлена. Также обновляйте браузер, которым пользуетесь.

Если вирусы нанесли системе непоправимый ущерб, и у вас нет возможности установить и воспользоваться антивирусом - обратитесь к эксперту из сервисной службы по ремонту компьютеров или смартфонов.

ТОГБУ «Центр поддержки семьи и помощи детям «Семейный причал»
Служба постинтернатного сопровождения выпускников

Компьютерные вирусы: культура безопасности!



Внимание!

Вирусы часто маскируются под настоящие, безопасные программы. Компьютерные вирусы - широкий спектр программ, вредных и опасных для вашего компьютера. Они бывают разные: самостоятельными программами или умеющими заражать ваши файлы или программы

К сведению

Вирусы имеют следующие вредоносные функции:

1.Мешают нормальной работе устройства, замедляют его, а в некоторых случаях повреждают даже операционную систему таким образом, что без тщательного ремонта или восстановления, пользоваться устройством становится невозможно.

2.Крадут персональные данные пользователя: выгружают данные из системы, включая логины и пароли, платежные данные, личные файлы и многое другое.

3.Передают злоумышленникам все, что пользователь печатает на своей клавиатуре («клавиатурные шпионы»).

4.Блокируют устройство с целью шантажа: полностью блокируют работу на устройстве, а для разблокировки требуют перевести деньги на указанный счет.

5.Используют ваш компьютер для майнинга - добычи криптовалюты. Такие программы, проникнув на ваше устройство, используют его мощность для того, чтобы добывать криптовалюту. Любые программы-майнеры, как вирусные, так и нет, очень сильно нагружают компьютер. Последствием их работы является значительное падение скорости работы устройства, перегрев и даже выход из строя отдельных деталей и, *в* конечном итоге, всего устройства.

НЕ НАДЕЙТЕСЬ НА ДОБРОСОВЕСТНОСТЬ МОШЕННИКОВ!

Перевод денег по указанным данным не поможет разблокировать устройство.

Как можно определить, что ваше устройство заражено вирусами?

1. Замедление вашего компьютера или устройства.
2.Появление новых папок и файлов без вашего участия.
3.Чрезмерный нагрев устройства.
4.Быстрая разрядка мобильного устройства.
5.Внезапные отключения или перезагрузка устройства.
6.Самостоятельный запуск программ, движение курсора мыши и т.п.
7.Появление на устройстве новых программ или приложений, которые вы не устанавливали.
8.Телефон самостоятельно делает звонки или отправляет сообщения контактам.
9.Появление рекламных баннеров, уведомлений и всплывающих окон. Как правило, в браузере, но иногда они могут появляться и при обычной работе компьютера.
10.Компьютер может самостоятельно отправлять электронные письма или сообщения в социальных сетях.
11.Чрезмерный расход денег на телефонном счете, появление ненужных платных подписок или платных функций, которые вы не оформляли.

Если ваш компьютер заражен вирусами, лучшим решением будет очистить его с помощью надежной антивирусной программы.