Основы безопасной работы на компьютере

1. Работайте на компьютере под учетной записью с ограниченными правами

Это одно из очень важных условий безопасной работы, т.к. серьезно ограничивает возможности запущенного вредоносного кода, при этом, не ущемляя пользователя в работе со стандартным кругом задач. **Права администратора необходимы только для настройки операционной системы, установки программного обеспечения и других административных задач.**

2. При работе с электронной почтой обращайте особое внимание на отправителя почтовой корреспонденции

Будь то работа с почтой через WEB-интерфейс одной из известных почтовых систем mail.ru, yandex.ru и т.п., или в локально установленных программах почтовых клиентов MS Outlook, Outlook Express, The Bat. **Если отправитель почтового сообщения неизвестен – открывать вложение из такого письма категорически не рекомендуется, чтобы ни содержало данное сообщение.** Никакие обновления, патчи, апдейты для компьютеров не распространяются по почте! Даже если отправитель Вам известен, и Вы давно ведете с ним переписку, это не гарантия того, что вложение безопасно. Такие вложения рекомендуется предварительно сохранять в специально созданную папку на жестком диске и проверять их средствами антивирусной защиты. После успешной проверки вложения открывайте его уже из этой папки.

3. Аккуратно пользуйтесь сменными носителями (флэшки, дискеты, компакт-диски), как своими, так и "со стороны"

Это очень распространенный способ заражения компьютера. Не пользуйтесь автозапуском(появляющееся окно с предложением что-либо запустить при подключении флэшки) и избегайте открывать какие-либо файлы с любых сменных носителей без предварительной проверки их антивирусными программами.

4. Использовуйте наиболее безопасный браузер Mozilla Firefox, Google Chrome, Opera

В процессе исправления ошибок в коде браузеров программисты постоянно совершенствуют свои продукты, делая их безопаснее. Поэтому однозначно нельзя назвать какой-то определенный браузер наиболее безопасным. Также желательно отказаться от отображения ActiveX-содержимого на WEB-страницах (запрещается в настройках браузера).

5. Неплохо также подумать о безопасности при работе с программами Instant Messaging

Службы мгновенного обмена сообщениями, такими как ICQ, Mail.ru-агент и им подобными. В этом случае рекомендации будут примерно такими же, как и при работе с электронной почтой. Не принимайте файлы из неизвестных источников, к файлам из известных источников также следует относиться с осторожностью. Проверяйте все полученные файлы антивирусными программами.

6. Интернет необходимо использовать для работы, а не для развлечений.

Большинство "заразы" попадает на Ваш компьютер благодаря Вам самим. Например, когда Вы следуете призывам типа "загрузи и приколись", "кликни сюда, здесь бесплатно…", "прикол, смотреть здесь" и т.п. Очень часто злоумышленники пользуются доверчивостью пользователей, охотно "кликающих" по ссылкам с заманчивыми названиями и таким образом загружающими и запускающими какую-либо вредоносную программу.

7. Заботьтесь о сохранности своих данных

Помните, что результат Вашего интеллектуального труда в виде документов, баз данных, почтовой базы, каких-то других файлов необходимо периодически сохранять в архивах. Если этого не делать, то позднее Вам придется жалеть о том, что не позаботились об этом раньше.

8. Используйте качественный антивирусный продукт

9. Ежедневно проводите полное сканирование компьютера средствами антивирусной защиты

10. Обновляйте операционную систему

Обновления и новые версии закрывают уязвимости, по которым вредоносное программное обеспечение может попасть в Вашу систему и заразить ее.