Правила безопасности работы в интернете

Правило № 1. Защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете.

-установите Антивирус;

-регулярно обновляйте сигнатуры угроз, входящие в состав программы;

-задайте рекомендуемые экспертами параметры защиты вашего компьютера. Постоянная защита начинает действовать сразу после включения компьютера и затрудняет вирусам проникновение на компьютер.

-задайте рекомендуемые экспертами параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю. Если вы не установили компонент Фаервол, рекомендуется сделать это, чтобы защитить компьютер при работе в интернете.

Правило № 2. Будьте осторожны при записи новых данных на компьютер:

-проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-карты и пр.) перед их использованием.

-осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми.

-внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.

-если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса.

-внимательно относитесь к выбору посещаемых вами Интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или Интернет-червями.

Правило № 3. С недоверием относитесь к вирусным мистификациям - программам-шуткам, письмам об угрозах заражения.

Правило № 4 Регулярно устанавливайте обновления операционной системы Microsoft Windows.

Правило №5 Покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

Правило 6. Будьте осторожны с электронной почтой

-не стоит передавать какую-либо важную информацию через электронную почту.

-установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

Правило 7 . Используйте сложные пароли.

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

Правило 8. Не отправляйте SMS-сообщения.

-сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

-при отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

-поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

Правило 9. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

Правило 10. Используйте брандмауэр.

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

Правило 11. Делайте резервные копии.

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.