Безопасный Интернет для школьников

Путешествуя по сети Интернет и посещая различные сайты, возможно ты и не подозреваешь, что информацию получаешь не только ты, но и сами сайты собирают сведения о своих посетителях. Посещенный тобой сайт знает адрес твоего компьютера в Сети - без этого связь с Интернетом вообще была бы невозможна. Это безобидная информация, но недобросовестный сайт, на котором ты ненадолго остановился, может узнать о тебе намного больше: адрес электронной почты, какие сайты, когда и сколько раз ты посещал, а также записать на жесткий диск твоего компьютера целую порцию электронных вирусов. Некоторые любители пощекотать людям нервы могут попробовать ради развлечения через Интернет взломать твой компьютер и уничтожить на нем все данные.
Что же нужно делать, чтобы защитить свой компьютер от нежелательных вмешательств?

Правила соблюдения безопасности:

При просмотре электронной почты

- **Не открывай файлы**, вложенные в электронные письма, если эти письма отправлены от неизвестного корреспондента или же просто вызывают у тебя сомнения.

- **Не открывай файлы**, прикрепленные к электронным письмам и имеющие расширение .exe, даже если их прислали твои друзья. Лучше попроси друзей отправить эти файлы в архиве ZIP или RAR.

- **Если ты получил письмо от хорошо знакомого тебе человека**, но оно вызывает у тебя какие-то подозрения (например, отсутствует какой-либо текст в письме, а к самому письму прикреплен непонятный файл), не открывай его—в нем могут оказаться вирусы. Современные вирусы могут распространяться независимо от воли пользователя, так что с компьютера твоего друга незаметно для него может производиться рассылка «виртуальной заразы».

- **Ни в коем случае не открывай** приложения к письмам, полученным от неизвестных людей.

- **Не оставляй свой электронный почтовый адрес незнакомым людям.** В противном случае, твои шансы увидеть в почтовом ящике письмо, зараженное вирусами, существенно увеличивается.

При посещении Интернета

- **Не посещай** сетевые конференции и Web-чаты, посвященные социально опасным тематикам (хакерство,

терроризм и т.д.). В подобных сообществах находятся недобросовестные люди, которые могут попытаться взломать твой компьютер через Интернет или же забросать твой электронный почтовый ящик компьютерными вирусами.

- **Проверяй программы**, загруженные из Сети. Некоторые программы могут передавать сведения о тебе, твои пароли и файлы посредством Интернета на компьютер хакера. Такие программы называют «троянскими конями» (на жаргоне компьютерщиков - «троянами»).

- **Обязательно установи на своем компьютере антивирусную программу.**

Как работает антивирусная программа?

Антивирусный сканер предназначен для сканирования всех имеющихся на компьютере носителей информации (жестких дисков, CD-приводов и т.п.) на предмет наличия компьютерных вирусов среди полезных файлов. Если во время процедуры сканирования будут найдены вирусы, то антивирус сможет удалить их с вашего ПК, чем обезвредит файлы.
Антивирусный монитор постоянно пропускает через себя, как сквозь сито, все файлы, которые загружаются в память. Если среди запускаемых файлов будут обнаружены зараженные вирусами, антивирусная программа сразу же сообщит об этом владельцу и уничтожит пойманный файл.

Какой антивирус выбрать?

Сейчас много антивирусных программ: **NOD32, Антивирус Касперского, Norton Antivirus, Doctor Web.** Существует также бесплатный антивирус**AVAST**, загрузить который можно из Интернета.

- **Используйте файерволл (брандмауэр).**

Что такое файерволл (брандмауэр)?

Чтобы полностью контролировать входящий на ваш компьютер и исходящий из него поток данных, можно использовать специальную программу - файерволл (брандмауэр) (от англ. **firewall** - «огненная стена»). Эта программа выполняет функцию фильтра всей входящей и исходящей информации. Например, она может зафиксировать попытку хакера взломать компьютер и сделает ваш ПК невидимым для его атак. С другой стороны, файерволл (брандмауэр) помогает отслеживать сетевую активность установленных у вас программ, и если среди них затесалась зараженная вирусом, файерволл не позволит ей выйти в Сеть и передать сведения о вашем ПК хозяину.

Какие существуют файерволлы (брандмауэры)?

Их много, как и антивирусов. Самые известные - **ZoneAlarm, Outpost Firewall, AtGuard.** Но и в самой программе Windows XP ServicePack 2 имеется встроенный брандмауэр, который можно настроить самостоятельно. Найти его можно в разделе **Центр обеспечения безопасности** Панели управления.

Соблюдать вышеуказанные правила несложно. Если вы обезопасите свой компьютер от посторонних вмешательств, то путешествие по просторам Интернета станет для вас спокойным и приятным занятием!