Повышение компьютерной безопасности

Тема компьютерной безопасности на сегодняшний день является едва-ли не самой актуальной для всех участников сети, начиная с сервис-провайдеров и заканчивая пользователями. Это связано с развитием сетевых технологий Интернет, можно сказать, что компьютерная безопастность - обратная сторона медали.

Сетевые вирусы и трояны представляют немалую угрозу ПК абонентов, поэтому задача обеспечения сетевой безопасности - общая.
При запуске новых сетей наши системные администраторы устанавливают:
- сетевые экраны, запрещающие распространение вредоносных программ между сетями (активная безопасность),
- систему отслеживания сетевых атак (пассивная безопасность).
Пользователям сети необходимо позаботиться о безопасности собственного компьютера. Включите брандмауэр (для пользователей Windows XP) или установите программное обеспечение, так называемое, файервол (firewall) для пользователей других операционных систем. Будьте внимательны! Многие программы обеспечения безопасности полуавтоматические, т.е. требуют участия пользователя.

Также следует отметить еще один важный аспект сетевой безопасности - уязвимость программного обеспечения компьютера. Для того чтобы решить эту проблему, в первую очередь, необходимо следить за периодическими обновлениями (так называемыми заплатками), предоставляемыми компанией-производителем. Для пользователей Windows XP настоятельно рекомендуем посетить сайт компании Microsoft, предоставляющий обновления.

Помимо сетевых вирусов и троянов есть еще одна проблема безопасности: недобропорядочные пользователи сети, желающие использовать ресурсы других пользователей. **Просим Вас обратить внимание на следующий момент: если Ваш компьютер не может зарегистрироваться в сети (получить IP-адрес) или получить другой сервис нашей сети, обязательно свяжитесь с нашей техподдержкой и сообщите все подробности.**
Сетевые вирусы - самая распространенная компьютерная болезнь. Эти вирусы способны самостоятельно передавать свой код на удаленный сервер, при этом они обладают возможностью также самостоятельно запустить зараженный файл. Такие вредители активно распространяются в локальных и глобальных сетях, они жестоко перебирают все локальные диски и сетевые диски с правом доступа и копируются туда под случайным именем. Наиболее распространенное название сетевых вирусов - сетевые черви (worms),они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров, и рассылают по этим адресам свои копии. В прошлом сетевые вирусы были способны на создание письма, содержащего зараженный файл-документ, затем выбирали из списка адресов случайных адресатов и рассылали по ним зараженное письмо, при получении письма автоматически запускается MS Word, то вирус "автоматически" внедряется в компьютер адресата зараженного письма. Еще одним примером является "червяк", который использует для своего распространения протокол FTP (File Transfer Protocol) и передает свою копию на удаленный ftp-сервер в каталог Incoming. Опасность сетевых паразитов в том, что они по определенным датам активизируются и уничтожают файлы на Вашем зараженном компьютере. Одним из разновидностей вирусов является троянский вирус, такие вирусы узнают Ваш идентификатор и пароль для доступа в Интернет и отправляют их на определенный почтовый адрес. В результате злоумышленники получают возможность доступа в Интернет за Ваши деньги. Распространения вируса базируется на том, что вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя. Особой разновидностью вирусов являются скрипт-вирусы, один из файлов (WScript) используется для интерпретации сценариев в полноэкранном режиме, второй (CScript) - в режиме командной строки. И тот, и другой интерпретаторы понимают сценарии, написанные на Visual Basic Script и JavaScript активные элементы которые могут выполнять разрушительные действия. Программа передается по сети при загрузке Web-страниц с серверов Интернета в браузер локального компьютера.

Для защиты своего ПК:

- Используйте лучшие антивирусные программы и регулярно их обновляйте.
- Убедитесь в том, что ваша антивирусная программа включает следующие услуги: техническую поддержку, систему оповещения о появлении вирусов, службу быстрого реагирования.
- Убедитесь в том, что Ваш антивирус постоянно включен.
- Прежде чем открывать сообщения, полученные по электронной почте, проверьте их на вирусы.
- Ничего не скачивайте с сомнительных сайтов.
- Не скачивайте файлы, предлагаемые Вам в чатах или новостях.
- Устанавливайте «заплатки», выпускаемые разработчиками программного обеспечения.
- При выключении компьютера или при перезагрузке вынимайте дискету из дисковода.
- Проверяйте содержимое архивов.
- Следите за подозрительной активностью на вашем ПК.
- Используйте встроенные функции безопасности антивирусных программ.
- Регулярно создавайте резервные копии.
- Следите за новостями.

Пользуйтесь только лицензионным ПО.