Безопасность в сети “Интернет”

Безопасность в интернете – очень важная проблема. И касается она всех.

Она становится все актуальнее в связи с массовым приходом в интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим.

Страдает не один пользователь, а и многие другие, объединенные в одну глобальную структуру.

Основная сила плохого Интернета - Вирусы

Помимо обычных вирусов настоящее время существует несколько классификации вирусов такие как: трояны, фишинг,

Вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ

внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр и другое.

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение:

1) Трояны могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.

2) Фишинг - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Заманить вас на такой поддельный сайт могут разными способами, а цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.

3) **Кейллогер – это программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.**

Начальная защита компьютера пользователя.

В идеале, купив ПК, пользователь должен выполнить целый ряд операций, прежде чем броситься бороздить бесконечные просторы сети. Сейчас мы представим некоторые самые первые уроки безопасности в интернете.

•Несмотря на то что Windows имеет встроенный файрволл, рекомендуется установить более надежный, так как имеющийся - далеко не самый лучший. Выбирайте платный или бесплатный, исходя из их рейтингов.

•Следующий шаг – установка антишпионского и антивирусного ПО. Нужно сразу же его обновить и настроить на автоматическое обновление. Также оно должно запускаться автоматически, вместе с ОС. И постоянно, в фоновом режиме, работать. И обязательно проверяйте любую устанавливаемую программу.

•Как только появляются обновления для Internet Explorer и других используемых вами браузеров, тут же скачивайте их и устанавливаете.

•Отключайте все неиспользуемые службы на своем устройстве, это уменьшит шансы для хакеров получить к нему доступ.

•Удаляйте сразу же все письма подозрительного содержания, не вздумайте открывать файлы из неизвестных источников. Игнорируйте все предложения легкого заработка, никому не высылайте свои пароли, не переходите по подозрительным ссылкам.

•Используйте только сложные пароли, состоящие из сложного набора цифр, букв и символов. Для каждого случая назначайте свой, оригинальный.

•Выходя в сеть из мест общего пользования, будьте аккуратны и осторожны. Это же касается и использования прокси-серверов. Желательно не проводить никаких банковских и других подобных операций из таких мест.

•Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее.

•Нежелательно посещать сайты для взрослых или подобные им ресурсы. Велика вероятность подхватить троян.

•Следите за интернет-траффиком, даже если он безлимитный. Если он без особой причины значительно увеличился, это может быть признаком активности вируса.

Если будете соблюдать эти минимальны правила безопасности в сети интернет, то избежите многих проблем. Это, конечно, далеко не все. Опасностей столько, что нельзя о них забывать ни на минуту.