БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Безопасность в интернете – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим. Поэтому данная статья и буде посвящена такому вопросу, как безопасность в сети интернет. Ведь страдает не один пользователь, а и многие другие, объединенные в одну глобальную структуру.

ОПАСНОСТИ, ПОДСТЕРЕГАЮЩИЕ НАС В СЕТИ

Если сказать кратко, то существуют две основные возможности того, как может ваш компьютер стать жертвой. Первое – вы сами, странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, заражаете свой компьютер. Второе – возможна также ситуация, когда злоумышленники преднамеренно, с помощью, например, троянских программ или вирусов, делают ваше устройство источником опасности. В результате всего этого компьютер, иногда даже тайно от своего владельца, начинает выполнять рассылку спама, участвует в DDoS-атаках на различные сайты, крадет пароли. Бывает и так, что провайдер вынужден принудительно отключить такое устройство от глобальной сети. Получается, что если пользователь не осведомлен о том, что представляют собой основы безопасности в сети интернет, придется ему тяжело.

ЗАЧЕМ НУЖЕН ЗЛОУМЫШЛЕННИКАМ ДОСТУП К КОМПЬЮТЕРУ ПОЛЬЗОВАТЕЛЯ

Зря обычный пользователь думает, что его компьютер никому не нужен. Это раньше

хакеры часто писали вирусы просто ради интереса, сейчас же это делается почти всегда с коммерческой выгодой. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Или сделать так, что при включении компьютера вместо стандартного рабочего стола появятся какие-либо прикольные картинки. Сейчас же они делают все возможное, чтобы владелец ПК как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции.Для чего все это делается? Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в

социальных сетях, форумах. Случается так, например, что вы ложитесь спать с 20 000 рублей на электронном кошельке, а утром получаете СМС-сообщение о том, что денег на

нем уже нет. А с почты все ваши контакты, да и не только, получают спам-письма, а то еще и трояны. Хакеры могут объединить множество зараженных компьютеров в единую мощную сеть, провести DDoS-атаку даже на мощные государственные серверы. Из самого простого, но также приносящего деньги: заблокируют работу операционной системы и потребуют деньги за устранение проблемы. И, кстати, деньги возьмут, но компьютер оставят заблокированным. Так что безопасность в сети интернет должна стать основой вашей работы в ней.

КАК ЗЛОУМЫШЛЕННИКИ ПРОНИКАЮТ В КОМПЬЮТЕР? ПОДРОБНАЯ ИНФОРМАЦИЯ

Для того чтобы взломать защиту ПК, даже если она есть, хакеры применяют целый ряд способов, и пользователи зря думают, что, просто установив антивирус, они избавились от опасности, например, подцепить вредоносную программу. Поэтому, прежде чем искать информацию о том, как правильно соблюдать безопасность в сети интернет, нужно понять, а откуда берутся вирусы и трояны. Сейчас мы перечислим основные пути их проникновения и методы воровства различной информации.

1. Первый метод называется социальной инженерией. Благодаря различным психологическим приемам, уловкам и доверчивости пользователей хакеры присылают вам вполне безобидный файл или письмо, а вы сами и запускаете троянчик в нем. Или же по просьбе якобы администрации сервиса выдаете все свои пароли и явки.
2. Второй метод – предлагается разное бесплатное программное обеспечение, пиратские диски, где спрятано множество вирусов, троянов и тому подобной гадости.

3. В ПО, в том числе и из самых надежных проверенных источников, постоянно появляются дыры в безопасности. Это относится и к операционным системам. Вот злоумышленники внимательно и следят за такими моментами, стараются их не упустить, а использовать в собственных целях. Зайдете на какую-нибудь страничку сто раз проверенного сайта и - раз - ваше устройство заражено.
4. Четвертый способ получил особое распространение в последнее время. Это фишинг, когда создаются поддельные сайты. И вы вместо странички своего банка оказываетесь на его поддельной копии. О том, что может быть дальше, говорить не будем, сами догадаетесь.

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.

1. 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.
2. 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.

3. Как только появляются обновления для Internet Explorer и других используемых вами браузеров, тут же скачивайте их и устанавливаете.
4. Отключайте все неиспользуемые службы на своем устройстве, это уменьшит шансы для хакеров получить к нему доступ.

ДАЛЬНЕЙШИЕ УРОКИ БЕЗОПАСНОСТИ

Теперь немного информации о том, как обеспечить безопасность работы в сети интернет. Выполнив указанное в предыдущем разделе, продолжайте не забывать о ежедневной защите.

1. 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.
2. Используйте только сложные пароли, состоящие из сложного набора цифр, букв и символов. Для каждого случая назначайте свой, оригинальный.

3. 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.
4. Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее.

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

6. 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.

ЕЩЕ НЕКОТОРЫЕ УРОКИ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Сейчас кратко расскажем еще о некоторых мерах предосторожности. Если с вашего банка пришло письмо с проверкой пароля, не вздумайте им его отправлять. Банки никогда таких запросов не делают. Все почтовые программы имеют фильтр от спама. Доверяйте ему. Получив письмо о выигрыше в миллион рублей или наследстве в пять миллионов долларов, удаляйте их сразу же. Рекомендуем устанавливать комплексную защиту. Она надежнее, чем антивирус – от одного производителя, файрволл – от другого, а антишпионская программа – от третьего.

Отдавайте предпочтение платным версиям. Так как Opera и Internet Explorer – самые распространенные браузеры, для них и вирусов существует более всего. Используйте альтернативные варианты: Apple Safari, Google Chrome и Mozilla Firefox. Не пользуйтесь нелицензионным программным обеспечением, так как в нем изначально может быть установлено шпионское ПО. Если делайте покупки в онлайн-магазинах, то пользуйтесь только проверенными вариантами. Это же относится и к любому иному онлайн-сервису. Выполняйте все эти требования, и тогда безопасность в сети интернет будет более-менее гарантирована.

ДЕТИ И ИНТЕРНЕТ

В связи с развитием современных технологий все большее количество детей получает возможность выхода в интернет. И если раньше они в основном играли в игры, даже не выходя в сеть, то теперь все совсем по-другому, да вы и сами все знаете. Поэтому появилась новая задача – обеспечить безопасность детей в сети интернет. Это достаточно сложно, так как Всемирная паутина изначально развивается полностью бесконтрольно.В ней есть очень много информации, доступа к которой у детей быть не должно. Ко всему прочему, их нужно научить, как не "наловить" вирусов и троянов. Кто же им поможет с этим, как не взрослые. К тому же очень важна и информационная безопасность в сети

интернет, так как дети – совсем неискушенные пользователи. Они легко могут попасться на удочку опытного мошенника или злоумышленника.

КАК НАУЧИТЬ ДЕТЕЙ ПРАВИЛЬНО ПОЛЬЗОВАТЬСЯ ИНТЕРНЕТОМ

Самый первый совет заключается в том, что первые сеансы в сети ребенок должен проводить с кем-нибудь из взрослых. Желательно пользоваться такими программами, как "Родительский контроль", чтобы контролировать все действия детей в интернете.Нужно ограничивать самостоятельное использование почты и чатов, ведь это может быть даже опасно. Так как там, например, педофилы могут искать себе жертв. Дадим несколько рекомендаций относительно того, как можно постараться обеспечить максимально безопасность детей в сети интернет.

РЕКОМЕНДАЦИИ

1. Сделайте так, чтобы дети делились с вами всеми своими неудачами и успехами при освоении интернета.

2. Научите ребенка рассказывать обо всем, что вызывает у него беспокойство.
3. Расскажите, как соблюдать конфиденциальность, помогите выбрать регистрационные данные, не разглашающие реальных, ведь информационная безопасность в сети интернет – залог того, что удастся избежать многих неприятностей.
4. Объясните, что в виртуальном пространстве не нужно никому называть свою фамилию, домашний адрес, номер школы и т. п.
5. Научите, что нет разницы между поступками в реальной жизни и в интернете.
6. Посоветуйте не встречаться с друзьями из сети, так как ожидания могут быть обмануты, не верить всему тому, что им говорят/пишут.
7. Обязательно установите специальное ПО и контролируйте своих детей.

Советы родителям детей 14-16 лет

Когда вашему ребенку 14-16 лет, маловероятно, что вы сможете больше его разбираться в компьютерах, интернете и всех подобных вещах. Хотя, конечно, о контроле и влиянии на него забывать нельзя. Тем более надо помнить о такой проблеме, как обеспечение безопасности в сети интернет. Ведь, если компьютер общий, или все устройства подключены к единой домашней сети, то и угрозы будут общими. К тому же просматривать отчеты о деятельности ребенка вы всегда сможете. Рекомендуется не конфликтовать с ребенком по этому поводу, а пробовать общаться и находить общий язык. Несмотря на возражения, постарайтесь заставить принять правила пользования

интернетом, скажите, какие сайты нельзя посещать.ПК, имеющий выход в сеть, должен быть установлен в общей комнате. Это будет немного сдерживать вашего ребенка. Установите ПО, блокирующее нежелательные сайты, не разрешайте без согласования с вами устанавливать любые программы. И не забывайте следить за тем, чтобы дети не стали зависимыми от интернета. Надеемся, что наши советы помогут защитить ваши компьютеры от угроз.