Безопасность в сети Интернет

Перед подключением к Интернет, Вы должны подумать о том, как обезопасить себя и свои данные.За очень короткий промежуток времени в интернете без надлежащей защиты, можно серьезно навредить своему компьютеру.

Установка обновлений для операционной системы

После подключения к Интернету, операционная система станет автоматически скачивать обновления с сервера Microsoft. Со временем обновления собираются в специальный комплект — Servise Pack. Некоторые пользователи отключают автоматическое обновление, опасаясь, что может слететь активация операционной системы Windows. Сами же обновления, если посмотреть на установленные, почти полностью касаются проблем безопасности операционной системы. Так Microsoft закрывает обнаруженные уязвимости в операционной системе. После установки обновлений система будет работать более стабильнее и безопаснее.

Компьютер, подключенный к Интернету, подвергается множеству угроз. Жертвами киберпреступников, как правило, становятся не продвинутые программисты и эксперты, а обычные пользователи, которых сегодня в сети подавляющее большинство. Злоумышленники пользуются тем, что рядовой пользователь мало информирован о потенциальных опасностях интернета, и вследствие этого

совершает типичные ошибки – месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе, не пользуется защитными программами. Вот пример тех угроз, что могут ожидать каждого из нас при работе в сети Интернет

Вирусы - компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов. Их основные цели – красть и уничтожать.

Неосторожное поведение пользователя - неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.

Не думая о безопасности в интернете, люди совершают ошибки. Например, регистрируясь в какой либо социальной сети, где просят указывать верные личные данные- фамилия и имя, это для начала. Пользователи бездумно вводят все это, разумеется это же не секрет, какая мол тут интернет безопасность. Далее, разумеется нужно фото, и тут вроде бы нет никакой угрозы безопасности в интернете. Ну дальше больше! Для удобства поиска ваших потенциальных друзей вам порекомендуют заполнить профайл. Такой себе маленький файлик, где нужно заполнить личные данные о себе. Ну так вот, в профайле вам нужно будет к примеру, заполнить ряд колонок. Это может быть школа, ВУЗ, ваши интересы, увлечения и прочее, прочее. На первый взгляд безобидная информация ведь, тем более применимо к данному сайту – на котором вы все это заполняете. Сайты это могут вам предлагать заполнить даже под предлогом заботы о вашей безопасности. Затем попросят указать номер телефона, вроде бы на случай если забудете пароль сайта - Вам будет выслан код для смены пароля. А некоторые вконец обнаглевшие просят ввести паспортные данные и находятся такие, кто вводит. Последствия самые плачевные: Ваше фото может быть использовано в непристойных местах интернета с самыми грязными подписями, вместо забытого пароля исчезнут деньги

со счёта телефона, появится кредит на Ваше имя и на немалую сумму и так далее до бесконечности и всё из за Вашей же небрежности к безопасности в интернете.

Для чего кому-то нужно взламывать ваш компьютер?

Даже если вы самый что ни на есть обыкновенный пользователь и на вашем компьютере нет какой-либо ценной и секретной информации, не нужно пребывать в иллюзии, что ваш компьютер никому (в плане его взлома) не интересен. С точки зрения хакеров и людей, распространяющих вредоносные программы, он всё равно будет представлять ценность. Времена, когда вирусы писали ради спортивного интереса, уже прошли и сегодня весь хакерский инструментарий используется ради получения коммерческой выгоды. В отличие от вирусов прошлого, которые могли отформатировать ваш винчестер или порадовать ничего не подозревающего владельца компьютера всякими неожиданными эффектами, сегодня вредоносные программы стараются маскироваться и скрывать свою деятельность, чтобы в тайне выполнять заложенные в них функции.
Такими функциями могут быть:
1) кража паролей от ваших электронных кошельков, почтовых ящиков, icq, сайтов, аккаунтов в различных сервисах и т. д. К сожалению, случаи, когда открыв в один прекрасный день свой кошелёк webmoney, пользователь обнаруживает в нём ноль, не редкость, причём установить, куда и кем были переведены деньги, в таких случаях весьма затруднительно. Украв пароль от почтового ящика, вредоносная программа может от вашего имени разослать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т.д.
2) достаточно прибыльным "бизнесом" в наше время является организация DDoS-атак, которые могут направляться на любой сайт или сервер, даже не имеющий каких-либо существенных уязвимостей. В результате таких атак сервер перегружается запросами, идущими с многочисленных компьютеров в разных регионах мира и сайт, на который направлена атака, таким образом отключается. Многочисленные случаи DDoS-атак на различные сайты были бы невозможны, если бы в распоряжении организаторов этих атак не находилось большое количество компьютеров обычных ничего не подозревающих пользователей, заражённых троянами, которые по сигналу извне начинают все вместе посылать запросы на сервер, выбранный в качестве жертвы.

3) организация массовых рекламных рассылок также является, к сожалению, прибыльным бизнесом, и для таких целей также практикуется заражение компьютеров обычных пользователей троянами.

4) перечисленные цели являются наиболее типичными, но, в принципе, цели могут быть ограничены лишь фантазией автора троянов и вирусов. Троян может зашифровать, например, некоторые из имеющихся на вашем компьютере файлов и затем требовать плату за восстановление информации, заставлять ваш модем звонить на платные телефонные номера и т. д. Последние 2 года были отмечены эпидемией т. н. "блокировщиков" Windows, когда попавшие на компьютер вирусы блокировали работу компьютера и требовали отправить платную смс для его разблокировки.

Источники опасностей.

Подхватить вредоносную программу, к сожалению, значительно легче, чем многие себе представляют. Для взлома компьютеров пользователей сети и кражи важных данных, например, паролей электронных платёжных систем, применяются следующие методы:

1) социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.
2) трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.
3) взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях. Для того, чтобы компьютер, имеющий уязвимости, был заражён, достаточно, например, всего лишь зайти на определённую страничку (ссылку на эту страничку хакер может прислать в письме, оставить на форуме и т. д.).
4) в последнее время получил распространение 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.

Меры по защите.

1) Установите файрволл (firewall). Хотя в Windows, начиная с версии XP и появился встроенный файрволл, его функциональность оставляет желать лучшего. Поэтому установите надёжный файрволл. Некоторые из подобных программ можно скачать бесплатно или за небольшую сумму.
2) Установите антивирусное и антишпионское ПО. Антивирусные программы должны быть свежими и регулярно скачивать базы с обновлениями через интернет. Антивирусное ПО должно запускаться автоматически при загрузке Windows и работать постоянно, проверяя запускаемые вами программы, в фоновом

режиме. Обязательно проверяйте на вирусы перед первым запуском любые программы, которые вы где-либо скачиваете или покупаете.

Использование антивирусных программ

Вирусы (в этой статье под этим словом подразумевается все вредоносное программное обеспечение) могут проникнуть на компьютер из Интернета, со съемных носителей, с оптических дисков и тому подобного. Чтобы противостоять этому, прежде всего, следует обязательно установить на компьютер антивирус. Существует большое разнообразие антивирусных решений, как платных, так и бесплатных. Вам придется самим решить, каким решением воспользоваться. Из бесплатных антивирусов наиболее популярны Avast!, Avira AntiVir, AVG Antivirus, Microsoft Security Essentials (при установке данной программы будет проверяться подлинность вашей копии Windows). Платные решения имеют некоторые преимущества перед бесплатными, в частности более частые обновления антивирусных баз, дополнительные модули безопасности и другие компоненты. Не существует 100% защиты от вирусного заражения, потому что сначала разрабатывается вирус, а уже потом появляются средства для его нейтрализации. В любом случае лучше быть в основном защищенным, чем оставаться без защиты. Следует помнить, что любой антивирус замедляет работу компьютера, но для безопасности с этим стоит смириться. Производители антивирусов совершенствуют свою продукцию и сейчас это уже не так заметно, как это было раньше.

После установки антивируса выполните полную проверку своего компьютера. Помимо того, что антивирус производит защиту компьютера в реальном времени, необходимо, не реже раз в месяц, проводить полную проверку компьютера и всех дисков (если у вас есть, например, внешние жесткие диски). Это нужно делать для дополнительной защиты ваших данных. Во время такой проверки бывает, что антивирус обнаруживает новые вирусные угрозы. Некоторые вирусы хорошо маскируются и начинают проявлять свою активность через значительный промежуток времени.

Нельзя устанавливать одновременно на компьютер два антивируса от разных производителей, они будут конфликтовать друг с другом. Антивирус и брандмауэр могут быть от разных производителей, потому что они выполняют разные задачи. Убедитесь, что у вас в настройках системы включен сетевой экран — брандмауэр (файрволл). Брандмауэр защищает компьютер от сетевых атак и контролирует выход программ в Интернет. В операционную систему Windows установлен штатный брандмауэр. Правда он уступает специализированным брандмауэрам, но лучше такая защита, чем вообще никакой. Предпочтительнее установить брандмауэр стороннего производителя, например бесплатные программы: ZoneAlarm, Outpost Firewoll Free, Comodo Firewoll.
Оптимальным решением для домашнего использования будет установка на свой компьютер антивирусного решения класса Internet Security. В такое решение входят антивирус, брандмауэр и другие дополнительные модули безопасности одного производителя. К сожалению программы такого класса платные. Исключения – Outpost Security Suite Free и Comodo Internet Security.

Для разовой проверки и лечения системы дополнительно можно использовать специальные бесплатные антивирусные сканеры, например Dr.Web CureIt, Kaspersky Virus Removal Tool и другие подобные программы. Они производят сканирование и лечение системы, но для повседневного использования не подойдут.
Если с вирусами справиться невозможно, то можно воспользоваться специальным загрузочным диском с антивирусной программой. Такие диски созданы многими производителями антивирусов и такой образ можно скачать с сайта производителя совершенно бесплатно, например Dr.Web Live CD, Kaspersky Rescue Disk и другие им подобные решения. Кроме официальных, существует также много подобных самодельных образов. Такие образы включают большое количество программ. После скачивания образ нужно записать на диск, а после этого уже загружаться с диска для сканирования и лечения компьютера.
Проверить файлы на компьютере можно и в Интернете, через онлайн-сканеры антивирусных компаний. Например, сервис VirusTotal проверяет файл с помощью 43 (на сегодняшний день) онлайновых программ.
Следует помнить, что в Интернете существует множество фальшивых антивирусов. Вы наверняка встречали в Интернете такие всплывающие объявления, в которых написано, что ваш компьютер заражен. Фальшивые антивирусы находят на вашем компьютере множество вирусов и предлагают загрузить программу для лечения вашего компьютера. Эта программа сама затем станет источником вирусов.
Для лечения от вирусов-блокираторов в антивирусных компаниях созданы специальные онлайновые службы, на которых вы можете бесплатно получить код разблокировки для вашего компьютера. Также для решения этой проблемы были созданы специальные программы.

3) Своевременно скачивайте и устанавливайте все критические обновления для Windows, Internet Explorer и т. п.
4) Не устанавливайте или удалите лишние ненужные службы Windows, которые не используете, например, службу доступа к файлам и принтерам и т. п. Это ограничит возможности хакеров по доступу к вашему компьютеру.
5) Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам.
6) Не используйте простые пароли. Нельзя в качестве паролей использовать простые комбинации символов, вроде "qwerty" или "666666". Такой пароль будет взломан программой для перебора паролей за считанные секунды. Не используйте короткие пароли (меньше 6 символов), не используйте в качестве паролей слова, которые есть в словаре. Не используйте один и тот же пароль на все случаи жизни.
7) Будьте осторожны при выходе в интернет из мест общего пользования (например, интернет-кафе), а также при использовании прокси-серверов. Пароли, который вы вводите, в этом случае, с большей вероятностью могут быть украдены.
8) При использовании электронных платёжных систем типа webmoney или яндекс-деньги, работа с ними через веб-интерфейс является менее безопасной, чем если вы скачаете и установите специальную программу (webmoney keeper или интернет-кошелёк для яндекса).

9) Не посещайте порносайты и прочие подобные им ресурсы сомнительной тематики. Подобные сайты являются основным источником впаривания троянов пользователям интернета, при помощи использования уязвимостей в Internet Explorer и др. подобных программах.
10) Даже если у вас безлимитный доступ, всё равно следите за траффиком - его непонятное возрастание может быть свидетельством активности вредоносной программы, а также отключайте соединение с интернетом тогда, когда оно не используется.