ПРАВИЛА ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

Защита от вредоносных программ

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

Управление «К» МВД РФ напоминает: для защиты пользователей от вредоносных программ разработано множество действенных контрмер. Надо лишь знать их и своевременно использовать.

Виды вредоносных программ

Вредоносные программы – любое программное обеспечение, которое предназначено для скрытного (не санкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом «вирусы». На самом деле вредоносные программы можно разделить на три группы:

компьютерные вирусы;

сетевые черви;

троянские программы.

Компьютерные вирусы – это программы, которые умеют размножаться и внедрять свои копии в другие программы, т. е. заражать уже существующие файлы. Обычно это исполняемые файлы (*.exe, *.com) или файлы, содержащие макропроцедуры (*.doc, *.xls), которые в результате заражения становятся вредоносными.

Компьютерные вирусы существуют давно. В последнее же время, когда компьютеры стали объединять в компьютерные сети, подключать к Интернету, в дополнение к традиционным компьютерным вирусам появились вредоносные программы нового типа: сетевые черви и троянские программы.

Сетевые черви – это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальны сетям и Интернету (например, через электронную почту). Особенность червей – чрезвычайно быстрое «размножение». Червь без Вашего ведома может, например, отправить «червивые» сообщения всем респондентам, адреса которых имеются в адресной книге Вашей почтовой программы. Помимо загрузки сети в результате лавинообразного распространения, сетевые черви способны выполнять опасные действия.

Троянские программы не размножаются и не рассылаются сами, они ничего не уничтожают на вашем компьютере, однако последствия от их деятельности могут оказаться самыми неприятными и ощутимыми. Задача троянской программы – обеспечить злоумышленнику доступ к Вашему компьютеру и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Просто однажды Ваша частная переписка может быть опубликована в Интернете, важная бизнес-информация продана конкурентам, а баланс лицевого счета у интернет-провайдера или в электронных платежных системах неожиданно окажется нулевым или отрицательным.

Безопасное использование электронной почты

Являясь удобным видом связи, как личной, так и деловой, электронная почта остаётся одним из самых популярных способов распространения вредоносных программ в Интернете.

Обычное сообщение электронной почты – это просто текст, сам по себе он не может быть опасен. Но к сообщению можно прикрепить файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

ТАКТИКА БОРЬБЫ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ

Вредоносные программы срабатывают при запуске на Вашем компьютере. Тактика борьбы с ними достаточно проста:

не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

если они к Вам все-таки попали, ни в коем случае не запускать их;

если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

КАК УБЕРЕЧЬСЯ ОТ ПОЛУЧЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Если Вы получили сообщение с вирусом, значит, Вы уже невольно выполнили первый шаг на пути к заражению Вашего компьютера, поскольку опасный файл сохранился на жестком диске. Пока это не фатально, но очень опасно, поэтому, прежде всего, необходимо предпринять меры к тому, чтобы этого не происходило впредь.

У многих операторов связи имеются на почтовых серверах фильтры, отсекающие подозрительные послания. Однако, несмотря на очевидную эффективность общесистемного фильтра, для обеспечения безопасности его все-таки недостаточно, поскольку он рассчитан на обезвреживание уже известных вирусов, тогда как новые вирусы могут беспрепятственно попадать в почтовый ящик. Поэтому пользователю необходимо принять дополнительные меры безопасности.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик –запретить прием сообщений, содержащих исполняемые вложения. Если абонент включает подобный фильтр, то все сообщения, содержащие исполняемые файлы, будут автоматически удаляться непосредственно на почтовом сервере.

Несмотря на кажущуюся радикальность подобной меры, она очень эффективна и в большинстве случаев не приводит к неудобствам или ограничениям возможностей пользователей.

Во-первых, как правило, по электронной почте чаще всего рассылают документы и изображения, но не программы.

Во-вторых, в случае необходимости получения программы по почте, можно договориться с отправителем, чтобы он предварительно упаковал ее с помощью какого-либо архиватора, например, Winzip или WinRar. Польза получится двойная, поскольку размер полученного файла-архива должен быть гораздо меньше размера и сходного файла.

Имеется ещё один способ не сохранять подозрительные сообщения на своем компьютере. Надо сначала просматривать только заголовки сообщений и удалять ненужные письма непосредственно на сервере, не скачивая их на свой компьютер.

КАК ЗАПРЕТИТЬ ВЫПОЛНЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

Бывают обстоятельства, при которых невозможно организовать работу так, чтобы не получать сообщения с исполняемыми файлами. В этом случае есть вероятность получить сообщения с вредоносными программами. Значит, необходимо принять меры, чтобы вредоносные программы ни в коем случае не были запущены на выполнение.

Чтобы запустить файл вложения на выполнение, следует открыть сообщение в отдельном окне, дважды щелкнув по строке сообщения в списке (сообщение с вложением помечено скрепкой) и открыть файл-вложение, дважды щелкнув по имени файла в заголовке сообщения (поле «Присоединить»).

Учитывая сказанное, необходимо взять за правило:

не открывать сообщение (дважды щелкнув мышкой), особенно если оно пришло от неизвестного отправителя. Текст можно прочитать в режиме быстрого просмотра: когда при одиночном щелчке мышкой на сообщении в списке текст сообщения отображается не в отдельном, а в основном окне программы.

Управление «К» МВД РФ рекомендует немедленно удалять все подозрительные сообщения. Никогда не открывайте сразу присланные файлы-вложения, в том числе полученные от друзей, коллег или от имени известных фирм. Принимайте во внимание, что сообщения от якобы знакомых лиц могут оказаться рассылками, отправленными сетевыми червями. Также имейте в виду, что без вашего ведома ни одна уважаемая организация не будет рассылать файлы, даже если это важные данные, такие, как обновления системы или очередная защита от вирусов.

РАСШИРЕНИЕ ФАЙЛА – ЭТО ВАЖНО

Обращайте внимание на расширение файла. Особую опасность могут представлять файлы со следующими расширениями:

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.eml, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vbs,*.vbe, *.wsf, *.wsh, *.wsc.

Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

КАК ПРАВИЛЬНО УДАЛЯТЬ СООБЩЕНИЕ ИЗ ПОЧТОВОЙ ПРОГРАММЫ

Будьте очень осторожны при получении сообщений с файлами-вложениями. Подозрительные сообщения лучше немедленно удалять.

Чтобы удалить сообщение в почтовой программе полностью:

удалите сообщение из папки «Входящие»;

удалите сообщение из папки «Удаленные»;

выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

К сожалению, нельзя исключать случаи, когда присылаемые файлы все-таки будут запущены. Однако и в этих случаях можно принять контрмеры.

В первую очередь, следите, чтобы у вас были установлены самые последние обновления программ. Нелишним будет установить персональный межсетевой экран (firewall). В нём следует указать исчерпывающий список программ и доступных им портов и сервисов. Как только какая-либо незнакомая программа попытается отправить почту, она тут же будет обнаружена, и зараза не распространится с Вашего компьютера дальше.

Кроме того, отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы (обращение к файлам, загрузочной области диска, системному реестру и т. п.), способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

БУДЬТЕ БДИТЕЛЬНЫ!

Управление «К» МВД РФ рекомендует больше внимания обращать на то, что происходит на вашем компьютере во время сеанса связи с Интернетом. Если Вы заметите, что в то время, когда Вы не выполняете никаких действий, не происходит обновление антивирусного программного обеспечения и компонентов операционной системы, а индикатор активности передачи данных по сети говорит об обратном, немедленно прекратите связь и проверьте компьютер антивирусными программами. Индикатором активности работы с сетью может служить внешний модем (лампочки мигают), значок двух соединенных компьютеров, появляющийся при установлении связи внизу на панели задач (мигает).

Безопасное использование телеконференций и ICQ

Самым густонаселенным вирусами местом в Интернете, по мнению специалистов-антивирусников, остается, так называемая, сеть Usenet, включающая в себя разнообразные группы новостей (телеконференций).

Другими словами, новости – это очень ненадежный источник в смысле получения файлов, поэтому относиться к ним надо более чем осторожно.

Старайтесь пользоваться новостями по их прямому назначению: для поддержания дискуссий, обмена мнениями, информацией, но не в качестве источника бесплатных программ. Форма взаимодействия в новостях – это все тот же обмен почтовыми сообщениями, поэтому при работе с новостями используйте те же рекомендации, что и при работе с электронной почтой.

Другой неприятностью при работе с новостями (и другими подобными сервисами) может стать огласка вашего электронного почтового адреса, который впоследствии может быть использован для спам-рассылок или рассылок сообщений с вирусами.

Когда вы помещаете сообщение в группе новостей, в нем всегда содержится ваш обратный адрес. Это потенциально опасно, поскольку существуют специальные программы, которые способны автоматически сканировать подобные объявления, выуживая из них почтовые адреса.

Однако такие программные автоматы легко обмануть. Измените свой обратный адрес, включив в него некоторую выделяющуюся часть, например, I.Ivanov-DEL-@provider.ru: обычные пользователи поймут, каков Ваш настоящий адрес, а программы будут использовать обманку «вслепую».

Безопасное использование пейджеров ICQ

Пейджеры ICQ также являются сервисами повышенной опасности. Дело в том, что, кроме просто обмена сообщениями, они дают возможность обмениваться файлами, которые могут оказаться вредоносными программами.

Правила работы с файлами такие же, что и при приеме файлов-вложений по электронной почте: никогда не открывайте присланные файлы, предварительно не проверив их антивирусной программой. Не поддавайтесь желанию немедленно посмотреть фотографии собеседника. Сначала проверьте, не является ли присланный файл подделкой под файл-изображение, старайтесь не разглашать информацию о себе.

Защита IP-адреса компьютера

Другая потенциальная опасность ICQ – возможность определения IP-адреса Вашего компьютера, который может быть использован для воздействия извне. Работая в ICQ, обязательно установите флажок, запрещающий показывать IP-адрес.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

1. АНТИВИРУСНЫЕ ПРОГРАММЫ – ВАШИ ПЕРВЫЕ ЗАЩИТНИКИ

Установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. ОБНОВЛЕНИЯ – ЭТО ПОЛЕЗНО И БЕЗОПАСНО

Отслеживайте появление новых версий операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.

По возможности отказывайтесь от использования старых операционных программ в пользу более современных. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления.

Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

НАСТРОЙТЕ СВОЙ КОМПЬЮТЕР ПРОТИВ ВРЕДОНОСНЫХ ПРОГРАММ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. ПРОВЕРЯЙТЕ НОВЫЕ ФАЙЛЫ

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять.

Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ

По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. РЕЗЕРВНОЕ КОПИРОВАНИЕ – ГАРАНТИЯ БЕЗОПАСНОСТИ

Регулярно выполняйте резервное копирование важной информации. Подготовьте и храните в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

Помните! Если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в ближайший отдел полиции либо напишите заявление на официальном сайте МВД России www.mvd.ru