Содержание:

Как не стать жертвой компьютерных мошенников

Что делает среднестатистический пользователь в Интернете? Ищет информацию, скачивает музыку и фильмы, пишет в блог, посещает развлекательные сайты, пользуется почтой и т.п. Но вот однажды он сталкивается с заманчивым предложением заработать энную сумму денег за короткое время. Неважно, что именно ему предлагают, в его голове уже начинают крутиться мысли о легком заработке. Даже если он достаточно осторожен и не доверяет всему, что пишут, качественный дизайн и грамотный текст могут развеять все его сомнения. Что уж говорить о неопытных подростках… Человек отсылает нужную сумму на кошелек или проводит какие-то другие действия, и терпеливо ждет. Мошенник же получает свои деньги.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег с простодушных пользователей. Практически полная безнаказанность, анонимность мошенников, большое количество доверчивых людей – все это подпитывает такой вот своеобразный вид ‘бизнеса’.

Большинство пользователей просто забывают о том, что в Интернете действуют те же законы, что и в жизни. Сейчас редко найдешь человека, который бы попытался выиграть у наперсточника на вокзальной площади, а вот когда ему же предложат отослать деньги на так называемый ‘волшебный’ кошелек, с тем, чтобы потом получить удвоенную сумму, все защитные психологические барьеры вдруг оказываются снятыми, и он с радостью соглашается. Все это напоминает 90-е годы, когда люди только после своего горького опыта (и чаще неоднократного) становились более осторожными, встречаясь с очередным предложением ‘легких’ денег. В Интернете, как мы видим, ‘90-е’ в самом разгаре…

Главное, что нужно помнить всем - ‘халявы’ не бывает. Никто никогда не даст денег просто так. Деньги не появляются из неоткуда, даже если они ‘электронные’.

А Интернет – это просто средство передачи информации.

Как известно, средствами получения денег является либо производство товаров, либо предоставление услуг. Для Интернета данное утверждение звучит так: либо вы получаете прибыль с производства интеллектуальной собственности, либо с предоставления сопутствующих услуг....

1. Мошенничества, связанные с Интернет-магазинами.

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.

Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.

Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.

Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

2. Фишинг.

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.

Одной из разновидностью данного вида правонарушения являются звонки на сотовые телефоны граждан якобы от представителей банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что никакого кредита не брал, ему предлагается уточнить данные, содержащиеся на пластиковой карте. Этого уже достаточно для покупки товаров в Интернет-магазинах.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить
свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.

3. Интернет-попрошайничество.

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

4. Мошенничества в отношении иностранных граждан (брачные аферы).

Не встретив в реальной жизни свою половину, многие мужчины продолжают искать ее в Интернете. Поиски начинаются на сайтах знакомств и дневниках, где будущие избранницы размещают свои фотографии.

Этим пользуются злоумышленники, используя фото девушек, привлекая психологов, программистов, переводчиков и посредством этих сайтов завязывают переписку с доверчивыми иностранцами.

Западные женихи «клюют» на объявления, где нетребовательные русские красавицы говорят о том, что нуждаются в серьезных отношениях. А взамен вечной любви, порой после месяцев переписки, просят решить их финансовые проблемы - помочь обеспечить сиделкой больных родителей, расплатиться с кредитом, перевести деньги на перелет к жениху в дальнее зарубежье и т.д.

После получения денег невесты перестают выходить на связь. Пылкие иностранные поклонники, поняв, что их обманули, обращаются в полицию. Злоумышленники рассчитывают только на женихов из дальнего зарубежья, т.к. представители ближнего зарубежья предпочитают приехать в гости к невесте сами, что невыгодно для мошенников.

5. Осторожно!!!!! Вирус!!!!!

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная.

Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения, например:

- программка для бесплатной отправки подарков! - http://re-url.me/abc, мне не забудь отправить!

- привет. http://www.894.joo.ru. Лови программку по бесплатному повышению рейтинга, но не давай никому больше. Это не спам.

Основные темы, которые используются для «рекламы» скачивания и запуска зараженных программ:

- бесплатное повышение рейтинга «ВКонтакте»;

- программа перехвата SMS сообщений с телефона;

- дополнительные функции в социальных сетях, которые не существуют (подарки, VIP-доступ и т.д.)

После перехода по ссылке компьютер пользователя автоматически запускает вредоносную программу.

Наши рекомендации

Пострадавшим рекомендуется изменить пароль доступа к указанным ресурсам, а также установить версии антивирусных программ с обновленными антивирусными

базами.

Следует помнить, что ресурсы популярных сайтов никогда не потребуют от уже зарегистрировавшегося пользователя дополнительной авторизации, тем более за деньги путем отправки смс.

6. Осторожно!!! Новый вид мошенничества!!!

В Российском сегменте сети Интернет стала появляться информация о так называемых «звуковых» наркотиках, якобы оказывающих влияние на бинауральные ритмы человека. Реклама аудионаркотиков осуществляется посредством массовой рассылки писем на электронные почтовые адреса пользователей и на номера в системах быстрого обмена сообщениями. Доступ к прослушиванию аудио-файлов возможен после введения специального цифрового кода, получение которого происходит исключительно после оплаты в виде отправки смс-сообщения. Ресурсы, предлагающие такого рода продукцию, располагаются на площадях зарубежных провайдеров и зарегистрированы по фиктивным анкетным данным.

По мнению специалистов, достичь рекламируемого эффекта посредством звуковых колебаний невозможно. Единственным результатом применения «звуковых» наркотиков являются головные боли, частичная потеря памяти и снижение мозговой активности.

Таким образом, информация о «цифровых наркотиках» - это хорошо спланированная «черная» пиар-компания, способная привлечь новых потенциальных покупателей звуковых файлов, и очередной способ получения денег мошенниками.

СОВЕТЫ, КАК ОБЕЗОПАСИТЬ СЕБЯ

1. Электронная почта

Электронная почта - на сегодняшний день один 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 прикреплять файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

Вредоносные программы - это так или иначе исполняемые файлы (самостоятельные или командные (скрипты)), которые срабатывают при выполнении на данном компьютере. Можно сформулировать следующую тактику в борьбе с ними:

- во-первых, не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

- во-вторых, если уж они к Вам попали, ни в коем случае не запускать их на выполнение;

- в-третьих, если они все же запустились, принять меры, чтобы, по возможности, они не причинили ущерба.

Если Вы получили сообщение с вирусом, значит, Вы уже невольно выполнили первый предварительный 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 ряд фильтров, отсекающих 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 все еще могут беспрепятственно попадать в почтовый ящик. Поэтому пользователю необходимо предпринять дополнительные меры безопасности.

Самый действенный способ оградить от вредоносных программ свой почтовый

ящик - это 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, при необходимости получить по почте программу 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 исходного файла.

Имеется еще один способ не сохранять подозрительные сообщения на своем компьютере. Идея состоит в том, чтобы сначала получать с сервера и просматривать только заголовки сообщений и удалять ненужные письма непосредственно на сервере, не скачивая их на свой компьютер. Для этого можно использовать специальные программы.

Если же обстоятельства таковы, что Вы не можете организовать работу так, чтобы не получать сообщения с исполняемыми файлами, а значит, сообщения с вредоносными программами могут быть Вами получены, то необходимо предпринять меры к тому, чтобы вредоносные программы ни в коем случае не были запущены на выполнение.

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

Учитывая сказанное, необходимо взять за правило не открывать сообщение (дважды щелкнув мышкой), особенно если сообщение пришло от неизвестного отправителя. Прочитать текст всегда можно в режиме быстрого просмотра (когда при одиночном щелчке мышкой на сообщении в списке текст сообщения отображается не в отдельном, а в основном окне программы). Все подозрительные сообщения немедленно удаляйте.

Также никогда не открывайте немедленно присланные файлы-вложения, в том числе файлы от друзей, коллег или присланные от имени известных фирм. Принимайте во внимание, что сообщения якобы от 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.

Нелишним будет установить персональный межсетевой экран (firewall). В ней 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. Такие программы обычно автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

Наконец, рекомендуем больше внимания обращать на то, что происходит на Вашем компьютере во время сеанса связи с Интернет. Если Вы заметите, что в то время, когда Вы не выполняете никаких действий с сетью, индикатор активности передачи данных по сети говорит об обратном, немедленно прекращайте связь и проверяйте свой 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).