Виды мошенничества в сети интернет. Как не стать жертвой мошенников

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 этот своеобразный «бизнес».

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.

Главное, что нужно помнить всем — «халявы» не бывает. Никто никогда не даст денег просто так. Деньги не появляются из ниоткуда, даже если они «электронные». 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.

Насторожить должна 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.

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,

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.
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.

I Вредоносные программы и как обезопасить себя в Интернете

Основным источником опасности для пользователей компьютеров были и остаются вредоносные программы, которые с развитием сетевых технологий получили новую среду для своего распространения.
В обиходе часто все вредоносные программы называют словом «вирусы», хотя, строго говоря, это не так.

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 локальным сетям, по 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 обычно состоит в том, чтобы обеспечить злоумышленнику доступ к Вашему компьютеру и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Просто в один «прекрасный день» 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 быстро окажется нулевым или отрицательным.

Блокировщики Windows

Одной из разновидностью вирусов которых являются блокировщики Windows. Вирус проникает на компьютер пользователя (этот процесс может происходить автоматически и незаметно) и добавляет свой код в автозапуск системы.

После перезагрузки компьютера операционная система блокируется, появляется сообщение о необходимости отправки смс на номер… При этом могут содержаться угрозы об уничтожении данных.

Не бойтесь этого развода. Для разблокировки системы нужно ввести код, который можно найти в интернете при помощи поисковых систем или на сайтах производителей антивирусных программ.

I 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 (вложение или присоединение), который может оказаться зараженным вирусом или вредоносной программой.

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.

Прежде всего, необходимо предпринять меры к тому, чтобы этого не происходило впредь. Самый действенный способ оградить свой почтовый ящик от вредоносных программ — запретить прием сообщений, содержащих исполняемые вложения. В этом случае 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, 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. Можно и самостоятельно просматривать только заголовки сообщений и удалять ненужные письма непосредственно на сервере, не скачивая их на свой компьютер.

Если же обстоятельства таковы, что Вы не можете не получать сообщения с исполняемыми файлами, то необходимо предпринять меры к тому, чтобы вредоносные программы ни в коем случае не были запущены на выполнение. 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.

Никогда не открывайте немедленно присланные файлы-вложения, в том числе файлы от друзей, коллег или присланные от имени известных фирм. Помните, 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.

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

Для того, чтобы в почтовой программе полностью удалить сообщение:

- удалите сообщение из папки Входящие;
- удалите сообщение из папки Удаленные;
- выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

К сожалению, необходимо отметить, что даже при твердом намерении не открывать немедленно присылаемые файлы нельзя исключать случаи, когда они все-таки будут запущены: вследствие ошибки программного обеспечения, по ошибке или недоразумению. Однако и в этих условиях возможно предпринять контрмеры. В первую очередь следите, чтобы у Вас были установлены самые последние обновления программ.

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.

2. Новости (телеконференции), ICQ

Самым густонаселенным вирусами в Интернете местом, 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, и относиться к ним надо более чем осторожно. Старайтесь пользоваться новостями по их прямому назначению: для поддержания дискуссий, обмена мнениями, информацией,— но не как источником 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.

Измените свой обратный адрес, включив в него некоторую выделяющуюся часть, например, I. Ivanov-DEL-@provider.ru: люди поймут, каков Ваш истинный адрес, а программы будут использовать обманку как есть.

Пейджеры ICQ также являются сервисами повышенной опасности. Дело в том, что, помимо просто обмена сообщениями, эти сервисы дают возможность обмениваться также файлами, которые могут оказаться вредоносными программами. Правила работы с файлами должны быть такими же, что и при приеме файлов-вложений по электронной почте: никогда не открывайте присланные файлы, предварительно не проверив их антивирусной программой. Когда в пылу общения хочется немедленно посмотреть фотографию собеседника, посмотрите внимательно, не является ли присланный файл подделкой под файл-изображение, старайтесь не разглашать информацию о себе.

Другой потенциальной опасностью ICQ является возможность определения IP-адреса Вашего компьютера, который может быть использован для воздействия извне. Работая в ICQ, обязательно установите флажок, запрещающий показывать IP-адрес.

Рекомендации по обеспечению безопасной работы в Интернете

Суммируя все сказанное, кратко можно сформулировать следующие рекомендации, направленные на повышение безопасности работы пользователя в Интернете:

- установить антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы;
- отслеживать появление новых версий операционных систем и своевременно устанавливать обновления к ним, устраняющие обнаруженные ошибки.
- настроить операционную систему так, чтобы обеспечивались основные правила безопасности при работе в сети. По возможности отказаться от использования старых операционных программ в пользу более современных.
- регулярно обновлять пользовательское программное обеспечение для работы в сети, такое, как Интернет-браузер, почтовые программы, устанавливая самые последние обновления.
- выполнить настройки почты, браузера и клиентов других используемых сервисов, уменьшающие риск воздействия вредоносных программ и подверженность сетевым атакам.
- никогда не устанавливать и не сохранять файлы, полученные из ненадежных источников: скаченные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях,— без предварительной проверки антивирусной программой. Подозрительные файлы лучше немедленно удалять.
- при получении извещений о недоставке почтовых сообщений обращать внимание на причину и в случае автоматического оповещения о возможной отправке вируса немедленно проверять компьютер антивирусной программой.
- по возможности, не сохранять в системе пароли (для установки соединений с Интернетом, для электронной почты и др.), периодически их менять. Регулярно выполнять резервное копирование важной информации.
- подготовить и иметь в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузить систему с диска и проверить антивирусной программой.

Управления «К» МВД России предупреждает

В период новогодних праздников и в настоящее время в социальных сетях многим пользователям приходят сообщения от посторонних лиц или от друзей, находящихся в контактном листе, с просьбой посетить определенный ресурс или проголосовать за них, отправив смс на короткий номер.

Управление «К» предупреждает: не поддавайтесь уловкам мошенников, посещая указанные ресурсы или отправляя смс на обозначенный номер! Вероятнее всего, страница пользователя, от которого приходят подобного рода сообщения, взломана, и от его имени осуществляется массовая рассылка. При переходе на указанные ресурсы велика вероятность заразить компьютер какой-либо вредоносной программой, а после отправки смс на указанный номер можно потерять со счета немалую сумму денег.

Во избежание несанкционированного доступа к вашим страницам в социальных сетях, в том числе и к содержимому электронной почты, а также для предотвращения возможных последствий, связанных с действиями мошенников, следует предпринять следующие меры:

1. Воздержитесь от выполнения указанной в сообщении просьбы.
2. Свяжитесь с другом, от которого вы получили вышеуказанное сообщение, и уточните у него, действительно ли он является автором послания.
3. Если выяснится, что страница пользователя взломана, ему необходимо поменять пароли в социальных сетях и электронной почте, а также проверить компьютер на наличие вирусов.

Остерегайтесь предложений об установлении местонахождения человека по номеру его мобильного!

В последнее время многие пользователи Интернета сталкиваются с размещенной в сети информацией о том, что они могут установить местонахождение человека по номеру его мобильного телефона. Для этого требуется отправить sms с набором определенных цифр на указанный номер и за небольшую сумму получить код доступа к услуге.

Однако после проведения вышеуказанных манипуляций клиенту так и не удается осуществить поиск интересующего его человека, зато с его счета списывается кругленькая сумма.

Управление «К» МВД России предупреждает, что определить местонахождение человека по номеру мобильного телефона можно исключительно с его согласия. Такую услугу предоставляют некоторые операторы сотовой связи в установленном порядке. Однако если подобное предложение исходит не от оператора сотовой связи, а от третьих лиц, то это является не чем иным, как мошенничеством!

Мошенничества с кредитами. Будьте бдительны!

Специалистами Управления «К» МВД России предупреждают об организованных преступных группах, занимающиеся мошенническими действиями, связанными с содействием в получении кредита. Размещая в интернете или печатных изданиях объявления о содействии в кредитовании, злоумышленники гарантируют привлекательные процентные ставки и получение кредита на сумму, как правило, более свыше 500 тыс. рублей в короткий срок. Предлагается связаться с «сотрудницами организации» по указанному в объявлении мобильному телефону и перечислить через систему денежных переводов определённую сумму. После подтверждения факта перечисления денежных средств к потенциальной жертве выезжает «специалист» для заполнения необходимых документов, где доверчивые граждане собственноручно расписывались в том, что денежные средства были перечислены по собственному желанию и претензий не имеется. Долгожданного кредита так никто и не получает.

Финансовые пирамиды обжились в Интернете

В Интернете каждый день появляются все новые ловушки и пирамиды, но, к сожалению, несмотря на горький опыт, многие продолжают вступать в ряды мошенников. Что же может остановить нечистых на руку вербовщиков? Только уголовная ответственность — считают законодатели.

Министерство финансов предложило наказывать не только организаторов, но и участников пирамид. Вступление в финансовую пирамиду грозит штрафом до 1,5 миллионов рублей и лишением свободы сроком до семи лет.

Ирина Лобанова,
руководитель проектов НАФИ:
Внешне такие мошеннические онлайн-сообщества похожи на обычные инициативные группы в социальной сети и люди слишком поздно понимают, что попали в финансовую пирамиду. В группе риска самые социально незащищенные слои населения: студенты, пенсионеры, женщины в декрете.

Как же не попасть
в финансовую пирамиду?

1. Если в Интернете или по телефону вам поступило сообщение с просьбой перевести любую, пусть даже самую маленькую сумму денег — стоит насторожиться.
2. Если вам обещают большие деньги за работу в Интернете — помните, если вы не гений-программист, такое невозможно. Задайте себе вопрос: за что мне будут платить? Кликать на рекламу или рассылать сообщения? Это пирамида, однозначно.
3. Важный признак мошеннической схемы — непрозрачность структуры. Спросите конкретно: кем вы будете работать и какие обязанности исполнять? Менеджер широкого профиля или сотрудник офиса? Слишком расплывчато..
4. Насторожитесь, если вам обещают руководящую должность и «золотые» горы. С чего бы в этой организации вы сразу на «вес золота» и уже скоро станете начальником?
5. Не менее важным признаком является непрозрачность механизмов инвестирования средств, а также отсутствие явных признаков экономической деятельности. Например, реклама организации обещает высокие проценты за счет инвестирования в высокодоходные инструменты фондового рынка, однако в ходе мониторинга выясняется, что в действительности организация не торгует на бирже, а выплата обещанных процентов осуществляется только за счет привлечения денег «новых» участников.
6. В офисе компании всего несколько столов, помещение пустовато и не обжито, значит, эта компания работает совсем недавно и не может вызывать доверия.

Помните, что в финансовой пирамиде действительно зарабатывают только те, кто на верхушке, собирая деньги с тех, кто только начал подниматься. Среди тех, кто бывает в сети практически ежедневно, верно распознают признаки пирамиды 30%, а среди тех, кто использует Интернет эпизодически — 19%. Для сравнения: только каждый четвертый россиянин способен распознать признаки финансовой пирамиды (23%).