

Алексей Анатольевич Гладкий
Мошенничество в Интернете. Методы удаленного
выманивания денег, и как не стать жертвой
злоумышленников



МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

**Методы удаленного выманивания денег,
и как не стать жертвой злоумышленников**



Текст предоставлен правообладателем
«Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать
жертвой злоумышленников»: Авторское; 2012

Аннотация

Мошенничество возникло практически одновременно с появлением человечества и, стоит признать, этот вид деятельности успешно эволюционировал. По всему земному

шару в поисках добычи снуют разномастные проходимцы, жулики, мошенники, вымогатели и прочая малопочтенная публика. Они проникли практически во все сферы человеческой деятельности, и было бы очень странно, если бы Интернет выпал из сферы их интереса.

Хочется верить, что эта книга поможет читателям избежать попадания в мошеннические сети, хитроумно расставленные по всему Интернету. Вы узнаете, где и чего следует опасаться, как проверить заманчивое предложение о сотрудничестве, и почему ни в коем случае нельзя переводить деньги неизвестным лицам (если, конечно, вы не хотите оказать им благотворительную помощь). Помните, что Интернет – это мощный инструмент, с помощью которого злоумышленники выманивают огромные суммы денег у беспечных обывателей.

Алексей Анатольевич Гладкий

Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников

Введение

Мошенничество возникло практически одновременно с появлением человечества и, стоит признать, этот вид деятельности успешно эволюционировал. По всему земному шару в поисках добычи снуют разномастные проходимцы, жулики, мошенники, вымогатели и прочая малопочтенная публика. Они проникли практически во все сферы человеческой деятельности, и было бы очень странно, если бы Интернет выпал из сферы их интереса.

В последние годы мошенничество в Интернете цветет махровым цветом, а количество обманутых и пострадавших от него людей растет не по дням, а по часам. Хищение денег, кража конфиденциальной информации, вымогательство, откровенный обман и элементарное «кидалово» – несть числа приемам и способам, которыми оперируют современные Остапы Бендеры для «сравнительно честного отъема денег у населения».

Причем далеко не всегда они действуют нагло и стремительно (хотя такого тоже хватает). Современный интернет-злоумышленник хитер, коварен, но в то же время – тактичен и вежлив. Он умеет расположить к себе потенциальную жертву (благо через Интернет это несложно), и вызвать если не уважение к себе, то, по крайней мере, полное доверие. Когда же наступает «прозрение» и жертва осознает, что ее обманули – предпринимать что-либо очень сложно, а зачастую – почти нереально.

Характерной особенностью интернет-мошенничества является то, что злоумышленника трудно поймать и привлечь к ответственности. Ведь физически он может находиться даже на другом краю земного шара. И если он получает от своих жертв деньги с помощью электронных платежных систем (WebMoney, Яндекс. Деньги и т. п.) – вычислить его очень и очень сложно. Но даже если мошенника удастся вычислить и привлечь к ответственности (а его действия, кстати, прямо подпадают под юрисдикцию Уголовного кодекса РФ), то вернуть свои деньги вряд ли удастся.

Следовательно, лучший способ обезопасить себя от интернет-мошенников состоит в том, чтобы не попадаться на их уловки. И в этой книге мы расскажем о некоторых распространенных способах, которыми пользуются злоумышленники с целью обмана излишне доверчивых граждан. Надеемся, изучение предлагаемого материала поможет вам своевременно распознавать интернет-мошенников и тем самым защитить себя от их посягательств.

Глава 1. Обман при устройстве на работу и в предложениях заработка

Рыба ищет, где глубже, а человек – где лучше. В поисках нового места работы или дополнительной подработки многие пользуются Интернетом, где и попадают в лапы многочисленных мошенников.

В первую очередь отметим, что основной принцип действий у большинства из них скопирован под одну кальку: пользователю предлагается быстрое и сказочное обогащение, которое не требует практически никакого трудового участия. Единственное маленькое условие – необходимо перевести некоторую сумму денег по указанным реквизитам, и после этого доходы потекут рекой. «Ведь это классическое правило бизнеса – чтобы получить доход, нужно сделать определенные вложения!» – завлекают «благодетели». Разумеется, после перевода денег пользователь в лучшем случае получает какие-нибудь бессмысленные инструкции, а в большинстве случаев – таинственный «благодетель» просто исчезает, не отвечая на письма (разумеется, ни телефона, ни адреса проживания он не сообщает). Бывают и другие ситуации – например, часто жертвами мошенников становятся фрилансеры, готовые выполнить «тестовую» работу и не удосужившиеся поинтересоваться координатами своих анонимных работодателей.

В этой главе мы расскажем о схемах, которыми пользуются интернет-злоумышленники для обмана соискателей работы и приработка.

Фрилансер, будь бдителен!

В последние годы стремительно растет популярность фриланса – удаленной работы через Интернет. Если кто-то не знаком с этим явлением – поясним: сущность заключается в том, что человек выполняет работу в удаленном режиме, сидя за домашним (или за другим доступным) компьютером. Он получает задание и отправляет выполненную работу, как правило, через Интернет (по электронной почте, через FTP-сервер, и т. п.).

Преимущества такой работы очевидны: не нужно ходить в офис, работать можно по свободному графику (хоть ночью), таких понятий, как опоздание или прогул, не существует, и т. д. Поэтому неудивительно, что число людей, для которых фриланс является основным видом заработка, постоянно растет. Фрилансерами могут быть специалисты любых сфер деятельности, которые с технической точки зрения могут работать подобным образом: переводчики, программисты, веб-разработчики, тестировщики, журналисты, писатели (в том числе технические писатели), копирайтеры, редакторы, сценаристы, художники, специалисты по работе с графикой и видео, и т. д. Но даже если вы по своей профессии не относитесь ни к одной из этих категорий – вы все равно можете заниматься фрилансом: ведь никто не мешает врачу или учителю в свободное время писать книги и методички для удаленных работодателей, инженеру-конструктору – готовить чертежи или техническую документацию, музыканту – писать партитуры, и т. д.

Привлекательность фриланса отлично осознают и мошенники, и это намного упрощает их деятельность. Самыми легкими их жертвами становятся те, кто спит и во сне видит себя фрилансером (немало людей, готовых хоть завтра бросить работу – были бы привлекательные заказы от удаленных работодателей). Один из самых распространенных приемов обмана состоит в том, что соискателю предлагается выполнить тестовое задание. Если вы копирайтер – это может быть статья или фрагмент текста, если программист – написание фрагмента программного кода или разработка приложения, если веб-разработчик – создание веб-страницы, и т. д. Причем нередко мошенники прямо заявляют: мол, это задание тестовое, оно не оплачивается, но если вы выполните его качественно – мы возьмем вас на работу, и вот тогда вы будете работать за деньги. Стоит ли говорить, что после выполнения такого задания незадачливый фрилансер либо получает отказ в приеме на работу, либо никто вообще с ним не выходит на связь!

ВНИМАНИЕ

В современной России такое мошенничество – это целая индустрия, которая постоянно развивается и совершенствуется, во многом благодаря откровенной безнаказанности.

Отметим, что подобный «развод» может прикрываться не только тестовым заданием, но и вполне реальной работой. Ведь часто на подобные предложения откликаются опытные люди, у которых есть образцы работ. В этом случае мошенники отвечают в том духе, что, мол, примеры ваших работ нам понравились, и мы предлагаем вам сразу начать работать за деньги (разрабатывать сайт, создавать программный код, писать статьи и книги, переводить тексты, и т. д.). Только вот денег вам, как вы догадались, никто не заплатит.

Ниже мы приводим несколько примеров, как и с какими целями может использоваться подобные мошеннические приемы.

◆ Создание веб-ресурсов. Каждый обманутый фрилансер из числа веб-разработчиков готовит отдельную страницу в виде «тестового задания», такие же наивные копирайтеры готовят контент для данного сайта, а обманутые веб-дизайнеры разрабатывают дизайн. Получается, что над созданием ресурса работает целая команда людей – незнакомых друг с другом, находящихся в разных городах (а возможно – и странах), и в конечном итоге – обманутых. Мошенники лишь координируют их действия и собирают из готовых фрагментов, подобно конструктору.

◆ Разработка программных продуктов. Каждый соискатель пишет свой фрагмент программного кода, такие же фрилансеры из числа технических писателей документируют продукт, и т. д. Когда все фрагменты будущего продукта готовы – удаленным разработчикам вежливо говорят «спасибо, вы нам не подходите». Или вообще ничего не говорят.

◆ Написание книг. Не секрет, что в России действует многочисленная армия «литературных негров», силами которых создается большинство всей современной российской беллетристики (это касается как художественной, так и нехудожественной литературы). Солидные издательства рассчитываются с удаленными работниками полностью и в срок, но существует немало «деятелей», которые делают неплохой бизнес на «халяве», то есть на неоплаченных текстах. Они могут называть себя по-разному: менеджерами проектов, литературными агентами, и т. д. Обычно такой «менеджер проектов» работает примерно так: приглашает на «тестовое задание» несколько удаленных авторов, каждый из которых пишет отдельную главу книги, затем удаленный редактор редактирует текст, удаленный верстальщик делает верстку, и т. д. После этого всем фрилансерам дается полный «отлуп», готовая и сверстанная книга в электронном виде продается в издательство, и «менеджер проектов» получает свой гонорар. Пытаться делать что-либо в такой ситуации почти бесполезно, и все ваши попытки доказать, что именно вы являетесь истинным автором книги, будут выглядеть нелепо.

◆ Перевод текстов. Алгоритм примерно такой же: удаленному переводчику предлагается перевести пару страниц «на пробу» (или – на условиях последующей оплаты и постоянного сотрудничества). После того как он сдает работу, с ним на связь никто не выходит, и на его письма никто не отвечает.

◆ Написание статей, журналистских материалов, и т. д. Удаленный автор или журналист присылает работу (или несколько работ) – и на этом связь с ним прекращается.

◆ Написание сценариев для сериалов, фильмов, компьютерных игр. Известны случаи, когда по украденным таким способом сценариям создавались популярные телевизионные сериалы и разрабатывались компьютерные игры, ставшие впоследствии бестселлерами.

Во всех перечисленных примерах расчет мошенников безошибочный: поскольку обманутые люди незнакомы друг с другом, они не могут скоординировать свои действия и объединиться с целью поимки и разоблачения злоумышленников. Да никому и не хочется этим заниматься – проще смириться с тем, что время на работу было потрачено впустую. Если же кто-то все же пожелает каким-то образом добиться правды – это будет очень сложно: электронная переписка доказательством не является, координат «работодателей» нет, их ФИО никто не знает (разумеется, мошенники представляются под вымышленными

именами), да и находиться они могут в другой стране. Причем даже если вы вовремя догадаетесь, что вас пытаются банально «развести», и вовремя «соскочите с крючка» – мошенник ровным счетом ничего не потеряет, поскольку легко и быстро найдет вам замену.

Тем не менее, если вы хотите заниматься фрилансерской деятельностью – ставить крест на своих планах не стоит. Достаточно соблюдать несложные меры предосторожности, которые хоть и не дают 100 %-ной защиты от мошенников, но позволяют свести возможный риск к минимуму, и сделать вероятные потери совсем несущественными и не заслуживающими внимания.

Прежде всего, помните: вы должны четко знать, с кем вы намерены иметь дело, и где находится ваш потенциальный работодатель. Например, если вы получили электронное письмо с предложением выполнить работу (неважно, тестовую или нет), и в нем отсутствуют контактные данные отправителя (электронный адрес не в счет) – будьте особо бдительны. Напишите ответное письмо с требованием прислать адрес работодателя и телефон, по которому вы могли бы с ним побеседовать. Как правило, мошенники просто не отвечают на подобные письма, понимая, что этого человека «развести» не получится. Или присылают нелепые отговорки – мол, мы меняем адрес, телефон пока не подключили, и т. п. В любом случае знайте: без контактных данных работодателя (и их последующей проверки – как минимум нужно позвонить) к работе приступать нельзя, поскольку если вам их не дают – это однозначно «лохотрон».

ВНИМАНИЕ

Мошенник может настойчиво требовать от вас подробное развернутое резюме и прочие сведения, но при этом о себе он не скажет ни слова, несмотря на все ваши требования. Желая получить от вас максимум информации, он тем самым стремится обезопасить себя: например, вдруг программный код, который вы ему пришлете, является украденным, или присланный вами текст книги является плагиатом, и т. д. Имея же ваше резюме с образцами работ, он, по крайней мере, будет знать, что вы действительно программист или копирайтер, а не такой же жулик, который на халяву решил подзаработать.

Многие мошенники, предлагающие удаленную работу, сразу спрашивают: можете ли вы подъехать в офис для личной беседы? Такой вопрос должен насторожить: это, скорее всего, «проверка на вшивость». Если вы ответите, что, мол, я не могу приехать, поскольку живу в другом городе – вам тут же с радостью ответят, что «это желательно, но не критично, можете приступать к работе». Злоумышленники будут знать, что вы живете далеко, следовательно – вас можно обманывать без страха и упрека.

СОВЕТ

В подобной ситуации всегда отвечайте: да, я готов приехать в офис – даже если работодатель находится в другом регионе. Если вам назначат встречу – тогда можно извиниться и сказать: мол, извините, я не заметил, что вы находитесь в другом городе. По крайней мере, это будет свидетельствовать о том, что работодатель от вас не прячется.

Получив предложение об удаленной работе, наведите справки о своем потенциальном работодателе. С помощью Интернета это несложно: введите в любой поисковик название фирмы, или ФИО написавшего вам человека, на худой конец – просто электронный адрес, и ознакомьтесь с результатами поиска. В большинстве случаев даже такая элементарная проверка позволяет быстро расставить все точки над «i».

Еще один эффективный способ проверки удаленных работодателей – так называемые «черные списки работодателей», которые во множестве представлены в Интернете. Эти списки формируются по всем сферам, в том числе и по удаленной работе. Если вы сомневаетесь в честности работодателя – возможно, он уже кого-то обманул, и информация о нем есть в «черном списке». Если же вы стали жертвой мошенника – не поленитесь внести

в такой список о нем информацию: возможно, кому-то эти сведения помогут избежать обмана. Найти «черный список» просто – для этого достаточно в любом поисковике ввести соответствующий запрос.

ПРИМЕЧАНИЕ

Иногда информация попадает в «черные списки» от конкурентов вполне порядочного работодателя. Однако в большинстве случаев содержимому «черных списков» можно доверять.

Ну и, конечно, ни в коем случае не соглашайтесь переводить деньги «за материалы для работы», «услуги по пересылке задания» и т. п. Более подробно на этом мы остановимся позже, а здесь поведаем непреложную истину: если в качестве условия приема на работу вас кто-то просит перевести пусть даже немного денег – это однозначно «лохотрон».

Платное «устройство на работу»

Искать работу с помощью Интернета очень удобно – можно подать объявление и ждать результатов, не выходя из дома. Тем более что сайтов по данной тематике имеется великое множество. Само собой, без интернет-мошенничества здесь тоже не обошлось.

Одна из популярных схем выманивания денег выглядит так: пользователь получает письмо (не обязательно спамерское – это может быть просто отзыв на оставленное резюме), в котором красочно описываются сказочные перспективы – «я был почти нищим, весь в долгах, но благодаря этой замечательной программе быстро разбогател – теперь у меня много денег, вилла на Канарах, куча машин», и тому подобная чепуха. Причем это описание достаточно длинное – оно может занимать несколько страниц. Короче говоря, пользователя, получившего письмо, вначале «грузят» по полной программе.

Если человек, получивший такое письмо, недостаточно опытный – он его не удалит немедленно, как это надо бы сразу сделать, а дочитает до конца. Вот в конце-то и будет сказано о главном условии подобного «счастья» – нужно всего-навсего перевести по указанным реквизитам (чаще всего – на кошелек WebMoney либо аналогичной платежной системы) некоторую сумму денег (сумма варьируется от 10 долларов США до «плюс бесконечности»). Причем – не просто перевести, а оплатить какой-либо информационный пакет, либо ключ, либо инструкции, либо еще что-нибудь, необходимое для дальнейшей «работы». Нужно сказать, что в большинстве случаев пользователь после оплаты действительно получает по почте какую-то информацию, но никаким положительным образом это на его финансовом благополучии не скажется, поскольку приобретает он бессмысленный набор фраз типа «проявляйте усердие, и удача будет с вами».

Еще один способ выманивания денег заключается в том, что мошенник предлагает «содействие в трудоустройстве». Самый примитивный вариант – это когда предлагается прислать свои данные, а вместе с ними некоторую сумму денег за «услуги по поиску работы» и ждать ответа. Само собой, ждать придется бесконечно.

Более «хитрый» вариант может выглядеть так. Пользователь получает отзыв на свое резюме, которое он разместил в Интернете ранее. В письме сообщается, что его резюме весьма заинтересовало руководство крупной (российской или зарубежной) компании, и будет предложено пройти удаленное тестирование. Для этого нужно будет заполнить либо анкету на сайте, либо ответить на присланные вопросы, либо еще что-то подобное. После этого придет письмо с содержанием типа «поздравляем вас, вы прошли предварительное тестирование, результаты отличные». В этом же письме (а может – в следующем) будет предложено продолжить тестирование, но для получения следующих вопросов (анкет и т. п.) нужно заплатить определенную сумму денег. Вот на этом этапе и нужно немедленно прекратить сотрудничество с «агентством», «работодателем» или как там еще мог представиться мошенник. В принципе, не исключено, что после оплаты пользователь получит еще какие-то тесты, анкеты либо вопросы, но после их заполнения и отправки ответ

будет либо «к сожалению, повторное тестирование вы не прошли», либо «вы успешно прошли тестирование, но пока вакансии для вас нет», либо что-то аналогичное. В любом случае, если при поиске работы требуют деньги за содействие, за тестирование, за «бланки анкет» либо за что-то еще, нужно помнить – это мошенничество, и ничто иное.

Следует отметить, что агентства по трудоустройству, само собой, могут потребовать плату за свои услуги, но это ни в коем случае не предоплата (в данном случае «предоплата» и «мошенничество» – это синонимы). Обычно плата за трудоустройство взимается в виде определенного процента с первой зарплаты соискателя, полученной им на новом месте работы, и этот процент строго оговаривается заранее.

Обработка писем на дому

Способ мошенничества, о котором мы расскажем в данном разделе, имеет давнюю историю. Он зародился лет двадцать назад, и первое время реализовывался не с помощью Интернета, а посредством обычной почты. С развитием же интернет-технологий действовать мошенникам стало намного проще.

Сущность способа состоит в том, что мошенники предлагают людям зарабатывать умопомрачительные деньги путем простой обработки писем. Ниже приводится пример электронного письма, с помощью которого мошенники привлекают потенциальных жертв.

Вы уже готовы зарабатывать от 500\$ в неделю изменить свою жизнь? Тогда наше предложение именно для Вас!

Надомная работа по программе «Hotemailer's Program» от латвийской почтовой компании «Sauna, Ltd». Заполнение конвертов по схеме 2\$ за конверт. По этой программе успешно работают заполнители в странах ближнего и дальнего зарубежья.

С помощью «Hotemailer's Program» очень многие люди стали довольно состоятельными людьми и смогли осуществить свои самые заветные желания, значительно улучшить свой социальный статус, им стали доступны не достигаемые ранее блага.

Если и Вы готовы примкнуть к рядам этих людей, то Вам невероятно повезло, ибо то, что мы Вам предлагаем – это просто удача для Вас!

Простая, приятная работа, которую Вы можете выполнять дома в спокойной обстановке всего несколько часов в день. Но эта простая работа принесёт Вам (при должном старании) 50\$ и более в ДЕНЬ!!! Разве это не то, что вы искали всю свою сознательную жизнь?

Не дайте ГОСПОЖЕ УДАЧЕ проскользнуть мимо Вас!

Только тот ничего не добивается, кто ни на что не решается! Примите правильное решение, и Ваша семья будет Вам благодарна всю жизнь!

Приступайте немедленно, и тогда Вы можете застать наше СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ, приуроченное ко второй годовщине «Hotemailer's Program» на рынке труда Украины, России и всего СНГ!

Место жительства не имеет абсолютно никакого значения! За дополнительной информацией обращаться на e-mail sauna_ukraine@hotpor.com

РЕШАЙТЕСЬ!

Заметьте: никаких контактных данных, кроме электронного ящика, в письме нет. После того как вы напишете письмо на этот ящик, вам придет ответ, сущность которого состоит в следующем: для начала работы вам следует перевести определенную сумму денег по указанным реквизитам. Стоит ли говорить, что после перечисления денег все сотрудничество с этой конторой бесславно закончится!

В данном конкретном случае мошенники завели себе простенький сайт на дешевом хостинге – чтобы создать иллюзию более-менее солидной конторы. Но последние сомнения

в нечистоплотности этих «деятелей» исчезают после знакомства с вывешенными на сайте контактными данными (рис. 1.1).



Рис. 1.1. Контактные данные мошенников

Обратите внимание – центральный офис «солидной почтовой компании» находится в абонентском ящике! После этого только самый наивный человек может еще верить в порядочность злоумышленников.

Кстати, важный момент: даже если мошенники дают ссылку на свой сайт – то этот сайт, как правило, имеет примитивный вид и хаактеризуется отсутствием всякого дизайна. А услуги хостинга в лучшем случае оплачены на непродолжительный срок, что составляет совсем незначительную сумму (в пределах 5-10 долларов США), или вообще являются бесплатными. Это касается всех интернет-мошенников, предлагающих удаленную работу. Проверить историю сайта (на каком хостинге зарегистрирован, на какой срок оплачен хостинг, и др.) можно с помощью специализированных ресурсов в Интернете.

Набор отсканированных текстов

Сплошь и рядом на сайтах, посвященных трудоустройству, а также на досках бесплатных объявлений можно встретить объявления о наборе удаленных сотрудников для набора отсканированного текста. При этом «работодатель» красочно описывает перспективы, высокие расценки и привлекательные заработки – правда, сам при этом не имеет ни сайта, ни контактного телефона, а электронный ящик у него открыт на бесплатном ресурсе. На рис. 1.2 показан пример такого объявления.

Описание объявления «Требуется наборщик текстов»

Требования:

- Знание русского языка, грамотность;
- Знание ПК и офисных программ;
- Доступ в Интернет для поддержки связи с офисом и передачи материала;
- Возраст от 16 лет;
- Место проживания не имеет значения.

Обязанности: Обработка материала любой тематики посредством текстового редактора, это может быть печатный или рукописный отсканированный текст.

Условия: свободный график, сдельная оплата до 30000 рублей в месяц.

Рис. 1.2. Явно сомнительное объявление о вакансии наборщика текстов

Первая мысль, которая приходит в голову после прочтения подобного объявления: если бы это было реально – половина населения России немедленно бросила бы работу и села набирать тексты по свободному графику за 30 000 рублей (фактически 1 000 долларов) в месяц!

Хотя на первый взгляд такая работа кажется вполне реальной: ведь набор текстов – это конкретный вид деятельности, в отличие от той же обработки почтовой корреспонденции или прочих сомнительных предложений. Но после того как вы отправите письмо с предложением своей кандидатуры, вам предложат перечислить некоторую сумму (это может быть и 50, и 100, и 300 рублей, и др.) в счет гарантии того, что вы действительно выполните порученное задание качественно и в срок, либо в качестве залога за присланные вам компакт-диски с заданием, и т. п.

Очевидно, что подобные обоснования «притянуты за уши» и не имеют под собой никаких оснований. Стоит ли говорить, что после отправки мошенникам денег никакого задания вы не получите! А может – получите, и даже выполните его, и отправите мошенникам – только вот денег за выполненную работу вам никто не заплатит.

Стоит отметить, что в последнее время злоумышленники сделали выводы из предыдущих ошибок и иногда готовы прислать по требованию соискателя реквизиты фирмы (адрес, ИНН, банковские счета), а также контактные телефоны. Это делается для того, чтобы усыпить бдительность потенциальных жертв. Вот только ничего общего с реальностью эти реквизиты иметь не будут: такая фирма либо вообще не существует, либо занимается совсем другими видами деятельности. Поэтому желательно уточнить следующие моменты:

- ◆ действительно ли существует такая фирма;
- ◆ действительно ли она находится по указанному адресу;
- ◆ действительно ли она набирает удаленных сотрудников для набора текста;
- ◆ действительно ли это ее телефон;
- ◆ действительно ли по этому телефону отвечает сотрудник данной фирмы (а не кто-то посторонний).

Также всегда полезно дать понять удаленному работодателю, что вы можете подъехать по указанному адресу для личной беседы. Даже если вы живете, например, в Красноярске, а удаленную работу предлагает московский работодатель – попросите адрес фирмы и скажите, что вы хотите побеседовать лично в офисе. Очень может быть, что после этого все дальнейшие вопросы отпадут сами собой...

А вообще помните: отсканированные тексты проще не набирать, а распознавать с помощью специальных программ (например, та же Fine Reader). И если вам предлагают набрать отсканированный рукописный или иной плохо распознаваемый текст – это, возможно, действительно реальная работа, а если текст хорошо распознается специальными программами – то задумайтесь: зачем работодателю платить кому-то за набор текста, если его можно распознать самому быстро, качественно и бесплатно?

Перевод текстов

Как мы уже отмечали ранее, удаленные переводчики также являются потенциальными жертвами мошенников. При этом схема обмана может выглядеть примерно так, как и в ситуации с набором текстов. Ниже мы приводим конкретный пример объявления, которое дали промышляющие подобным образом злоумышленники.

Здравствуйте!

Вас приветствует компания по переводам «Форум». В связи с расширением и увеличением работ мы проводим дополнительный набор сотрудников для удаленной работы, это выгодно и Вам и нам – Вам тем, что Вы в свободное от работы время можете дополнительно зарабатывать, ну а нам – тем что не надо дополнительного места

в офисе.

Условия работы: Вам будет выслан по электронной почте текст в документе WORD. Вам надо будет его перевести, и отправить обратно. Я могу Вам присылать объем работы на день (10 страниц), или же на неделю (50 страниц текста присылаю в понедельник и до воскресенья Вы должны будете прислать уже готовый перевод). График работы Вы устанавливаете себе сами.

Оплата: Перевод текстов с русского на украинский и наоборот (1500грн) в переводчике и соответственно редактирование (на дому). Кто знает испанский или итальянский – зарплата 900 грн. Подробности на e-mail: nabor-text@inbox.ru в теме письма укажите «Работа с текстом».

Автор этой книги не поленился и ради эксперимента написал письмо по указанному адресу. Через некоторое время пришел ответ, который показан на рис. 1.3.

Здравствуйте! Вас приветствует представитель компания "TRANSLATION ORG COMPANY" по переводу текстов. Вам на Вашу почту будут присылать по 10 страниц текста на русском или украинском языке, если у Вас есть переводчик на компьютере - Вы переводите текст. Вы в курсе, что очень часто перевод не всегда соответствует - поэтому Вам надо будет редактировать. Стоимость одной страницы русского - 7грн.15коп, перевод с итальянского или испанского 23грн.80коп. Тексты Вам будут присылать с понедельника по пятницу по 10 страниц текста - в месяц будет получаться 1500 грн.(русский),и 5000грн.(испанский или итальянский). Если Вы не будете успевать или же напротив захотите увеличить Ваш заработок, будете об этом сообщать, и Вам соответственно будут уменьшать или увеличивать объем работы. Выплата заработной платы два раза в месяц. Деньги будут перечисляться на Ваш интернет кошелек, или же на счёт в банке, или же почтовым перевод. Если у Вас еще нету Интернет кошелек, Вы можете его скачать к себе на компьютер по этому адресу:
<http://imoney.com.ua>.

Начало/ работы у нас услуга платная, цена ее 35 гривен (35 UAH). Оплату за регистрацию я возвращаю через неделю.35 гривен изначально нужны мне как залог, что Вы будете в срок и качественно выполнять Вашу работу. Потому что если Вы не выполните работу, которую Вам предоставят-перед агентством буду отвечать я, и выполнять эту работу придется мне, причём в очень краткие сроки.
Если вы будете согласны -напишите в теме СОГЛАСЕН(НА).Если же у Вас есть какое-то недоверие или же вопрос напишите ВОПРОС.

Мы вам гарантируем, что будем выплачивать деньги в срок. Сайта у нас нет, мы работаем только по электронной почте

Мне предоставляют тексты компании по переводу, они же и начисляют день-ги Вам на зарплату, а 35 гривен изначально мне надо как гарантия, что Вы будете в срок и качественно переводить текст. 35 гривен я Вам верну спустя неделю после Вашего перевода, когда я буду убеждена, что Вы качественно выполняете Вашу работу. По-поводу сроков - я могу Вам присылать объем работы на день (10 страниц), или же на неделю (50 страниц текста присылаю в понедельник и до воскресенья Вы должны будете прислать уже готовый перевод). Начислять зарплату я могу или же на Ваш Интернет кошелек, или же на Ваш банковский счёт, или же почтовым переводом.
Когда перечислите деньги на Интернет кошелек - укажите пожалуйста на ка-кой почтовый ящик Вам присылать тексты(на этот, или же Вам будет удоб-нее на какой либо другой).Также ОБЯЗАТЕЛЬНО укажите номер вашего Интернет кошелек, и с какого языка на какой Вы будете переводить. Что бы Вы не думали, что мы исчезнем - давайте для начала заплатим Вам за неделю Вашей работы. А потом уже будем выплачивать по два раза в месяц.
Мой интернет кошелек: 410044338522

Кошелек системы i-money
К сожалению возможно перечислить деньги только на интернет кошелек, и то с интернет кошелек. Потому, что мой горький опыт уже показал, что ко-гда перечисляли деньги с банка или же почтовым переводом на интернет ко-шелек -они просто напросто не приходили. Поэтому, лучше всего будет если Вы скачаете интернет кошелек - пополните его и перечислите деньги - а по-том можете его удалить если Вы предпочитаете получать оплату не через ин-тернет кошелек, а банковским или же почтовым переводом. Просто снять деньги с кошелек банковским переводом или же почтовым быстро и прове-ренно. А если зачислять деньги на интернет кошелек через банк - очень часто деньги просто напросто не доходят.
Всю информацию (как установить, как пополнить счет, снять деньги и т.д.) по кошелеку получите по адресу:
<http://imoney.com.ua>

С уважением, Яна Владимировна!

Рис. 1.3. Ответ, полученный от мошенников

Как видно на рисунке, в ответе полно грамматических, орфографических и стилистических ошибок, а также явных опечаток (может, и номер кошелек указан с ошибкой?). Ну а тот факт, что «сайта у нас нет, и мы работаем только по электронной почте», у любого здравомыслящего человека может вызвать лишь саркастическую улыбку. А если говорить серьезно, то все очень похоже на то, что данное письмо составлено и отправлено автоответчиком. Получается, что деятельность мошенника состоит из следующих этапов:

- ◆ размещение в Интернете объявлений о наборе удаленных переводчиков;
- ◆ настройка автоответчика для автоматической рассылки ответов тем, кто прислал на рассмотрение свои кандидатуры;
- ◆ получение денег из электронного кошелек, который пополняется за счет обманутых соискателей.

Иначе говоря, мошенник даже не утруждает себя тем, чтобы прочесть письма соискателей, а просто периодически проверяет кошелек и получает деньги.

Вырезание, склеивание, обработка, перебирание

В Интернете можно встретить массу объявлений, которых объединяет следующее: в них удаленным работодателям предлагается делать какую-либо надомную работу, не связанную с компьютером, а результат работы высылать бандеролью или посылкой. Есть и еще одна черта, которая является общей для всех подобных объявлений – это, как вы, наверное, уже догадались, требование выслать определенную сумму денег по указанным реквизитам в качестве «залога», «гарантии порядочности» и т. п. Что касается непосредственно вида деятельности, то это может быть все, что угодно: вырезание наклеек или этикеток, упаковка компакт-дисков, склеивание бумажных журавликов, обработка паром изделий из полиэтилена, перебирание черно-белых шариков (!) и их сортировка, и т. п. На рис. 1.4 показан пример такого объявления, в котором речь идет о вырезании этикеток для чая.

Здравствуйте, Вас беспокоит ДП «Heritage Group Ru»!

Спасибо, что откликнулись на наше объявление!!!

В настоящее время наша компания предлагает жителям любых регионов надомную работу по вырезке этикеток для чая.

Предлагаемая работа проста и доступна каждому. Никаких ограничений по возрасту, полу, образованию, месту жительства нет. Мы Вам будем платить по 2 руб. за каждую вырезанную этикетку. Пересылка рабочего материала, готовой продукции, а также оплата труда производится по почте. С Вашей стороны почтовых расходов не будет, т.к. они будут Вам компенсированы при выплате заработной платы.

Готовые этикетки Вы будете отправлять в наш адрес бандеролью.

Если у Вас возникнут сомнения, можете отправить готовые этикетки наложенным платежом, что станет гарантией их выкупа нами.

Количество заготовок этикеток высылаемых одному работнику ограничено - не более 10000 заготовок в месяц. Таким образом, максимальная заработная плата составляет 20000 руб. в месяц. Если для Вас эта норма окажется слишком большой, то Вы можете заказывать меньшее количество заготовок, но не менее 1000 шт. в месяц.

Этикетки служат в качестве элемента защиты нашей продукции от подделок. Они представляют собой форму правильного шестиугольника. Этикетки изготовлены из полимерной голографической пленки, которая портится механической нарезкой, поэтому их необходимо вырезать вручную.

ПОРЯДОК ТРУДОУСТРОЙСТВА

Для начала работы мы высылаем пробную партию заготовок в размере 1000 шт.

Для того чтобы приступить к работе, Вам необходимо внести залоговую сумму за заготовки в размере 300 руб. (или 30000 белорусских рублей) (из расчета 0.30 руб. за заготовку). При отправке нам готовых этикеток залоговая сумма Вам будет возвращена.

Мы не можем высылать заготовки всем желающим бесплатно, т.к. раньше некоторые писали нам из любопытства, не имея серьезных намерений сотрудничать с нами, и не выполняли заказанную работу, в результате чего мы несли убытки, поскольку голографическая пленка, из которой изготовлены заготовки достаточно дорогая.

Заготовки для вырезки мы будем высылать заказной бандеролью.

Более подробные инструкции о порядке расчета наложенного платежа, компенсации почтовых расходов и порядке дальнейшего сотрудничества Вы получите вместе с пробной партией заготовок.

В дальнейшем Вы можете заказывать большее количество заготовок одной бандеролью. Если Вы зарекомендуете себя дисциплинированным сотрудником, то мы, со своей стороны, после выполнения первой партии этикеток освободим Вас от внесения залоговой суммы за заготовки.

Если Вы согласны с условиями поставки первой партии, то пришлите письмо-запрос на получение пробной партии.

В ответ мы отправим Вам реквизиты для оплаты первой партии заготовок.

Наш сайт: <http://tea.imess.net/>

Форум удаленной работы ДП «Heritage Group Ru» heritageru.forum24.ru

С уважением,
менеджер - Ветрова Анна.

Рис. 1.4. Мошенники предлагают вырезать этикетки

Поскольку соискателям предлагается перечислить некий залог в размере 300 российских или 30 000 белорусских рублей (что в любом случае составляет примерно 10 долларов США), то уже ясно, что здесь действуют злоумышленники. Тем же, у кого остались

какие-то иллюзии, рекомендуем обратить внимание на указанный в объявлении сайт: <http://tea.imess.net> (в другом объявлении эта же контора указывает сайт <http://tea.ueuo.com>, что, впрочем, сути дела не меняет). Он располагается на бесплатном хостинге, и сразу возникает вопрос: почему фирма, которая предлагает простую надомную работу за очень неплохие деньги (20 000 рублей – это около 700 долларов США), не может позволить себе платный хостинг? Неужели для нее 10–15 долларов (за эти деньги можно купить хороший хостинг на год) – такая неподъемная сумма? Богатая фирма...

А фраза «Этикетки изготовлены из полимерной голографической пленки, которая портится механической нарезкой, поэтому их необходимо вырезать вручную», способна рассмешить даже безнадежных скептиков и зануд.

Что касается «форума удаленной работы», ссылка на который дается в объявлении, то на нем имеется несколько тем и разделов, посты в которых составлены в едином стиле (видимо, их сочинял специально нанятый человек). Как нетрудно догадаться, почти все посты в этом форуме примерно такого плана: отличная компания, я уже много денег заработал, присоединяйтесь, и т. п. Для разнообразия вставлено несколько постов якобы от сомневающихся («а не обман ли это», «а у вас действительно можно заработать»), которым тут же «отвечают» якобы опытные работники компании («да, не сомневайтесь», «все честно и справедливо»), и т. д. Ну и для пущей «достоверности» есть несколько постов, предупреждающих о том, что «под вывеской нашей честнейшей фирмы появились мошенники, будьте внимательны».

Вот такой «лохотрон».

Переход по ссылкам

Еще один популярный вид интернет-мошенничества состоит в том, что соискателю предлагается зарабатывать деньги путем перехода по ссылкам и посещения определенных веб-ресурсов. Подобных объявлений в Интернете сейчас множество, их можно встретить и на сайтах, посвященных трудоустройству, и на досках бесплатных объявлений. Внешне все выглядит пристойно, но на практике оборачивается полным «пшиком».

Вначале нужно зарегистрироваться в системе и завести себе электронный кошелек (чаще всего требуется WebMoney). За каждый переход по ссылке работнику начисляются либо деньги, либо бонусы, которые в конечном итоге конвертируются в деньги. Доход зачисляется на счет участника системы, откуда он может вывести деньги на свой кошелек.

Но не рассчитывайте на легкий заработок: за каждый переход начисляется мизерная сумма – обычно от одной до нескольких копеек. Таким образом, за день кропотливой и нудной работы вы заработаете максимум несколько рублей (несмотря на то, что вам ранее могли пообещать доход в размере и 300, и 500, и 1000 рублей в день). И учтите, что одними щелчками на ссылках дело может не ограничиться – в некоторых случаях для получения бонуса необходимо ответить на какой-либо несложный вопрос.

Но и это еще не все. У каждого такого сервиса существует правило: вывести деньги из системы на свой электронный кошелек можно только при достижении на счету определенной суммы. Другими словами, пока вы не накопите на счету определенную сумму – вывести деньги вы не сможете. У кого-то этот минимум составляет 10 долларов, у кого-то 20, и т. д. – все зависит от конкретного сервиса. При этом система возьмет с вас комиссию за вывод средств – она обычно составляет около 5 %. Так что если у вас и получится что-то заработать – это, во-первых, будет во много раз меньше того, что вам изначально было обещано, а во-вторых – вывести деньги будет не так просто.

В этой сфере существует немало откровенных мошенников, которые вообще ничего не выплачивают. Иначе говоря, вы можете несколько дней упорно ходить по ссылкам, копить бонусы, а когда на вашем счете накопится достаточная сумма для вывода средств – он или обнулится, или при попытке вывода отобразится сообщение об ошибке.

И еще. В Интернете можно встретить предложения о продаже специальных программ –

сборщиков бонусов. Они якобы избавляют пользователя от необходимости ходить по ссылкам – программа все делает сама, и фактически человек имеет возможность получать деньги, ни прилагая усилий. Учтите, что это обман: почти всегда мошенники продают под видом таких программ какие-нибудь «левые» файлы, но если вам и удастся каким-то чудом приобрести реального сборщика бонусов – вас моментально разоблачат, и ваш аккаунт будет немедленно заблокирован и обнулен.

Платные «комплексы» или «бизнес-пакеты»

Одним из распространенных видов интернет-мошенничества является предложение купить некие «бизнес-пакеты», в которых содержатся все необходимые инструкции для открытия и успешного развития своего прибыльного бизнеса. Расчет злоумышленников строится на том, что вести собственный бизнес, не выходя из дома, и получать умопомрачительные барыши хочет каждый.

На рис. 1.5 показан пример объявления, с помощью которого злоумышленники заманивают потенциальных жертв.

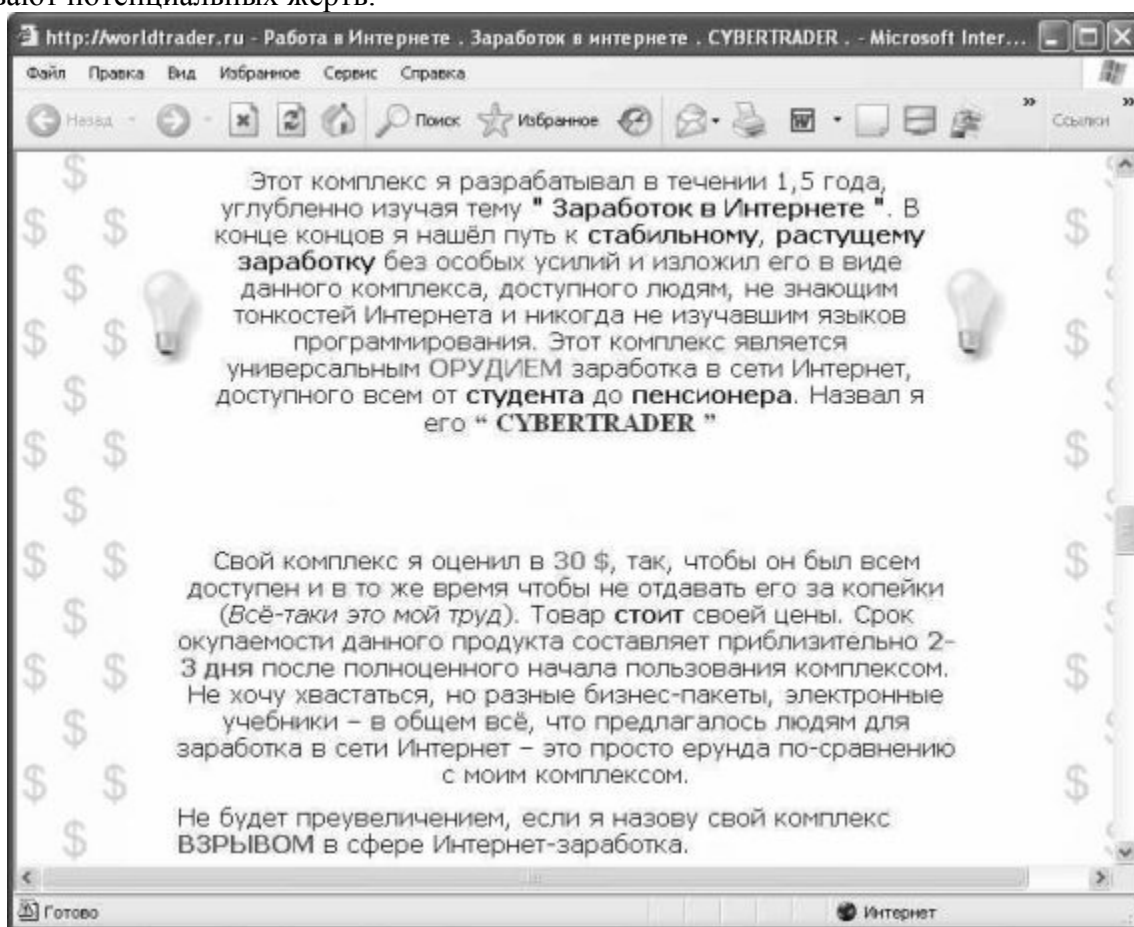


Рис. 1.5. Объявление о продаже платных «комплексов»

Отличительной чертой многих подобных объявлений (и подтверждение тому можно увидеть на рис. 1.5) является то, что мошенник всячески подчеркивает эксклюзивность и уникальность предлагаемого «комплекса» или «бизнес-пакета», по сравнению с которыми все остальные аналоги – полная чепуха. При этом больше никаких подробностей не сообщается, за исключением того, что «вложения окупятся очень быстро, и вы станете сказочно богаты». Да, насчет вложений: обычно за подобное мошенники просят от 10 долларов и выше (могут называться цены и 50, и 100 долларов).

При этом зачастую продажей одного «бизнес-пакета» или «комплекса» афера не

ограничивается. После первого приобретения выясняется, что это лишь первая часть «программы успеха», и чтобы получить вторую (без которой, разумеется, ничего не получится), нужно перечислить еще определенную сумму денег (как правило – больше, чем за первую часть). После второй может последовать третья, и так далее – до того момента, как жертва, наконец, «прозреет» и поймет, что ее попросту немилосердно обманывают.

Иногда мошенники предлагают купить сразу несколько «комплексов». При этом они говорят, что, мол, даже один «комплекс» принесет вам успех, но если вы приобретете два таких «бизнес-пакета» – ваши доходы вырастут в 10 раз, а если три – в 100 раз. При этом один пакет предлагается по цене, предположим, 50 долларов, два пакета – по цене 70 долларов, а 3 пакета – по цене 90 долларов (вроде как создается иллюзия того, что несколько пакетов покупать выгоднее, чем один).

После того как вы перечислите деньги, никакого интереса для злоумышленника вы представлять больше не будете. Впрочем, он может действительно выслать вам какие-то «комплексы» или «бизнес-пакеты» – как правило, это текстовые файлы, иногда «сдобренные» графиками и диаграммами. Но не обольщайтесь, поскольку никакой ценной информации в них содержаться не будет (суть многостраничного документа может сводиться к тому, что «кто не работает – тот не ест»).

Глава 2. Выманивание и кража денег из электронных кошельков

В последние годы стремительно растет популярность платежных интернет-систем, самыми популярными из которых являются WebMoney и Яндекс. Деньги. Иметь электронный кошелек удобно и выгодно: можно проводить платежи и осуществлять покупки, не выходя из дома. Суммы проходящих через них денег постоянно растут, и было бы удивительно, если бы мошенники оставили эту сферу без своего внимания. Вот несколько из примитивных, но в то же время – распространенных и эффективных способов «сравнительно честного отъема денег».

Волшебный кошелек

С помощью спамерского письма либо объявления, которое размещается на бесплатных досках в Интернете, забрасывается примерно такая «наживка»:

Здравствуйте! Я несколько лет занимал руководящую должность в службе технической поддержки компании «WebMoney». Неделю назад меня незаслуженно уволили. Но перед самым увольнением я узнал, что есть такой секретный кошелек, который возвращает переведенную на него сумму увеличенной в три раза максимум через день. Вот его номер: №№№. Пользуйтесь, пока есть возможность – он будет работать еще 35 дней, после чего автоматически ликвидируется!

Жертвами такого «развода» часто становятся пользователи, которые недавно установили себе платежную интернет-систему, не успели разобраться в ней, и потому способны поддаться на такую уловку.

А вот более хитрый способ подобного обмана. Здесь письмо выглядит примерно так же, как процитировано выше, но злоумышленник при этом сам поясняет: мол, это неправда, потому что «когда я отправил на этот кошелек 10 долларов, то на самом деле мне вернулось 20, а когда поверил им и отослал 100 долларов – обратно ничего не получил». Пример такого объявления показан на рис. 2.1.

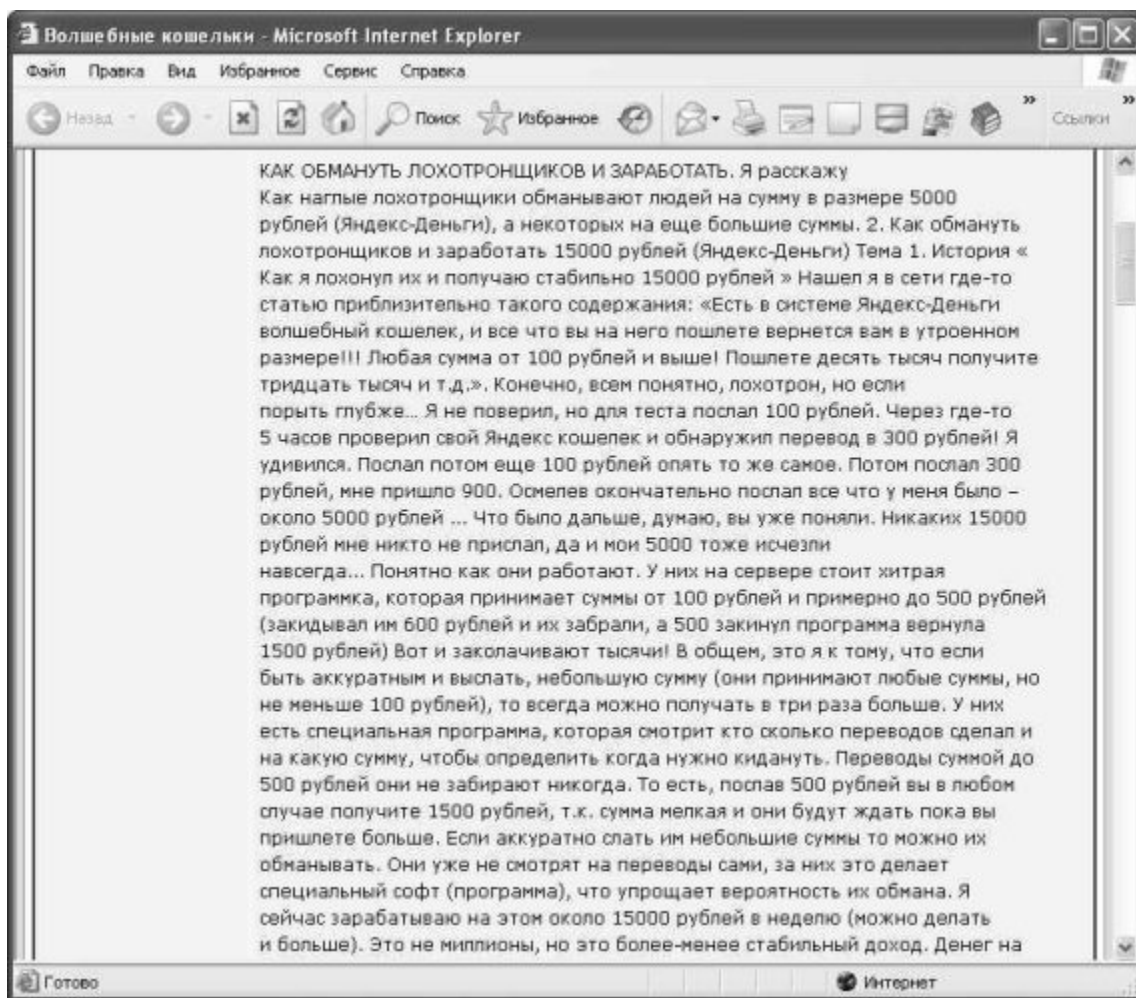


Рис. 2.1. Приманка, которой пользуются мошенники

У человека складывается мнение, что маленькие суммы переводить все же выгодно – и на этом он и попадается.

Можно ли взломать электронный кошелек?

Страсть русского человека к халяве поистине неистребима, чем успешно пользуются мошенники разных мастей. Залезть в чужой электронный кошелек – мечта многих нечистых на руку граждан, но учтите: все подобные попытки завершатся либо неудачей, либо еще и потерей денег из собственного кошелька.

Наберите в любом поисковике фразу «взлом электронного кошелька» или что-то в этом роде – и вам будет предложено огромное количество ссылок по данной теме. Все подобные «предложения» можно разделить на три основные категории.

♦ Различного рода «кряки», программы-взломщики и т. п. Их предлагают за деньги, стоимость подобных «продуктов» варьируется примерно от 10 долларов США до «плюс бесконечности» – здесь все зависит от фантазии и наглости мошенника. Вам скажут, что эта программа подбирает пароль, или умеет обходить файл ключей, вообще – могут «плести» все, что взбредет в голову злоумышленнику. В реальности же после перечисления денег вы либо ничего не получите, либо получите файл с трояном или программой шпионом, который моментально «срисует» идентификационные данные вашего кошелька (идентификатор, пароль, файлы доступа), и передаст эти сведения хозяину. Некоторые трояны умеют не просто воровать учетные данные, но и одновременно менять пароль. В этом случае троян идентифицируется в кошельке под вашим именем с использованием ваших данных, и тут же

меняет пароль, после чего сообщает хозяину новый пароль, в результате чего вы моментально теряете доступ к своему кошельку. Кстати, подобные продукты могут предлагать и бесплатно – в этом случае «лохи» ведутся на приманку практически без сомнений.

♦ WM-генераторы, автоматические переводчики денег, и т. п. Предлагая подобные «продукты», мошенники могут пояснять, что они используют «дырку» в системе защиты WebMoney или протоколе WebMoney Keeper (программы, которая устанавливается на компьютер пользователя для работы с деньгами WebMoney). Стоит ли говорить, что от подобных предложений нужно держаться подальше! Ибо в конечном итоге результат окажется таким же, как рассказано чуть выше.

♦ Специальные сайты для взлома WebMoney, вход на которые может быть как платным, так и бесплатным. Подобные ресурсы предлагают два вида «услуг». В первом случае при посещении сайта на компьютер пользователя автоматически устанавливается программное обеспечение, позволяющее взламывать кошельки. Отметим, что программное обеспечение если и будет установлено – то лишь с целью кражи идентификационных данных вашего WM-кошелька. Во втором случае предлагается заполнить определенную форму на сайте. В ней просят указать: номер кошелька, который вы хотите взломать, а также номер кошелька, на который вы хотите получить похищенные средства, а также (внимание!) – идентификатор и пароль вашего кошелька, путь к файлу ключей и код доступа к файлу ключей. Спрашивается – зачем эти сведения для обычного перевода денег с одного кошелька на другой?

Кстати, платный сайт такого рода может оказаться «меньшим злом», чем бесплатный. Дело в том, что мошенники иногда ограничиваются взиманием денег за вход: возьмут с вас 5-10-20 долларов – и на этом все может закончиться. Если же это ресурс бесплатный – не сомневайтесь, что в компьютер непременно проникнет троян, который моментально «сошьет» все ваши конфиденциальные данные своему хозяину. Хотя такое не исключено и на платных сайтах.

На рис. 2.2 показана страница, на которой предлагается воспользоваться программой для взлома электронных кошельков.



Рис. 2.2. Предложение скачать программу для взлома WM-кошельков

К программе прилагается инструкция, в которой подробно рассказывается, куда распаковать архив и как запустить «взломщика». Чтобы не быть голословными, ниже мы приводим текст такой инструкции, причем самые характерные места выделены жирным шрифтом.

*Установите на компьютер WebMoney Keeper Classic, скачав ее с сайта www.webmoney.ru. Пополните нужный кошелек (3 WMZ или 78 WMR) на нужную сумму. Распакуйте архив WMCrack.rar в любую папку и запустите WMCrack.exe. При этом сам WebMoney Keeper Classic должен быть закрыт. Прежде чем использовать WMCrack, Вам необходимо настроить программу. Для настройки WMCrack нажмите кнопку «Настройки программы» в окошке «кряка» (смотрите скриншот). В открывшемся окне **введите данные Вашего кошелька: WMID – идентификатор Вашего кошелька; введите R-кошелек и Z-кошелек; пароль – пароль от Вашего кошелька; файл ключа *.kwt – файл ключей; файл кошелька *.rwt – файл кошельков (он находится в папке вместе с файлом *.kwt или в папке C: and Settings\пользователь\Data); Пароль доступа – пароль восстановления ключей из резервной копии, Вы его указывали при регистрации; Почта – Ваш электронный адрес, на который Вы регистрировали Ваш кошелек.** Эта почта применяется для отчета, который придет после взлома. Убедитесь в правильности введенных данных («кряк» не может проверять корректность данных) и нажмите «Сохранить». Приступайте к взлому Webmoney. Все наши сайты блокируют, из-за нелегального использования, мы создали ещё пару сайтов, которые опять же заблокировали. Текущий сайт – это уже четвёртый сайт, который также ждёт блокирование. **Вы уже, наверное, задумались, – почему мы вам отдаем этот «кряк» бесплатно потому что, осенью 2009 года у нашей компании был взломан электронный кошелек и сумма на нём была очень большая, мы много раз писали письма в поддержку webmoney, но кто взломал наш кошелек – никто нам на этот вопрос не смог ответить. Поэтому мы создали WMCrack, чтобы мстить Webmoney.***

Орфография и стиль написания инструкции сохранены. Как говорится, по comments.

Вообщем, все предлагаемые в Интернете средства для взлома электронных кошельков объединяет то, что ни одно из них не способно взломать ни один кошелек. И учтите: если бы было так легко взломать электронный кошелек – этим бы занимались все, кому не лень, и в течение максимум нескольких дней вся система WebMoney была бы полностью опустошена.

Подложные письма от службы технической поддержки

Вид мошенничества, о котором мы расскажем в данном разделе, довольно примитивен, но, как ни странно, на него легко «ведутся» многие наши наивные сограждане.

Сущность состоит в том, что пользователь WebMoney или другой платежной системы получает электронное письмо якобы от службы технической поддержки. В нем сообщается, что необходимо подтвердить свои учетные данные, и предлагается выслать их по указанному адресу. При этом могут потребовать указать не только идентификатор и пароль, но также путь к файлу ключей и код доступа к файлу ключей. Как только вы отправите эти сведения – они немедленно попадут к злоумышленникам.

А вот еще один вариант подобной аферы. В данном случае от имени службы технической поддержки у жертвы требуют перевести определенную сумму по указанным реквизитам. В качестве обоснования могут привести все, что угодно: подтверждение работоспособности кошелька, залоговая сумма в счет гарантий порядочности, платное обновление WM Кеерер (без которого программа якобы не будет работать, и доступ к кошельку заблокируется, и т. п.).

ВНИМАНИЕ

Помните: ни одна служба технической поддержки никогда не требует у пользователей системы прислать или подтвердить свои регистрационные данные, либо, тем более – переводить куда-то деньги. Если вы все же сомневаетесь – просто позвоните в службу технической поддержки по телефонам, имеющимся на сайте www.webmoney.ru, или свяжитесь с техподдержкой по электронной почте.

В письме может содержаться ссылка с требованием перейти по ней, и ввести данные на открывшейся странице. Иногда эта страница является полной копией страницы сайта www.webmoney.ru, на которой пользователи системы указывают свои регистрационные данные. Поэтому будьте внимательны, и не ленитесь лишний раз проверить адрес, который отображается в адресной строке вашего интернет-обозревателя.

Подобные письма могут иметь ряд характерных признаков, с помощью которых можно распознать аферистов. В частности – мошенники к вам обращаются не по имени-отчеству или нику, а абстрактно – например, «Уважаемый пользователь системы WebMoney», или что-то в этом роде. Это неудивительно – ведь пока еще они не знают ваших регистрационных данных. Также учтите, что в своих требованиях мошенники могут быть настойчивыми, причем не исключены даже угрозы (мол, не оплатите платную активацию или не пришлете регистрационные данные – потеряете доступ к кошельку, и т. п.).

Виртуальные обменники

Одним из самых удобных интернет-сервисов являются электронные (виртуальные) обменные пункты, в которых можно обменять одну электронную валюту на другую. Например, вы хотите заплатить за телефон, но у вас в кошельке имеются только доллары, а мобильный оператор принимает оплату исключительно в рублях. В этом случае можно воспользоваться услугами многочисленных виртуальных обменников: процесс обмена занимает не более пары минут, курс вполне приемлемый, и все это можно сделать, не выходя из дома.

Найти электронный обменный пункт просто – нужно лишь набрать в любом поисковике соответствующий запрос. Выбор валют в виртуальных обменниках, как правило, хороший: здесь можно найти не только доллары или евро, но и, например, валюты стран СНГ. На сайте электронного обменного пункта вам предложат указать кошелек, с которого вы отдадите одну валюту, и кошелек, на который будет зачислена другая валюта.

И все было бы хорошо, если бы в этой сфере не вели активную деятельность мошенники. Под маской виртуальных обменников они обманывают доверчивых людей, причем зачастую это выглядит донельзя примитивно: вы перечисляете мошенникам деньги – и на этом все заканчивается.

Если вы являетесь обладателем WM-кошелька, то для обмена валют лучше использовать собственный сервис WebMoney. Для этого в программе WebMoney Keeper выполните команду контекстного меню Обменять □ Обменять WM на WM – в результате откроется окно автомата по обмену валют (рис. 2.3).

Автомат по обмену WMZ, WMR, WME, WMU сервиса Exchanger.RU

В нашем автомате Вы можете купить нужную Вам WM-валюту:

КУПЛЮ: max **19100000** WMR

ЗАПЛАЧУ:

Укажите пожалуйста ОДНУ (которую Вам удобно заполнить) из трех перечисленных ниже сумм, остальные две пересчитаются и заполняются автоматически:

Курс WMR/WMZ	31,1409
Сколько у Вас есть (должно быть) WMZ (сколько Вы хотите обменять)	<input type="text" value="50"/>
Сколько это будет WMZ с учетом +0.8% комиссии WMT	<input type="text" value="50.4"/>
Сколько Вы получите (нужно получить) WMR (сколько Вы хотите получить)	<input type="text" value="1557.04"/>
WMR кошелек на который будете получать (кошелек Вашего идентификатора 163989147778)	<input type="text" value="R346976716525 Российски"/>

Если Вы согласны с [правилами и алгоритмом работы автомата](#) и согласны с условиями данной сделки, то нажимайте кнопку Оплатить заявку.

Если Вы не успеете определиться с обменом за **81** секунд страницу необходимо будет обновить

Рис. 2.3. Автомат по обмену валют в программе WebMoney Keeper

В соответствующих раскрывающихся списках данного окна нужно указать, какую валюты вы продаете, какую – покупаете, кошелек для зачисления денег, а также сумму продаваемой валюты. Курс обмена отображается автоматически после выбора валют. Программа автоматически рассчитает сумму продаваемой валюты с учетом комиссии системы, которая будет снята с вашего кошелька, и покажет сумму, которая будет зачислена на соответствующий кошелек после обмена (для этого нужно нажать кнопку Оплатить заявку и следовать появляющимся на экране указаниям). Отметим, что подобные обменники имеются и в некоторых других платежных системах.

Если же вы решили воспользоваться услугами сторонних обменных пунктов – будьте внимательны и осторожны. Надо отдать злоумышленникам должное – они умеют сделать сайт, который может не вызвать подозрений даже у опытных пользователей, регулярно пользующихся услугами электронных обменных пунктов. По крайней мере, внешне все может выглядеть вполне прилично. Чтобы минимизировать возможность обмана, следуйте перечисленным ниже рекомендациям.

♦ Если по каким-то причинам вы не хотите пользоваться обменным автоматом платежной системы – обращайтесь к услугам только тех электронных обменных пунктов, в которых вы уверены (например, неоднократно работали с ними ранее). Если вы впервые меняете деньги – обратитесь к более опытным знакомым, чтобы они порекомендовали вам надежный виртуальный обменник.

♦ Если вы человек неопытный, а рекомендаций попросить не у кого – можете посмотреть содержимое черных списков обменников. Найти такие списки можно с помощью любого поисковика. Можно также просто ввести адрес электронного обменного пункта, вызвавшего у вас подозрения, в поисковую систему, и ознакомиться с результатами поиска.

♦ Если вы проверили обменный пункт «со всех сторон», но сомнения у вас остались – либо откажитесь от него, либо попробуйте обменять незначительную сумму. Если все прошло успешно – отправьте сумму побольше. **В любом случае крупные суммы менять за один раз не рекомендуется, даже если вы пользуетесь проверенным и вроде бы надежным обменником.**

♦ У любого честного обменного пункта имеется лимит на сумму обмена по каждой валюте. Это зависит от того, сколько электронных денег имеется в обменном пункте. Например, если в наличии есть 1000 долларов США, 100 000 российских рублей и 2000 евро, то и менять валюту можно только в этих пределах (то есть больше 1 000 долларов вы купить в данный момент не сможете). Бывает и так, что какой-то валюты нет в наличии, или ее совсем немного. Информация о максимальной сумме обмена всегда имеется на сайте обменного пункта. Если же такой информации нет – скорее всего, вы имеете дело с мошенниками (у них все просто – чем больше пришлют денег, тем лучше).

♦ Фальшивые обменные пункты почти всегда размещаются на бесплатных хостинговых площадках. Иногда они пользуются платным хостингом, но всегда – дешевым, причем оплачивают его ненадолго (поскольку понимают, что длительное время такой ресурс не просуществует – его просто заблокируют).

Ни в коем случае не переводите деньги на обмен, если у вас имеются какие-то сомнения относительно честности электронного обменного пункта. Помните, что в случае обмана вернуть перечисленные мошенникам деньги невозможно.

И опять обмен валют

Прикрываясь обменом валют, мошенники могут действовать и более изощренно. Справедливости ради отметим, что им очень помогает жадность и алчность пользователей, желающих быстро обогатиться, не прилагая для этого никаких усилий.

Итак, первое, что делает мошенник – это регистрирует доменное имя и заказывает хостинг (либо бесплатный, либо предельно дешевый). После этого он создает англоязычный сайт привлекательного дизайна, солидно оформленный и вообще вызывающий доверие. Как правило, он копирует дизайн и оформление известных зарубежных виртуальных обменников. Сайт оформляется от имени серьезной зарубежной организации, которая на протяжении многих лет якобы осуществляет активную деятельность в сфере финансов. На этом сайте предлагается обменять валюту в направлении **USD E-Gold – WMZ**, причем зачастую это единственное направление, в котором работает «серьезная и солидная финансовая компания». Для правдоподобности здесь могут предлагаться и другие направления обмена валют, но все они будут «временно недоступны» (в данном случае это явный признак того, что сайт является мошенническим!).

После этого мошенник заводит русскоязычную веб-страничку (как правило, на бесплатном хостинге), с минимумом дизайна и практически без всякого оформления. На этой странице он красочно описывает новый метод быстрого обогащения, суть которого состоит в следующем: нужно обменять имеющиеся WMZ на USD E-Gold в любом обменнике (для примера обычно приводятся известные электронные обменные пункты, тот же RoboXchange), после чего на «сайте одной зарубежной компании» (здесь он дает ссылку на свой англоязычный «обменник») их можно обменять обратно по очень выгодному курсу. Повторяя эти операции, якобы можно постепенно наращивать свой капитал, в результате чего он многократно увеличится.

Стоит ли говорить, что все деньги, перечисленные доверчивыми жертвами для обмена, оседают в кармане преступника!

Ссылку на эту русскоязычную страницу злоумышленник помещает на досках бесплатных объявлений, рассылает со спамовыми письмами, вообще – всячески «раскручивает» и «оптимизирует» свой проект. Ну а после этого ему остается лишь сидеть перед компьютером и периодически проверять свой электронный кошелек, на который будут

приходить деньги от доверчивых любителей халявы.

Иногда на подобных мошеннических ресурсах устанавливается минимальная сумма обмена. Это своего рода защита от бдительных посетителей. Ведь многие люди очень осторожно пользуются неизвестными обменниками (и это правильно!), и для пробы посылают для обмена небольшие суммы (один-два доллара). Чтобы исключить подобное, мошенник сразу указывает, что операции с суммами меньше, например, 10 или 20 долларов не проводятся.

Предложение работать «оператором WebMoney»

Мошеннический прием, с которым мы познакомим вас в данном разделе, появился относительно недавно, но быстро завоевал популярность у интернет-злоумышленников.

Сущность его заключается в том, что вам предлагается поработать оператором системы WebMoney. Заманчиво, не так ли? А должностные обязанности выглядят еще более привлекательно: вам нужно будет лишь получать на свой кошелек чужие деньги, и переводить их по указанным реквизитам. И за эту приятную работу вам будут платить: 650\$ в месяц – при работе каждый день, 500\$ в месяц – при пятидневке, и 150\$ – при работе только в выходные дни. На рис. 2.4 показан пример такого объявления, размещенного на одном из российских сайтов.



Теперь расскажем Вам подробнее о работе:Наша компания создаёт для Вас новый рабочий счет.Получаем на него Персональный аттестат.Аттестат оформляется на юридическое лицо. Тем самым Мы гарантируем Вам прозрачность всех операций и нашу честность. В самом аттестате будет вписан Ваш электронный адрес.Это делается для того, чтобы в будущем аттестат можно было полностью переоформить на Вас. Таким образом, если Вы решите отказаться от работы, то рабочий аттестат останется за Вами. Аттестация счета требуется для ведения честного бизнеса в переводах средствУ Вас не должно быть ошибок в переводах, так как их исправить сможем только Мы.Ваша работа будет заключаться в следующем:На Ваш Рабочий кошелек каждый день будут приходить средства и указания, в которых будет подробно описано какую сумму и на какие кошельки Вам следует перевести деньги (WMR,WMZ).Ежедневные переводы, а их будет от 30 до 70, нужно осуществить в течение суток. В среднем на каждый перевод у Вас будет уходить 2-3 минуты.Данная Работа предполагается на дому ,т.к. предполагается не полная занятость (3-5 часа). Данная Работа предполагается, как подработка в свободное время.Ваша будущая Работа не будет связана с пирамидами, сетевым маркетингом,поиском клиентов итд. В будущем с опытом у Вас будет уходить меньше времени на обработку платежей.Нам выгодно нанимать сотрудников на дому ,так как не требуется содержания офиса. Оплата Интернета за счет работника.Зарплата за месяц зависит от графика и составляет 650\$ в месяц при работе каждый день,500\$ в месяц при пятидневке и 150\$ только в выходные дни.Определиться с графиком работы Вам надо сейчас.Для работы Вам нужно будет скачать программу WM Keeper Classic 3.5.0.2(<http://www.webmoney.ru/download.shtml>). Для работы подойдет любая версия кипера .Если Вы никогда не пользовались WebMoney, Мы думаем, что Вам не составит труда понять, как работает программа.Если Вы сами не сможете разобраться в программе, тогда Мы Вам пришлём информации ответим на вопросы по установке. Пришлем пошаговые инструкции, как начать работу.Таким образом, нам нужна гарантия того, что не получится так, что мы откроем счет,получим аттестат, затратив на это деньги, а Вы исчезните на следующий день. Такой гарантиейвыступают 17 WMZ (USD) или 500 WMR (Руб) которые Вы оплачиваете за Аттестацию дилеру. Аттестация, в таком случае занимаем 2 дня, после чего Вы сразу приступаете к работе по мере Вашей готовности. Можем посоветовать Вам оформить пластиковую карту в любом крупном банке для получения ЗП. Тогда Вы будете без комиссии снимать Вашу ЗП. Удобно оформить пластиковую карту в Сбербанке.В итоге: У Вас будет 2 кошелька: 1 - для ЗП,2-рабочий(с Персональным аттестатом, который Вы оплачиваете и получите после оплаты аттестации). Таким образом, наш риск уменьшается.Пока Вы работаете у нас - аттестат оформлен будет на нашу организацию.Сразу уточняем: Рабочий Аттестат будет оформлен не на физическое лицо ,а на юридическое ,то есть на нашу организацию.В самом аттестате будет вписан Ваш электронный адрес.Если Вы решили взяться за эту работу, Вам нужно дать свой ответ, и в течении трех дней перевести выше указанную сумму на наш Z-кошелёк или R-кошелёк.После оплаты Аттестации Вашего рабочего счета - Мы приступаем к созданию и аттестации кошелька, получаем для него (Персональный)аттестат. Это займет 1-2 дня. После чего, мы присылаем Вам файл-ключ, идентификатор и парольдля доступа. Код активации придет на Ваш электронный адрес, на который оформляется аттестат.Если Вы будете готовы к работе, то сразу сможете приступить к выполнению заданий.С этого дня Вы будете работать на нас и соответственно будет начисляться зарплата.Если у Вас появятся вопросы задавайте их на workmoney@fxt.ru

Рис. 2.4. Приглашение поработать «оператором WebMoney»

Особую улыбку вызывает требование перечислить деньги за какую-то липовую аттестацию. Кроме этого, объявление изобилует огромным количеством грамматических и стилистических ошибок – как, впрочем, и многие другие подобные фальшивки.

Обратите внимание – в объявлении из всех контактных данных имеется только электронный адрес. Даже сайт «солидная компания» сделать не удосужилась. Если вы

напишете по указанному адресу письмо с требованием прислать реквизиты фирмы (ИНН, юридический адрес, контактные телефоны, банковские реквизиты и др.) – не сомневайтесь, что ответа вы не получите.

Обман с автоматическими сборщиками денег

Одним из распространенных мошеннических способов является продажа программ, которые якобы умеют собирать деньги из чужих электронных кошельков и доставлять их в указанный кошелек. Эти «программы» мошенники называют автоматическими сборщиками денег.

Характерной особенностью является то, что стоимость такой программы намного меньше, чем она якобы может собрать денег всего за один день. Иначе говоря, лишь за пару часов она окупится, и вы будете получать прибыль! Обычно стоимость таких «программ» злоумышленники оценивают примерно в 10–20 долларов США, при этом гарантируя, что за один день программа соберет с чужих кошельков минимум 80-100 долларов.

Поражает наивность людей, которые способны поверить в подобную белиберду, но они находятся, причем таких «лохов» немало. Видимо, страсть к халяве и быстрому сказочному обогащению у некоторых людей затмевает разум – за что, собственно, и приходится платить. Во-первых, ни один подобный «автоматический сборщик денег» не способен похищать деньги с чужих кошельков (это в принципе исключено самой конструкцией системы электронных платежей, независимо от того, какую систему вы используете – WebMoney, Яндекс. Деньги или др.). Во-вторых, если после перечисления денег мошенник вам ничего не пришлет – это еще далеко не самый худший вариант, поскольку за ваши деньги вам могут прислать вирус, троян, шпионский модель и вообще что угодно, только не «автоматический сборщик денег».

Для рекламы «автоматических сборщиков» злоумышленники специально создают сайты – ведь продукт вызывает намного больше доверия, если у него есть свой сайт. Учтите, что такие сайты могут располагаться на хороших платных хостингах, иметь привлекательный дизайн и грамотно составленный контент. На сайте может работать форум или иметься гостевая книга – правда, ни один критический пост вы опубликовать не сможете, поскольку будет действовать жесткая модерация (по умолчанию возможность «прямой речи» просто блокируется). Некоторые особо «продвинутые» мошенники идут дальше: они специально создают в Интернете подделки на свой же сайт, и на своем сайте дают ссылки на эти подделки с предупреждением – мол, берегитесь, там мошенники, они подделали мой сайт и прикрываются моим честным именем!

Помните: никаких автоматических сборщиков денег с чужих электронных кошельков не бывает, и не может быть в принципе. И не забывайте, что бесплатный сыр бывает только в мышеловке.

Программа для генерирования карт WebMoney

Похожий способ «развода» доверчивых обывателей на деньги состоит в том, что вам предлагается купить так называемый WebMoney-генератор – программу, которая автоматически генерирует коды карт WebMoney. Стоимость такой «программы» у мошенников составляет от 10 долларов США до «плюс бесконечности», а главное ее «достоинство» якобы состоит в том, что с помощью генерирования кода можно быстро пополнить собственный кошелек суммой 100 долларов США.

Первый вопрос, который должен возникнуть при появлении такого предложения – почему же такая волшебная программа стоит так дешево, и зачем кому-то делиться таким замечательным изобретением, а не использовать его только для себя? Если вы зададите мошенникам такой вопрос, то либо не получите ответа, либо вам ответят в том духе, что, мол, возможности программы ограничены, и более чем на 100 долларов один и тот же

кошелек вы пополнить не сможете. Ответ явно неубедительный, однако многие будущие жертвы «развода» об этом не задумываются, и охотно перечисляют мошенникам деньги.

Что будет дальше – догадаться несложно: либо на ваши вопросы и письма перестанут отвечать, либо пришлют дистрибутив со шпионским модулем или троянской программой, который позволит мошеннику получить удаленный доступ к вашему компьютеру. Помните, что создать подобный WebMoney-генератор невозможно в принципе – во многом потому, что коды WebMoney-карт генерируются случайным образом.

Глава 3. Обман в интернет-магазинах

Интернет-магазины относятся к числу наиболее удобных и востребованных интернет-сервисов. Это неудивительно: ведь приобретение товаров в интернет-магазинах имеет целый ряд неоспоримых преимуществ. Например, товары, приобретаемые в интернет-магазинах, стоят значительно дешевле, чем аналогичные товары в стационарных торговых точках. В некоторых случаях разница в цене может достигать 30–50%! Чтобы купить товар в интернет-магазине, не нужно никуда идти – достаточно иметь компьютер с выходом в Интернет. Заказать покупку можно, например, из дома, или со своего рабочего места – и через некоторое время товар будет доставлен курьером по указанному вами адресу. К тому же интернет-магазины предлагают очень широкий ассортимент продукции, которым зачастую не могут похвастаться стационарные магазины.

Было бы странно, если столь мощный сегмент остался без внимания мошенников, и в этой главе мы расскажем, как обманывают доверчивых покупателей в интернет-магазинах или их подделках.

Правила совершения покупок в интернет-магазине

При покупке товаров в интернет-магазинах следует соблюдать определенные меры предосторожности, чтобы не стать жертвой мошенников (которые могут, например, подсунуть некачественный или поддельный товар). Некоторые из таких мер перечислены ниже.

- ◆ Рекомендуется совершать покупки только в известных интернет-магазинах, реклама которых, например, у всех на слуху или которыми уже пользовались ваши знакомые.

- ◆ На сайте хорошего интернет-магазина обязательно должен быть указан один или несколько контактных телефонов. Рекомендуется позвонить по этому телефону и побеседовать с представителем магазина (например, спросить его о том, как давно на рынке работает данный магазин, задать пару вопросов об ассортименте товара, о распространяемых на товар гарантиях, и т. д.).

- ◆ При получении товара следует проверить документацию на него (разумеется, если таковая должна быть; например, не стоит требовать технический паспорт на ковер или кастрюлю, а вот на электрочайник, мобильный телефон или ионизатор воздуха – нужно потребовать).

- ◆ При получении товара обязательно следует поинтересоваться условиями гарантийного обслуживания, а также проверить исправность своей покупки.

- ◆ Не стоит забывать, что при возникновении каких-либо подозрений вы вполне можете отказаться от покупки – никто не вправе заставить вас за нее платить.

И постарайтесь узнать, где находится не виртуальный, а «живой» адрес интернет-магазина (офис, стационарная торговая точка, и т. п.).

Неоправданная дешевизна товара

Относительно недавно (пару лет назад) в Рунете стали появляться рекламные

объявления от интернет-магазинов, реализующих продукцию по откровенной дешевке – всего за 20–40 % от их примерной рыночной стоимости. Такая ценовая политика объяснялась тем, что, мол, эта продукция приобретена по краденым кредитным картам за рубежом и доставлена в Россию.

Стоит ли говорить, что находилась масса желающих «затариться» по дешевке! Люди, позарившись на низкие цены, переводили злоумышленникам немалые средства. Причем перечисление осуществлялось не через банковские учреждения и не почтовыми переводами, а только через WebMoney либо другую платежную Интернет-систему, благодаря чему мошенники сохраняли свою анонимность.

Разумеется, ни один клиент не получил оплаченный товар, поскольку все деньги благополучно достались мошенникам.

Фальшивая витрина

Вид мошенничества, о котором мы здесь расскажем, возник в скором времени после появления первых интернет-магазинов. Он довольно прост, но, тем не менее, от него пострадало достаточно много людей.

Сущность заключается в том, что мошенники, купив соответствующий скрипт и зарегистрировав доменное имя, рисуют витрину, похожую на настоящий интернет-магазин. Выставляться «на продажу» может все, что угодно – как и в любом другом интернет-магазине. Разница заключается в том, что цены, как правило, являются весьма привлекательными. Самый простой вариант – когда покупателю просто не высылается оплаченный им товар. Иногда мошенники позволяют себе дополнительно поиздеваться над жертвой – например, известен случай, когда вместо оплаченного ноутбука обманутому покупателю прислали его картонную копию, причем с учетом мелких деталей (разъемы, порты, копия клавиатуры, и др.).

Ситуация намного усложняется, когда цель создания аферы – хищение денег с кредитных карт потенциальных покупателей. В этом случае сумма причиненного ущерба не ограничивается только суммой «покупки»: с кредитной карты будут похищены все деньги. В данном случае на сайте фальшивого магазина может действовать специальная программа или код, запоминающий реквизиты кредитной карты жертвы.

«Плавающая» цена в интернет-магазине

Вид мошенничества, о котором мы здесь расскажем, охотно используется как мелкими, так и крупными, уважаемыми и известными интернет-магазинами. Он был позаимствован у реальных супер- и гипермаркетов, которые часто грешат подобным выманиванием денег у покупателей.

Покупатель заходит на сайт интернет-магазина и видит, что цены на интересующие товары его вполне устраивают. После непродолжительного выбора он оформляет заказ и ждет доставки. Но при получении товара выясняется, что его цена отличается от той, что была указана на сайте. Как правило, эта разница относительно невелика, к тому же при желании покупатель может отказаться от покупки. Но в большинстве случаев товар все же приобретается – хотя бы потому, что человек уже настроился на покупку, и не хочет отказываться от нее ради небольшой переплаты. При большом количестве покупателей интернет-магазин с помощью этого нехитрого приема может дополнительно получать неплохую прибыль.

Отметим, что разницу в цене иногда можно заметить еще на стадии оформления заказа. То есть на витрине указана одна цена, а в форме заказа – другая. Опять же, вы можете отказаться от покупки – но на практике большинство покупателей соглашается переплатить небольшую сумму, чем вновь искать интересующий товар.

Розыгрыши и лотереи в интернет-магазинах

Различного рода конкурсы, розыгрыши и лотереи – неотъемлемая часть современной торговли. С помощью таких нехитрых приемов коммерсанты привлекают покупателей, а мошенники от интернет-торговли – обманывают людей.

Сущность заключается в том, что покупателям обещают участие в розыгрыше или лотерее, где можно выиграть дорогую вещь (домашний кинотеатр, музыкальный центр, плазменный телевизор, мебель, автомобиль и т. п.). Для участия в этом мероприятии нужно купить в магазине одну или несколько дешевых вещей (открытки, компакт-диски, шариковые ручки и т. п.). Поскольку стоят такие мелочи совсем немного, находится масса желающих поучаствовать в розыгрыше крупных привлекательных призов, попутно купив себе какую-то мелочевку (мол, в хозяйстве все сгодится).

Стоит ли говорить, что в реальности никто никаких розыгрышей и лотерей не проводит! Подобные ухищрения – не что иное, как самый настоящий «лохотрон». Известно, что многие интернет-магазины, даже довольно крупные и известные, сбывают всякую мелочь именно под видом участия в розыгрышах и лотереях. И учтите, что подобным образом интернет-магазины могут избавляться также от залежалого и некондиционного товара.

Продажа некондиционного или «б/у» товара

Любой продавец желает всеми правдами и неправдами избавиться от некондиционного товара. Здесь возможны три варианта: продать этот товар покупателю, вернуть его поставщику или, списав на убытки, оставить себе. Очевидно, что большинство коммерсантов предпочитают решать данную проблему первым способом: ведь поставщики очень не любят принимать товар обратно (при этом они до последнего убеждают, что передали в торговую точку хороший товар, а им пытаются вернуть плохой), ну а если списывать все подобные расходы на себя, то торговля может оказаться невыгодной.

Такой товар обычно присутствует на витрине наравне со всеми остальными товарами. Его описание на первый взгляд ничем не отличается – правда, цена может быть ниже, чем у имеющихся аналогов. Этот фактор должен насторожить особо: почему это вдруг данный товар стоит дешевле?

В подобных случаях рекомендуется повнимательней присмотреться к описанию товара на его странице, в частности – обратить внимание, нет ли где-нибудь текста, набранного мелким шрифтом. Обычно мошенники помещают на страницу некондиционного товара информацию об имеющихся дефектах – чтобы обезопасить себя на случай непредвиденных обстоятельств (например, если человек решит обратиться в правоохранительные органы). Например, где-то в нижнем углу мелкими буквами может быть написано: «треснута крышка», «подтекает уплотнитель», «товар продается без гарантии», «обшарпанный внешний вид», и т. п.

Аналогичным образом интернет-магазины могут реализовывать товар, бывший в употреблении. Причем в некоторых торговых точках оборот от продажи такого товара составляет более 50 %. Здесь ситуация аналогична – товар продается значительно дешевле имеющихся аналогов, а на странице с его описанием мелкими буквами может быть написано, что «товар был в употреблении», «товар продается без гарантии», и т. п.

ВНИМАНИЕ

Часто некондиционный или бывший в употреблении товар доставляется покупателю не курьером, а по обычной почте (например, наложенным платежом, или после совершенной на сайте магазина предварительной оплаты). В такой ситуации покупателю попросту некому предъявлять претензии.

Из всего этого можно сделать вывод: если вам предлагают товар по неоправданно

низкой цене – скорее всего, здесь дело нечисто.

Глава 4. Обман в интернет-лотереях, казино и на аукционах

Интернет-лотереи, электронные аукционы и виртуальные казино (рис. 4.1) – настоящий Клондайк для мошенников разных мастей.



Рис. 4.1. Главная страница интернет-казино

Далее мы расскажем о том, как злоумышленники выманивают деньги у некоторых излишне азартных, и в то же время – доверчивых граждан.

Фальшивое казино

Самый примитивный способ «развода» на деньги – организация фальшивых интернет-казино. Мошенники «рисуют» красивый сайт с привлекательным дизайном, яркими картинками и баннерами, и т. д. Всем желающим предлагается принять участие в игре, «вероятность выигрыша в которой составляет 70 %» (процент может быть разный – в зависимости от наглости мошенников).

Самое интересное заключается в том, что никакой игры в таком казино на самом деле не ведется. Хотя выглядеть все может очень прилично: игроки делают ставки, и т. д. но на самом деле деньги сразу попадают в кошельки злоумышленников, а незадачливый игрок получает сообщение «Сожалеем, Вы не выиграли, но Вам обязательно повезет в следующий раз» или нечто в этом роде.

Существует и иной вид мошенничества – когда за участие в игре предлагается пройти платную регистрацию. Это, конечно, уже верх цинизма – игрок готов играть и оставлять

деньги в казино, а ему предлагают еще и платно зарегистрироваться за это! После оплаты регистрации жертве предлагается какое-то время подождать – мол, на электронный адрес придет письмо с инструкциями об «активации статуса игрока» (или нечто подобное). Стоит ли говорить, что никакие писем мошенники не присылают!

Отметим, что злоумышленники в подобных ситуациях могут прикрываться названиями или адресами настоящих интернет-казино, в которых игра ведется по-честному. Например, в рекламном объявлении может быть сказано примерно следующее: мол, игра ведется по этому адресу, но регистрация игроков нашего казино осуществляется на другом сайте, для перехода на который используйте эту ссылку. Поскольку злоумышленники прикрываются настоящим, честным казино, то даже если вы захотите проверить это казино (например, можно почитать отзывы о нем игроков в Интернете, ознакомиться с черными списками и т. п.) – у вас может не возникнуть никаких подозрений. Перейдя по ссылке, вы регистрируетесь на постороннем сайте, отправляете мошенникам деньги – и после этого они попросту забывают о вашем существовании.

Помните: если вам предлагают платную регистрацию за право играть в казино – это, скорее всего, самый обыкновенный «лохотрон».

Задержка с выводом средств

Вывод средств, полученных в результате выигрыша в интернет-казино или лотерее – еще одна лазейка, позволяющая мошенникам получать дополнительные деньги, а точнее – успешно избегать причитающихся игрокам выплат выигранных сумм.

Не секрет, что во многих казино вывод средств с баланса игрока на его электронный кошелек осуществляется не сразу, а через определенное время, которое может составлять как несколько часов, так и несколько дней. Алгоритм действий выглядит примерно так: игрок оформляет заявку на вывод средств – и через некоторое время в его кошелек поступают деньги. Все время, на протяжении которого обрабатывается заявка, деньги продолжают числиться на балансе продавца, и он в любой момент может воспользоваться ими для участия в игре.

Этим и пользуются мошенники от лотерейного бизнеса. Всеми правдами и неправдами они уговаривают клиента сыграть еще раз – мол, если уж вам повезло, то будет везти и дальше, все равно деньги у вас на балансе есть, попробуйте увеличить выигрыш и т. д. Если человек пойдет у них на поводу – он наверняка «спустит» все имеющиеся деньги в казино, не дожидаясь их вывода из системы. Чего, собственно, и добиваются злоумышленники. Очевидно, что в подобной ситуации с точки зрения закона все выглядит безупречно, поэтому привлечь мошенников к ответственности не удастся.

Заманчивый лот на аукционе

Одной из распространенных форм интернет-торговли является организация и проведение аукционов. На онлайн-аукционах можно найти все, что угодно: бытовую технику, антиквариат, сувениры, автомобили, одежду, обувь, товары для детей, предметы досуга, и т. д. Поскольку число участников электронных аукционов постоянно растет, эта сфера деятельности не могла остаться без внимания мошенников.

Один из распространенных видов обмана заключается в следующем. После проведения торгов участнику, которому не достался выгодный лот, приходит по электронной почте письмо примерно следующего содержания:

Добрый день!

Как нам стало известно, вы хотели приобрести на нашем аукционе такой-то товар, но лот выиграл другой покупатель. Спешим вас обрадовать: впоследствии он передумал и отказался от покупки, поэтому вы можете реализовать свою мечту и приобрести то, что

хотели. Правда, поскольку аукционные торги уже завершились, оформлять сделку придется в частном порядке. Если вы согласны – перейдите по следующей ссылке за дополнительными сведениями.

С уважением, администрация аукциона.

Когда клиент переходит по указанной ссылке, то попадает на сайт мошенников, где ему предлагается перевести деньги за покупку по указанным реквизитам (как правило, перевод денег осуществляется посредством электронной платежной интернет-системы). После отправки денег связь с мошенникам обрывается – они не отвечают на письма, а их сайт зачастую быстро исчезает.

Чтобы не стать жертвой подобного мошенничества, избегайте совершения сделок вне аукционной площадки, какие бы заманчивые предложения вам не делались. Если же соблазн столь велик, что вы не можете устоять – не переводите деньги, пока не наведете необходимые справки по телефону и не убедитесь в том, что вы имеете дело с реальным продавцом, а не с мошенником. Дополнительную настороженность должен вызывать факт расчета с помощью электронной платежной системы.

Мобильный аукцион

Данный вид мошенничества появился несколько лет назад, и активно практикуется не только в Интернете, но и на телевидении. Злоумышленники откровенно не боятся никакой ответственности, поскольку с точки зрения действующего законодательства их действия нарушением закона не являются (а если и является, то доказать их вину практически невозможно).

В один прекрасный день человеку попадает на глаза объявление, в котором ему предлагается принять участие в аукционе или викторине. Сущность игры состоит в том, что нужно правильно ответить на один или несколько несложных вопросов, что даст право участия в розыгрыше привлекательных призов (мобильные телефоны, ноутбуки, телевизоры, бытовая техника, мебель, оплаченное путешествие и др.). Ответ нужно прислать в виде СМС-сообщения, которое (внимание!) является платным (причем иногда его стоимость является довольно чувствительной). Если вопросов несколько – то ответ на каждый из них необходимо присылать отдельным СМС-сообщением (то есть одной «эсэмэской» отвечать сразу на все вопросы не разрешается).

Ну а дальше все зависит только от наглости и фантазии мошенников. Самый простой вариант – когда в реальности никакой аукцион или викторина не проводится, и мошенники, получив свои деньги от околпаченных людей, попросту исчезают. Иногда же людям действительно выдаются выигранные призы – но их стоимость, как правило, значительно меньше стоимости отправленных СМС. Но даже в этом случае стоимость получения хоть какого-нибудь приза стремится к нулю.

Отсюда вывод: не верьте различного рода обещаниям о выгодных конкурсах, аукционах и лотереях – в большинстве случаев вы впустую потратите деньги и испортите себе настроение.

«Крупный выигрыш в лотерею»

Данный вид мошенничества существует давно, однако и сегодня находятся люди готовые поверить в быстрое сказочное обогащение.

Суть обмана проста, как три копейки. Вы получаете электронное письмо, СМС-сообщение или сообщение ICQ, в котором говорится, что вы выиграли в лотерею огромный приз – 100 000 долларов. Вообще суммы могут называться разные – и сотни тысяч, и миллионы долларов, но смысл от этого не меняется: вы имеете шанс почти моментально стать сказочно богатым человеком.

Но для этого необходимо выполнить одно условие, а именно – перевести небольшую сумму денег за «регистрацию», «активацию счета», «услуги по перечислению денег» и т. п. Могут попросить выслать 10, 20, 50, 500 долларов или любую другую сумму, которая может выражаться в виде процента от «выигрыша».

После перевода денег по указанным реквизитам о вас просто забудут, и на ваши обращения никто отвечать не будет. Распознать подобное мошенничество несложно – оно обычно «шито белыми нитками» и сразу становится понятно, что вас пытаются «развести». Особенно, если вы не принимали участия ни в каких лотереях и розыгрышах.

Как показывает практика, большинство подобных писем составлено на английском языке, причем нередко – с большим количеством ошибок.

«Сбой» в системе интернет-казино

В последние годы на многих досках бесплатных объявлений и прочих рекламно-информационных ресурсах можно встретить объявления вроде этого:

Добрый день! Вы наверняка слышали про интернет-казино, а также о том, что в них выиграть практически невозможно. Так вот: до последнего времени это было действительно так. Но с недавних пор все кардинально изменилось! В результате многолетних и регулярных игр в интернет-казино, расположенном по адресу (дается ссылка на сайт казино), мне удалось обнаружить дыру в скрипте (прореху в системе безопасности, программный сбой и т. п.), в результате чего можно не только выиграть, но и вывести из казино кучу денег! Зачем я об этом рассказываю? Дело в том, что недавно я выиграл в этом казино крупную сумму, но мне ее не выплатили. Как любой нормальный человек, я на них очень разозлился, но сейчас я знаю, как им отомстить, а потому с радостью делюсь со всеми своим изобретением! С помощью известного мне приема я уже вывел не только свой выигрыш, но даже намного больше денег! Перейдите по ссылке, чтобы узнать подробности!

Если вы перейдете по предложенной ссылке, то, скорее всего, попадете на сайт процветающего казино, где вам предложат поиграть (рис. 4.2).



Рис. 4.2. Бонусами и крупными выигрышами пытаются заманить клиенты владельцы казино

А секрет заключается в том, что вы перешли по реферальной ссылке человека, который впоследствии будет денежное вознаграждение в виде процентов от всех ваших проигрышей в этом казино. Попросту говоря, это один из способов заманивания в казино новых игроков, причем так могут действовать не только рефералы, но и владельцы подобных ресурсов.

И помните: если бы действительно можно было так просто выводить из казино деньги – неужели с вами кто-то стал бы делиться секретом? Конечно же, нет, и все деньги успешно вывели бы и без вашей помощи.

Глава 5. Выманивание денег с помощью специальных программных средств

Существует категория злоумышленников, которые обладают очень неплохими знаниями в сфере IT-технологий. Это позволяет им практически безнаказанно заниматься мошенничеством, вымогательством, шантажом и прочими подобными вещами. В этой главе мы расскажем о том, как мошенники выманивают деньги с помощью специальных программных средств.

Удаленное шифрование данных

В отличие от перечисленных выше схем выманивания денежных средств через Интернет, которые больше напоминают элементарный «развод» или «кидалово», описываемый в этом разделе способ интернет-мошенничества относится к разряду

«продвинутых» и требует от злоумышленника определенной квалификации.

Речь идет об удаленном шифровании данных. Смысл этого способа заключается в том, что злоумышленник, получив доступ к удаленному компьютеру, шифрует в нем определенные файлы, документы и т. п. таким образом, что пользователь не может их самостоятельно расшифровать. Через определенное время пользователь зараженного компьютера получает электронное письмо с требованием перевести определенную сумму денег (это может быть и 100, и 10000 долларов, и любая другая сумма) по указанным реквизитам – за это ему будет выслан ключ для расшифровки информации. Разумеется, пользователь в большинстве случаев готов отдать требуемую сумму, лишь бы вернуть свои данные.

Этот прием в настоящее время набирает все большую популярность. Следует отметить, что злоумышленники сейчас предпочитают шифровать данные не у какого-то домашнего пользователя (хотя такие случаи тоже нередки), а на корпоративных компьютерах и серверах – ведь домашний пользователь при всем желании не сможет заплатить столько же, сколько какая-нибудь даже небольшого размера фирма.

При возникновении подобной ситуации можно считать удачей, если злоумышленник требует перевести деньги банковским переводом – в этом случае его относительно легко вычислить (разумеется, обратившись своевременно в соответствующие органы). Но если в качестве платежных реквизитов указывается кошелек WebMoney, Яндекс. Деньги либо аналогичной интернет-системы, то здесь шансы обнаружить злоумышленника невелики. В данном случае хорошо, если после получения денег он не поленится выслать ключ для расшифровки данных.

Можно сказать, что удаленное шифрование данных является одним из самых изощренных и опасных видов интернет-мошенничества.

Использование мошенниками шпионского ПО

Для реализации своих преступных замыслов мошенники активно используют специальное программное обеспечение – так называемые программы-шпионы (SpyWare). Далее мы расскажем о том, что они собой представляют, какие виды SpyWare наиболее распространены и чего следует опасаться в первую очередь.

Общие сведения о шпионских программах – SpyWare

В настоящее время существует несколько видов шпионского ПО. Например, у многих злоумышленников пользуются популярностью сканеры жесткого диска. Этот шпион тщательно изучает все содержимое жесткого диска вашего компьютера (какие программы установлены, какие файлы и папки хранятся, и др.) и отправляет собранные сведения своему хозяину. Таким образом, злоумышленник получает сведения о том, где хранятся файлы ключей WebMoney, в каком каталоге установлен WebMoney Keeper, а также прочие секретные сведения.

Информацию о том, чем вы занимаетесь на компьютере, может собирать экранный шпион. Сущность его состоит в том, что он периодически через определенные промежутки времени (которые заданы злоумышленником) делает снимки экрана (на компьютерном сленге – скриншоты), и отправляет их хозяину. Подобные сведения могут представлять интерес, например, для шантажистов и вымогателей.

Также немалой популярностью у злоумышленников пользуются так называемые «прокси-шпионы». После того как такой SpyWare проникает в компьютер, то этот компьютер будет выполнять роль прокси-сервера. На практике это означает, что злоумышленник при работе в Интернете сможет прикрываться именем (точнее – IP-адресом) ничего не подозревающего пользователя, и если его действия будут носить деструктивный или противозаконный характер – отвечать придется безвинному человеку. В частности, это

может обернуться не только внушительными штрафами, но даже привлечением к уголовной ответственности.

Еще один популярный у злоумышленников вид spyware – это почтовые шпионы. Их главная задача – сбор сведений об адресах электронной почты, хранящихся в данном компьютере, и отсылка этой информации хозяину. Сведения собираются обычно в почтовых программах и адресных книгах, а также органайзерах. Такая информация имеет высокую ценность для тех, кто занимается рассылкой спама. Кроме этого, почтовые шпионы могут вести откровенно деструктивную деятельность: редактировать содержимое писем, менять пароль доступа и т. д., а это уже широкое поле деятельности для шантажистов и вымогателей.

Для борьбы со шпионским программным обеспечением предназначены специальные программные средства – защитные утилиты и программы категории AntiSpyware. С некоторыми из них мы познакомимся ниже, в последней главе книги.

Есть еще одна опасная категория шпионских программ – клавиатурные шпионы, или кейлоггеры. О них речь пойдет в следующем разделе.

Чем опасны клавиатурные шпионы?

Клавиатурный шпион – это программа либо устройство, с помощью которого осуществляется постоянное наблюдение за всеми нажатиями клавиш на клавиатуре (а во многих случаях – и за всеми щелчками мыши) с целью получения информации обо всех набираемых пользователем текстах. Зачем это нужно? Ответ на данный вопрос у каждого злоумышленника свой: одному нужно перехватывать чужие почтовые сообщения, другому – получить номера кредитных карт, третьему – взломать пароли, четвертому – украсть у разработчика исходные тексты еще не вышедшей программы, а пятому – все вместе взятое, и еще что-нибудь.

ВНИМАНИЕ

С помощью клавиатурного шпиона злоумышленник может в кратчайшие сроки опустошить все кредитные карты и электронные кошельки жертвы.

Характерной особенностью клавиатурных шпионов является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако чтобы установить такое устройство, необходим доступ к компьютеру в отсутствие пользователя. Поэтому на домашних компьютерах такой вид клавиатурных шпионов встречается редко, чаще – на офисных и рабочих компьютерах, а также на компьютерах «общественного пользования»: в студенческих аудиториях, на почте, в интернет-клубах и др. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Достаточно широко распространены в настоящее время так называемые перехватывающие клавиатурные шпионы. Такие шпионы в большинстве случаев представляют собой программу, состоящую из исполняемого файла с расширением *.exe, и dll-библиотеки, с помощью которой осуществляется управление процессами записи информации. Перехватывающий клавиатурный шпион без проблем запоминает практически любой набранный текст: документы, письма, исходные коды программ (данная возможность нередко используется для кражи исходников еще не вышедших программ), номера кредитных карт, пароли (в том числе и самозаполняющиеся) и т. д.

Клавиатурный шпион (имеется в виду программа, а не устройство) может проникнуть в компьютер разными способами: например, как и любой другой шпионский модуль – в

составе какой-либо устанавливаемой на компьютер бесплатной программы (как правило – от неизвестного либо сомнительного разработчика), либо через программу обмена сообщениями, и т. д. В последнее время нередки случаи, когда для «получения» в свой компьютер клавиатурного шпиона достаточно было просто зайти на определенный сайт.

Стопроцентной защиты от клавиатурных шпионов, как и от других вредоносных программ, в настоящее время не существует – ведь известно, что на каждое противоядие можно найти новый яд. Однако при соблюдении мер предосторожности можно свести к минимуму их вероятность их появления на компьютере. О том, как бороться с клавиатурными шпионами, будет рассказано в заключительной главе книги.

DOS-атака на сайт с последующим вымогательством денег

Многие наверняка знакомо такое понятие, как DOS-атака. Сущность заключается в том, что какой-либо веб-ресурс подвергается мощной программной «бомбежке», в результате чего сайт или начинает очень сильно «тормозить», или попросту «падает». Долгие годы этот метод использовался преимущественно для того, чтобы вывести из строя сайты конкурентов, или просто отомстить той или иной организации.

Однако с недавних пор этот технический прием стал активно использоваться мошенниками. Алгоритм их действий прост: на сайт-жертву организуется мощная DOS-атака. После того как сайт успешно «ляжет», злоумышленники связываются с его владельцем или администрацией, и диктуют свои условия: мол, платите такую-то сумму денег – и сайт «оживет». Чтобы «подтолкнуть» жертву к принятию «правильного» решения, мошенники могут добавить, что в случае оплаты они гарантируют сайту защиту от подобных атак в будущем. В случае отказа атаки будут продолжаться, причем их мощность будет с каждым разом увеличиваться.

Стоит ли говорить, что после перечисления денег мошенникам никакая защита сайту от DOS-атак обеспечиваться не будет! Более того – выманив деньги один раз и «почувыв слабинку», мошенники наверняка повторят свои действия.

В подобных ситуациях настоятельно рекомендуется не идти на поводу у мошенников, а объединить свои действия с владельцем хостинга и обратиться с соответствующим заявлением в правоохранительные органы.

«Заражение» компьютера с предложением купить надежный антивирус

Известно, что многие пользователи беспечно относятся к вопросам компьютерной безопасности. Не у всех имеется надежное антивирусное средство, а уж за актуальностью сигнатурных баз следят единицы. Этим и пользуются мошенники, имитируя заражение компьютера вирусом и предлагая для защиты «недорогие антивирусные» средства.

На практике все выглядит примерно так. В один прекрасный день пользователь Интернета получает сообщение о том, что его компьютер инфицирован вирусом. Это сообщение может отобразиться, например, в виде всплывающего окна. Причем оно может выглядеть устрашающе – с соответствующим визуальным и звуковым оформлением (резкие цвета и рисунки, неприятные скрежещущие звуки, и т. п.). Это делается для того, чтобы у пользователя не осталось сомнений в заражении его компьютера мощным вредоносным программным обеспечением. При этом сообщение об инфицировании может оформляться от имени программного продукта, предлагаемого мошенниками – например, «Программа такая-то бесплатно проверила ваш компьютер и обнаружила у вас вирус, и чтобы избавиться от него, перейдите по ссылке». Если вы перейдете по этой ссылке – попадете на страницу, где вам будет предложено купить надежное антивирусное средство, гарантирующее не только избавление от обнаруженного вируса, но и надежную защиту от любых заражений в будущем.

Ну а дальше возможны варианты. Иногда мошенники, получив деньги, просто перестают отвечать на любые обращения и исчезают. Иногда они действительно присылают какую-то программу или архив – но пользоваться такой «покупкой» категорически не рекомендуется. Как показывает практика, вы получите не «надежный недорогой антивирус», а трояна или SpyWare, который «поселится» в вашем компьютере и будет, во-первых, информировать злоумышленника обо всех выполняемых на компьютере действиях, а во-вторых – предоставлять ему доступ к хранящимся на вашем компьютере файлам, папкам и приложениям. Помимо прочего, мошенник сможет получить доступ к вашим электронным кошелькам.

В некоторых случаях злоумышленники предлагают загрузить «антивирус» бесплатно. В этом случае сомневаться не приходится – вы получите либо троян, либо программу-шпиона.

Поэтому, если вы получили непонятно от кого сообщение об инфицировании компьютера – не следуйте рекомендациям мошенников, а просканируйте компьютер хорошей антивирусной программой с новейшими сигнатурными базами.

«Платный» Internet Explorer

Мошенническим приемом, о котором мы сейчас расскажем, пользуются мошенники, которые имеют неплохие знания в области IT-технологий. Поэтому подобные способы относятся к одним из наиболее изощренных методов «сравнительно честного отъема денег у населения».

При очередном запуске Internet Explorer пользователь замечает, что он автоматически попадает на страницу компании Microsoft. На этой странице отображается информационное сообщение о том, что теперь обозреватель Internet Explorer является платным, и за него нужно заплатить с помощью СМС-сообщения – в противном случае использование программы невозможно. Стоимость одного сообщения – всего 30 рублей (сумма может быть и другая).

На самом деле в компьютер пользователя была внедрена специальная вредоносная программа, которая автоматически переправляла Internet Explorer **на подложную страницу, являющуюся копией страницы компании Microsoft**. Вообще о том, что это подвох, можно было бы догадаться и сразу: вряд ли столь солидная и уважаемая компания, как Microsoft, будет собирать деньги с пользователей своих программных продуктов с помощью СМС-сообщений.

Кстати, если на сайте написано, что стоимость одного СМС составляет 30 рублей – будьте готовы к тому, что с вашего счета после отправки сообщения снимут рублей 100–150.

Устранить проблему можно самостоятельно без отправки СМС и прочих контактов с мошенниками. Для этого в свойствах Internet Explorer (переход в данный режим осуществляется с помощью команды главного меню обозревателя Сервис □ Параметры) откройте вкладку Дополнительно, и нажмите в ней кнопку Сброс (рис. 5.1).

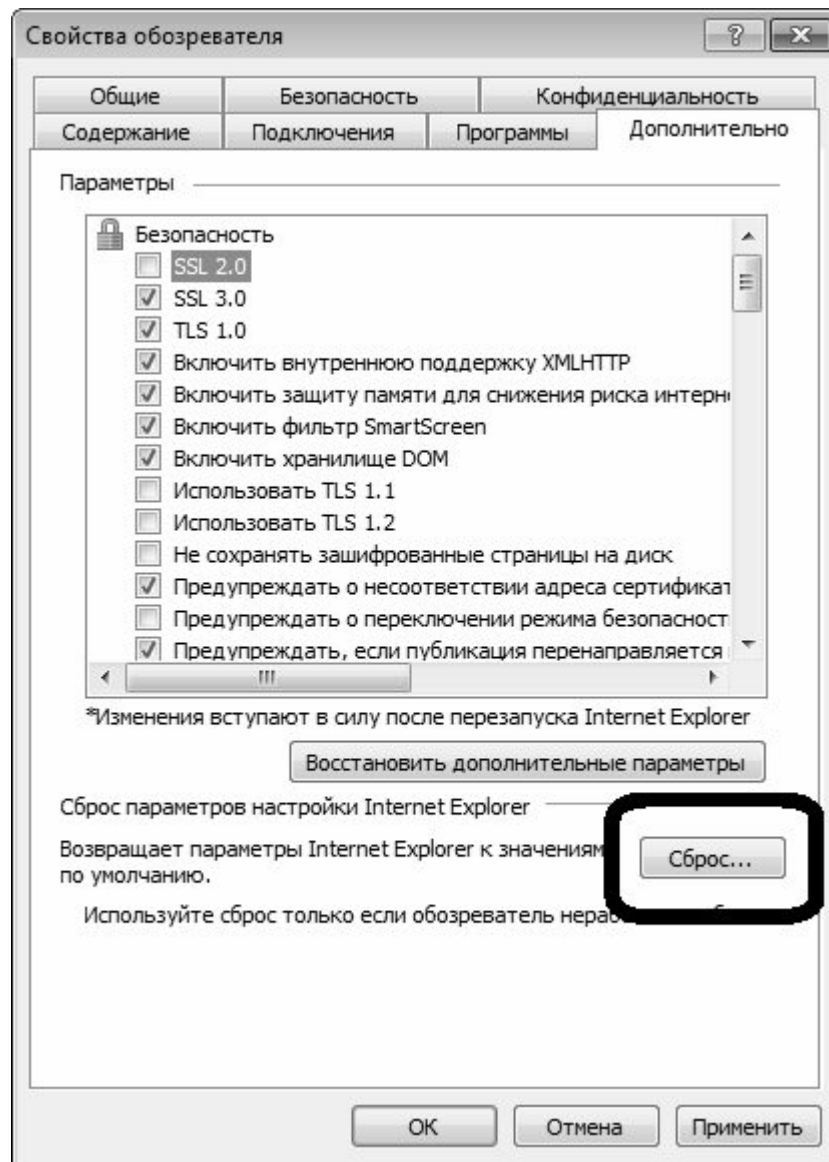


Рис. 5.1. Возврат к настройкам по умолчанию

Тем самым вы вернетесь к настройкам Internet Explorer, используемым по умолчанию. После этого перейдите на вкладку Программы, и откройте список надстроек обозревателя (рис. 5.2).

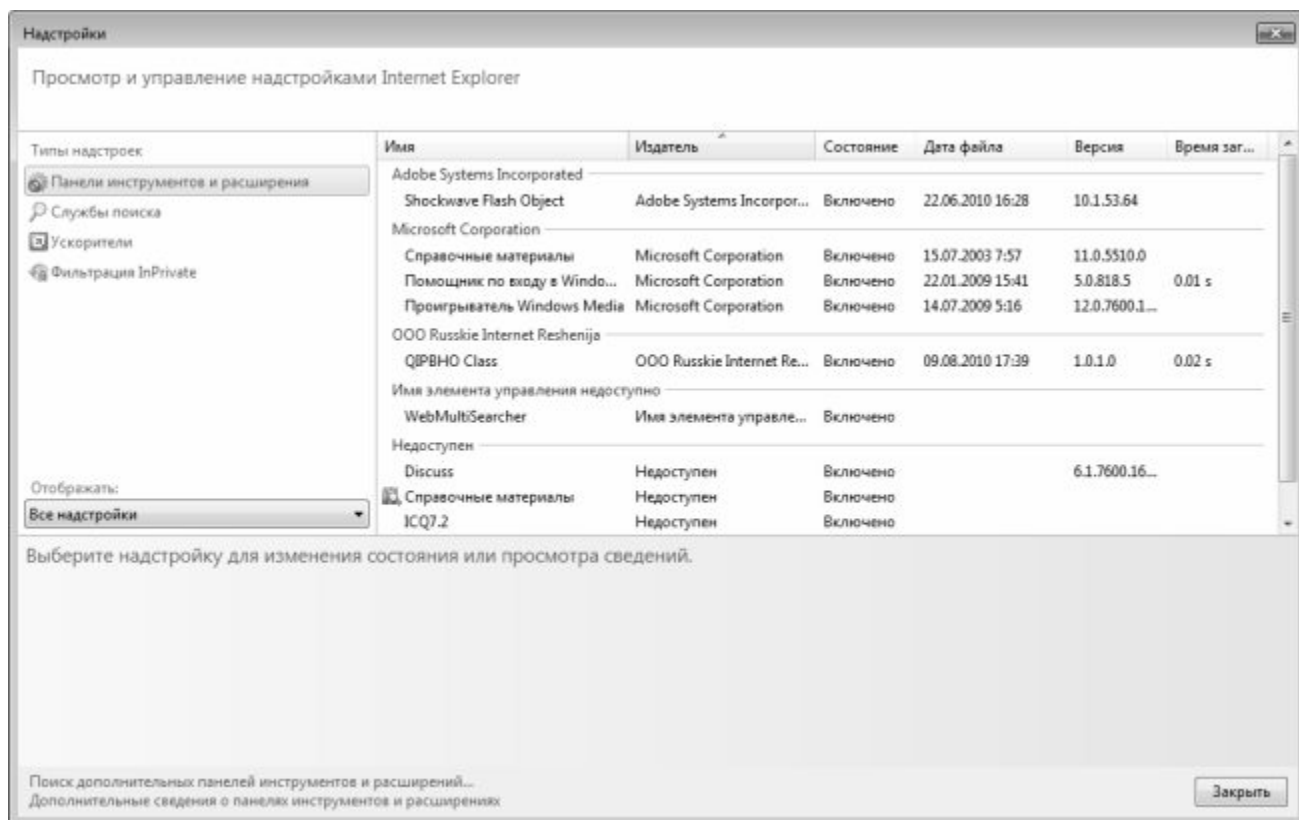


Рис. 5.2. Список надстроек в Internet Explorer 8

В этом списке отключите все имеющиеся надстройки. Затем закройте обозреватель, запустите его вновь и откройте какую-либо страницу, после чего вновь вызовите список надстроек. Посмотрите, какая надстройка включилась самостоятельно, найдите соответствующий ей файл и удалите его.

А вообще при всем уважении к компании Microsoft стоит отметить, что обозреватель Internet Explorer не отличается высокой степенью безопасности и надежной защитой от проникновения извне. Во многом это обусловлено не конструктивными или иными недостатками программы, а тем, что данный продукт изучен злоумышленниками лучше, чем имеющиеся аналоги.

Глава 6. Прочие виды обмана и выманивания денег

В данной главе мы расскажем еще о нескольких распространенных способах мошенничества, которым не нашлось места в предыдущих главах книги.

Кража персональных данных с последующим выманиванием денег

Одним из наиболее изощренных методов мошенничества является кража персональных данных с последующим выманиванием денег. При этом деньги могут выманиваться как у вас, так и ничего не подозревающих ваших знакомых.

Главная задача мошенника – получить доступ к вашему электронному почтовому ящику, ICQ или иным инструментам для общения в Интернете. Обычно это делается путем подбора пароля, поскольку очень многие пользователи совершенно безответственно относятся к паролю и используют в его качестве легко угадываемый набор символов (подробнее об этом см. в следующей главе раздел «Избегай стандартных паролей»). Также для этого могут использоваться SpyWare (о них шла речь выше) и прочие технические,

программные, психологические и иные средства.

После того как мошенник получил доступ, например, к вашему ICQ, он всем найденным в адресной книге контактам рассылает от вашего имени просьбу прислать определенную сумму денег на указанный электронный кошелек. Эту просьбу он может обосновывать чем угодно, например – внезапными неприятностями (попадание в дорожно-транспортное происшествие, болезнь или смерть близкого человека, пожар, ограбление, квартирная кража и т. д.). Иногда злоумышленник просит просто одолжить немного денег «до полочки».

Разумеется, большинство людей удовлетворят просьбу хорошего знакомого (друга, родственника, ребенка) и переведет сумму по указанным реквизитам, не подозревая, что деньги попадут к мошенникам. В конечном итоге рассчитываться по долгам приходится жертве, у которой были украдены персональные данные.

Иногда злоумышленники действуют иначе: они просто предлагают жертве вернуть доступ к своим аккаунтам (почтовым ящикам, ICQ и др.) за деньги. В случае отказа могут последовать угрозы: мол, по всем имеющимся адресам мы разошлем сообщения такого характера, что с тобой никто иметь дела не будет: семья отвернется, с работы уволят и т. д. Но даже если вы согласитесь заплатить злоумышленникам требуемую сумму – нет никакой гарантии, что они действительно вернут вам доступ к вашим аккаунтам.

На основании вышеизложенного делаем два вывода. Во-первых, нужно пользоваться хорошими надежными паролями, чтобы исключить вероятность их подбора или взлома (подробнее об этом см. в следующей главе раздел «Избегай стандартных паролей»). А во-вторых – если вы получаете от знакомого человека электронное письмо, сообщение ICQ и т. п. с просьбой оказать финансовую помощь – не спешите переводить деньги по указанным реквизитам, поскольку эта просьба может исходить от мошенника. В подобной ситуации рекомендуется связаться с этим знакомым по телефону или иным альтернативным способом, чтобы уточнить – действительно ли просьба о финансовой помощи исходит от него.

Нигерийский спам

«Нигерийский спам» – это схема выманивания денег, при которой пользователь получает письмо примерно следующего содержания:

Я, такая-то, являюсь вдовой недавно умершего короля Бахрейна (Сомали, Габона, Джибути или иной экзотической страны), и как его родственница подвергаюсь гонениям в родной стране. Мой покойный супруг оставил наследство 200 млн. долларов США, но самостоятельно я их получить не могу – капиталы моего бывшего мужа подлежат аресту, поэтому мне нужно содействие постороннего лица. Вы можете мне помочь. Для этого вам нужно открыть счет в зарубежном банке, на который будут перечислены денежные средства. Вам за это причитается 3 % от легализованной суммы.

Затем суть дела излагается более подробно, и главное заключается в том, что пользователь должен перевести по указанным реквизитам определенную сумму денег для покрытия «накладных расходов». Причем просьбы о «предварительных платежах» могут быть неоднократными. Как ни странно, в наше время еще находятся чудаки, которые охотно попадают на эту удочку и пересылают злоумышленникам немалые суммы денег. Причем среди жертв подобного мошенничества есть образованные, грамотные люди, нередко имеющие собственный бизнес. Поймать такого «спонсора» для преступников считается большой удачей – ведь сотрудникам правоохранительных органов известны случаи, когда суммы перечисленных преступникам средств составляли сотни тысяч долларов США.

Пример «нигерийского спама» показан на рис. 6.1.



Рис. 6.1. Типичный пример «нигерийского спама»

Причем в подобном письме история возникновения денег может быть разной – не только «мне удалось завладеть деньгами бывшего шефа», но и, например, «помогите спасти часть капиталов (эдак миллионов 500 долларов) бывшему олигарху, попавшему в беду... для этого откройте счет... причитается вознаграждение... накладные расходы небольшие...».

Почему этот вид мошенничества получил название «нигерийский спам»? Дело в том, что в первых таких письмах, которые рассылались по всему миру, фигурировало имя бывшего нигерийского диктатора Сани Абачи (якобы люди, имеющие доступ к его счетам, не могли снять деньги без посторонней помощи). В настоящее время в этих письмах можно встретить имена любых известных людей (чаще всего попавших в неприятность – например, преследуемых официальными властями, или вообще умерших), но первоначальное название так и осталось.

«Бесплатная эротическая экскурсия» по страницам сайта

Во все времена «клубничка» представляла немалый интерес для обывателей, поэтому в Интернете существует огромное количество сайтов, посвященных данной «пикантной» теме. Неудивительно, что мошенники никак не могли обойти вниманием этот сегмент Интернета.

Один из известных способов «развода» состоит в следующем. Фирма, которая занимается продажей, например, эротических картинок, требует у посетителей при регистрации на сайте вводить данные своих кредитных карт. Поскольку на такое согласны далеко не все, администрация портала зарегистрированным посетителям предлагает бонус – бесплатную эротическую экскурсию по страницам сайта. Посетитель с радостью соглашается, и лишь через некоторое время узнает, что с его кредитной карты производилось

списание средств – как выясняется, именно в счет оплаты за просмотр «веселых картинок» на эротическом сайте. Несмотря на то, что это откровенный обман, привлечь мошенников к ответственности не получится – хотя бы потому, что в реальности услуга была все же оказана.

Просьба выслать СМС за разблокировку персональной страницы в социальной сети

О популярности социальных сетей (www.vkontakte.ru, www.odnoklassniki.ru и т. п.) скоро будут слагать легенды – с каждым днем число их пользователей стремительно растет и исчисляется десятками миллионов, во многих офисах чуть ли не половину рабочего времени клерки посвящают посещению подобных ресурсов. И было бы очень странно, если бы этот «Клондайк» остался без внимания мошенников.

Рассмотрим прием, с которым доводилось сталкиваться участникам системы www.vkontakte.ru. При попытке авторизоваться и войти на свою персональную страницу пользователь получает сообщение о том, что его страница заблокирована за рассылку спам-сообщений (причина может быть названа и другая), и за разблокировку нужно отправить СМС-сообщение по указанному номеру.

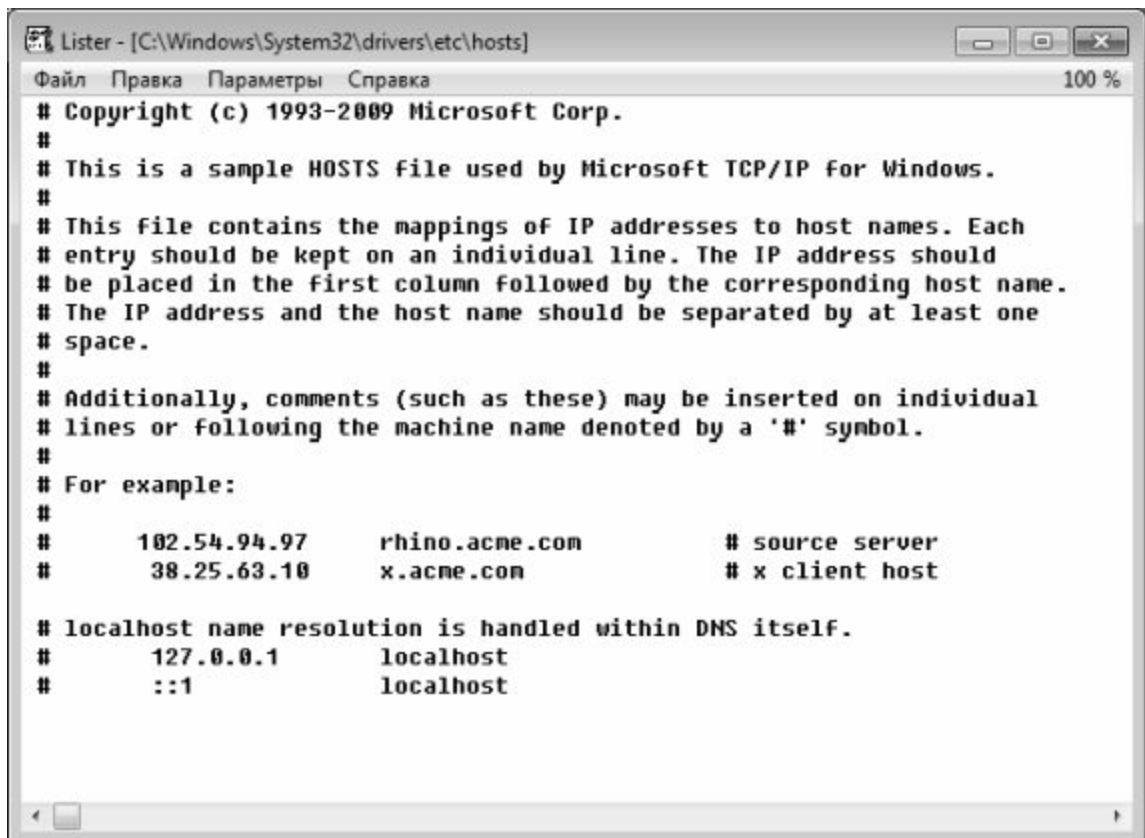
Как ни странно, находились пользователи, которые немедленно отправляли СМС и лишались тем самым немалой суммы денег со своего телефонного счета – и это при том, что они никогда не рассылали никакой спам и не занимались прочими неблагоприятными вещами! Разумеется, деньги оседали в карманах мошенников.

Помните, что подобные сообщения исходят от злоумышленников, и будет очень хорошо, если после получения требуемой суммы они действительно разблокируют вашу страницу. Но подобную проблему можно решить и самостоятельно, причем совершенно бесплатно и без всяких СМС.

Для этого в каталоге **C:** найдите файл **hosts** (этот файл не имеет расширения), и удалите в нем строки следующего вида (в зависимости от того, с какой социальной сетью возникла проблема):

- ◆ XXX.XXX.XXX.XXX vkontakte.ru
- ◆ XXX.XXX.XXX.XXX odnoklassniki.ru

Вместо XXX в этих строках отображаются цифры от 1 до 255. Обычно данный файл в оригинальном варианте имеет следующий вид (рис. 6.2).



```
File  Edit  Parameters  Help  100 %
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

Рис. 6.2. Файл **hosts**

Этот файл может иметь как русский, так и английский текст, но в любом случае его структура должна быть такова, как на рис. 6.2. Удалив из него все лишнее, вы решите проблему с доступом на свою персональную страницу.

Реклама и продвижение сайтов

Каждый владелец сайта желает, чтобы у него было много посетителей. Посещаемый ресурс способен привлекать клиентов, приносить прибыль, способствовать появлению выгодных деловых партнеров, дальнейшему развитию бизнеса, и т. д.

Учет числа посещений ведется с помощью специальных счетчиков. Сегодня абсолютно бесплатно можно получить счетчики, например, на следующих сервисах: www.hotlog.ru (это один из самых популярных статистических ресурсов, рис. 6.3), www.mail.ru или www.bigmir.net.



Рис. 6.3. Статистический сервис www.hotlog.ru

А вообще можно набрать в любом поисковике запрос «счетчик посещений» – и вам будет предложено множество ссылок, по которым вы найдете счетчики на любой вкус.

В настоящее время развелось немало мошенников, которые делают вид, что занимаются продвижением сайтов. В реальности они лишь пускают пыль в глаза, однако их «услуги» по «раскрутке и оптимизации сайта» стоят недешево.

ВНИМАНИЕ

Многие мошенники подкупают тем, что за свои услуги они могут не требовать предоплаты.

В общем случае обман происходит примерно следующим образом. Человек вводит в поисковую систему запрос «услуги по продвижению сайтов», и в предложенном списке (рис. 6.4) выбирает какую-нибудь организацию.

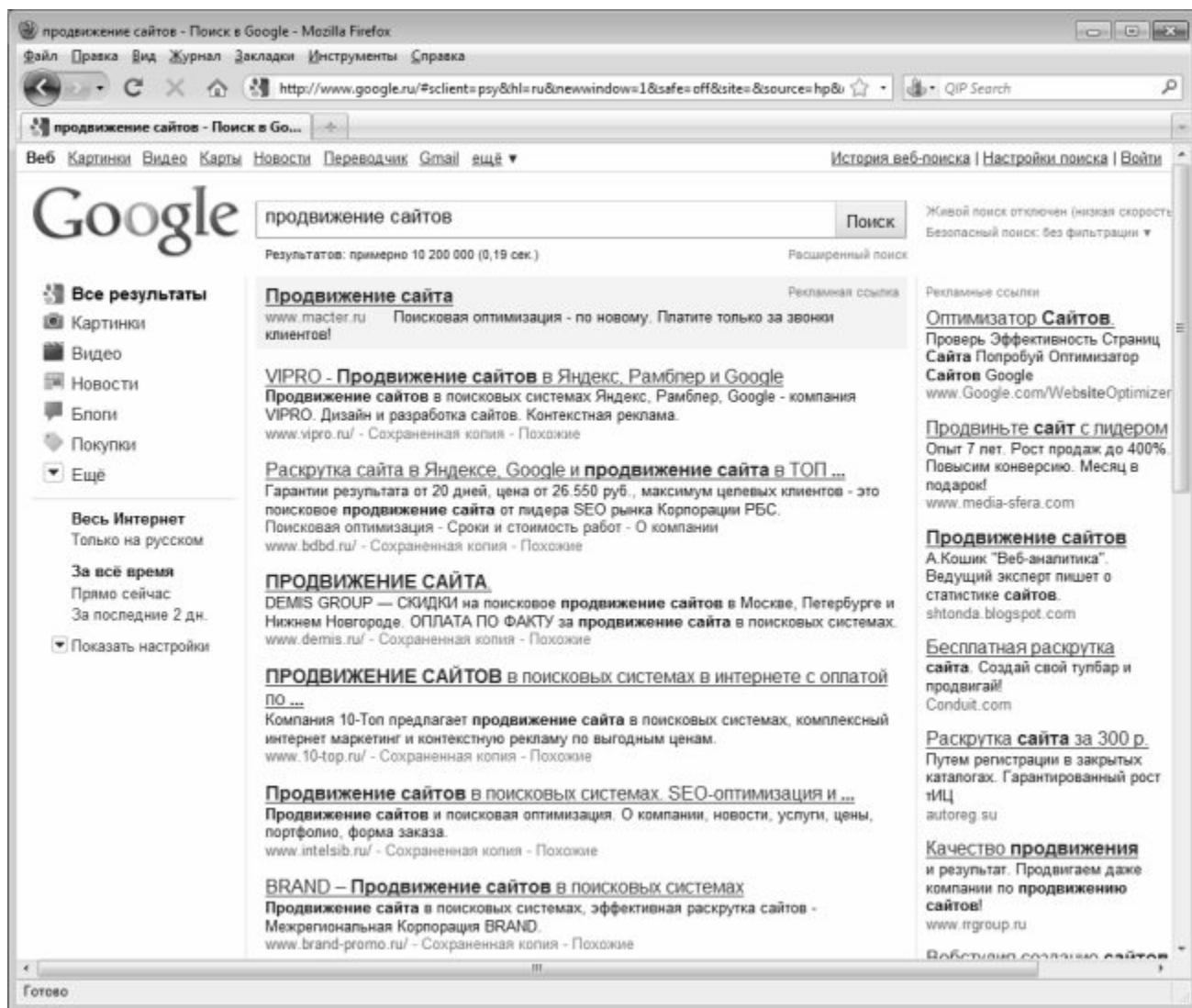


Рис. 6.4. Под вывеской «продвижения сайтов» могут скрываться мошенники

Связавшись с ней, он объясняет ситуацию (мол, такой-то сайт нужно раскрутить, и т. п.), после чего стороны оговаривают стоимость услуг и сроки окончания работ.

Мошенники могут предложить клиенту, чтобы он наблюдал за тем, как растет число посетителей его сайта. Человек реально видит: вчера было столько-то посещений, сегодня их стало намного больше, а на следующий день счетчик вообще показал цифры, о которых и мечтать не приходилось, и т. д. Когда наступает срок сдачи работ, заказчик с чистой совестью рассчитывается с «исполнителями», поскольку результат налицо.

Сразу после расчета ситуация кардинально меняется. Человек видит, что число посещений вновь резко снизилось, более того – вернулось практически на начальный уровень. Следовательно, деньги за раскрутку и продвижение сайта были потрачены зря.

А секрет состоит в том, что никто и не занимался оптимизацией, продвижением и раскруткой веб-ресурса. Вся «работа» мошенников заключалась в том, чтобы с помощью нехитрых манипуляций искусственно «накрутить» показания счетчика. Как только они получили деньги от заказчика – они прекратили его «накручивать», следовательно – данные о посещаемости вернулись на прежний уровень.

ПРИМЕЧАНИЕ

Сегодня в Интернете можно найти утилиты, предназначенные как раз для искусственной накрутки установленных на веб-ресурсах счетчиков. Если вас устроит такая «псевдопосещаемость» – вы можете накрутить показания счетчиков

и самостоятельно, и вовсе не обязательно обращаться для этого к мошенникам.

Если вы намереваетесь заказать раскрутку и продвижение сайта у профессионалов – постарайтесь найти их по рекомендации людей, которым вы доверяете. В крайнем случае, если такой возможности нет, хотя бы не поленитесь навести об организации, к которой вы хотите обратиться, справки в Интернете.

Удаление с экрана навязчивой рекламы за СМС

Одним из наиболее неприятных и изощренных видов мошенничества является удаление с экрана навязчивой рекламы за СМС.

В один прекрасный день пользователь замечает, что на экране монитора появляется рекламное окно. Это может произойти в любой момент – например, при загрузке компьютера, при активизации какой-либо функции, или просто без привязки к действиям пользователя. Причем рекламное окно появляется независимо от наличия действующего подключения к Интернету.

Характерной особенностью данной аферы является то, что такое окно может иметь явно неприличный характер. Например, подобным образом часто рекламируются интернет-магазины, торгующие товарами сексуально-эротического ассортимента (попросту говоря, секс-шопы). Причем эта реклама не просто навязчивая – ее так просто удалить с экрана вы не сможете: окно не закрывается (или при попытке закрытия вы автоматически будете перенаправлены на сайт секс-шопа), через Диспетчер задач его также отключить невозможно. Оно исчезает обычно само, но – лишь по истечении немалого промежутка времени (это может быть, например, 100 секунд, или 3 минуты). В течение этого времени вы будете вынуждены наблюдать рекламу эротических и порнографических материалов. Стоит ли говорить, насколько вредной является такая реклама, если к компьютеру имеют доступ несовершеннолетние!

Рекламный модуль проникает в компьютер в виде трояна незаметно для пользователя, а иногда – при невольном его содействии (посещение зараженного сайта, распаковка непроверенного зараженного архива, и т. п.). Для избавления от него мошенники требуют отправить СМС-сообщение на указанный номер – эта информация отображается на видном месте в рекламном окне. Но даже если вы отправите СМС – не обольщайтесь, ибо не факт, что вам сразу вышлют инструкции по удалению рекламы. Во-первых, после получения денег вы перестанете представлять для мошенников всякий интерес, а во-вторых – одного СМС может быть недостаточно. Часто в подобных рекламных окнах мельчайшим шрифтом где-нибудь внизу или в углу написано, что для удаления рекламы требуется отправить три (пять, десять и т. д.) СМС.

Но не спешите делиться с мошенниками своими деньгами – решить проблему можно и самостоятельно. Обычно в таких случаях помогает Интернет – для этого нужно в любом поисковике кратко описать проблему (например, Как удалить рекламу с экрана, и т. п.), и ознакомиться с результатами. Можно задать вопрос на специализированных сервисах – например, <http://otvety.google.ru>, <http://otvet.mail.ru> и т. п., или поискать ответ среди задаваемых ранее вопросов. Например, автор этой книги успешно решил подобную проблему, найдя подходящий ответ на <http://otvet.mail.ru>: опытный пользователь подсказал, какой файл и где именно нужно удалить, чтобы избавиться от рекламы.

«Бесплатные» диеты

Очень многие желают похудеть с помощью специальных диет, которыми завален как Интернет, так и печатные издания. Мошенники придумали хитрый способ зарабатывать на желающих сбросить лишний вес.

Человек в поисках диеты заходит на соответствующий сайт и видит несколько ссылок

на какие-нибудь известные и «раскрученные» диеты, причем рядом с каждой ссылкой большими буквами написано **БЕСПЛАТНО**. Человек идет по ссылке и выясняет, что для бесплатного получения информации ему нужно лишь зарегистрироваться на сайте. Регистрация также бесплатна, но есть один нюанс: помимо набора стандартных данных (ФИО, электронный адрес и т. п.) нужно указать номер своего мобильного телефона, на который будет бесплатно высылаться вся необходимая информация. Пример «диетного лохотрона» показан на рис. 6.5.

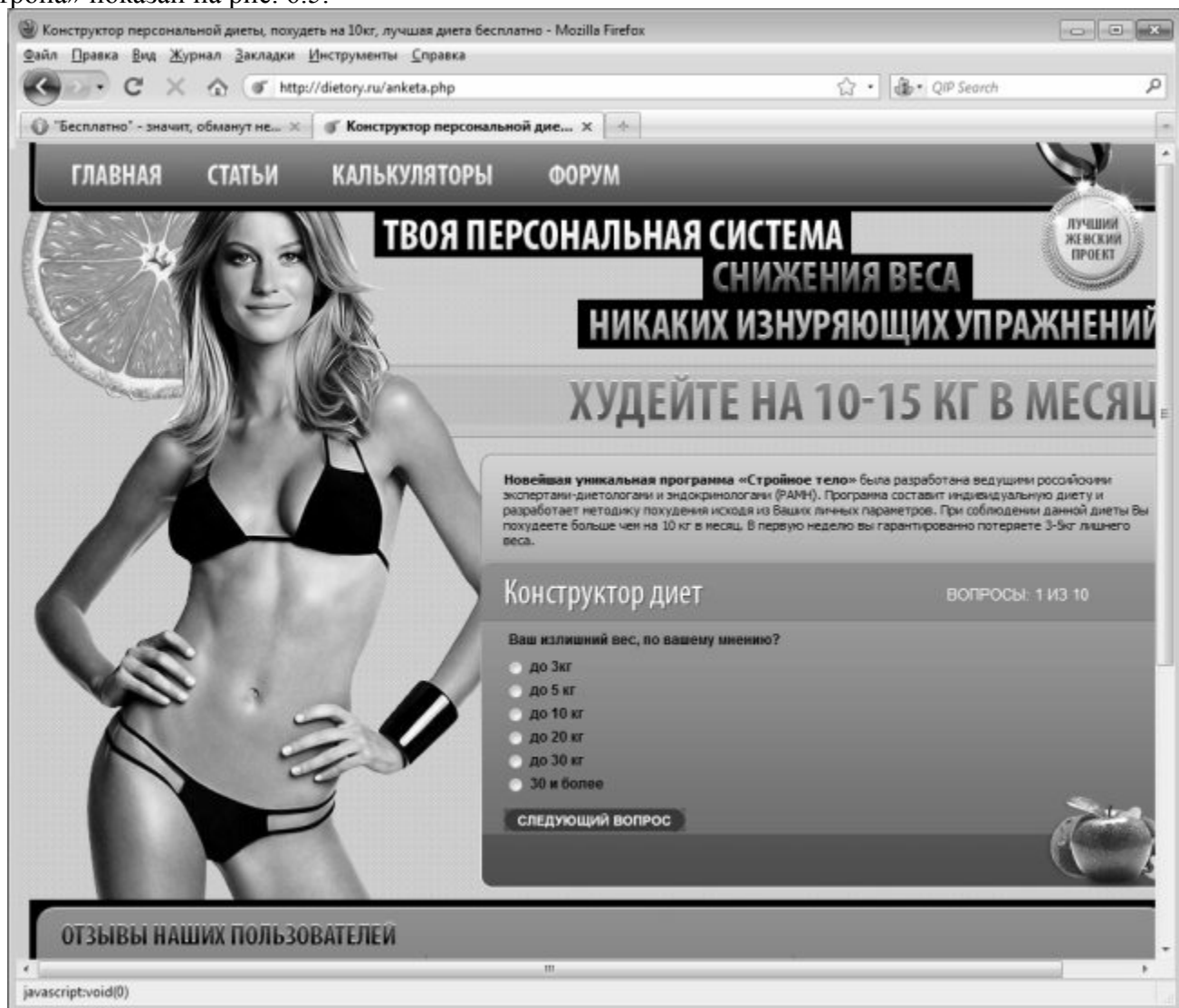


Рис. 6.5. Диетный лохотрон

Если вы столкнулись с чем-то подобным – ознакомьтесь с правилами подписки на данном сайте (почти незаметная ссылка находится внизу страницы). Вероятнее всего, в них будет присутствовать пункт, пример которого приведен ниже.

«Плата за услуги «Подписка» в течение 1 дня с даты выполнения Абонентом действий указанных в пункте 3, не взимается. Если по окончании 1 дня с даты выполнения Абонентом действий, указанных в пункте 3 Абонент не отказывается от предоставления услуги «Подписка» способами, описанными в пункте 7, то услуга «Подписка» начинает предоставляться на платной основе. Со счета абонента раз в 3 дня происходит списание денежных средств в размере 160 руб 87 коп (включая НДС 18 %).

На рис. 6.6 выделены ключевые фразы подобных «правил подписки».

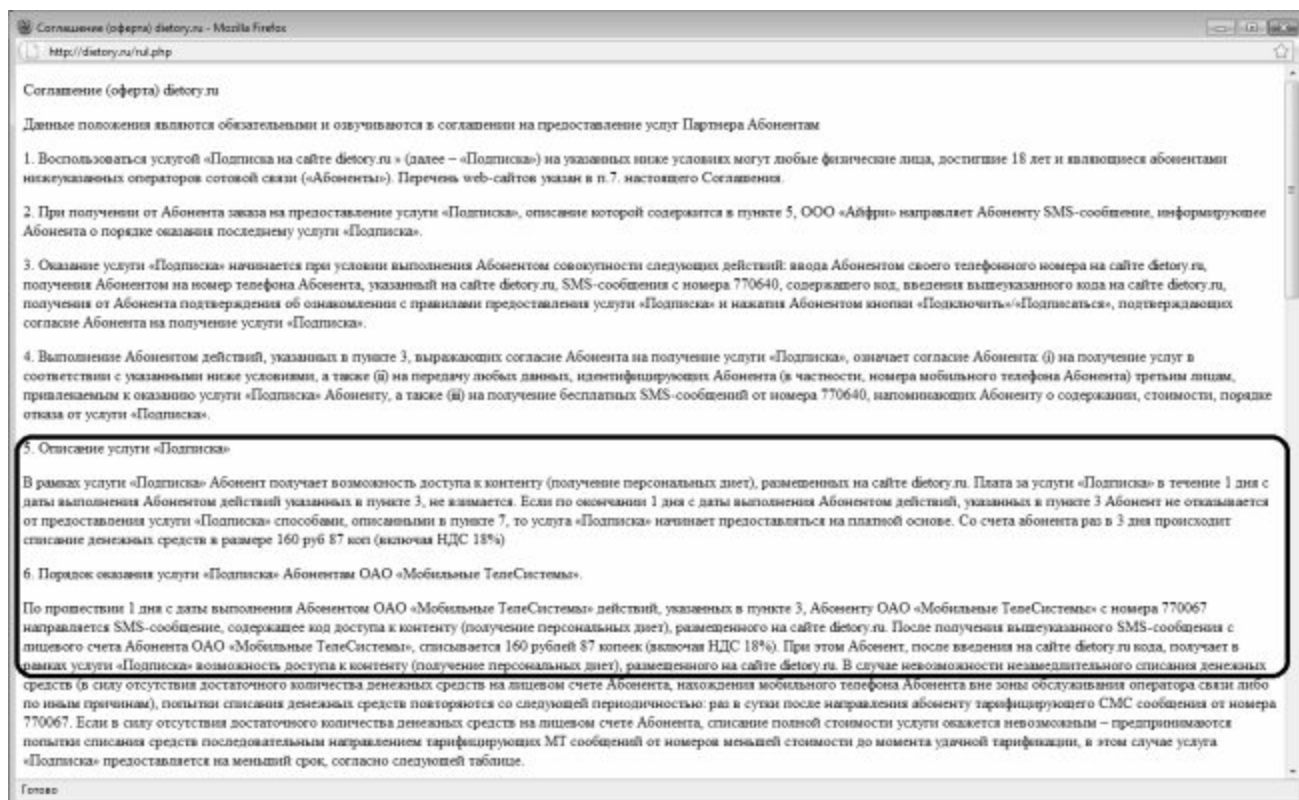


Рис. 6.6. Фрагмент правил предоставления информации о диетах

Вообщем, до тех пор, пока вы опомнитесь и увидите, что с вашего телефонного счета исчезают деньги, может пройти несколько дней. Разумеется, вернуть потерянные деньги вы не сможете, поскольку с точки зрения действующего законодательства мошенники таковыми не являются – они честно предупредили, что бесплатно услуга предоставляется только 1 день, а если вы этого вовремя не заметили – это только ваши проблемы.

Обман с доверительным управлением на Forex

Все гениальное просто, и это крылатое выражение находит свое подтверждение в том, как мошенники обманывают доверчивых игроков на валютном рынке Forex, а также на фондовых рынках, где ведется торговля ценными бумагами.

На валютном рынке Forex предлагается такая услуга, как размещение временно свободных денежных средств под доверительное управление. Суть операции состоит в том, что трейдер (биржевой игрок) распоряжается деньгами инвестора (заключает сделки, и т. д.) по своему усмотрению. Иначе говоря, инвестор разрешает трейдеру пользоваться своими средствами на бирже как угодно, лишь бы это приносило прибыль.

Если в результате биржевой игры действительно удастся получить доход – клиент отдает трейдеру предварительно оговоренную часть (например, 30 % или 50 % прибыли). Если же биржевая игра получилась неудачной и принесла убытки, то стороны сразу определяют его максимально допустимый размер (обычно где-то треть от суммы вклада), при достижении которого игра должна прекратиться. В данном случае все потери ложатся полностью на инвестора, трейдер ничем не рискует – таковы правила, о которых инвестор знает заранее.

Этот нюанс и позволил появиться гениально простому, и в то же время – очень эффективному способу мошенничества. Трейдер через Интернет находит двух инвесторов, располагающих временно свободным капиталом, убеждает их в своем высоком профессионализме и уверяет, что распорядится деньгами лучше, чем кто-то другой. Получив средства в доверительное управление, трейдер-мошенник выбирает позицию и на одном

счете открывает ее вверх, а на другом – вниз (иначе говоря, играет одновременно на повышение и на понижение курса). В результате у одного инвестора образуется доход, а у другого – убыток такого же размера.

Когда убытки инвестора, которому не повезло, достигают оговоренной заранее суммы – трейдер сворачивает деятельность на его счете. Инвестор забирает свои оставшиеся деньги – но трейдер-то при этом ничего не теряет! Зато со счета другого инвестора, где получился доход, мошенник законно получает причитающуюся часть прибыли.

Аналогичным образом мошенники действуют не только на валютном, но и на фондовых рынках, на которых ведутся торги ценными бумагами.

«Липовая» защита доменного имени

Предположим, вы являетесь владельцем сайта, расположенного по адресу www.resurs.com. Это сайт вашей компании или вашего бизнеса, имеющий постоянных посетителей и, образно говоря, давно и прочно занимающий свое место. В определенный момент вы получаете по электронной почте письмо, автором которого является некая служба мониторинга доменных имен. В этом письме вам сообщается, что есть злоумышленники, которые хотят зарегистрировать очень похожее доменное имя – например, www.resurs.org, причем точно известно, что они будут осуществлять мошенническую деятельность.

Следовательно, тень от их неблагоприятной деятельности может пасть и на вполне благополучный сайт www.resurs.com. Это может привести к потере доверия со стороны постоянных клиентов, а в некоторых случаях даже к неприятностям с правоохранительными органами. Поэтому настоятельно рекомендуется предотвратить регистрацию такого доменного имени, тем более что стоит это будет всего 50 долларов США (сумма может быть разной – и 20, и 100 долларов).

Как нетрудно догадаться, в данном случае мошенником является тот, кто предлагает защиту от злоумышленников. Прием простой, если не сказать – примитивный, но, как ни странно, на него попадают владельцы даже уважаемых и известных веб-ресурсов.

ФИШИНГ

Вид мошенничества, который мы рассмотрим в данном разделе, используется для кражи данных кредитных карт (номера кредитной карты, пароля, пин-кода и т. д.) с целью последующего присвоения чужих денежных средств.

Первые попытки фишинга были зафиксированы в конце 90-х годов прошлого столетия, и с тех пор популярность этого вида мошенничества постоянно растет. При этом мошенники могут действовать следующим образом.

Пользователь получает электронное письмо от лица своего банка с просьбой (а точнее – с требованием) срочно перейти по указанной в письме ссылке и подтвердить свои регистрационные данные. Ссылка приводит пользователя на поддельный сайт, который является точной копией сайта банка. Разумеется, ничего не подозревающий пользователь спокойно вводит свои конфиденциальные данные в форму на этом сайте, и в этот же момент эти данные попадают к злоумышленникам.

Здесь возможны различные варианты. Например, мошенники могут потребовать ввести регистрационные данные либо для их подтверждения, либо для подтверждения якобы полученного крупного денежного перевода, и др.

Каким же образом можно распознать, что полученное от имени банка письмо – фальшивка?

В большинстве случаев подобные письма могут иметь следующие признаки:

- ◆ к пользователю обращаются не лично по имени и фамилии, а общим приветствием – вроде «Уважаемый клиент»;
- ◆ в письме обязательно будет присутствовать гиперссылка на сайт и предложение туда

перейти;

- ◆ требования подтвердить свои конфиденциальные данные весьма настойчивы;
- ◆ в письме возможно наличие угроз (заблокировать счет, прекратить сотрудничество и т. п.) в случае отказа от выполнения требований;
- ◆ не исключено наличие в письме грамматических и иных ошибок.

Также для заманивания пользователя на фальшивый сайт может использоваться внедренная в его компьютер вредоносная программа. Ее задача заключается в том, чтобы автоматически перенаправить пользователя на фальшивый сайт, как только он наберет в интернет-обозревателе определенный веб-адрес (как правило – адрес своего банка). Ну а дальше – обычная схема: ввод конфиденциальных данных в предложенную форму, после чего они попадут в руки мошенников.

Иногда для фишинга используются специальные клавиатурные шпионы. Их отличие от обычных клавиатурных шпионов (кейлоггеров) заключается в том, что они активизируются только после входа пользователя на определенный сайт (например – сайт банка). В результате все выполненные на этом сайте действия (в том числе и ввод данных кредитной карты) становятся известны злоумышленникам.

Поиск спутника жизни

Достаточно популярен вид интернет-мошенничества, в котором предлагается найти «спутника жизни за границей».

В России на эту удочку попадаются в основном потенциальные невесты, которые заплатят деньги кому угодно, лишь бы выйти замуж за границу. За границей – наоборот, обманутыми в большинстве случаев становятся потенциальные женихи, желающие найти себе русскую невесту. Известны случаи, когда один мошенник обманывал десятки и даже сотни людей, высылая им фотографии «кандидатур», вступая в переписку от имени «кандидата» и т. п. Затем он просил произвести либо оплату за услуги, либо поступал еще проще – от имени избранника (избранницы) просил денег «на дорогу» либо на что-нибудь подобное. Разумеется, после получения денег мошенник бесследно исчезал.

Ресурсов, предлагающих подобные услуги, в Интернете существует великое множество. Не стоит слепо доверять всем подряд, даже если предложение кажется «улыбкой судьбы». Перед тем как воспользоваться услугами ресурса, не поленитесь навести справки о нем. Во-первых, для этого можно просто ввести его название или адрес в поисковой запрос и ознакомиться с результатами поиска, а во-вторых – в Интернете достаточно «черных списков», в которых содержатся сведения о мошенниках, предлагающих найти спутника жизни за границей.

Оплата за хакерские услуги

В качестве «приманки» для выманивания денег пользователя могут применяться различного рода хакерские услуги. Наиболее распространенные способы – взлом почтовых ящиков, подбор паролей, атака на сайты и т. п. (рис. 6.7)

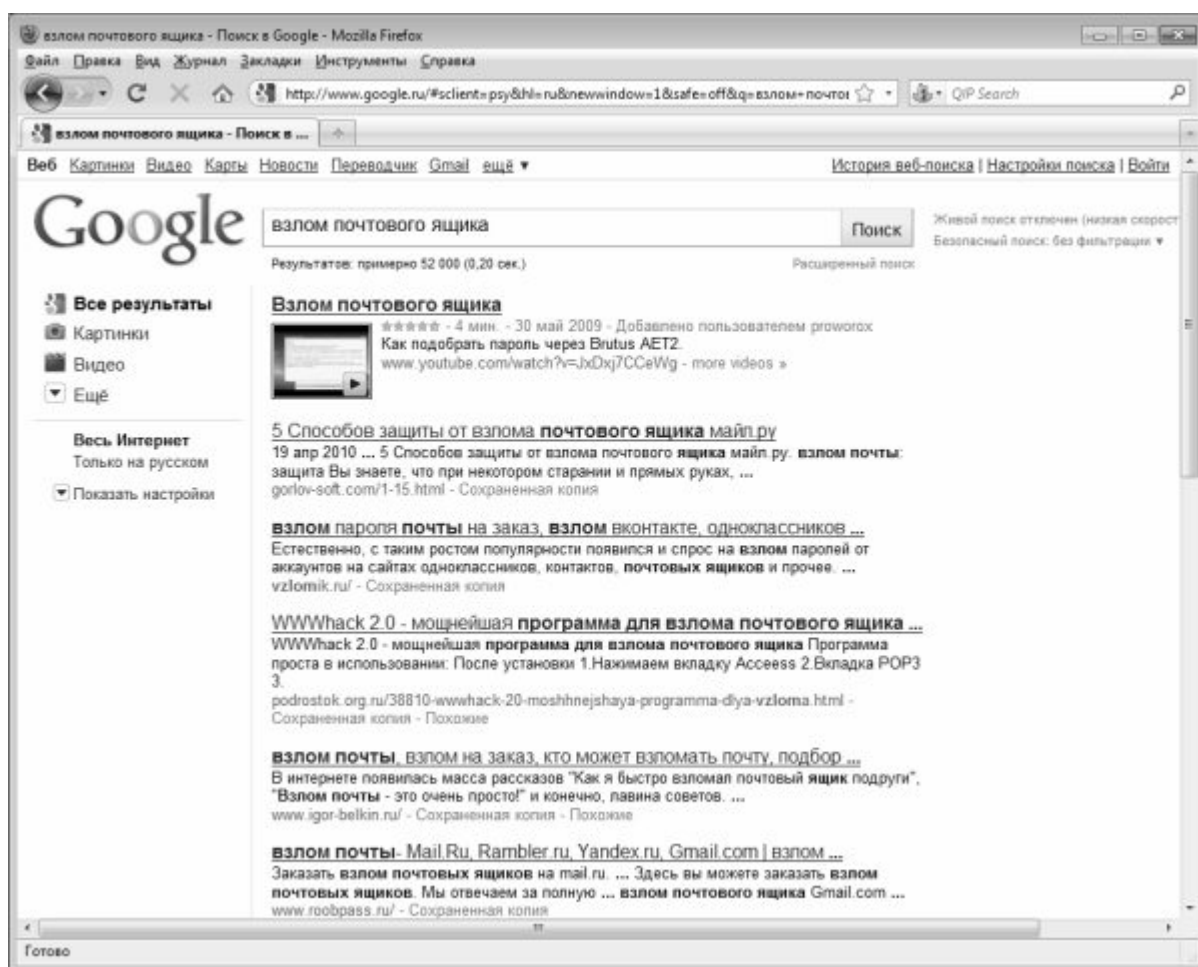


Рис. 6.7. Предложения о взломе почтовых ящиков – «лохотрон»

Например, какой обыватель откажется от возможности просмотреть содержимое почтового ящика своего начальника? Или конкурента? Или жены? Вариантов заинтересовать доверчивого пользователя более чем достаточно. И все это удовольствие – всего за 10-20-30 (сумма может быть любой) долларов США! После перевода денег пользователь будет долго и безнадежно ждать оплаченной информации...

Например, если вы хотите «обрушить» сайт конкурента и обратитесь с этой целью к поисковой системе, то получите множество ссылок, из которых минимум 90 % – мошеннические предложения. Как правило, злоумышленники не интересуются спецификой сайта, не задают вопросов, которые могут быть интересны специалистам, реально оказывающим такие услуги. Обычно разговор короткий: переводите деньги на счет – и завтра сайт будет «лежать». Стоит ли говорить, что это банальный и наглый «развод»!

Как мошенники могут использовать социальные сети

Выше мы уже отмечали, что социальные сети пользуются популярностью не просто у обывателей, но и у мошенников. Во многом это обусловлено тем, что подавляющее большинство пользователей таких сетей не имеют почти никакого представления об опасности, которая может исходить из Интернета. Многие из них вообще имеют компьютер только для общения в социальных сетях. Жертвами мошенников становятся в первую очередь именно такие беспечные пользователи.

Известно, что в социальных сетях каждый пользователь может оставлять о себе самые разнообразные данные: возраст, место работы или учебы, оконченная школа или факультет института, хобби и др. Кроме этого, в списке гостей содержится информация о круге общения данного человека. Этих сведений предприимчивым злоумышленникам бывает

вполне достаточно для того, чтобы успешно «разводить» людей на деньги.

Вот характерный пример. Человеку присылают СМС-сообщение примерно следующего содержания: *«Папа, я попал в неприятность, нахожусь в милиции. Передай брату Антону, чтобы искал адвоката, скажи однокласснику Сергею, чтобы временно уехал за город, а Света (жена) пусть приготовит мне передачу. Но в первую очередь положи, пожалуйста, на этот номер деньги: мой телефон в милиции забрали, но в камере есть нелегально телефон, мне дали с него позвонить, но нужно положить на него деньги. Сразу после пополнения баланса я сообщу подробности. Очень жду».*

Не правда ли, эмоциональное сообщение? Отметим, что иногда мошенники не СМС отправляют, а звонят человеку и эмоционально, сбивчиво, а потому – очень правдиво говорят примерно то же самое (якобы их попросил связаться с родственниками попавший в неприятность человек). При этом ситуации могут обыгрываться самые разные: попадание в милицию, дорожно-транспортное происшествие, попадание в больницу, и т. д.

Успешность данной аферы в определяющей степени зависит от умения мошенника ошеломить человека, сбить его с толку и вынудить его немедленно, на эмоциях пополнить баланс указанного телефона (иначе говоря, заставить человека сделать что-то прежде, чем подумать). И в этом ему очень помогают реальные данные о человеке, полученные из социальных сетей. Именно там он узнает, что у этого человека есть брат Антон, одноклассник Сергей и жена Света. Причем брат Антон работает юристом (следовательно – у него, по идее, должны иметься связи в адвокатской среде), одноклассник Сергей имеет криминальное прошлое (значит, у него могут быть причины скрываться от милиции), а жена Света очень любит мужа и, конечно же, приготовит ему передачу в камеру.

Но это еще не все. Зачастую мошенники не гнушаются «проиллюстрировать» свои послания. И если мобильный телефон жертвы поддерживает передачу фотографий – то в подтверждение СМС он может получить фотографию своего родственника, сидящего в камере в окружении бритых уголовников. Как нетрудно догадаться, эта фотография также берется из персональной странички человека в социальной сети, после чего соответствующим образом обрабатывается в Фотошопе или другом графическом редакторе. Если же мошенники обыгрывают ситуацию, например, с попаданием близкого человека в дорожно-транспортное происшествие – они могут прислать фотографию, где этот человек лежит окровавленный под машиной, и т. п.

Надо отдать злоумышленникам должное – они отлично понимают, на какие «болевы точки» человека нужно надавить, чтобы он, немедленно бросив все, побежал пополнять баланс неизвестного ему телефонного счета.

Чтобы не стать жертвой подобного «развода», нужно в подобной ситуации прежде всего связаться со своим «попавшим в беду» родственником и выяснить, действительно ли это так. Иногда для этого бывает достаточно просто позвонить ему на мобильный телефон или связаться по ICQ.

И еще: без особой надобности не выкладывайте в социальных сетях слишком много информации о себе: фотографии (особенно своих детей!), круг общения, род занятий, и т. п. Иначе ваши шансы стать жертвой мошенников многократно увеличиваются.

Фиктивные реалити-шоу

Несколько лет назад в Рунете появился относительно новый вид интернет-мошенничества, сущность которого заключалась в приглашении всех желающих поучаствовать в новом реалити-шоу.

Схема мошенничества базируется на распространении в Интернете рекламных объявлений, в которых сообщается, что на одном из федеральных телевизионных каналов открывается новое реалити-шоу, участвовать в котором могут все желающие. Вернее, все желающие могут подавать заявки, а к участию допускаются только те, кто прошел предварительный отбор. Всем участникам такого шоу гарантируется огромная популярность,

известность и успех (или крупные выигрыши вроде квартиры или машины), и эта информация неудержимо толкает наивных обывателей в сети мошенников.

Вначале на сайте будущего реалити-шоу предлагается оформить соответствующую заявку для предварительного рассмотрения кандидатуры. Обычно такая заявка имеет шаблонный вид, в ней указывается набор стандартных данных – пол, возраст, род занятий, образование, фотография, семейное положение и т. д. Если человек допускается к участию в реалити-шоу (кто бы сомневался!) – ему предлагается перечислить по указанным реквизитам определенную сумму денег в качестве уплаты за «регистрацию участников», «компенсацию накладных расходов» и т. п. Основания для перечисления денег могут приводиться разные, и, как правило, подчеркивается, что реалити-шоу будет проходить в другом городе, что, несомненно, связано с дополнительными расходами.

О том, что происходит дальше, догадаться нетрудно: после перечисления денег мошенники перестают отвечать на электронные письма. Кстати, если в объявлении о наборе участников в реалити-шоу отсутствуют контактные данные организаторов (кроме электронного адреса) – это однозначно «лохотрон». Иногда мошенники после получения могут сообщить, что, мол, условия конкурса изменились, и вы теперь нам не подходите, а деньги мы вернуть не можем, поскольку вы в любом случае были зарегистрированы. Но это редкость – обычно они исчезают вместе с деньгами.

Помните, что организаторы настоящих реалити-шоу никогда не проводят набор участников через Интернет. Все организационные подробности озвучиваются через эфир телеканала, на котором предполагается выпуск шоу. Что касается отбора кандидатов, то он не ограничивается рассмотрением каких-то поверхностных шаблонных анкет, а проходит в несколько этапов. Конечно, анкетирование потенциальных участников тоже проводится – но это только первый этап, за которым обычно следует личное собеседование и видеосъемка. В некоторых реалити-шоу на этапе анкетирования или личного собеседования необходимо представить свое портфолио. **При этом все этапы отбора проводятся совершенно бесплатно.**

Характерной особенностью данного мошеннического приема является то, что по закону злоумышленников очень трудно привлечь к ответственности. Это обусловлено тем, что в соответствии с действующим законодательством обращаться по факту мошенничества в правоохранительные органы имеет смысл только после той даты, на которую была назначена съемка. Иначе говоря – только после того, как обман фактически был совершен. До этой даты факт мошенничества недоказуем. Этот юридический нонсенс предоставляет злоумышленникам достаточно времени для того, чтобы позаботиться о своей безопасности и успешно замести следы.

Предсказания и составление «индивидуальных» гороскопов

Узнать свое будущее в той или иной степени интересно большинству обывателей. Кто-то для этого учится расшифровывать сны, кто-то ходит к гадалкам, а с появлением Интернета появилась возможность находить и изучать самые разнообразные гороскопы и предсказания.

подавляющее большинство имеющихся в Интернете гороскопов находятся в свободном доступе и открыты для просмотра всеми желающими. По большому счету, это логично, поскольку ценность и актуальность подобных гороскопов весьма сомнительна: в большинстве случаев они представляют собой ничего не значащий набор общих фраз.

В связи с этим в Интернете объявилось великое множество мошенников, готовых «за небольшую плату» составить индивидуальный гороскоп или предсказание будущего всем желающим. Эти мошенники не имеют никакого понятия об астрологии и прочих подобных науках, зато очень неплохо научились выискивать подходящие гороскопы в Интернете и адаптировать их к конкретному пользователю. Относительная достоверность их предсказаний объясняется рядом факторов.

Например, перед составлением гороскопа мошенник просит клиента предоставить некоторую информацию о себе. Если клиент, предположим, в ближайшем будущем оканчивает институт – в гороскопе появится информация о том, что его скоро ждет «интересная работа». Если у человека тяжело болеет старенькая бабушка – ему предскажут «временные трудности, после которых наступит облегчение, возможно получение внепланового дохода». Расшифровать логику мошенника нетрудно: временные трудности – это уход за больным и его смерть, облегчение – когда со временем уйдет боль утраты, и в то же время ни за кем не надо ухаживать, а внеплановый доход – оставшаяся от бабушки квартира или иное наследство.

Также информацию о клиенте мошенник может получить из социальных сетей (ведь клиент ему сообщит ФИО, адрес и иные данные, по которым его легко можно найти в социальной сети). Например, в социальной сети можно узнать, что человек недавно женился (следовательно – предсказать ему скорое появление наследников), и т. д.

Так что не стоит слишком сильно доверять различного рода предсказателям и составителям гороскопов, оказывающим свои услуги за деньги – их методы работы банальны и не содержат никакой мистики.

Продажа «чудодейственных» медикаментов

Разнообразие и ассортимент существующих интернет-афер порой просто поражает. Некоторые виды обмана (например, продажа программ для взлома электронных кошельков, «бизнес-пакетов» для быстрого обогащения, кражи денег из интернет-казино и т. п.) можно назвать логичными – в конце концов, многие пострадавшие становятся жертвами собственной алчности, жадности и лени. Однако способ мошенничества, о котором мы сейчас расскажем, отличается немалой долей самого настоящего цинизма.

Речь идет о продаже «чудодейственных» медикаментов в Интернете. Чего только не предлагают доморощенные «интернет-провизоры»: волшебные таблетки «от всех болезней», средства для улучшения мужской силы, пилюли от головной боли, от подагры, мази от радикулита и вообще – любые лекарства от всех болезней. Иногда складывается впечатление, что сайты подобной тематики разрабатывались на основании справочника медицинских болезней – настолько широк ассортимент предлагаемых лекарств от всех мыслимых и немыслимых «болячек».

При этом никаких сертификатов и гигиенических удостоверений на продаваемые медикаменты зачастую просто не существует. Оплаченный в такой интернет-аптеке товар доставляется курьером или отправляется по электронной почте, после чего претензии предъявлять некому. Отметим, что подобным образом часто продаются просроченные медикаменты, которые не только не лечат, но способны нанести немалый вред здоровью.

На сайтах, где осуществляется продажа «чудодейственных препаратов», иногда широко представлена информация о том, что «наши препараты прошли все государственные исследования», «рекомендованы врачами специалистами», «проверялись в Академии здоровья», и т. п. Но даже если на сайте будет выложена отсканированная копия сертификата или иного документа, подтверждающего качество продукции – не факт, что она будет подлинной. Мошенники могут взять действующий сертификат совершенно другого лекарства, отсканировать его и внести требуемые «корректировки» с помощью Фотошопа или другого графического редактора. Насчет «рекомендаций врачей-специалистов» – это вообще пустые слова, поскольку эти рекомендации никогда ничем не подтверждаются. Ну а насчет проверки медикаментов в Академии здоровья или иных организациях с вызывающим уважением названием – так при элементарной проверке может выясниться, что такой организации и в помине не существует. Эти «маркетинговые ухищрения» интернет-мошенники позаимствовали на телевидении – ведь часто приходится наблюдать рекламу с «рекомендациями лучших диетологов» или «ведущих собаководов», которых никто никогда не видел и не слышал.

Поэтому не стоит экспериментировать со своим здоровьем и покупать различного рода «чудодейственные препараты» у сомнительных продавцов. Тем более что многие из таких препаратов вообще не зарегистрированы на территории Российской Федерации и продаются фактически нелегально.

Глава 7. Помоги себе сам. Как не стать жертвой мошенников

Ранее мы уже неоднократно говорили о том, что каждый пользователь Интернета в состоянии самостоятельно обезопасить себя от посягательств удаленных злоумышленников. В данной главе мы приведем конкретные рекомендации относительно того, что для этого нужно сделать, и чего делать не стоит.

Ответственность за мошенничество в сфере IT-технологий

Поскольку действия интернет-мошенников прямо подпадают под юрисдикцию Уголовного кодекса РФ, мы приведем статьи УК, в соответствии с которыми злоумышленников можно привлечь к ответственности.

Статья 159 УК РФ. Мошенничество

1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, – наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет.

2. Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, – наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года либо без такового.

3. Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере, – наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от двух до шести лет со штрафом в размере до десяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Мошенничество, совершенное организованной группой либо в особо крупном размере, – наказывается лишением свободы на срок от пяти до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Чтобы не стать жертвой мошенников. Полезные советы по безопасности

Дабы максимально оградить себя от посягательств злоумышленников, при работе в Интернете следует соблюдать меры предосторожности и правила, которые перечислены ниже.

◆ Прежде чем выходить в Интернет, установите на компьютер хорошую антивирусную программу. Следите за тем, чтобы антивирусные базы все время были актуальными, и помните, что в мире ежечасно появляется несколько новых вирусов.

◆ Никогда не храните логины, пароли, пин-коды, номера кредитных карт и прочие конфиденциальные сведения в открытом виде – например, в обычном текстовом файле, или на бумажке, прикрепленной к монитору. Как показывает практика, множество афер совершается благодаря тому, что беспечная жертва своевременно не позаботилась о хранении секретных данных в надежном месте.

◆ Если вы подключаетесь к Интернету через телефонную линию, никогда не выключайте динамик модема. Это позволит сразу распознать попытки интернет-мошенников несанкционированно подключить ваш компьютер к тому или иному удаленному веб-ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг подобной направленности).

◆ Если вы все же хотите хранить все конфиденциальные данные в одном файле – заархивируйте этот файл и защитите архив надежным паролем (минимум из 16 символов). Рекомендуется использовать для этого архиватор WinRAR – как показывает практика, расшифровать такой пароль практически нереально.

◆ Если вы услышали, что модем начал самопроизвольно набирать какой-то номер без вашего участия – срочно отключитесь от Интернета путем физического отсоединения кабеля. Затем просканируйте компьютер специальной программой категории Antispyware (антишпионским приложением) – очень может быть, что в компьютер тайно внедрен шпионский модуль автоматического дозвона. В конечном итоге это чревато получением астрономических счетов от телефонной компании.

♦ Не доверяйте посторонним свои учетные данные, а также не предоставляйте право пользования своими электронными кошельками, управления банковскими счетами через Интернет, и т. п. К сожалению, нередко мошенниками становятся именно те, кому вы больше всего доверяете. Кроме этого, даже если доверенное лицо является кристально честным человеком, ваши конфиденциальные данные у него могут просто похитить.

♦ Будьте максимально бдительны и осторожны при посещении неизвестных страниц в Интернете. Сегодня широко распространены шпионы и вирусы, для заражения которыми достаточно просто зайти на определенную веб-страницу.

♦ Электронную корреспонденцию, поступившую от неизвестных и сомнительных отправителей, перед открытием обязательно проверяйте надежной антивирусной программой (с актуальными базами). Несоблюдение этого правила может привести к тому, что ваш компьютер быстро превратится в «шпионское гнездо».

♦ После скачивания из Интернета файлов, архивов и т. п. надо сразу же проверить их антивирусной программой, и только после этого запускать на выполнение, распаковывать и т. д. Помните, что многие вредоносные программы распространяются в виде исполняемых файлов либо архивов.

♦ Если вы пользуетесь операционной системой Windows – регулярно проверяйте ее на предмет безопасности. В частности – своевременно скачивайте с сайта Microsoft и устанавливайте на свой компьютер все последние обновления, касающиеся безопасности (так называемые «заплатки»).

♦ Никогда не отвечайте на запросы и письма, в которых содержится просьба прислать ваши секретные данные (логин, пароль, пин-код и т. п.) по указанному адресу. Этот нехитрый способ (разновидность так называемой «социальной инженерии») позволяет злоумышленникам получить чужие логины, пароли, пин-коды кредитных карт, и иные конфиденциальные сведения.

♦ Если при посещении различных ресурсов в Интернете (форумы, страницы регистрации, и т. д.) требуется оставить о себе некоторые данные, то они должны содержать минимум сведений. В частности, никогда и никому не сообщайте свои паспортные данные, домашний адрес, различные пароли и т. п. Несмотря на то, что владельцы и руководители многих Интернет-ресурсов гарантируют полную конфиденциальность, не будьте наивными: если кому-то надо получить эту информацию, он ее получит, и вполне может использовать для шантажа, вымогательства и т. п.

♦ По окончании работы в Интернете обязательно отсоединяйте кабель от линии соединения с Интернетом. Помните, что в противном случае ваш компьютер будет уязвимым даже в выключенном состоянии.

Помимо перечисленных правил безопасности, при работе в Интернете руководствуйтесь нормами и принципами, которые диктуется здравым смыслом и элементарной осторожностью.

Признаки, по которым можно определить, что вас хотят обмануть

Несмотря на то, что видов и способов интернет-мошенничества существует достаточно много (в чем вы могли убедиться, ознакомившись с предыдущими главами книги), многие злоумышленники действуют шаблонно, по примерно одинаковому алгоритму. Здесь мы приведем несколько характерных признаков, по которым можно безошибочно определить, что вас хотят «развести» на деньги.

♦ Письмо с предложением (о работе, об участии в бизнес-проекте, о выгодных покупках, об инвестициях, поиск спутника жизни и пр.) является спамом. Помните – ни одна серьезная организация не будет опускаться до того, чтобы деловые предложения распространять в виде спама. Ей просто это не нужно – по-настоящему выгодные и перспективные проекты навязчивой рекламы не требуют.

♦ Письмо или объявление изобилует большим количеством грамматических,

орфографических, стилистических и прочих ошибок. Это может свидетельствовать о том, что его составлял либо полуграмотный, либо безответственный и небрежный человек. Естественно, это в принципе исключает возможность того, что он способен предложить что-то действительно стоящее и заслуживающее внимания. Если же вы получили такое безграмотное письмо в ответ на свое сообщение – вероятнее всего, оно сгенерировано автоответчиком. В этом случае злоумышленник даже не удосуживается почитать, что вы там ему написали, а просто информирует вас о том, сколько и куда нужно перечислить денег (подробно сдобривая эту информацию сказками о «крутизне» фирмы, о будущих астрономических доходах и т. п.).

♦ В предложении о работе вам обещают поистине сказочные доходы, иногда подтверждая это отсканированными копиями якобы «чеков» с умопомрачительными суммами. При этом работа занимает немного времени, не требует специального образования и подготовки, легка и приятна.

♦ Вам неоднократно подчеркивают преимущества надомной работы, делая акценты на «болевых точках», которые есть у большинства обывателей: мол, зачем работать «на дядю» – лучше на себя; зачем вставать каждое утро по будильнику – спите сколько хотите и работайте по свободному графику; зачем ждать очередной отпуск – ведь намного лучше отдыхать тогда, когда вам хочется, а не когда начальник соизволит отпустить вас; зачем унижаться перед руководством, выпрашивая отгул – лучше самостоятельно планировать свое время и т. п.

♦ В мошенническом предложении непременно будет содержаться просьба перечислить (перевести, заплатить и т. п.) определенную сумму по указанным реквизитам под тем или иным предлогом – в зависимости от того, что именно вам предлагают. Это может быть «плата за регистрацию», «залог как подтверждение порядочности», «инвестиции под высокие проценты», перевод денег на «волшебный кошелек», «аванс под выгодную покупку», «ставка на участие в игре» и т. д. **В любом случае, обоснование платежа значения не имеет – важно помнить одно: если в любом поступившем из Интернета предложении, рекламе и т. п. содержится требование или просьба перевести деньги – это однозначно «лохотрон».**

♦ Как правило, мошенники просят перечислить деньги на электронный кошелек WebMoney (чаще всего), Яндекс. Деньги или других электронных платежных систем. Это обосновано тем, что при банковском или почтовом переводе злоумышленника можно вычислить, а вот электронные платежные системы гарантируют полную анонимность.

♦ Мошеннические предложения характерны тем, что в них отсутствуют координаты и контактные данные. Максимум, что они предоставляют – электронный почтовый адрес, иногда – сайт. Иначе говоря, ни фирма, ни виртуальное казино, ни интернет-магазин, ни «инвестиционный фонд» своего адреса и сайта не имеют. Даже мобильный телефон (не говоря уже о городском) злоумышленники давать боятся. Если в объявлении все же присутствует какой-то почтовый адрес – это или абонентский ящик (см. рис. 1.1), или фальшивый адрес, который либо вообще не существует, либо в нем находится совершенно посторонняя организация, не имеющая к мошенникам никакого отношения. Учтите, что фальшивый адрес может быть составлен хитро: например, злоумышленники указывают вполне реальную улицу, реальный почтовый индекс, а вот номер дома – вымышленный, причем ненамного отличающийся от реального. В частности, если на данной улице последний номер дома 43, то мошенники могут указать в объявлении несуществующий дом № 44. Такой нехитрый прием зачастую позволяет ввести в заблуждение даже тех жертв, которые неплохо знают данный район. Например, знаете ли вы последний номер дома на улице, где вы живете или работаете? А иногда даже номер дома указывается верно, но к нему добавляется несуществующий корпус или строение.

♦ Если в мошенническом предложении есть ссылка на веб-сайт компании – то этот сайт будет располагаться на бесплатном хостинге, а если и на платном – то срок аренды хостинга будет минимальным, как и размер оплаты. Иначе говоря, «известная фирма с мировым

именем», «успешное онлайн-казино», «интернет-магазин с многомиллионным оборотом», «крупнейший инвестиционный фонд» и прочие «Рога и копыта» не имеют даже 15–20 долларов США, чтобы арендовать более-менее приличную хостинг-площадку. Еще одна характерная особенность состоит в том, что мошеннические сайты, как правило, сделаны наспех, содержат минимум информации, практически не имеют дизайнера, и зачастую состоят всего из одной-двух страниц.

♦ Если мошенники предлагают способ заработка, то никаких возрастных, половых, профессиональных и прочих требований к будущим сотрудникам они не предъявляют. Стандартный набор критериев – возраст от 16 до 60 лет (или вообще не ограничен), образование значения не имеет, опыт работы не требуется, специальная подготовка не нужна. При этом мошенники могут делать упор на то, что их предложение будет особенно интересно врачам, учителям, преподавателям, военным и представителям прочих профессий с традиционно невысоким уровнем заработка.

♦ В подтверждение своей «порядочности» мошенники могут предъявлять электронные копии различного рода «сертификатов». Как правило, основные реквизиты на этих «сертификатах» являются неразличимыми. Это может касаться серии и номера документа, даты его выдачи, наименования организации, выдавшей документ, а также печатей и штампов. Но даже если все данные на сертификате хорошо читаются – не обольщайтесь: очень может быть, что организации, якобы выдавшей сертификат, вообще не существует. С особым подозрением следует относиться к сертификатам, которые якобы выданы зарубежными структурами и составлены на иностранном языке: проверить наличие этой организации вы не сможете.

Таковы основные признаки, которые могут помочь вам своевременно распознать мошенников. В целом суть большинства из них в том, что человеку предлагается быстро стать богатым, не прилагая для этого никаких усилий. Поэтому важно помнить известную истину: бесплатный сыр бывает только в мышеловке.

Избегай стандартных паролей!

Многие пользователи часто совершают одну и ту же ошибку, пользуясь стандартными, шаблонными паролями. Один из самых характерных примеров – когда пароль совпадает с логином. Подобрать такой пароль элементарно, а дальше злоумышленник будет действовать в зависимости от того, к чему относится данный пароль. Если это кредитная карта или банковский счет, управлять которым можно через Интернет – все деньги с этого счета исчезнут моментально. Если это пароль к электронному почтовому ящику – злоумышленник получает доступ ко всей вашей переписке, в том числе и конфиденциального и личного характера. Это дает ему практически неограниченные возможности для шантажа и вымогательства, кроме этого – он может писать от вашего имени любые письма всем имеющимся адресатам. Если этот пароль используется для входа в блог – можно ожидать появления в собственном блоге провокационных, оскорбительных и прочих записей. Другими словами, беспечность при выборе пароля может обернуться огромными финансовыми потерями и прочими неприятностями.

Ниже мы приводим перечень наиболее часто встречающихся стандартных паролей. Если в этом списке вы найдете свой пароль – рекомендуется немедленно заменить его, поскольку эти пароли хорошо известны даже начинающим мошенникам.

- ♦ password
- ♦ parol
- ♦ monkey
- ♦ myspace1
- ♦ password1
- ♦ blink182
- ♦ 123456 (варианты – 1234567, 12345678, 987654321 и другие логичные

последовательности цифр)

- ◆ Qwerty
- ◆ abc123
- ◆ letmein

Кроме этого, стандартными являются пароли с названием марки автомобиля, породы собаки, населенного пункта, и т. п. Если вы не хотите дать мошенникам лишнюю возможность для реализации своих преступных замыслов – потрудитесь придумать нестандартный пароль, тем более что это совсем несложно.

Советы пользователям системы WebMoney

Как мы уже отмечали ранее, электронные платежные системы притягивают мошенников подобно магниту. Поскольку самой популярной такой системой является WebMoney, мы дадим несколько советов и рекомендаций ее пользователям, соблюдение которых позволит минимизировать риск попадания в сети злоумышленников.

◆ Если с электронными кошельками вы работаете через WebMoney Keeper (эта программа предоставляется пользователям системы бесплатно, скачать ее можно на сайте www.webmoney.ru), то настоятельно рекомендуется использовать последнюю версию программы. Отметим, что в некоторых случаях вы можете вообще не получить доступ к кошелькам, пока не установите последний релиз. Дело в том, что разработчики системы постоянно следят за надежностью системы безопасности, и вовремя вносят необходимые изменения в программу. Если вы будете пользоваться устаревшими версиями WebMoney Keeper – риск стать жертвой мошенников существенно возрастает.

◆ В настройках безопасности включите опцию автоматического контроля IP-адреса. Благодаря этому доступ к вашему кошельку будет возможен только с вашего IP-адреса. Но учтите, что если вы будете работать через прокси-сервер, или по каким-то причинам прятать свой IP-адрес с помощью предназначенных для этого утилит – кошелек может не открыться, пока вы не войдете в Сеть под «родным» IP-адресом.

◆ Файлы ключей храните только на внешних носителях. Если они будут находиться на жестком диске, удаленный злоумышленник может легко получить к ним доступ. Оптимальный вариант – записать их на компакт-диск или флеш-накопитель, и подключать такой носитель только при работе с системой WebMoney. Этот нехитрый прием, хоть и не дает стопроцентной защиты от злоумышленников, по крайней мере сводит к минимуму вероятность того, что удаленный мошенник успеет получить доступ к файлам ключей.

◆ Как можно больше увеличьте размер файла ключей – например, до 100 Мб. В этом случае даже если мошенник и найдет у вас эти файлы – выкачать их ему будет очень сложно ввиду большого размера.

◆ По умолчанию файл ключей системы WebMoney имеет расширение *.kwm. Попробуйте изменить его на какое-либо другое – например, *.txt. В сущности, программе WebMoney Keeper без разницы, какое расширение будет у файла ключей, а вот злоумышленника, имеющего доступ к вашему компьютеру, тем самым можно ввести в заблуждение.

Как самостоятельно распознать наличие в компьютере программ-шпионов

Отличительной чертой Spyware является то, что их трудно распознать с помощью штатных антивирусных программ. Для борьбы с ними предназначены специальные утилиты, которые можно скачать в Интернете. Но помните: многие шпионские программы маскируются именно под утилиты для борьбы с ними. В результате, установив на свой компьютер утилиту для борьбы с Spyware, можно вместо нее заполучить сам шпионский модуль. Поэтому для борьбы со Spyware рекомендуется либо использовать утилиты

известных разработчиков, либо воспользоваться рекомендациями других пользователей, уже столкнувшихся с подобной проблемой ранее.

Характерные признаки наличия в компьютере SpyWare

В некоторых случаях пользователь может самостоятельно, без применения специальных программ категории AntiSpyware распознать присутствие в компьютере шпионского ПО. Характерные симптомы, позволяющие это сделать, перечислены ниже:

- ◆ при запуске Internet Explorer по умолчанию начинает открываться совершенно незнакомая веб-страница (а не пустая страница или не та, что была ранее определена пользователем как домашняя страница);

- ◆ значительно увеличивается исходящий трафик;

- ◆ наблюдаются сбои в работе операционной системы;

- ◆ появление неоправданно высоких счетов за телефонную связь (наверняка в компьютер проник шпионский модуль автоматического дозвона);

- ◆ в Internet Explorer появились незнакомые элементы управления (кнопка, пункт контекстного меню, инструментальная панель и т. п.);

- ◆ появились незнакомые элементы в списке Избранное, причем удаление их невозможно;

- ◆ в окне Диспетчер задач на вкладке Процессы видно, что какой-то новый процесс использует ресурсы компьютера почти полностью;

- ◆ на экране монитора периодически произвольно появляются рекламные окна, причем даже при отсутствии действующего подключения к Интернету;

- ◆ на рабочем столе появляются незнакомые иконки либо значки, при активизации которых осуществляется автоматический переход на незнакомую веб-страницу.

Кроме этого, для обнаружения Spyware можно провести небольшую «ревизию» содержимого компьютера. В частности, следует проверить содержимое папки Program Files, каталога автозагрузки, а также раздела Установка и удаление программ в Панели управления. Некоторые шпионские программы помещают свой значок в правую часть панели задач (рядом с часами), поэтому при возникновении подозрений нужно посмотреть – не появился ли в панели задач неизвестный значок? Также нужно проверить содержимое подменю Пуск □ Все программы – некоторые шпионские модули могут проявиться здесь. В Internet Explorer следует проверить страницу, открываемую по умолчанию, а также папку Избранное.

Антишпионская программа SpywareBlaster

Одним из эффективных антишпионских средств по праву считается программа SpywareBlaster (рис. 7.1), разработчиком которой является фирма JavaCoolSoftware. Она предназначена для использования в операционных системах Windows любой версии, начиная с Windows 95.



Рис. 7.1. Программа SpywareBlaster

Программа отличается эргономичным и в то же время простым и интуитивно понятным пользовательским интерфейсом, в котором большинство параметров настраиваются путем установки/снятия соответствующих флажков либо переключателей. Среди всего многообразия параметров работы программы особо следует отметить возможность блокировки настроек домашней страницы (в результате чего уже ни один шпионский модуль не сможет изменить, например, адрес страницы, загружаемой по умолчанию). Также в программе реализована возможность создания «отката» для настроек интернет-обозревателя (кстати, данная утилита поддерживает работу не только с Internet Explorer, но и с другими популярными интернет-обозревателями – в частности, Netscape, Mozilla). В данном случае достаточно зафиксировать текущие настройки интернет-обозревателя (причем можно сохранить несколько различных конфигураций настроек), и при необходимости вернуться к ним в любой момент (обычно – при возникновении подозрений на то, что в настройки интернет-обозревателя без участия пользователя внесены нежелательные изменения).

Кроме упомянутых выше, программа SpywareBlaster имеет еще ряд интересных возможностей.

Антишпионская программа AVZ

Еще одна полезная утилита для борьбы со шпионскими модулями – программа AVZ (рис. 7.2), которая распространяется бесплатно. Многие пользователи считают ее одной из лучших программ для поиска и удаления не только программ-шпионов, но и рекламных модулей. Кстати, помимо борьбы со шпионскими и рекламными модулями, эта программа успешно борется и с некоторыми вирусами. В некотором роде программа является аналогом знаменитой Ad-Aware.

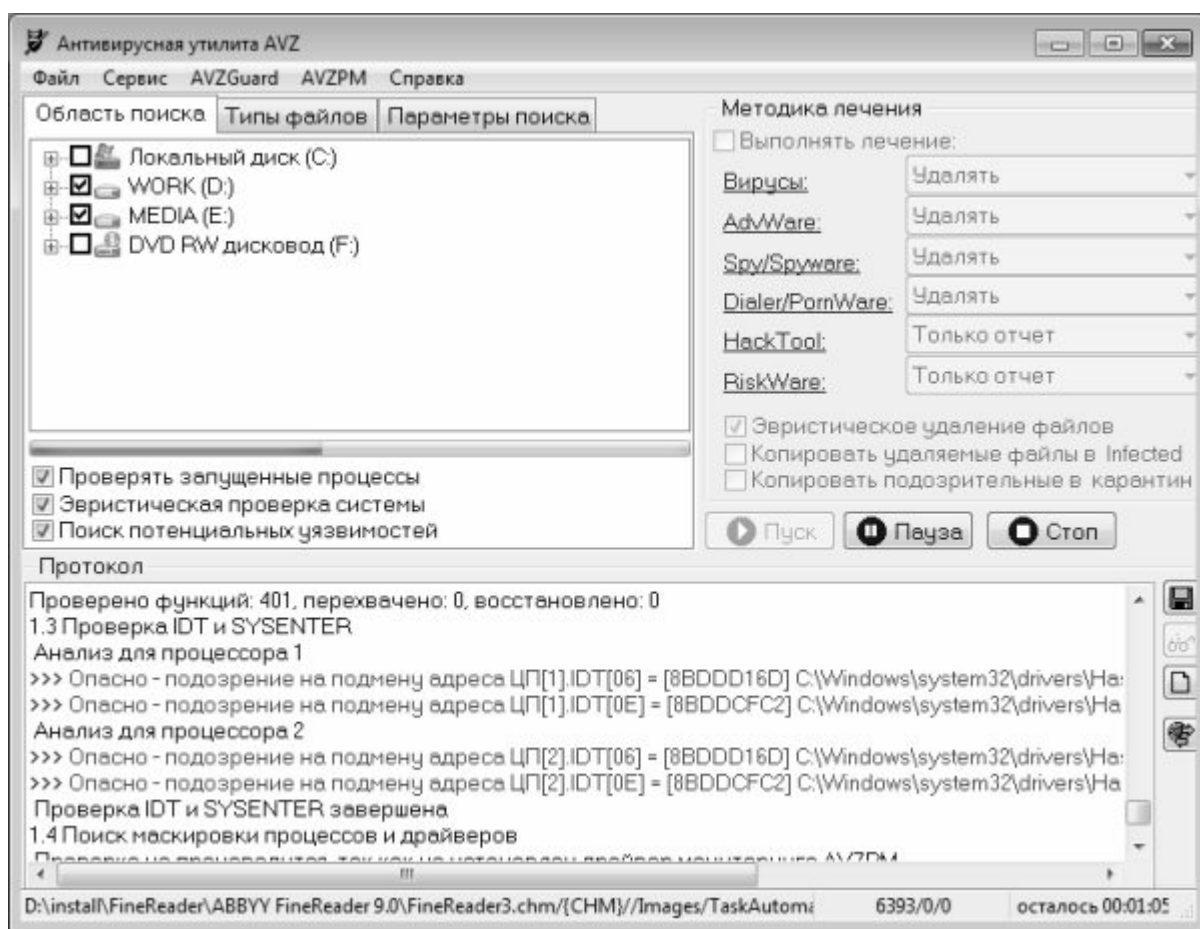


Рис. 7.2. Программа AVZ

Русскоязычный интерфейс программы удобен и понятен пользователю. Предварительная настройка AVZ проста, причем во многих случаях параметры, предложенные по умолчанию, являются оптимальными. Для каждого типа вредоносного объекта, который был обнаружен в процессе сканирования (вирус, программа-шпион и др.), можно указать, каким образом с ним поступить: удалить, выдать только отчет, и др. Кроме этого, можно настроить сканирование на выборочный поиск вредоносных программ – например, искать и удалять только шпионские модули, а все остальное игнорировать.

В программе автоматически ведется протоколирование процесса сканирования. Полученный протокол при необходимости можно сохранить в отдельном файле для последующего изучения.

Программа Anti-keylogger для борьбы с клавиатурными шпионами

Для борьбы с клавиатурными шпионами можно использовать программы, предназначенные для борьбы и с другими Spyware (две из них рассмотрены выше выше), а также специализированные программы, которые называются анти-кейлоггеры. Одной из таких программ является Anti-keylogger, которую разработали российские специалисты.

К достоинствам программы можно отнести ее многоязычность (она поддерживает в том числе и русский язык), а также удобство в эксплуатации. Программа обладает простым и дружелюбным пользовательским интерфейсом. В разделе Опции предусмотрена возможность настройки параметров работы программы. Кроме этого, в разделе Лист исключений реализована возможность ведения списка исключений; в этот список можно включать программы, которые не должны распознаваться как клавиатурные шпионы.

Характерной особенностью программы Anti-keylogger является то, что для ее работы не

предусмотрено использование сигнатурных баз. Это позволяет ей выявлять и блокировать любые виды клавиатурных шпионов, как известные большинству аналогичных программ, так и нет.

Превентивная защита от клавиатурных шпионов

Как мы уже отмечали ранее, клавиатурные шпионы могут иметь как аппаратное, так и программное исполнение. Для защиты от аппаратных кейлоггеров рекомендуется по возможности минимизировать доступ к компьютеру посторонних лиц – это в первую очередь относится к компьютерам, которые установлены на рабочих местах. Ну и, конечно, периодически нужно проверять, не появилось ли между клавиатурой и системным блоком какое-нибудь неизвестное устройство. Иногда это касается и домашних компьютеров – вспомните, кто имеет доступ к вашему компьютеру? Одно дело – если только вы, и другое – если, например, к вашему сыну-студенту периодически приходят «продвинутые» в компьютерном отношении друзья и возятся около компьютера. В последнем случае, вполне возможно, вам потехи ради (или с более серьезными намерениями) вставят какого-нибудь «жучка».

Что касается программных шпионов-перехватчиков, то в качестве профилактики можно применять меры, как и для защиты от вирусов и прочего вредоносного софта.

Что же делать, если предполагается, что в компьютер уже проник клавиатурный шпион? Прежде всего – просканировать компьютер специально предназначенной программой. Для поиска и уничтожения клавиатурных шпионов можно использовать некоторые программы из числа тех, что предназначены для борьбы и с другими Spyware; кроме этого, есть программы, специализирующиеся именно на клавиатурных шпионах (об одной из них мы рассказали в предыдущем разделе). Однако бывают ситуации, когда выполнение немедленного сканирования невозможно, и в то же время необходимо срочно выполнить какие-либо действия с конфиденциальными данными. Как же поступить в таком случае?

При возникновении подобных ситуаций рекомендуется использовать так называемую виртуальную клавиатуру. Виртуальная клавиатура – это программа, интерфейс которой представляет собой изображение клавиатуры, а ввод нужных символов осуществляется с помощью мыши. Поскольку принцип действия большинства клавиатурных шпионов заключается в перехвате вводимых с клавиатуры символов, то использование виртуальной клавиатуры достаточно эффективно.

ВНИМАНИЕ

Помните, что некоторые клавиатурные шпионы снимают копии экрана еще и после каждого щелчка мыши. Для защиты от таких шпионов предусмотрены специальные виртуальные клавиатуры, в которых для ввода символа достаточно просто подвести указатель мыши к соответствующей позиции. Благодаря этому можно ввести информацию без единого щелчка мышью.

При частой или регулярной работе с конфиденциальными данными (например, если вы регулярно совершаете платежи через Интернет с помощью кредитной карты или системы электронных платежей) рекомендуется постоянно использовать виртуальную клавиатуру – ведь никогда нельзя полностью быть уверенным в том, что в компьютер не проник клавиатурный шпион.

Заключение

Хочется верить, что эта книга поможет читателям избежать попадания в

мошеннические сети, хитроумно расставленные по всему Интернету. Теперь вы знаете, где и чего следует опасаться, как проверить заманчивое предложение о сотрудничестве, и почему ни в коем случае нельзя переводить деньги неизвестным лицам (если, конечно, вы не хотите оказать им благотворительную помощь). Помните, что Интернет – это мощный инструмент, с помощью которого злоумышленники выманивают огромные суммы денег у беспечных обывателей.

Автор выражает надежду, что предложенный материал был полезен и интересен читателю. Вопросы и пожелания направляйте по адресу: arsen211@yandex.ru.