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 случае 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 завлекают потенциальных жертв.

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

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

С помощью «Homemailer'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 досягаемые ранее блага.

Если и Вы готовы примкнуть к рядам этих людей, то Вам неимоверно 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 «Homemailer's Program» на рынке труда Украины, России и всего СНГ!

Место жительства не имеет абсолютно никакого значения! За дополнительной информацией обращаться на e-mail sayma_ukraine@hotpop.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 пере-водчик 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 получатся 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 объём работы. Выплата заработной платы два раза в месяц. Деньги будут перечисляться на Ваш ин-тернет кошелек, или же на счёт в банке, или же почтовым перевод. Если у Вас еще нету Интернет кошелька, Вы можете его скачать к себе на компью-тер 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 изна-чально нужны мне как залог, что Вы будете в срок и качественно выполнять Вашу работу. Потому что если Вы не выполните работу, которую Вам пре-доставят-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 недовери 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 объём 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 ин-тернет кошелька, 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

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

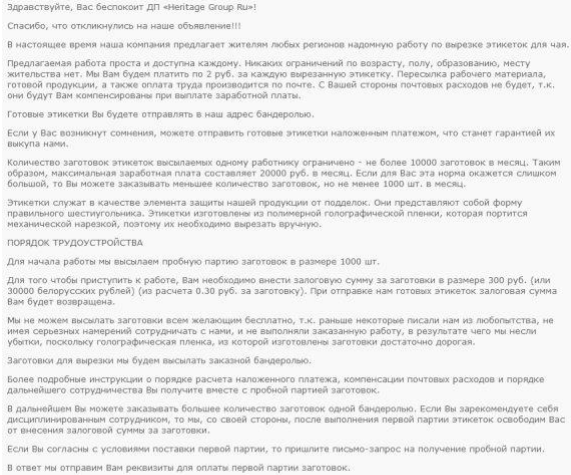
♦ получение денег из электронного кошелька, который пополняется за счет обманутых соискателей.

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.

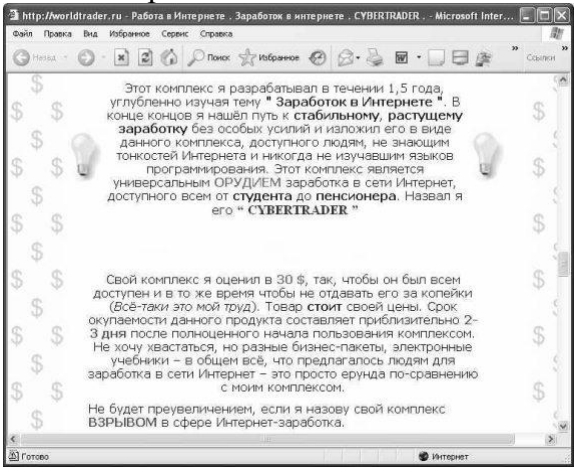


Рис. 1.5. Объявление о продаже платных «комплексов»

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 которым 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 вышлет 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.

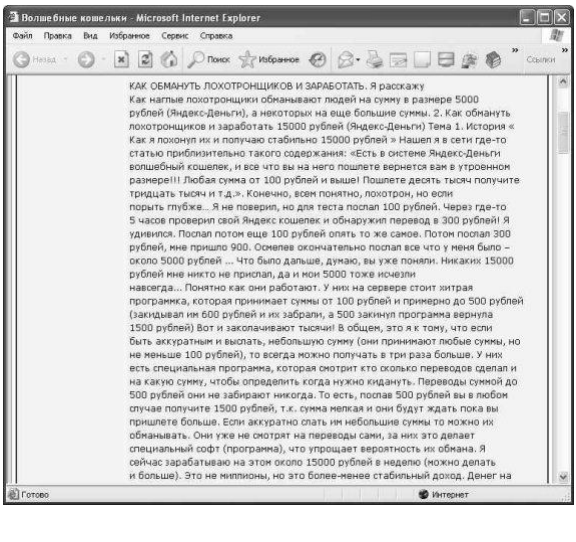


Рис. 2.1. Приманка, которой пользуются мошенники

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, вообщем — 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 «сольет» 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.