КНИГИ ДЛЯ ДЕЛА

Алексей Гладкий

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

Методы удаленного выманивания денег, и как не стать жертвой злоумышленников

Алексей Анатольевич Гладкий

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

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.

Содержание

Введение 5
Глава 1. Обман при устройстве на работу и в предложениях заработка 8
Фрилансер, будь бдителен! 10
Платное «устройство на работу» 19
Конец ознакомительного фрагмента. 21

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 мето-

дички 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».

Конец ознакомительного фрагмента.