**Сетевое мошенничество в вопросах и ответах**

**Деятельность разномастных жуликов, проходимцев, мошенников и прочей малопочтенной публики всегда являлась частью истории человечества. Уже на заре эволюции будущий гомо сапиенс не гнушался стянуть у зазевавшегося соплеменника кусок мамонтятины, кокос или иную добычу. Если потенциальная жертва проявляла бдительность, в ход шли отвлекающие маневры вроде брошенной в сторону палки-копалки.**

С тех пор мало что изменилось принципиально, усовершенствовались лишь методы «сравнительно честного отъема». С течением времени образ проходимца принимал разные формы — от небритого громилы в подворотне с его традиционным «кошелек или жизнь» до респектабельного клерка в дорогом костюме и галстуке. А с развитием ИТ-технологий и появлением Интернета злоумышленник предстал в виде «юзера» — умного, изворотливого, изобретательного и коварного.

В последние годы стремительно растет число людей, пострадавших от деятельности интернет-мошенников. Современные Остапы Бендеры не щадят никого и с одинаковым успехом разводят на немалые деньги как «чайников», так и опытных пользователей Паутины.

Неудивительно, что читатели присылают в редакцию немало вопросов по теме мошенничества в Сети. На самые интересные из них мы и отвечаем в сегодняшнем выпуске рубрики.



**Обозреватель Internet Explorer всегда распространялся бесплатно в комплекте с Windows. Но на днях при выходе в Интернет я попал на страницу Microsoft, где сообщается, что за дальнейшее использование браузера нужно отправить SMS на указанный номер. Нет ли здесь подвоха?**

Еще как есть! В ваш компьютер внедрен шпион, который автоматически переправляет Internet Explorer на подложный сайт, являющийся точной копией страницы Microsoft. Обман очевиден, поскольку столь уважаемая компания, разумеется, не станет связываться с оплатой через SMS. Если вы отправите сообщение на указанный номер — будьте готовы к тому, что с вас снимут денег в несколько раз больше, чем обещано на сайте.

Для устранения проблемы восстановите параметры Internet Explorer, предлагаемые по умолчанию. Затем в свойствах обозревателя на вкладке «Программы» отключите все надстройки. Закройте браузер, запустите его вновь и перейдите на какую-нибудь страницу. Вызовите список надстроек, посмотрите, какая из них включилась самостоятельно, и «убейте» соответствующий ей файл. И пользуйтесь Explorer абсолютно бесплатно!

Известно, что злоумышленники умеют неплохо подбирать пароли к почтовым ящикам, кредитным картам и прочим ресурсам. Как защититься от взлома?

Здесь проблема скорее не в ловкости мошенников, а в беспечности пользователей. Характерный пример — когда пароль совпадает с логином. Не стоит использовать распространенные, шаблонные варианты — они тоже подбираются почти моментально. Вот несколько самых популярных стандартных паролей: password, parol, monkey, myspace1, password1, blink182, 123456 (и другие логичные последовательности цифр), Qwerty, abc123, letmein. Если вы используете нечто подобное — срочно меняйте от греха подальше. Также стандартными являются пароли с названием марки автомобиля, породы собаки (кошки, лошади, крокодила), населенного пункта и т.п. Проверить надежность выбранной комбинации символов можно с помощью специального онлайн-сервиса Microsoft: [**www.microsoft.com/rus/protect/your-self/password/checker.mspx**](http://www.microsoft.com/rus/protect/your-self/password/checker.mspx).



**Недавно наткнулся в Интернете на предложение купить за 20 долл. программу для взлома электронных кошельков WebMoney. Авторы уверяют, что гарантия 100%. Я не жулик, но меня интересует: неужели в мой кошелек можно так легко проникнуть?**

Как сказал бы Коровьев из «Мастера и Маргариты» Михаила Булгакова, это типичный «случай так называемого вранья». Подумайте сами — зачем за 20 долл. продавать программу, которая запросто вскрывает чужие кошельки и крадет из них деньги? Не проще ли самому озолотиться?

Да если бы что-то подобное существовало, всю систему WebMoney опустошили бы в течение суток! Но она живет и никто на нее не жалуется… Равно как и на «Яндекс.Деньги» и прочие электронные платежные системы.

Доверчивому простаку со скрытыми криминальными наклонностями они в лучшем случае не ответят, получив с него денежки, а в худшем — пришлют под видом взломщика кошельков шпионскую софтину, которая при первой возможности «сольет» им все, что найдет в его компьютере. И в первую очередь — идентификатор, номер и пароль кошелька, а также файл ключей и код доступа к нему.



**Я начинающий фрилансер, выполняю работы для удаленного заказчика. Хотел бы расширить свою деятельность, но опасаюсь «кидалова». Как проверить порядочность потенциального работодателя?**

Фриланс — дело тонкое. Прежде всего уточните адрес работодателя и его контактный телефон. Если вам отказывают или не отвечают — это «развод». Введите в любой поисковик название фирмы или фамилию работодателя (сойдет и e-mail) и ознакомьтесь с результатами — это часто проясняет ситуацию. Если вас спрашивают, где вы живете и можете ли подъехать в офис — возможно, это проверка «на вшивость»: ведь чем дальше находится фрилансер, тем проще и безопаснее его кинуть. Поэтому всегда отвечайте: да, я готов встретиться лично (даже если работодатель располагается в другом регионе). Мошенников это отпугнет, а перед порядочным заказчиком, пожелавшим вас лицезреть, можно извиниться и объяснить все мерами безопасности. По крайней мере, вы будете знать, что от вас не прячутся.

Учтите, что тестовое задание зачастую не оплачивается — после его отправки вам могут просто не ответить (такой «развод» — целая индустрия). И не вздумайте перечислять кому бы то ни было деньги «за материалы для работы», «услуги по пересылке задания» и т.п. — это однозначно лохотрон.

**При работе в Интернете на экране появилось всплывающее окно с сообщением о том, что некая программа бесплатно просканировала мой компьютер и обнаружила в нем вирус. Для избавления от него предлагается перейти по указанной ссылке. Стоит ли это делать?**

Ни в коем случае. От вируса это вас не избавит, а скорее всего его и вовсе нет. Хотя сообщение об «угрозе» может выглядеть впечатляюще (соответствующее оформление, неприятные визжащие и скрипящие звуки). Если вы перейдете по ссылке — попадете на сайт, где вам будет предложено недорого купить «надежную антивирусную программу». В лучшем случае после получения денег мошенники просто испарятся. В худшем — пришлют вам софтину, которая в реальности окажется трояном, вирусом или spyware-модулем. А иногда вредоносный код начинает загружаться сразу после щелчка мышью на такой ссылке. Лучше после сомнительного предупреждения просканируйте компьютер надежным проверенным антивирусом с актуальными базами — и все тайное станет явным.

**Я решила похудеть и зашла на сайт с диетами. Этот ресурс является бесплатным, для доступа к информации достаточно лишь зарегистрироваться. Но через некоторое время с баланса моего мобильника стали списываться немалые суммы. Как оказалось, так называемый бесплатный сайт брал деньги за предоставление диет! Это что — новый вид мошенничества?**

Да, по сути это обман, хотя с точки зрения закона все стерильно. В процессе регистрации на сайте вы указали номер своего мобильного телефона, на который должна высылаться вся необходимая информация.

А вот правила подписки на данном сайте (они открываются по едва заметной ссылке) вы наверняка не читали. В них указано, что бесплатно услуга оказывается лишь один день. Если после этого вы не отказались от нее, то дальнейшее предоставление информации осуществляется за деньги. На этом и строится весь расчет: пока жертва заметит, что с баланса пропадают средства, пройдет несколько дней. Пока сообразит и разберется, за что именно они списываются — еще какое-то время. Вот и весь фокус. Требовать деньги назад бессмысленно, ведь в правилах подписки все расписано честно и подробно. А то, что линк на эту информацию почти незаметен — это уж, извините, такого закона нет, чтоб крупные ссылки делать.

**При попытке открыть свою страницу на сайте**[**www.vkontakte.ru**](http://www.vkontakte.ru/)**отобразилось сообщение, что она заблокирована за рассылку спама. Вновь сделать доступной ее обещают только после отправки SMS на указанный номер. В чем дело, я ведь никогда спамом не занимался?**

Типичная уловка, активно используемая мошенниками в социальных сетях. Проблема решается просто, быстро и бесплатно. В каталоге C:WINDOWSsystem32driversetc найдите файл hosts (он не имеет расширения) и удалите в нем строки следующего вида (в зависимости от названия социальной сети):

XXX.XXX.XXX.XXX vkontakte.ru
XXX.XXX.XXX.XXX odnoklassniki.ru

Вместо ХХХ в них отображаются цифры от 1 до 255. Вот, собственно, и все!



**Как почитаешь — так кругом одни мошенники. Посоветуйте, как обезопасить себя от «кидалова» в Интернете?**

Как ответил бы Остап Бендер, «полное спокойствие может дать человеку только страховой полис». Однако есть несколько признаков, по которым можно распознать мошенников.

Когда вам что-то предлагают в спамовом письме — это лохотрон. Если полученное сообщение изобилует ошибками — то же самое. Зачастую подобные письма генерируются роботами.

Типичный обман — когда вам предлагают легкую работу, обещая при этом умопомрачительный доход. К письму могут приложить копии плохо сфабрикованных чеков с большим количеством нулей. При этом делают оговорку: чтобы стать богатым и счастливым, нужно перечислить совсем немножко денег на этот кошелек. Акцент делается на «болевых точках»: зачем работать на дядю — лучше на себя, ездить в офис не нужно — все можно делать дома, да еще по свободному графику и т.д.

Если в письме или на сайте указан минимум контактных данных, это серьезный повод для опасений. Отсутствие реального почтового адреса или телефона — дополнительный индикатор «развода».

Если ресурс, на котором размещено выгодное предложение, находится на бесплатном или дешевом хостинге с минимальным сроком аренды — даже не связывайтесь.

Не верьте копиям сертификатов, которые часто размещают на сайтах, — проверить их достоверность вы все равно не сможете, а на компьютере можно сфабриковать что угодно, хоть удостоверение шефа ЦРУ.

С подозрением относитесь к любым предложениям и ресурсам, делающим упор на бесплатное предоставление чего-либо: деньги с вас все равно вытянут, только вы это не сразу заметите. И помните: в 99% случаев мошенники обогащаются лишь за счет вопиющей беспечности добропорядочных людей.