**[Ловушки интернета - примеры и методы защиты от них](http://www.securrity.ru/articles/571-lovushki-interneta-primery-i-metody-zashhity-ot.html)**

автор: [**Administrator**](http://www.securrity.ru/user/Administrator/) | [31 октября 2009, 13:12](http://www.securrity.ru/2009/10/31/) | Просмотров: 8636
теги: [Статьи](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [Ловушки](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [интернет-угроз](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD-%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [примеры](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [методы](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [защита](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [жертвы](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [Киберпреступники](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/), [КОМПЬЮТЕР](http://www.securrity.ru/tags/%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD%EF%BF%BD/)

**1. Введение**

С самого раннего детства мы учимся анализировать - осознанно или нет - жесты и интонацию других людей. Как показали исследования, примерно в 60% случаев мы больше обращаем внимание на жестикуляцию человека, чем на его слова, и используем полученную информацию для оценки того, насколько правдив говорящий в момент речи.

Это необходимо нам для того, чтобы не стать жертвами обманщиков и мошенников и других людей, которые пытаются манипулировать нами. Однако обман и мошенничество представляют угрозу не только в реальной жизни - последнее время отмечается значительный рост количества разнообразных интернет-угроз.

Это означает, что при оценке потенциальной опасности необходим новый подход - электронные письма и сообщения от друзей в социальных сетях лишены жестов и интонации, и здесь мы можем ориентироваться только на текст и изображение. Означает ли это, что мы больше не можем доверять интуиции?

Казалось бы, это так, по крайней мере, на первый взгляд. Однако интернет предоставляет другие возможности, позволяющие компенсировать недостаток интуиции; тем не менее, для того, чтобы использовать эти возможности, мы должны знать, чего следует остерегаться.

Киберпреступники и мошенники вряд ли смогут изобрести колесо, поэтому однажды столкнувшись с мошенничеством или вредоносной программой и четко усвоив, что это такое, Вы сможете использовать эту информацию в будущем.

В этой статье мы рассмотрим некоторые типичные примеры и предложим методы защиты. В первую очередь статья будет полезна для новичков в Сети, однако, возможно, приведенные примеры также будут интересны и для завсегдатаев интернета.

**2. Классические почтовые угрозы**

Допустим, Вы новичок в интернете. Общение с ним Вы, скорее всего, начнете с того, что заведете себе учетную запись в системе электронной почты. Действующий адрес электронной почты необходим не только для переписки с друзьями и близкими, он также потребуется Вам для того, чтобы совершать покупки через интернет или регистрироваться на форумах или в социальных сетях.

К сожалению, точно так же, как Ваш почтовый ящик может быть забит ненужными рекламными листовками, ящик электронной почты может оказаться заполненным нежелательными сообщениями.

Спам составляет до 89% всех электронных сообщений. Это сообщения, которые вас совершенно не интересуют: Вам предлагают кредиты под низкие проценты, скидки на Виагру и море других продуктов и услуг.

Такого рода предложения ни в коей мере не легитимны, и сообщения нередко содержат ссылки на сайты, зараженные вирусами, троянскими или другими опасными программами. Такие сообщения необходимо удалять, не открывая, - в этом случае они не смогут нанести вред вашему компьютеру - Вам лишь придется потратить время на их удаление.

Легко сказать, что эти письма нужно просто удалять, - иногда искушение их открыть так велико. Киберпреступники умны: они проявляют особую активность накануне таких больших праздников, как Рождество, Пасха и, конечно же, День святого Валентина.

Этот праздник - особенно хорошая возможность для мошенников, ведь именно в день Святого Валентина можно, не стыдясь, сказать о своих чувствах, даже если Вы едва знакомы. Если бы Вы получили сообщение в День святого Валентина с темой «Я тебя люблю», Вы ведь открыли бы его?

Киберпреступники используют для своих целей не только праздники и «горячие» темы. Интернет часто называют вершиной развлекательных технологий - он изобилует сайтами, на которых размещены исключительно забавные статьи, картинки и видеоролики.

Нам всем иногда хочется отвлечься и отдохнуть, и этим пользуются киберпреступники, рассылая сообщения с интересными заголовками, например: «Смотри смешное видео!» или «Забавное фото!».

Однако надо обязательно удержаться от искушения открыть приложенный файл: с 99,99% вероятности он может содержать программы, способные нанести вред данным, хранящимся на вашем компьютере, отслеживать Вашу активность в Сети или попросту украдут у Вас что-нибудь...

В статье [Лаборатория Касперского представила отчет о спам-активности в третьем квартале 2009](http://www.securrity.ru/articles/570-laboratoriya-kasperskogo-predstavila-otchet-o.html) сообщается, что 0,46% всех электронных сообщений содержат вредоносные приложения.

Казалось бы, цифра невысока, однако если принять во внимание, что ежедневно пересылается 500 000 видов спам-сообщений, общее число сообщений окажется достаточно значительным, особенно если учесть, что каждое сообщение рассылается на миллионы электронных адресов.

**3. Фишинг**

Пожалуй, одним из наиболее известных видов мошенничества является фишинг. Вы получаете сообщение, в котором вас просят перейти по указанной ссылке и ввести личную информацию: пароль, номер банковского счета и т.д.

Сообщение может выглядеть так, как будто оно пришло от банка, интернет-магазина eBay, платежной системы, например, PayPal и.т.д. Как бы убедительно ни выглядело сообщение, это все равно фальшивка: если вы нажмете на ссылку и введете запрашиваемую информацию, Ваши данные окажутся в руках киберпреступников, и те смогут использовать их в своих целях.

Многие банки приняли дополнительные меры по безопасности для предотвращения попыток фишинга, в результате чего фишинговых сообщений, нацеленных на наиболее популярные банки, становится меньше. Однако это не значит, что такой вид мошенничества больше не используется - он всего лишь видоизменился в соответствии с веяниями времени.

Фишинговые сообщения - явление глобальное: один и тот же базовый текст переводится на разные языки, а само сообщение конструируется таким образом, чтобы выглядеть так, как будто это письмо от известного банка или финансовой организации.

Мошенники кладут много сил на разработку дизайна сообщений, и нередко бывает сложно отличить использованные в них логотипы и цвета от оригинала. С другой стороны, текст часто изобилует грамматическими и орфографическими ошибками, что должно сразу же насторожить пользователя.

Помимо этого, если отправитель сообщения обращается к вам «Уважаемый клиент» вместо того, чтобы назвать Вас по имени, то это явный показатель фишинга. Сейчас, когда даже информационные рассылки могут быть персонализированы, очень маловероятно, что отправитель легитимного сообщения не будет использовать в обращении Ваше имя.

И наконец, легитимные банки никогда не запрашивают PIN-код, код авторизации операции (TAN) или другую конфиденциальную информацию, тем более через электронную почту.

Как мы уже говорили, от фишинговых атак могут пострадать не только банки. В последнее время многие фишинговые сообщения рассылаются для сбора информации об учетных записях в электронных платежных системам типа PayPal или сайтах-аукционах типа eBay.

Фишинг составляет 0,94% всех спам-сообщений, и целых 60% таких сообщений нацелены на PayPal. Такие сообщения зачастую содержат угрозы о том, что счет может быть закрыт по той причине, что он якобы не использовался в течение какого-то времени.

Для того чтобы сохранить учетную запись, Вам предлагается войти в систему. А для этого, конечно же, в письме Вам услужливо предоставляется ссылка. При переходе по ссылке Вы попадаете на страницу, которая выглядит, как сайт соответствующей платежной системы, после чего Вас просят ввести логин и пароль.

Несмотря на свою схожесть с оригиналом, такой веб-сайт - фальшивка. Никогда не пользуйтесь полученными по электронной почте ссылками на страницы, где Вас просят ввести конфиденциальную информацию.

Используйте закладки в Вашем браузере или сами вводите адрес в адресной строке Вашего браузера. Даже если ссылка кажется верной, сценарий javascript, выполняющийся в фоновом режиме, может открыть адрес, который полностью отличается от отображаемого.

*Еще лучше оригинала? Фальшивый сайт eBay, используемый при фишинге:*


Если Вы не уверены в легитимности сообщения, позвоните в соответствующую компанию или напишите туда и выясните, посылали ли они Вам сообщение.

Однако если Вы хотите связаться с компанией через электронную почту, не отвечайте на сомнительное сообщение: зайдите на сайт компании и воспользуйтесь указанной контактной информацией.

В этом случае Ваш запрос гарантированно будет отправлен по назначению, а не на фальшивый обратный адрес, используемый мошенниками или спамерами.

**4. Кто хочет стать отмывателем денег?**

В современной экономической ситуации многие находятся в поисках работы, поэтому информация о вакансиях не бывает лишней. Предположим, Вы получаете по электронной почте предложение о работе, в котором Вам обещают хорошую зарплату за работу на дому с минимальными затратами времени и усилий.

Даже если у Вас уже есть хорошая работа, дополнительные 1500-2000 евро в месяц выглядят определенно привлекательно. Что же для этого нужно делать? Всего-навсего получать деньги со счета A и переводить их на счет B через Western Union, за вычетом некоторой суммы, которая остается Вам в качестве комиссионных.

К сожалению, если что-то выглядит слишком хорошо и просто, значит, в этом есть какой-то подвох. Деньги, которые Вас просят переводить, получены с помощью фишинга или другим обманным путем; Ваша же роль - стать частью запутанной цепочки, по которой мошенникам идут деньги.

Это усложняет поиск преступников, однако транзакция, которую Вы совершили, совершенно прозрачна. Производя такие переводы, Вы становитесь так называемым «денежным мулом», виновным в отмывании денег или соучастии в преступной деятельности.

Если Вас поймают, Вам грозит крупный штраф, а возможно, и уголовное преследование. Еще раз повторим, что такие сообщения нужно просто удалять, каким бы заманчивым ни казалось предложение.

**5. Поддельные антивирусные программы**

Представьте себе такую ситуацию: Вы просматриваете сайты с целью найти новое фоновое изображение для рабочего стола на вашем компьютере. Вдруг на экране появляется сообщение о том, что Ваш компьютер заражен 527 троянскими программами, вирусами и червями.

Это может показаться Вам странным, ведь на Вашем компьютере установлена защитная программа, и она никак не отреагировала на угрозы. Возможно, она плохо работает? Или что-то пропустила?

Оправившись от потрясения, Вы еще раз перечитываете сообщение. Вам сообщают, что Вы можете загрузить новое антивирусное ПО, которое поможет решить Вашу проблему.

И что самое замечательное - программа совершенно бесплатна! Со вздохом облегчения Вы решаете воспользоваться выгодным предложением и устанавливаете новое ПО.

После запущенной вручную проверки программа обнаруживает еще больше вирусов на Вашем компьютере. На этот раз перед вами другое сообщение: для удаления вредоносных программ нужна полная версия продукта, которую необходимо купить.

При быстром просмотре сайта Вы видите цены в пределах от ?30 до ?80. Так как антивирусная программа, которая уже была установлена на компьютере, Вас подвела, Вы надеетесь на вновь найденное «чудесное решение», оплачиваете его и щелкаете по ссылке «Обезвредить». Кажется, на этот раз все угрозы исчезли... Но так ли это на самом деле?

Такой вид мошенничества известен уже давно - преступники используют опасения пользователя, что компьютер серьезно заражен. Поддельные антивирусы могут действовать по-разному.

Чаще всего, работая в Сети, пользователь видит всплывающее окно, которое будто бы производит проверку жесткого диска компьютера. Затем выдается сообщение о некотором количестве найденных на компьютере вредоносных программ (число выбирается случайным образом).

Немного менее распространенный подход называется «drive-by загрузка»: Вы просматриваете зараженный сайт, и нежелательное ПО попадает на Ваш компьютер. В случае с поддельными антивирусами программа с короткими интервалами выводит сообщения о том, что Ваш компьютер заражен.

На Вашем рабочем столе даже может измениться фоновое изображение - чтобы напомнить Вам о заражении (которого, как мы помним, на самом деле нет).

Поменять его обратно не так легко; соответствующая опция исчезла из меню настроек, и хотя существуют другие способы, они требуют более продвинутых технических навыков, чем те, которыми обладает большинство людей. Таким образом, оказывается, что ПО, которое сначала казалось «чудесным решением», на самом деле совершенно бесполезно.

*Поддельная антивирусная программа:*


Зато поддельные антивирусы приносят очевидную выгоду киберпреступникам, которые получают прибыль от продажи «лицензий» на фальшивые защитные программы.

Помимо этого, фальшивки нередко содержат действительно вредоносные программы, которые могут использоваться для получения доступа к Вашему компьютеру, кражи Ваших персональных данных с целью их дальнейшей перепродажи или для превращения компьютера в зомби-машину и рассылки огромного количества спама.

И хотя может показаться, что это не особенно доходное дело, спамеры часто платят большие деньги за приобретение или аренду таких компьютеров, чтобы обеспечить большую рассылку своих сообщений, что является еще одним способом получения прибыли для киберпреступников.

Мошенники изо всех сил стараются, чтобы сообщения программы об обнаружении вирусов были убедительными, а сама программа выглядела как настоящее антивирусное решение.

Кроме того, такие программы нередко имеют названия, очень напоминающие названия легитимных защитных приложений. Все это помогает придать фальшивке сходство с оригиналом и одурачить даже достаточно опытных пользователей Сети.

Что же делать? Убедитесь, что на Вашем компьютере установлена надежная антивирусная программа. Если Вы видите такие сообщения, не пугайтесь и, конечно же, не покупайте предлагаемое ПО. Воспользуйтесь антивирусной программой, уже установленной на Вашем компьютере, для полной проверки системы.

**6. Осторожно: скрытая подписка!**

Сегодня практически для любых целей можно найти бесплатное программное обеспечение. Каждый может выбрать что-то для себя: игры, программы-проигрыватели, клиенты систем мгновенного обмена сообщениями и т. д., причем источников, откуда эти программы можно загрузить, достаточно много.

Скажем, Вы ищете новое ПО для офиса - программы для обработки текста, электронных таблиц, и т. д. Вы вводите запрос, и поисковая система выдает большое количество вариантов.

Самая первая ссылка звучит многообещающе. Казалось бы, это легитимный веб-сайт со всеми необходимыми файлами, и вы, не долго думая, заходите на него.

Однако прежде чем вы можете загрузить все, что вам нужно, Вас просят зарегистрироваться и указать свое имя, адрес и действующий адрес электронной почты.

И хотя это кажется Вам несколько странным, тем не менее, Вы слышали о порталах, где регистрация необходима, чтобы загружать файлы с максимальной скоростью.

Таким образом, испытывая определенное раздражение, но чувствуя себя опытным пользователем, имеющим опыт регистрации в различных интернет-магазинах, социальных сетях и форумах, Вы вводите требуемую информацию в соответствующих полях формы.

Вы быстро ставите галочку, подтверждая свое согласие с условиями обслуживания, не утруждаясь их прочитать, потому что «вообще-то там всегда написано одно и то же». И уже через пару минут Вы радостно загружаете нужную программу.

Однако вскоре вас ждет неприятный сюрприз в виде электронного сообщения с требованием заплатить ?96. Оказывается, согласившись с условиями, Вы подписались на услуги по поддержке на 2 года. И если вы не заплатите, на вас подадут в суд.



Такой род жульничества особенно популярен в Германии. По подсчетам, от 10 до 20% жертв действительно платят эти деньги.

Однако не нужно поддаваться на угрозы такого рода. В данном случае мошенники пытаются вымогать у Вас деньги, сыграв на вашей законопослушности.

В конце концов, Вы сами знаете, что не прочитали условия договора (возможно по той причине, что все равно бы их не поняли или никогда раньше не слышали ни о каких негативных последствиях).

И если Вы получаете такое электронное сообщение, сначала наведите справки: попробуйте найти в интернете описание похожих случаев или позвоните адвокату. Скорее всего, угроза не имеет под собой никаких юридических оснований и останется всего лишь угрозой, так как киберпреступники рады и тем деньгам, которые они получают от 10-20% жертв.

**7. Мошенничество в социальных сетях**

Такие социальные сети как Одноклассники, Вконтакте, Facebook или MySpace пользуются особой популярностью у молодых людей. Эти сайты позволяют поддерживать связь с друзьями, обмениваться информацией, а также искать новых друзей.

Также существуют и социальные сети для пользователей постарше; они используются для установления и поддерживания деловых контактов или поиска школьных друзей. Какой бы сайт Вы ни использовали, Вас везде может подстерегать опасность.

Предположим, что Ваш близкий друг просит Вас о помощи. Скорее всего, Вы сразу же согласитесь помочь. А теперь перенесем эту ситуацию в контекст социальной сети.

Друг посылает Вам сообщение о том, что он застрял в лондонском аэропорту Хитроу, ему угрожали оружием и ограбили. Он остался без денег, кредитной карточки и билета на самолет и просит переслать ему $400 через Western Union, чтобы он смог добраться домой.

Возможно, Вы зададите себе вопрос, почему деньги необходимо перевести именно через Western Union? Друг утверждает, что для него это единственный способ их получить.

Вы спрашиваете, как ему позвонить, но, естественно, его телефон украли. У Вас закрадывается все больше и больше подозрений - друг ведет себя странновато и использует выражения, которые Вы никогда раньше от него не слышали.

Возможно, причиной тому - сложная ситуация, в которую он попал. Так как вам небезразлична судьба друга, и вы не хотите, чтобы вас мучили угрызения совести, в итоге Вы переводите деньги. И после этого он пропадает.

Что же на произошло на самом деле? В настоящее время этот вид мошенничества очень популярен и эффективен, так как о нем еще относительно мало известно.

Объяснение достаточно простое: киберпреступники получают доступ к учетной записи Вашего друга и пытаются вытянуть деньги из всех, кто находится в его списке контактов.

Если Вы часто пользуетесь социальными сетями, количество ваших друзей может насчитывать несколько сотен, и Вы не всегда в курсе, где они находятся в данный момент, что делает такую историю более правдоподобной.

Однако в вышеописанном случае налицо признаки попытки мошенничества. Европеец, находясь в Лондоне, вряд ли станет просить другого европейца прислать американские доллары.

То же самое относится к используемому языку и выражениям. Если Вы получаете такое сообщение, свяжитесь с другом напрямую.

Даже если в сообщении он пишет, что его мобильный телефон украли, все равно попытайтесь набрать его номер: Вы будете приятно удивлены, когда он возьмет трубку и Вы не только сможете поболтать с ним, но также узнаете, что никакого сообщения он не посылал.

Чтобы защитить свою учетную запись в социальной сети от использования мошенниками, необходимо следовать нескольким несложным правилам. Один из возможных способов защиты Вашей учетной записи связан с тем, как устроена система восстановления пароля.

При регистрации в социальной сети обычно Вам предлагается ответить на «секретный вопрос». Если Вы забудете пароль, Вы сможете создать новый, ответив на заданный вопрос.

Обычно пользователю предлагается выбрать всего лишь из трех «секретных вопросов» общего типа, например, таких, как имя Вашего домашнего любимца или название Вашей первой школы. Если Вы указали эту информацию в своем профиле или на своей странице, добраться до вашей учетной записи будет проще простого.

Чтобы сохранить секретность своей учетной записи, Вы можете сколь угодно часто менять вопрос и ответ. Никому не сообщайте свой логин и пароль.

Кроме того, не попадайтесь на удочку мошенников, рассылающих фишинговые сообщения (описаны выше) и используйте современный антивирус с актуальными антивирусными базами: это поможет вам избежать попадания на Ваш компьютер троянских программ, которые могут выкрасть пароль и переслать его киберпреступникам.

**8. Опасность коротких URL**

Начиная с 2006 года количество пользователей Twitter неуклонно увеличивается. Более 25 миллионов пользователей хотят знать ответ на лозунг сайта «Что ты делаешь?».

Twitter - это социальная сеть, которая отличается от всех остальных - формат микроблогов ограничивает длину сообщения 140 символами, что затрудняет включение в сообщения ссылок, на долю которых может приходиться добрая половина разрешенной длины сообщения.

В этом случае в дело идут менее известные интернет-сервисы, которые переводят длинные сложные адреса в значительно укороченную форму. У сервисов, сокращающих URL, есть свои недостатки: сложно сказать, куда на самом деле отсылает короткая и невнятная ссылка, что отрицательно сказывается на ее прозрачности.

Воспользовавшись этой возможностью, киберпреступники используют такие сервисы для перевода адресов зараженных веб-сайтов в короткую форму.

В таких сообщениях, которые могут распространяться автоматически, Вам обещают сенсационные новости, к примеру, о смерти знаменитости (например, Майкла Джексона).

При отсутствии каких-либо сенсационных событий киберпреступники просто придумывают что-нибудь сами - например, известия о предполагаемой смерти Бритни Спирс широко распространялись на Twitter, в то время как сама певица была жива и здорова.

Сообщения, содержащие ссылки на зараженные веб-сайты, являются всего лишь более изощренной версией мошенничества с использованием электронной почты - в данном случае преступники пытаются сыграть на вашем любопытстве.

К сожалению, такой вид мошенничества показывает, что короткие URL небезопасны. Вы можете защитить себя, используя дополнительные модули для браузеров: например, популярное расширение Firefox, [Long URL Please](http://www.securrity.ru/external.php?link=https://addons.mozilla.org/ru/firefox/addon/9549), которая переводит короткие адреса в исходный формат при удержании курсора мыши на ссылке. Это дает возможность понять, насколько безопасен сайт, на который отсылает ссылка.

**9. Фильмы, игры, музыка и... вредоносные программы**

Если Вы только начинаете пользоваться интернетом, скорее всего, вы начнете с поиска фильмов, музыкальных файлов, ТВ-передач или компьютерных игр.

Помимо правового аспекта загрузки такого контента, о котором уже много писали, необходимо обратить внимание и на другие вопросы. Если Вы ищете контент такого рода, возможно, одноранговые сети покажутся Вам самым легким способом получить его, и Вы загружаете программу, которая поможет Вам зайти в сеть и качать все, что вам нужно.

Хотя вы где-то читали, что такие файлы могут содержать вирусы, вы просто игнорируете этот факт. Однако вы поступаете так на свой собственный страх и риск.

К примеру, к играм часто прилагаются инструменты для взлома, используемые для того, чтобы обойти защиту от копирования. Хакеры предоставляют такие инструменты, так как, по их мнению, любой контент должен быть бесплатным или потому что хотят произвести впечатление на хакерское сообщество.

Что касается самих загрузочных файлов, они могут содержать вредоносное ПО. Киберпреступники хорошо знают о наличии огромного рынка бесплатного контента и, маскируя вредоносные программы под популярные файлы или просто добавляя к популярным файлам вредоносные программы, они увеличивают число потенциальных жертв.

Например, вместе с игрой может загружаться банковская троянская программа - хотя молодые люди нечасто пользуются виртуальными банковскими услугами, компьютер, на который они загружают файл, может принадлежать их родителям, которые регулярно проверяют свой счет через интернет. Таким образом мошенники получают возможность убить сразу двух (или нескольких) зайцев.

Шансы попадания вредоносного ПО на компьютер из одноранговой сети довольно высоки. Поэтому, если, копируя нелегально игры или фильмы, Вы можете сэкономить, то загрузка троянской программы, предназначенной для кражи ваших банковских данных, может обойтись Вам в сотни евро, что мгновенно сводит всю выгоду к нулю. Несомненно, быть честным оказывается выгодно.

**10. Заключение**

Киберпреступники очень изобретательны и по мере возникновения новых интернет-технологий и приложений начинают применять их в своих мошеннических целях.

То есть уже известные схемы приспосабливаются ими к новым возможностям. Лучший пример - классическое спам-сообщение со ссылкой на вредоносный веб-сайт. Теперь уже многие знают, что ни в коем случае нельзя нажимать на ссылки в электронных сообщениях от неизвестных отправителей.

Однако когда это подход был приспособлен для использования в социальных сетях, количество людей, проходящих по ссылкам в нежелательных сообщениях, оказалось весьма большим.

Еще несколько лет назад по внешнему виду сайта можно было определить подделка это или нет: ошибки в правописании, невзрачный внешний вид, и т.п.

Однако сейчас киберпреступники стали намного более изощренными. Если Вы подозреваете, что имеете дело с мошенниками, поищите больше информации в интернете; если это действительно их рук дело, скорее всего, другие жертвы уже сообщили об этом.

Найдите на подозрительных сайтах контактную информацию и сравните ее с другими источниками.

И наконец, следуйте здравому смыслу. Как мы уже говорили, если что-то напоминает вам бесплатный сыр, то неплохо вспомнить и о мышеловке...

Если Вас что-то настораживает, руководствуйтесь своей интуицией, основанной на опыте работы в интернете. Здоровый скептицизм поможет Вам защитить себя от обманщиков и мошенников, а надежная антивирусная программа в актуальном состоянии и обновленные антивирусные базы сделают все остальное.