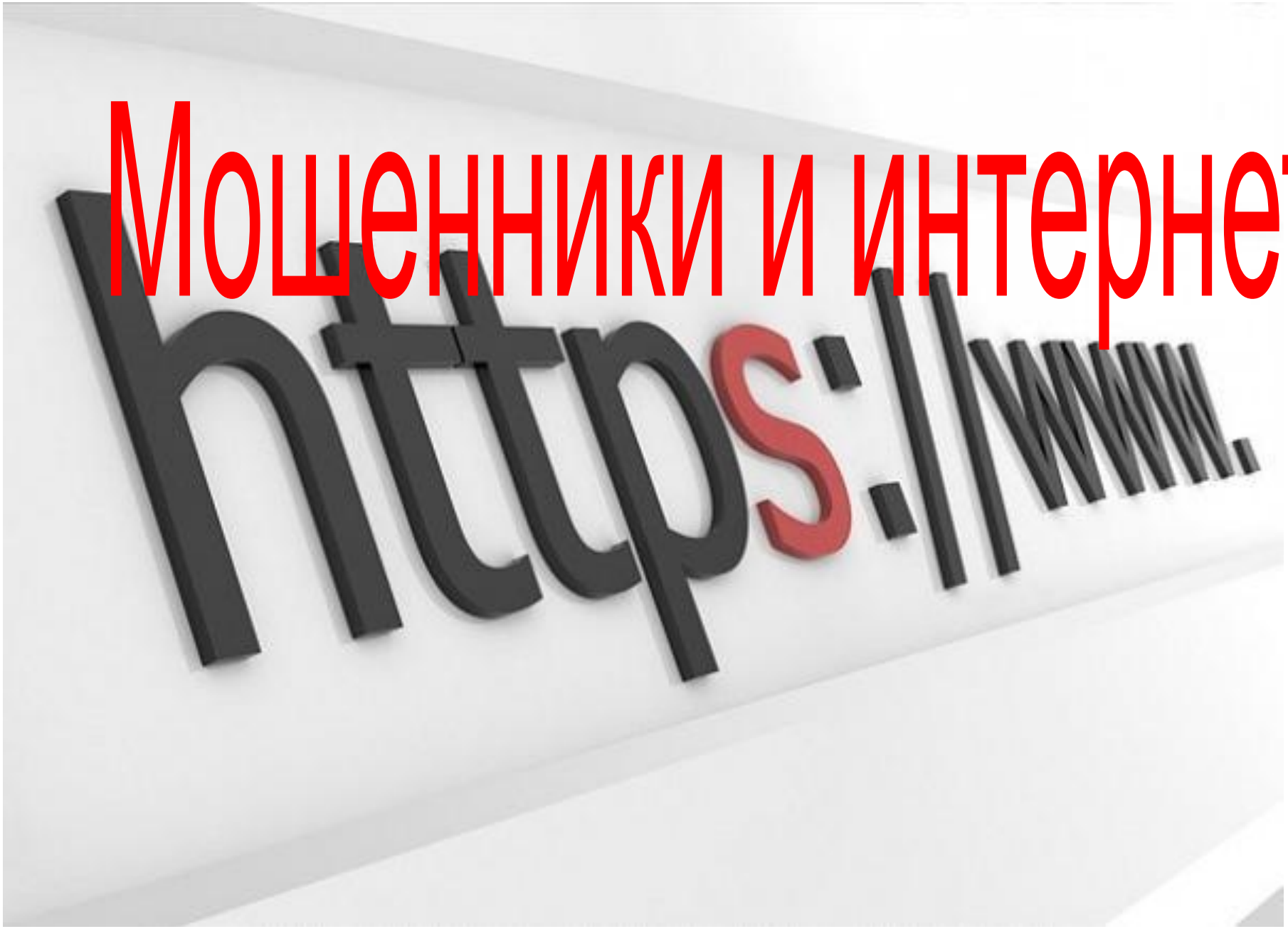
Мошенники и интернет



Особенности Интернет-мошенничества

Мошенничество, как свидетельствует его длительная история, усиливается во времена кризисов и неурядиц в обществе. Нынешний всплеск офлайн и онлайн мошенничества – не исключение. В 2009 году – более 80000 зарегистрированных случаев (прирост – 4,4%) в различных сферах: бизнес, торговля, услуги, финансы и др. Но на самом деле их намного больше – мошенничество часто латентно: владельцы ресурсов не раскрывают фактов мошенничества на своих ресурсах, боясь потери клиентов, особенно, постоянных. Особенно, в банках.

Способы мошенничества и обмана в интернете:

Волшебный кошелек яндекс и webmoney.

Волшебные кошельки яндекс и webmoney можно отнести к самым популярным у интернет-мошенников способам обмана доверчивых пользователей.

В силу простоты всей мошеннической схемы волшебные кошельки уже достаточно долгое время существуют в интернете. Смысл обмана кошелька заключается в удвоении и даже утроении денежных средств посланных на него в течении нескольких минут или часов. «Волшебники» кошельков в основном афишируются с помощью спама, отсылают миллионы писем на эл. почты, захламляют своими сообщениями как форумы, так и социальные сети (вконтакте, одноклассники, мой мир и т.д.), также спамят сайты знакомств, их единственная и главная цель, охватить максимальное внимание большинства обитателей сети, тем самым авось кто клюнет, наивных людей полно же.

Заработок на обмене валют.

Заработок на обмене валют очень интригующие предложение, которое можно увидеть на каком-нибудь сайте в интернете или кликнув по баннеру с надписью типа: "заработай 35$ за 5 минут".

Заработать на обмене валют предлагают много и быстро, но на самом же деле это очередное мошенничество, которое распространилось в интернете сравнительно недавно. Мошенники предлагают всем желающим обменивать различные электронные валюты и при этом получать прибыль. Такое, по их словам, возможно благодаря существенной разнице курсов валют в российских и зарубежных обменных пунктах. Поэтому, те пользователи, которые хотят легко зарабатывать деньги в интернете, могут воспользоваться прилыгающийся к сообщению инструкцией.

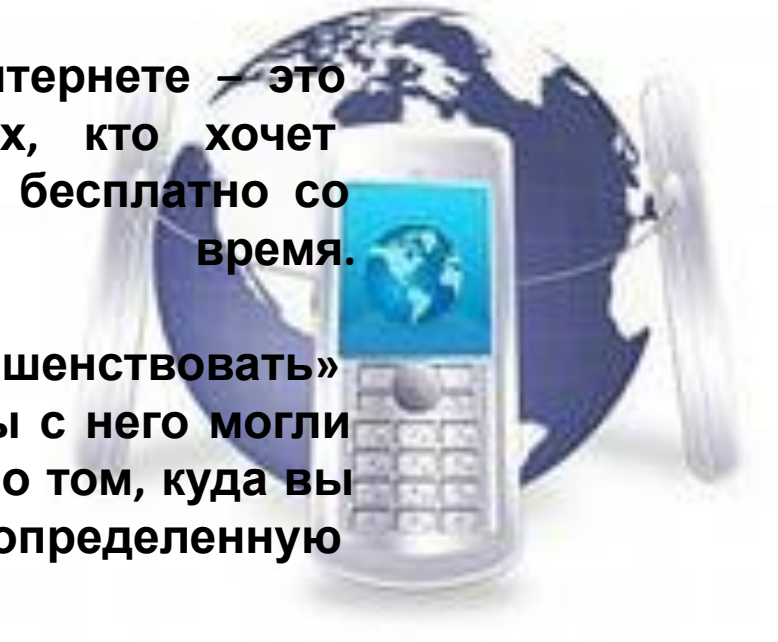
Обман на вложении денег в интернете.

Количество сайтов, занимающихся обманом на вложении денег в интернете, огромное. Чаще всего речь идет о вкладах webmoney и Яндекс.Деньги, потому что это наиболее распространенные платежные системы, и, следовательно, мошенники используют именно их для принятия электронных денежных средств вкладчиков. На сайтах, которые занимаются таким мошенничеством, вложение денег, предполагает, как правило, получение очень высоких процентов, намного выше, чем в банках. Под управлением капиталом может пониматься эффективная работа на валютном рынке Forex, вложение в акции или прибыльные проекты, работа на финансовых рынках и так далее, как говориться, кто на что горазд. В реальности под всем этим чаще всего скрываются пирамиды и сайты однодневки владельцы, которых собирают деньги и исчезают

Неожиданный выигрыш в интернете.

Многие люди в тайне мечтают выиграть большую сумму денег, чтобы наконец то не испытывать проблем с деньгами и жить безбедно до самой старости. Но, к сожалению, такая удача улыбается крайне редко и далеко не всем, чаще встречаются мошенники, которые сообщают о таком мега-выигрыше. В интернете этот лохотрон действует так - на электронную почту пользователя приходит спам-письмо, в котором его поздравляют с выигрышем крупной суммы денег, разыгрывавшейся среди участников какого-либо интернет-ресурса. Чаще всего, говорится, что это крупный зарубежный интернет-проект, а письмо пишется на английском, где из всего текста ярче всего видно сумму выигрыша с большим количеством нулей.

Бесплатная сотовая связь. Звонить с сотового бесплатно - реально?



Очередной лохотрон, гуляющий в интернете – это бесплатная сотовая связь, для тех, кто хочет заплатить один раз и потом звонить бесплатно со своего мобильного все время.

Мошенники предлагают «усовершенствовать» мобильный телефон, чтобы Вы якобы с него могли делать бесплатные звонки, не парясь о том, куда вы звоните и сколько общаетесь, за определенную плату.

И причем способов одурачить, таким образом, было придумано несколько, с различными историями и псевдо техническими подробностями, как именно возможно сделать связь на халяву.

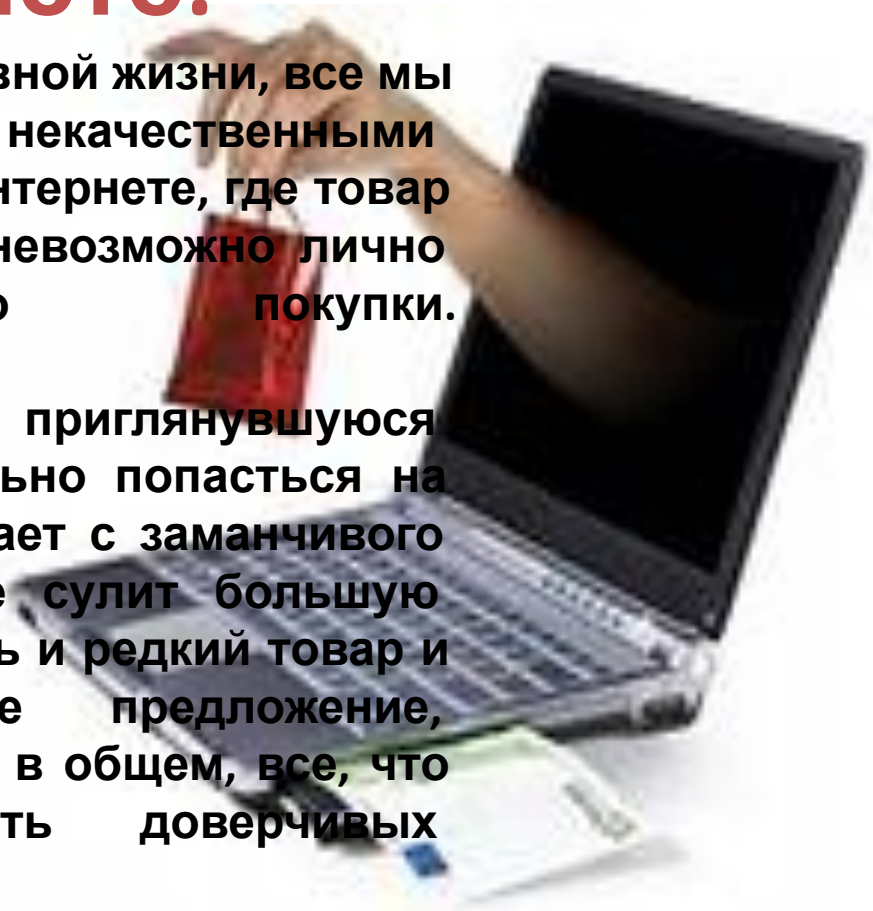
Фишинг - кража личных данных в интернете.

Фишинг - очень хитрый способ обмана в интернете. Целью мошенников фишеров является кража данных пользователей - логинов, паролей и другой секретной информации для получения доступа к их аккаунтам на различных-интернет сервисах. Фишеры могут применять различные приемы для своих атак, направленных на кражу Ваших персональных данных.

К примеру, к Вам может прийти письмо на электронную почту якобы от лица администрации сервиса Яндекс.Деньги, с просьбой пройти по ссылке для повторной активации Вашего аккаунта в системе или под каким-нибудь другим предлогом.

Ссылка, по которой предложат пройти, будет замаскирована под настоящую, но не являться таковой.

Обман при покупке товаров в интернете.



Покупая товары и вещи в повседневной жизни, все мы сталкивались с подделками и некачественными продуктами. Что уже говорить об интернете, где товар не лежит перед нами на полке и невозможно лично проверить его до покупки.

Таким образом, задумав купить приглянувшуюся вещицу в интернете, вполне реально попасться на обман. Обман, как правило, начинает с заманчивого рекламного предложения, которое сулит большую выгоду покупателю. Тут может быть и редкий товар и низкая цена, и специальное предложение, действующие ограниченное время, в общем, все, что серьезно может заинтересовать доверчивых пользователей.

На самом деле товар или вещь, которую предлагают купить может вообще не существовать или в лучшем случае быть дешевой подделкой.

Таким обманом, могут заниматься недобросовестные

Как распознать мошенника? Главные отличительные признаки.

Чаще всего уловки мошенников апеллируют к наиболее живучим порокам человека - жадности и желанию заработать крупные деньги, ничего для этого не делая. **Помните:** для любого реального заработка нужно вложение сил и времени, а бесплатный сыр бывает только в мышеловке!

Все, кто предлагает вам начать зарабатывать, сделав для этого предоплату/залог/вступительный взнос - это мошенники, заработают в этом случае только они. Ни один серьезный работодатель не требует предоплату с работника, работодатель платит вам, а не наоборот!

Первое, на что необходимо обратить внимание на сайте, предлагающем вам заработок - это доменное имя. Любая уважающая себя компания, организация или предприниматель имеет домен второго уровня, например: «www.название сайта.ru». Мошенники, как правило, используют домены третьего уровня «www.название сайта.название беплатного хостинга.ru», например: «www.site.narod.ru» или «www.site.by.ru» они это делают потому, что домен третьего уровня можно получить бесплатно, а вот за домен второго уровня придется платить.

Всю информацию о владельце сайта можно получить в службе WHOIS нажатием одной кнопки. Обратите внимание, как долго существует сайт - как правило, мошенники не работают более 2-3 месяцев, они срывают деньги и исчезают, либо их сайт банится хостингом по жалобам потерпевших.

Если сайт принимает деньги за какой либо товар, то владелец данного сайта должен иметь персональный аттестат платежной системы, через которую он ведет расчеты – WebMoney, RBKmoney и др. Процедура получения данных аттестатов довольно сложна, необходим пакет документов, заверенный у нотариуса, необходимо заплатить деньги - мошенник с этим связываться не будет, тем более, что все личные данные (включая паспортные) отправляются на проверку в данную платежную систему. Все уважающие себя продавцы ставят ссылку для проверки их аттестатов, то есть они говорят: «мы полностью открыты перед покупателями, все наши данные Вы можете проверить, мы не собираемся Вас обманывать».

Кроме того, на сайте, предлагающем вам какую-либо работу/услугу/товар, должны быть контактные данные владельцев – e-mail, телефон, ICQ. То есть должна быть возможность связаться с владельцем сайта. Кстати, хороший способ проверить владельца сайта - это написать ему письмо с любым вопросом, если вы получите ответ в течение 2-5 дней, то скорее всего это порядочные люди, если же ответа вы не получите - бегите от этого сайта подальше.

Среди признаков сомнительности любой сделки можно также назвать стойкое нежелание продавца назначить телефонный разговор или личную встречу. Просто попробуйте попросить у него номер телефона. Здесь, как в известном анекдоте, 80% отсеиваются на диктанте.

Как не попасть в ловушку мошенников?

Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой url стоит в адресной строке или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от сайта платежной системы. Расчет в этом случае - на то, что вы введете на таком сайте свои данные, и они станут известны мошенникам

Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на сайтах самих платежных систем, но никак не на других ресурсах.

Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.

Обязательно делайте резервные копии ключей или программ в тех платежных процессорах, в которых это предписывается: вы сохраните уйму времени, нервов и денег.

Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос, в качестве гарантии, за пересылку данных и тому подобное — не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей - они сами платят за работу.

Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» - это предложения от участников финансовых пирамид. Не ведитесь на такие предложения, в пирамидах выигрывают только их создатели.

Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не глядя. Техническая поддержка платежных систем никогда не рассылает таких писем.

Не давайте деньги в кредит неизвестным вам лицам - в интернете не существует гарантий возврата кредитов.

В 99% случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому семь раз подумайте, прежде чем один раз оплатить товар или услугу.

Будьте бдительны!