Виды мошенничества в интернете и с банковскими картами

Отсутствие должного внимания к вопросам безопасности операций, проводимых в сети Интернет, может сделать их уязвимыми для преступников. Следуя рекомендациям, приведенным в данном разделе, вы сможете оградить себя и свои средства от посягательств мошенников.

Мошенничество в Интернет-магазинах

Как обезопасить себя от мошенничества при покупке товаров через Интернет? Некачественный товар трудно распознать на расстоянии, а условия сделки не всегда ясны.

Прежде всего, покупателя должны насторожить слишком низкая цена предлагаемого продукта, а также отсутствие фактического адреса продавца. В этом случае обязательно наведите справки о магазине, позвоните туда и выясните уже известные вам особенности товара. Нечеткие ответы или неверная информация должны стать поводом для отказа от покупки. Если сомневаетесь, то оплачивайте товар только по факту его получения.

Телефонные мошенничества

Способы, применяемые аферистами, чрезвычайно разнообразны. Например, клиенту звонят якобы с радиостанции и сообщают о выигрыше в лотерею. Однако для того, чтобы получить приз (или принять участие в розыгрыше джек-пота) клиенту предлагают активировать карту экспресс-оплаты и пополнить чужой телефонный счет. Если вам поступил такой звонок, убедитесь в том, что данная передача действительно идет в прямом эфире. Помните, что крупнейшие сотовые компании при проведении лотерей никогда не требуют активировать карты экспресс-оплаты. Кроме того, на мобильный телефон может поступить SMS-сообщение с предложением либо оградить вас от спам-рассылки, либо принять участие в акции от вашего сотового оператора. При этом предлагается отправить «бесплатное» SMS-сообщение на один из коротких номеров, а затем перейти по ссылке для удаления своего имени из списка рассылки. В результате этих манипуляций вы потеряете около 100–150 рублей, но спам получать все равно будете. Поэтому при получении такого сообщения позвоните оператору связи и сообщите о пришедшей на ваш телефон информации.

В последнее время абоненты сотовых операторов стали получать SMS-сообщения якобы от знакомых с просьбой положить на их счет деньги.

Если вы получили подобное сообщение, перезвоните по указанному номеру и выясните личность отправившего SMS-сообщение, и только потом примите решение.

Мошенничества с пластиковыми картами

В настоящее время специалисты выделяют несколько основных видов мошенничества с использованием пластиковых карт. Первый (и на данный момент наиболее распространенный) вид карточного мошенничества — это создание так называемых «белых карт» или «карт-клонов». Мошенники считывают с магнитной полосы карты пользователя секретную информацию, а затем изготавливают «белые карты» — кусочки пластика с магнитной полосой и нанесенной на нее украденной информацией. После этого злоумышленники могут свободно пользоваться счетом настоящего владельца карты, которому, в таком случае, будет очень сложно доказать свою непричастность к «левым» платежам.

Мошенничества при оплате банковскими картами.

Считывание секретной информации, хранящейся на карте, может производиться разными способами. Наиболее распространенный из них — сговор мошенников с сотрудниками магазинов, отелей, ресторанов, других торговых и развлекательных предприятий. Результатом такого сговора является передача информации о реквизитах карточек представителям криминальных структур. Если карта оказалась в их руках, происходит так называемый скиминг, когда платежную карту пропускают через специальное устройство (скимер) и считывают данные, которые хранятся на ее магнитной полосе. Таким образом, мошенники получают своеобразный оттиск карты. И уже ничего не стоит вписать в него необходимую сумму, сымитировать подпись, а все расчеты за операцию переадресовать на законного владельца карты.

Довольно распространен способ, когда криминальные структуры организуют свои собственные магазины. Цель существования подобных «торговых точек» проста — получить как можно больше данных о пластиковых картах клиентов. Часто мошенники используют для этого и Интернет-сайты. Воспользовавшись один раз услугами такого сайта (например, купил товар или скачал видеоролик), владелец карты с удивлением выясняет, что стал его подписчиком, и, таким образом, с него ежемесячно взимается плата за подписку, отказаться от которой довольно проблематично.

Еще одним видом карточного мошенничества является так называемый фишинг, когда данные о пластиковой карте получают от самого пользователя. Злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности. При этом аферисты просят доверчивых пользователей возобновить информацию о карте, в том числе, указать номер «кредитки» и ее ПИН-код либо отправив ответное письмо, либо пройдя на сайт банка-эмитента и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.

Разновидность данного правонарушения — звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что кредита он не брал, ему предлагается уточнить данные его пластиковой карты. В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя.

Для того чтобы уберечь свои деньги, помните: банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Как обезопасить себя от мошенничества?

Единственный реальный способ снизить вероятность мошенничества с пластиковой картой — это соблюдать нехитрые правила безопасности. Сотрудники банков призывают своих клиентов внимательнее относится к своим картам: не доверять карты третьим лицам, не оставлять их без присмотра, не записывать ПИН-код в легкодоступных местах и тем более на самой карте. Обязательно оставьте образец своей подписи на обратной стороне карты сразу же после ее получения. И никогда никому не сообщайте свой ПИН-код. Его не вправе требовать ни работники банка, выдавшего карту, ни обслуживающий персонал банкомата.

Ни в коем случае не упускайте карту из виду, расплачиваясь в ресторанах или магазинах. А лучше попросите, чтобы карту пропустили через импринтер в вашем в присутствии. Внимательнее смотрите, что делают с вашей картой, не расплачивайтесь кредиткой в сомнительных заведениях и обязательно храните у себя копии чеков. Известны случаи, когда при оплате услуг в ресторане, в течение всего лишь пары минут, пока карта находилась вне поля зрения владельца, с магнитной полосы карты считывалась конфиденциальная информация о ее держателе и сумме средств на карточном счете.

Проверяйте движения денег на вашем карточном счете. Существуют строго оговоренные сроки, в течение которых держатель карточки можете что-то предпринять. Особое внимание следует обратить на операции по счету, в которых использовалась карта.

И последний совет, который дают специалисты по безопасности банков своим клиентам,— незамедлительно сообщайте в банк о потере или краже платежной карты. Расследовать преступление по «горячим следам» гораздо легче, чем если владелец вдруг опомнится через пару недель.

Техника безопасности при оплате картой в сети Интернет

Не оставляйте данные о себе и своей карте на тех сайтах, о которых вы ничего не знаете. Спросите об этих сайтах у своих друзей и знакомых, поинтересуйтесь в соответствующих конференциях, узнайте, где располагается сама организация, с которой вы собираетесь производить денежные операции. При этом обращайте внимание на различные сертификаты, подтверждающие безопасность расчетов через данный сайт. Если адреса нет совсем или он не вызывает доверия, то прежде чем платить, подумайте, а стоит ли это делать?

Не используйте для оплаты в сети Интернет карты, на которых находятся крупные суммы денег. Лучше вообще завести для таких целей отдельную карту и переводить туда деньги по мере необходимости.

При появлении малейших подозрений о неправомерном списании денег со счета, обращайтесь в банк. У держателя карточки есть определенный срок для того, чтобы отказаться или оспорить неправомерное списание денег с карточного счета. Продолжительность этого срока следует уточнить в банке, выдавшем карту.

Мошенничества при операциях с банкоматами

Еще один способ электронного финансового мошенничества — это использование специальных технических средств для получения данных о карточке через банкоматы. Для этого, в частности, используются особые «накладки» на клавиатуру банкомата, которые запоминают нажатие клавиш, пока владелец карточки снимает средства. Другое устройство — специальные пластиковые конверты, размер которых немного больше размера карточки. Их закладывают в отверстие картоприемника банкомата. Банкомат, неестественно, не может считать данные с магнитной полосы, но и возвратить карту из-за конструкции конверта также невозможно. В это время подходит злоумышленник и предлагает свою помощь, но для этого держателю необходимо совершить ряд действий, в том числе и набрать ПИН-код. Несмотря на это карта не возвращается. Если владелец уходит, чтобы связаться с банком-эмитентом, мошенник же спокойно вынимает конверт вместе с кредиткой. ПИН-код он уже знает, и ему остается только снять средства со счета.

В картоприемник могут встраиваться не только конверты, но и специальные устройства на базе скимеров, считывающие информацию с карточки, когда законный пользователь снимает средства.

Очень часто на банкоматы незаметно устанавливается микрокамера. Она записывает человека, который набирает ПИН-код, и передаёт данные набора злоумышленникам.

Еще одно средство — это поддельные банкоматы, которые полностью имитируют настоящие. Они правильно считывают информацию с карточки, в том числе и ПИН-код, но деньги не выдают. Карточка возвращается владельцу, но вся информация о ней сохраняется в памяти такого «банкомата».

Этот способ очень дорогой и используется только крупными преступными группами.

Техника безопасности у банкомата

Во-первых, старайтесь не пользоваться банкоматами в безлюдных местах или в местах большого скопления людей. В пустынном месте при снятии денег держатель карточки становится слишком уязвимым объектом для ограбления. А толпе нельзя быть уверенным, что никто не увидит вводимый пользователем ПИН-код.

Во-вторых, не позволяйте увидеть вводимый вами ПИН-код посторонним людям. Не стесняйтесь закрывать от посторонних клавиатуру банкомата. И по возможности не ошибайтесь при вводе ПИН-кода. Ведь после трех ошибочных вводов кода банкомат задержит карту.

В-третьих, проверяйте, все ли было взято из банкомата. После завершения операции у держателя должны остаться: карточка, деньги и выписка о произведенной операции. Если чего-то не хватает, а банкомат не сообщил никакой дополнительной информации, то здесь что-то не так. Вполне возможно, держатель рискует стать жертвой мошенников.

В-четвертых, всегда сохраняйте выписки по итогам операции, которые выдает банкомат. Это позволит вам вести учет расходов и контролировать списание денег со счета.

Что грозит электронным мошенникам?

В 1997 году в России была введена уголовная ответственность за преступления в сфере компьютерной информации, а в 1998 году — в МВД России создано специальное подразделение по борьбе с преступлениями в сфере информационных технологий, так называемое подразделение «К». Так, наказание, предусмотренное Уголовным Кодексом РФ, за незаконное получение и использование сведений, составляющих банковскую тайну (ст. 183),

а также за неправомерный доступ к компьютерной информации (ст. 272), может составлять до пяти лет лишения свободы.

Как воруют деньги с пластиковых карт?

Для того чтобы снять деньги с вашей пластиковой карты, достаточно узнать ваш номер карты и CVS (последние три цифры с обратной стороны карты). Как узнают эти данные мошенники? Да очень просто, люди сами их говорят. В основном мошенники используют три — четыре способа выуживания данных карты у своих жертв.

Первый способ:

На телефон приходит смс о том, что вы выиграли ноутбук и просят обратиться по обратному телефону для получения приза, когда человек звонит по этому номеру на другом конце сотовой линии ему предлагают перевести стоимость ноутбука на его пластиковую карту и чтобы это осуществить им требуется номер карты и CVS. Жертва сообщает эти данные и прощается со всеми имеющимися деньгами на этой карте.

Обратите внимание, что все смс которые присылает вам банк, не имеют обратного телефона, а имеют лишь идентификатор, то есть в телефоне 'от кого:' отображается название банка

Второй способ:

В этом случае тоже на телефон приходит смс, но только уже с содержанием, что ваша карта заблокирована и просят позвонить по обратному телефону. Тут уже жертве предлагают подойти к ближайшему терминалу или банкомату, ввести номер кассы и номер разблокировки, причём при этом выбрать своего сотового оператора.

Это как раз из тех случаев, что доказывает нам какие у нас доверчивые люди в России, так как по факту жертва выбирает сотового оператора и вводит сумму, а не номер кассы, далее мошенник просит, вставит карту и оплачивает себе сотовый телефон. Прошу заметить, что деньги на телефон переводятся в режиме онлайн и в таком случае мошенник сразу же переводит их со своего сотового на какие-нибудь электронные кошельки. Конечно же сим-карты и электронные кошельки зарегистрированы на третье лицо. В таких случаях вернуть деньги уже нереально.

www.chclub.ru

Страхование карточки — возможно и такое

Некоторые «продвинутые» банки уже сейчас предоставляют услугу страхования пластиковых карт от утери и связанных с ней рисков мошенничества. Правда, по словам банковских работников, клиенты не спешат пользоваться такой услугой. Причина этому проста: цена эмиссии новой карты при утере старой не на много выше платы за страховку. Поэтому многие клиенты не хотят тратить лишние деньги на страховку. А ведь она в случае мошенничества с картой обеспечила бы владельцам полное возмещение всех украденных средств.

Банкиры советуют

Как защитить банковскую карту от воров

Все большее распространение банковских карт сопровождается появлением все большего числа разнообразных уловок, направленных на кражу средств со счета. Специалисты дали ряд рекомендаций, как обезопасить себя от возможной кражи.

Прежде всего, надо относиться к банковской карте так же, как и к собственным деньгам и хранить ее в безопасности. Не следует оставлять карту без присмотра, ведь мошенникам достаточно считанных секунд для копирования всей необходимой информации для перевода средств. Кстати, по этой же причине не стоит передавать саму карту третьим лицам, включая родных и близких. Именно для них большинство банков выпускают дополнительные карты. Но если кража состоялась, следует немедленно обращаться в службу поддержки и заблокировать карту.

Следующая часть рекомендаций касается использования банкоматов, которые зачастую используются мошенниками для краж. Каждый раз, подходя к терминалу, нужно осматривать его на наличие подозрительных предметов, которые выбиваются из общей структуры устройства. Даже убедившись в безопасности устройства, вводить ПИН-код рекомендуется, всегда прикрывая цифры от посторонних глаз.

Что же касается оплаты товаров и услуг, то расплачиваться картой в любом случае следует с осторожностью, тщательно проверяя стоимость покупки и сумму к списанию. В интернет-магазинах этот вопрос приобретает особую актуальность, совершать покупки на сомнительных сайтах — значит подвергать себя повышенной опасности остаться без покупки и без денег.

В итоге владелец серьезно повышает надежность своей карты, если соблюдает минимальные меры предосторожности. Впрочем, одного этого бывает недостаточно. Полезно подключить карту к услуге мобильного банка, который за символическую ежемесячную плату присылает на мобильный телефон владельца карты информацию по всем изменениям счета и совершенным транзакциям с карты,

Сегодня клиенты большинства банков также имеют возможность застраховать свои кредитные карты на случай возможной потери или хищения средств, правда, эта платная услуга пока еще не получила широкого распространения в России. Однако страхование карты, безусловно, является наиболее надежным способом защитить «кредитку». По классическим картам сумма возмещения в России может достигать 75 тысяч рублей, а по «золотым» картам — 150 тысяч рублей. При символической стоимости страховки от 100–150 рублей в месяц выгода от подобной услуги выглядит более чем очевидной. Инструментов мошенничества существует великое множество, но условно они делятся на несколько видов. Так, можно установить считывающие устройства на банкомат, крадущие информацию по карте. К ним относятся накладки на клавиатуру для записи нажатых кнопок или конверты-ловушки, которые «съедают» карты. Кроме того, мошенники крепят у банкоматов скрытые камеры, записывающие введенные пин-коды и номера карт. Некоторые преступники подключаются к кабелю, по которому проходит информация по операциям. Не уступает по популярности подобным технологичным устройствам и практика фишинга, при которой из держателя карты обманным путем «выуживаются» сведения по карте.

Памятка по безопасному использованию банковских карт

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.
4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
6. Телефон кредитной организации — эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации — эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).
8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию — эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации — эмитента банковской карты (кредитной

организации, выдавшей банковскую карту) предлагается предоставить персональные данные.

Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.

10. В целях информационного взаимодействия с кредитной организацией — эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в кредитной организации — эмитенте банковской карты.

11. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц. В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию — эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию — эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией — эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации — эмитента банковской карты, не возмещаются.

Рекомендации при совершении операций с банковской картой в банкомате

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.
8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата банковской карты.
9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.
10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию — эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
4. В случае если при попытке оплаты банковской картой имела место «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с банковской картой через сеть Интернет

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не сообщайте персональные данные или информацию о банковской (ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской (ом) карте (счете). В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

www.cbr.ru

Яндекс предупреждает !!!

В интернете есть мошенники, которые, пользуясь чужим именем, выманивают деньги или личную информацию. Завладев вашим логином или паролем на Яндексе, они могут воспользоваться вашим почтовым ящиком или средствами на счете.

Интернет-мошенничество (фишинг)

Распространенные способы мошенничества:

- вам сообщают, что вы выиграли приз от компании «Яндекс» и должны оплатить доставку или налог;
- вам предлагают отправить SMS, чтобы разблокировать почтовый ящик на Яндексе или счет в Яндекс.Деньгах;
- вы получаете письмо с просьбой прислать ваш пароль или ввести его после перехода по ссылке, которая на самом деле ведет не на сервис Яндекса, а на мошеннический веб-узел.

Если вы попали в подобную ситуацию, пожалуйста, ничего не оплачивайте, не отправляйте SMS и никому не передавайте ваш пароль. Такая разновидность интернет-мошенничества называется фишингом (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание). Цель фишинга — завладеть конфиденциальными данными пользователя (паролем, номером кредитки, PIN-кодом и пр.). В процессе фишинга мошенники завлекают пользователей на специально созданные подставные страницы (копии реально существующих популярных сайтов), используя массовые почтовые рассылки от имени владельцев настоящих сайтов (платежных систем, банков, провайдеров). Обычно такие письма приходят в виде уведомлений о каких-либо событиях (утеря данных, сбои в системе и т.п.), в связи с которыми пользователь должен предоставить, обновить или подтвердить те или иные конфиденциальные данные.

При этом в письме приводится ссылка, которая ведет не на официальную страницу сервиса, а на ее точную копию. Информация, введенная доверчивым пользователем на поддельном сайте, попадает в руки мошенников.

Чтобы не стать жертвой мошенников, рекомендуется внимательно проверять все сообщения и самостоятельно связываться с организацией, от имени которой пришло письмо. Для связи с организацией не нужно использовать указанные в подозрительном письме телефоны, адреса и ссылки.

Яндекс никогда не просит прислать пароль и не предлагает оплачивать то, что вы сами не заказывали.

Логин и пароль пользователи вводят самостоятельно, когда заходят на персональные сервисы Яндекса. Если вы обратились в службу поддержки, у вас могут попросить логин, но пароль — никогда.

Если вам предлагают ввести пароль после перехода по ссылке, которая кажется вам подозрительной, вместо этого введите логин и пароль на главной странице Яндекса, и вы безопасно попадете на любой сервис. Чтобы выявить подозрительную ссылку, посмотрите, не содержит ли она бессмысленный набор символов или опечатки.

Платные услуги Яндекса — это размещение рекламы (на Директе, Маркете и т.д.), а также срочная регистрация сайтов в Яндекс.Каталоге. Эти услуги вы всегда заказываете сами. Кроме того, при проведении некоторых операций в Яндекс.Деньгах взимается комиссия.

Ни за что больше платить не нужно. А если Яндекс дарит подарки, то он их просто дарит.

I Подмена сайта

Если вы зашли на один из сайтов Яндекса (Почта, Поиск и др.) или, нажав на один из результатов поиска, оказались не там, где ожидали, возможно, ваш компьютер заражен вирусом.

Действие вируса может проявляться и таким образом — при регистрации или авторизации на Яндексе предлагается подтвердить свои данные, отправив SMS на указанный номер.

Яндекс никогда не требует денег с пользователей за регистрацию и использование своих сервисов, а также не предлагает подтвердить регистрацию с помощью SMS.

Как это выглядит?

При попытке зайти на главную страницу http://www.yandex.ru, http://mail.yandex.ru или https://passport.yandex.ru предлагается ввести логин, пароль и отправить SMS на короткий номер. Страница похожа на ту, что используется для входа на почту.

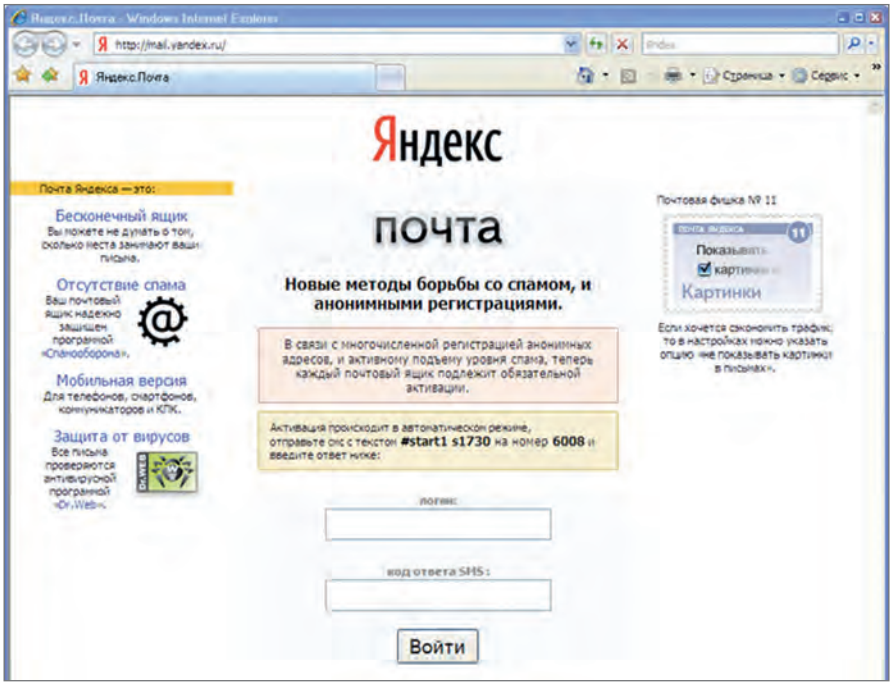
Распространяется этот вирус в основном через социальные сети.

Что с этим делать?

Быстрый способ

1. Сохраните файл hrepair.bat в любом месте, например, на рабочем столе.
2. Если Вы используете Windows Vista или Windows 7, щелкните на файле правой кнопкой мыши и выберите пункт Запуск от имени администратора.

Действие вируса может выглядеть так:



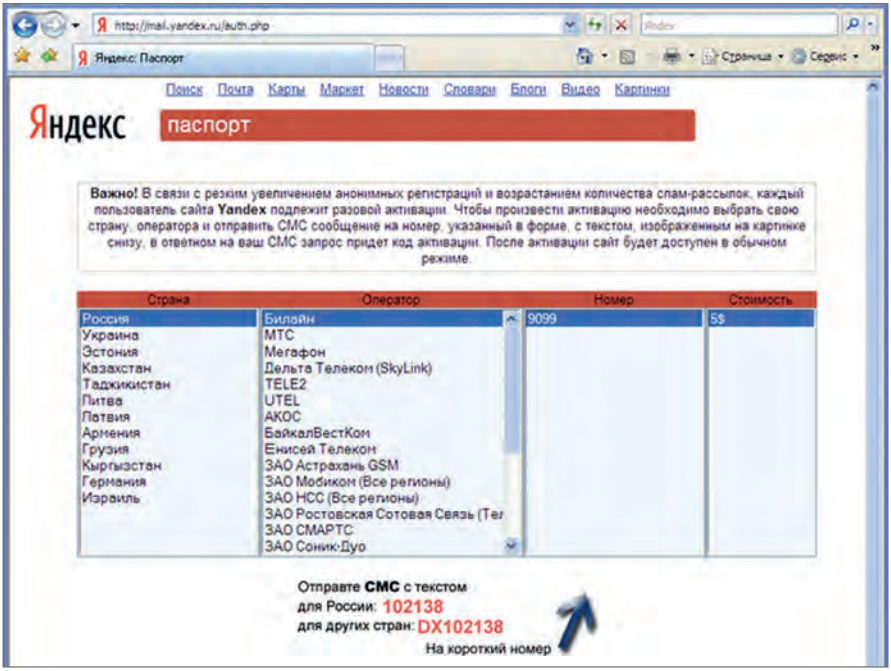
Если Вы используете Windows 2000/XP, просто дважды нажмите на файле.
3. Проверьте, удалось ли избавиться от проблемы, открывается ли Яндекс по адресу www.yandex.ru и mail.yandex.ru.

Самостоятельно поправить файл hosts

Проверьте свой компьютер антивирусной утилитой CureIt от «Dr.Web» или Virus Removal Tool Лаборатории Касперского.
Если антивирусная программа не обнаружила вредоносный код, вы можете удалить вирус вручную.
Перед этим внимательно ознакомьтесь с действиями, которые необходимо выполнить. Помните, что вы выполняете их на свой страх и риск.

Когда вы набираете адрес, например, http://www.yandex.ru, ваш компьютер определяет, к какому серверу нужно обратиться. В первую очередь он просматривает файл hosts (обычно этот файл находится в папке C:\WINDOWS\system32\drivers\etc), и, если в нем есть адрес сервера (IP-адрес) для указанного вами имени, то используется именно он. Если же подходящей записи нет, то нужный адрес сервера запрашивается у вашего провайдера.
SMS-вирус меняет содержимое файла hosts, дописывая туда адреса своих серверов так, чтобы они заменили адрес Яндекса и других популярных интернет-сервисов. В результате вам кажется, что вы видите страницу Яндекса и работаете с ней, но на самом деле вы находитесь на сервере злоумышленников.

Действие вируса может выглядеть так:



Для уничтожения последствий работы вируса, необходимо выполнить следующие действия:

1. Перейдите в папку C:\WINDOWS\system32\drivers\etc (возможно, у вас система Windows установлена в папку, отличную от C:\WINDOWS — учитывайте это) и найдите там файл с названием hosts.
Сохраните копию файла hosts на всякий случай!
2. Откройте файл с помощью Блокнота и поищите в нем строки следующего вида:
127.0.0.1 yandex.ru
127.0.0.1 http://www.yandex.ru
91.189.113.143 mail.ru
91.189.113.143 www.mail.ru
91.189.113.143 www.yandex.ru
91.189.113.143 yandex.ru
91.189.113.143 www.vkontakte.ru
91.189.113.143 vkontakte.ru
91.189.113.143 www.odnoklasniki.ru
91.189.113.143 odnoklasniki.ru

Адреса, т.е. 4 числа через точку, могут быть другими, например, не 91.189.113.143, а 83.133.122 и т.п.).

3. Удалите все строки, отличные от «127.0.0.1 localhost». Строку «127.0.0.1 localhost» удалять не следует.
4. После этого сохраните файл и перезапустите браузер — с этого момента у вас станет загружаться оригинальная страница http://www.yandex.ru.
5. Установите на файл атрибут только для чтения — это поможет избежать его изменения простыми вирусами. Для этого надо нажать на имени файла правой кнопкой мыши, выбрать пункт меню Свойства, установить флажок Только чтение и нажать OK.

6. Данный вирус вносит изменения в настройки компьютера, но не находится постоянно активным в памяти. Если вы знаете или предполагаете, в какой программе находится вирус (она может называться, например, vkontakte.exe или reiting.exe), то вы можете ее удалить или больше не запускать.

Если вы отправляли SMS на указанный мошенниками короткий номер, то обратитесь с запросом на возврат денег к своему сотовому оператору или в компанию, обслуживающую данный короткий номер.

www.bankir.ru

Внимание фальшивка!

Сегодня ни одна организация, работающая с наличными деньгами, не обходится без оборудования по проверке подлинности денежных знаков. Детекторы подлинности банкнот — один из наиболее востребованных видов банковского оборудования, выпускаемого компанией «ДОРС». В последнее время стали очень востребованы и счетчики банкнот, способные выявить фальшивку.

По словам директора ООО «ДОРС СПб» ***Владимира Журбилова****, ситуация с фальшивыми купюрами в регионе намного серьезнее, чем представляется на первый взгляд.*

Число фальшивок на Северо-западе очень велико и постоянно растет. Их качество находится на высоком уровне.

По данным Банка России, Северо-западный федеральный округ, занимает 2–е место в стране по оборачиваемости фальшивых денег. Порой основные защитные признаки воспроизводятся с такой достоверностью, что даже профессионал без специального оборудования не в состоянии сказать, настоящая ли это банкнота.

В подобной ситуации детекторы и счетчики банкнот с функцией определения подлинности — единственный способ сократить оборот фальшивых денег. Причем проверять с их помощью нужно все купюры.

Мелкий номинал — 50, 100 рублей — обычно подделывается менее тщательно, в расчете на то, что подлинность таких банкнот определяется «на глазок», без использования приборов. И элементарный ультрафиолетовый детектор с легкостью выявит фальшивку.

В то же время количество фальшивых пятитысячных банкнот на рынке постоянно растет и впервые, в 3 квартале 2013 г., превысило количество фальшивых 1000 рублевых купюр. Фальшивомонетчики уже научились их подделывать с высоким качеством и в огромных количествах. 1000 рублевая и 5000 рублевая купюры, по данным Центрального банка России, составляют 76% в обороте фальшивок.

DORS БАНКОВСКОЕ И КАССОВОЕ ОБОРУДОВАНИЕ

DORS-1000M2

DORS-50

DORS-60

Поэтому для надежной защиты от фальшивок необходимо применять детекторы и в первую очередь инфракрасные.

Компания «ДОРС», являющаяся крупнейшим производителем подобных приборов в России, выпускает множество моделей детекторов и счетчиков банкнот от простейших бытовых, определяющих подлинность по одному параметру, до сложных профессиональных исследовательских комплексов и автоматических детекторов, позволяющих проверить наличие всех защитных признаков.

Клиентам из числа небольших торговых предприятий я бы посоветовал детектор экономкласса, инфракрасный DORS-1000M2. Он доступен по цене, прост, удобен и надежен в эксплуатации.

Автоматические детекторы предназначены для проверки денежных знаков в режиме, исключающем влияние человеческого фактора в процессе проверки. Новый автоматический детектор с функцией автоматического определения типа валюты DORS-230, предназначен для проверки практически неограниченного количества валют, зависящего только от потребностей пользователей. При этом у детектора имеется уникальная возможность моментального обновления программного обеспечения через интернет.

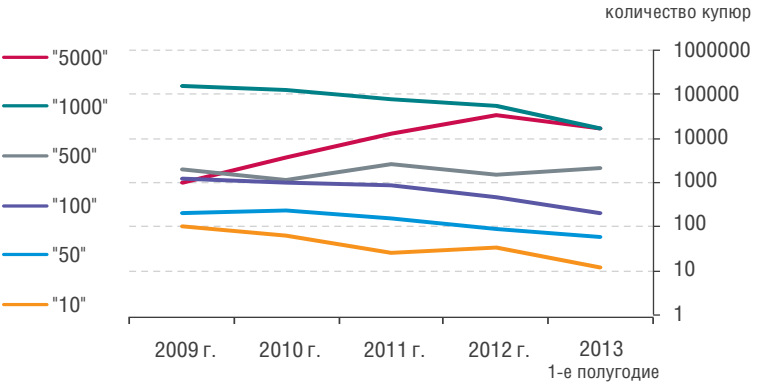
Новый мультивалютный счетчик банкнот DORS-750, очень облегчит работу кассиров при пересчете большого количества наличности. Большая скорость пересчета при 100% гарантии отсеивания фальшивых денег, достигнута за счет применения новейших конструкторских решений и уникальных запатентованных технологий полного сканирования банкноты по нескольким параметрам. Данный счетчик, также имеет возможность обновления программного обеспечения через интернет.

Продавцам товаров и услуг уже пора осознать серьезность проблемы. Нужно, чтобы детекторы появились в каждом ларьке и маршрутном такси, кафе и салоне красоты. Тогда мы с вами будем уверены, что все деньги, которые лежат в кассе, настоящие. Не нужно экономить на детекторах.

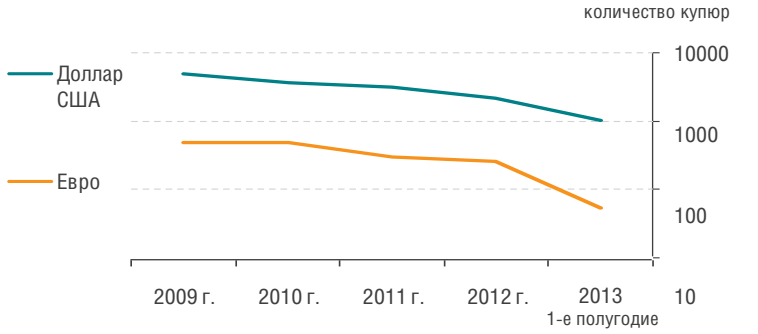
Их небольшая стоимость несоизмерима с существующей угрозой, потенциальными убытками и неприятностями с законом. Цена приборов, о которых я говорил выше, столь невелика, что окупается всего несколькими задержанными фальшивками.

В идеале хотелось бы, чтобы появились какие-то законодательно закрепленные инструкции, обязывающие все точки торговли и сферы обслуживания наравне с кассовыми аппаратами иметь и детекторы подлинности банкнот. И тогда любой человек будет уверен, что ему вместо сдачи не всучат фальшивку.

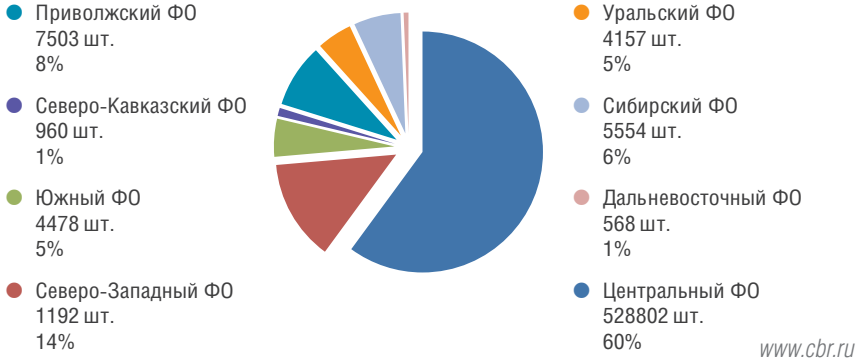
Динамика выявления поддельных денежных знаков



Динамика выявления поддельных денежных знаков иностранных государств



Выявление поддельных денежных знаков Банка России в Федеральных округах в 2012 г.



www.cbr.ru

Осторожно — фальшивый банк

Центральный банк обнаружил первый фиктивный банк — «Тон-банк». Как оказалось, регулятор не выдавал банковской лицензии этой организации. Фактически, единственное, что есть у банка — это сайт.

Согласно представленной на нем информации, кредитная организация была зарегистрирована в декабре 2000 года и получила лицензию № 2161 в ноябре 2005 года. Но лицензия с этим номером ранее принадлежала другому банку — Первому Федеральному, ликвидированному в 2004 году. Другие финансовые параметры, подлежащие обязательному раскрытию по требованию ЦБ, на сайте «Тон-банка» не представлены. Вместо этого на интернет-ресурсе размещен список отраслевых организаций, в которых он состоит. В этот перечень вошли «Системы обязательного страхования вкладов», Московская межбанковская валютная биржа (ММВБ), Международной платёжной системы Visa International и другие.

В сети указан адрес единственного офиса банка. Но в реальности по этому адресу никаких кредитных организаций не зарегистрировано. Как оказалось, в офисном здании размещены 18 других компаний, опрошенные представители которых о «Тон-банке» ничего не слышали. Телефон, указанный в разделе контактной информации «Тон-банка», не отвечал на звонки.

Судя по всему, основным способом коммуникации «банка» с клиентами был Интернет. К полудню 6 февраля на сайте банка можно было подать заявку на кредитную карту, которую банк обещал впоследствии переслать по почте. При заполнении заявки банк просил указать все персональные данные.

Как жалуются несостоявшиеся клиенты банка на различных форумах, после одобрения банк просил оплатить годовое обслуживание карты заранее. «Я выслал им все свои документы и через терминал отправил деньги на карту! Но мне так нечего и не пришло! может и не придет?»,— жалуется один из них.

В числе продуктов банка также значились кредиты наличными, автокредиты и ипотека. Ставки по всем кредитам находились в диапазоне от 12 до 20%. Максимальная сумма займа — 10 млн. рублей — предлагалась по программе ипотечного кредитования. Ставки по вкладам не превышают 12%.

Ресурс создавался в первую очередь для сбора данных о людях, которые нуждаются в кредитных картах и хотят заказать ее дистанционно, считает генеральный директор Group-IB Илья Сачков. «Полученные базы данных могли передаваться или продаваться в реально существующие финансово-кредитные организации, которые использовали их для продвижения собственных кредитных продуктов и предложений. Ведь фактически у вас на руках полный финансовый портрет человека, которому к тому же действительно требуются деньги и он готов взять кредит»,— указывает он.

В России обнаружился еще один фальшивый банк, созданный по образцу Тон-банка, о мошенничестве в котором предупреждал ЦБ.

В начале февраля 2013 г. Банк России предупредил, что впервые обнаружен фальшивый банк, который «выдавал» кредиты через интернет, «имел» офис в Москве, но на самом деле не существовал. Документы по Тон-банку были отправлены в правоохранительные органы. Буквально через неделю после этого,12 февраля, неким частным лицом был зарегистрирован еще один сайт банка, который предлагал аналогичные услуги, но имел единственный офис в Санкт-Петербурге.

По адресам baltcombank.ru и балткомбанк.рф Балткомбанк предлагает кредитные карты, потребкредиты, автокредиты и ипотеку, а также вклады. У банка один офис, но по адресу, указанному на сайте Балткомбанка (Санкт-Петербург, ул. Ефимова, д. 2), корреспондент «Интерфакса» не обнаружил офиса этой организации, а при попытке дозвониться в офис включается автоответчик.

На сайте говорится, что Балткомбанк имеет генеральную лицензию № 2951, которая якобы была выдана 22 мая 2007 г. за подписью первого зампреда ЦБ РФ Андрея Козлова, убитого за полгода до «выдачи лицензии». Согласно данным ЦБ РФ, банк с лицензией № 2951 (Кубанский народный банк приватизации) был ликвидирован 9 сентября 2002 г.

Схема создания банка абсолютно копирует первый фальшивый банк — Тон-банк: на его сайте можно было оформить только кредитную карту (хотя предлагалось множество разных продуктов). При заполнении заявки собиралась полная информация о потенциальном клиенте, которому нужно было заранее оплатить комиссии за открытие карты и ее годовое обслуживание. Обычно банки не берут плату за доставку карты, а комиссию за годовое обслуживание снимают только в случае активации карты.

Такие сайты, как правило, создаются в основном для сбора персональных данных для продвижения продуктов либо для мошеннических операций, объясняли ранее специалисты.

В марте ЦБ заявил, что участились случаи выявления в интернете сайтов, в наименованиях которых содержатся слова «банк», bank. На этих сайтах предлагают банковские услуги от лица организаций, в отношении которых Банк России не принимал решения о государственной регистрации и выдаче лицензии на осуществление банковских операций.

Финансовый ущерб его потенциальных клиентов до сих пор не оценен, но после этого ЦБ выявил еще несколько фальшивых банков, говорили представители Банка России.

В последнее время участились и случаи, когда появляются сайты, якобы принадлежащие реально работающим банкам (иногда крупным), но на самом деле они банком не регистрировались.

Сейчас ЦБ обсуждает с Минкомсвязи, как пресечь или выявить на ранней стадии случаи регистрации сайтов, содержащих слово «банк» или bank. Один из вариантов — обязательная проверка наличия банковской лицензии при регистрации доменного имени, содержащего эти слова, говорил собеседник «Ведомостей» в ЦБ.

Осуществление такого рода организациями банковской деятельности, в том числе с использованием интернета, может быть квалифицировано как осуществление незаконной банковской деятельности, ответственность за которую предусмотрена статьей 172 УК. Если организованная группа получает таким образом доход в особо крупном размере, УК предусматривает наказание до семи лет лишения свободы.

5 апреля Центробанк на своем сайте выложил список кредитных организаций и их сайтов. В этом списке Балткомбанка нет. Нет его и в списке участников системы страхования вкладов...

www.izvestia.ru