# Виды мошенничества в интернете и с банковскими картами. Виды мошенничества с банковскими картами, мобильными телефонами, фишинговыми ссылками и другое.

Широкое внедрение автоматизированных систем обработки и хранения информации – неотъемлемый атрибут современного мира. Но помимо множества удобств, у высоких технологий есть и обратная сторона. Ведь год от года увеличивается число преступлений в сфере электронных информационных систем. При этом объектами преступных посягательств становятся финансовые средства обычных граждан, доступ к которым возможен через глобальные компьютерные сети. 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? Ведь некачественный товар трудно распознать на расстоянии, а условия сделки не всегда ясны.

Прежде всего, клиента должна насторожить слишком низкая цена предлагаемого продукта. Сомнения должно вызвать и отсутствие фактического адреса или телефона продавца. В этом случае обязательно наведите справки о магазине и только после этого производите платеж.

Позвоните продавцу по телефону и выясните уже известные вам особенности товара. Нечеткие ответы или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки. Кроме того, пользуйтесь услугами курьерской доставки и оплачивайте товар по факту его получения. Это убережет вас от ситуации, когда деньги вы перечислили, но вещь так и не получили.

**Телефонные мошенничества.**

Главная цель телефонных мошенников – заставить раскошелиться абонентов крупных сотовых операторов. Способы, применяемые аферистами, чрезвычайно разнообразны. Например, клиенту якобы звонят 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. В том случае, если вам поступил такой звонок, включите указанную радиостанцию и 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. Оператор определит того, кто отправляет эти SMS-сообщение и заблокирует его счет.

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. Через такие компании проходит большое количество транзакций с пластиковыми картами, информация о которых сохраняется в компьютерных базах данных компании или на слипах (бумажных документах, подтверждающих факт осуществления платежа). Результатом такого сговора является передача информации о реквизитах карточек представителям криминальных структур.

В этом случае происходит так называемый скиминг. Настоящую платежную карту пропускают через специальное устройство (скимер) и считывают данные, которые хранятся на ее магнитной полосе. Таким образом, мошенники получают своеобразный оттиск карты. И им 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.

**Фишинг.**

Еще одним видом карточного мошенничества является так называемый фишинг. Цель фишинга – получить данные о пластиковой карте от самого пользователя. В этом случае 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. Сделать это предлагается несколькими способами: 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.

Еще один совет – ни в коем случае не упускайте карту из виду, расплачиваясь в ресторанах или магазинах. А лучше попросите, чтобы карту пропустили через импринтер (аппарат для осуществления электронных платежей) в вашем в присутствии. 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. Внимательнее смотрите, что делают с вашей картой в магазине или ресторане, не расплачивайтесь кредиткой в сомнительных заведениях и обязательно храните у себя копии чеков.

Проверяйте движения денег на вашем карточном счете. В этом случае держатель успеет выставить претензию своему банку, а он – платежной системе. 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.