

ОБРАТИТЕ ВНИМАНИЕ

На связи мошенники

Количество совершаемых дистанционных мошенничеств с каждым годом растет. Пострадать от этого вида преступлений может любой доверчивый гражданин, независимо от возраста и социального положения

Мошенничество – хищение чужого имущества путем обмана или злоупотребления доверием. В отличие от краж жертва сама передает свое имущество преступнику. Особенность дистанционного мошенничества в том, что злоумышленник и потерпевший в момент совершения преступления находятся на значительном расстоянии друг от друга, как правило, не знакомы и общаются посредством сети Интернет или телефонной связи.

При осуществлении преступной деятельности мошенники, как хорошие психологи, воздействуют на такие черты характера, как сострадание, жалость, доверчивость, наивность, а также на свойственное русскому менталитету качество как желание разбогатеть быстро, бесплатно, даром.

Основные виды дистанционного мошенничества:

- телефонное мошенничество
- мошенничество на интернет-площадках, сайтах бесплатных объявлений
- мошенничество в социальных сетях

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

1. Звонок из службы безопасности банка

Потерпевшему поступает звонок якобы от сотрудника банка или сотрудника службы безопасности банка, а также сотрудников правоохранительных органов (полиции, следственного комитета, ФСБ), который сообщает, что по счету происходят сомнительные операции (списание или попытка списания денег в другом регионе либо оформление кредита и т. п.).

В ходе доверительной беседы мошенник узнает у гражданина о наличии денежных средств на счете и далее говорит, что необходимо (либо для отмены сомнительных операций, либо для создания резервного счета, исключающего списание денег, либо возврата похищенных денег и т. п.) перевести денежные средства, находящиеся на счете, на безопасный счет либо безопасные ячейки или оформить кредит, который также обналечит и перевести на безопасный счет либо безопасные ячейки. Причем мошенники всегда говорят о том, что они являются действующими сотрудниками правоохранительных органов и работниками банка, а местные сотрудники и работники банков – мошенники. Требуя перевести денежные средства через банкомат по нескольким номерам несколькими суммами, которые они указывают, или на несколько счетов, также указанных ими. Как только гражданин переводит денежные средства, они списываются со счета и переводятся на счет виртуального кошелька мошенника.

Как поступать в такой ситуации?

Первое и самое главное правило – прервать разговор. Далее обратить внимание, что номер, с которого вам звонят, не связан с данным банком, а является обычным номером сотового оператора, как правило, другого региона или страны.

При этом надо помнить, что мошенники могут позвонить с номера, похожего на номер телефона «горячей» линии банка, и, к примеру, отличать всего лишь одной цифрой. Правильные номера телефонов банка указаны на оборотной стороне карты.

Банковские служащие не станут интересоваться количеством денежных средств, находящихся на вашем счете (банковской карте). У них данная информация имеется.

2. Звонок от сотрудников правоохранительных органов (полиция, следственный комитет, ФСБ)

Вам звонят с незнакомого номера. Мошенник представляется сотрудником полиции, следственного комитета или ФСБ. Как правило, мошенник сообщает, что на ваше имя пытаются отправить кредиты или снять денежные средства. После этого он якобы переключает вас на сотрудников Центрального Банка (либо службы безопасности банка). Потом приходит сообщение о том, что вас добавили в корпоративный чат-поддержку Центрального Банка и вам выделен специалист и предоставлены страховые ячейки для производства процедуры замены единого лицевого счета. Далее необходимо связаться со специалистом банка и перевести денежные средства на безопасный счет для их сохранения. Для этого вас направят к какому-либо банкомату, и возле банкомата с вами все время будет на связи мошенник, называющий номера сотовых телефонов, на которые необходимо перевести деньги.

5. «Вы выиграли машину, нужны деньги для ее оформления»

Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

На ваш мобильный телефон, как правило, в ночное время приходит смс-сообщение, в котором говорится о том, что в результате проведенной лотереи вы выиграли дорогой автомобиль. Для уточнения всех деталей вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошину и оформить необходимые документы. Для этого надо перечислить на счет своего мобильного телефона 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».

На самом же деле комбинация цифр и символов, которую Вы набираете, является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

Как поступать в такой ситуации?

Если вы узнали о проведении лотереи только в момент «выигрыша» и при этом ранее не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, вас пытаются обмануть. Оформление документов и участие в таких потерях никогда не проводится только по телефону и интернету.

МОШЕННИЧЕСТВО НА ИНТЕРНЕТ-ПЛОЩАДКАХ, САЙТАХ БЕСПЛАТНЫХ ОБЪЯВЛЕНИЙ

Авито, Юла, Циан и другие сайты бесплатных объявлений – крупнейшие российские интернет-площадки, на которых можно легко купить или продать любой товар: от одежды и животных до недвижимости и автомобилей. Являющийся по сути современным аналогом газетных страниц с частными объявлениями, этот ресурс привлекает не только честных продавцов, но и мошенников, использующих различные схемы для получения денег обманным путем. Мошенничество на интернет-площадках может принимать изощренные формы, а достаточная анонимность продавцов и покупателей и простая процедура регистрации на сайте – только по телефонному номеру или электронной почте – увеличивает риск стать жертвой мошеннических схем.

1. Мошенничество на интернет-площадках с предоплатой

Оплата товара вперед – обычная практика интернет-магазинов, которую с успехом применяют работающие на интернет-площадках мошенники. Их задача – заставить вас заплатить за несуществующий товар. Необходимость получения предоплаты может быть обоснована срочностью продажи, невозможностью встретиться с продавцом для оплаты товара наличными из-за его нахождения в другом городе или личной занятостью продавца. В отличие от реально работающих интернет-магазинов продавцы-мошенники не дают покупателям реальных контактных данных, договоров купли-продажи или других официальных документов, подтверждающих сделку. Отправив аванс или оплатив полную стоимость товара, покупатель не получает оплаченный заказ.

Как поступать в такой ситуации?

Если при общении с продавцом у вас возникают сомнения в наличии, свойствах или качестве товара, вы не понимаете схемы расчета за товар, его цена существенно ниже, чем аналогичные предложения на сайте или продавец пригласившегося товара находится в другом городе – откажитесь от рискованной сделки.

Чтобы избежать финансовых потерь при дистанционной покупке товара с предоплатой, можно:

- договориться с продавцом об оплате товара наложенным платежом при получении заказа в транспортной компании;
- попросить продавца подтвердить реальное наличие товара фотографиями с нескольких ракурсов или во время сессии в скайпе;
- самостоятельно проверить данные продавца через поисковые системы и отзывы покупателей на интернет-площадках;
- не перечислять деньги на сотовый телефон, так как в 90% случаев такую схему оплаты используют мошенники.

2. Мошенничество на интернет-площадках с автомобилями

Объявления о срочной продаже автомобилей по необоснованно низкой для модели, комплектации и состояния транспорта цене часто используются мошенниками в качестве «наживки» для схем с предоплатой. Чаще всего объявления-пустышки сопровождаются очень лаконичным текстом – без подробностей об особенностях комплектации или прошедшем обслуживании, а номерные знаки авто на фото не просматриваются или специально замазаны продавцом. Вас могут попросить внести залог, небольшую предоплату или полную стоимость машины под предлогом большого наплыва покупателей или даже оплатить транспортировку авто для осмотра из одного города в другой, разумеется, переводом средств на карту или телефонный номер. Если же автомобиль реально существует и вы можете лично осмотреть его перед покупкой, то такой транспорт может числиться в угоне. Перевитые номера агрегатов и фальшивые документы для неопытного покупателя создадут вид «чистого» авто; иметь зарубежную регистрацию или поддельные номера; находиться под банковским залогом.

Как поступать в такой ситуации?

Чтобы обезопасить себя при покупке авто по объявлению на интернет-площадках, доверьте осмотр авто профессионалам из авторесервиса или мастерских; проверьте регистрационные документы в ГИБДД; не приобретайте машину по доверенности. Не отправляйтесь на встречу с продавцом в одиночестве, особенно если сделка состоится в другом городе, в отдаленном районе или в позднее время. Лучше отказаться от рискованной покупки, сохранив и деньги, и здоровье.

3. Мошенничество на интернет-площадках при купле-продаже недвижимости

Обманные сделки купли-продажи с квартирами на интернет-площадках встречаются не очень часто, ведь процесс оформления сопровождается полной проверкой документов на недвижимость – как в государственных структурах у юристов и нотариусов, так и в банках при выдаче кредита на жилье. Мошенники используют объявления о продаже квартир для получения предоплаты. Как и в случае с автомобилями, такие объявления содержат минимум информации. Их отличия: на фото квартиры выглядят очень аккуратно, обставлена достаточно новой мебелью; цена недвижимости значительно отличается от рыночной – обычно на 30-40%; упоминание о возможности связаться с продавцом исключительно через электронную почту или телефонный номер иностранного оператора. Продавец не предоставляет точный адрес жилья и, ссылаясь на срочность продажи и свое нахождение в другом регионе или за границей, просит выслать существенную предоплату (от 10 тысяч долларов) на банковскую карту или через систему быстрых платежей и переслать подтверждающий операцию скан квитанции. Получив код перевода, мошенник обналечивает средства.

Как поступать в такой ситуации?

Оформляйте предоплату за квартиру только после детальной проверки документов и личного осмотра недвижимости. Договор залога необходимо составлять у нотариуса!

МОШЕННИЧЕСТВО В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети – удобный инструмент коммуникации: можно списаться с

дальним родственником, которого давно не видел и поделиться с ним последними фотографиями из своей жизни; поговорить со старым другом и посмотреть, чем он живет: почтить новости и здесь же обсудить их с друзьями или случайными людьми; послушать музыку, посмотреть новинки фильмов или просто завести новые знакомства.

1. Благотворительные фонды

В социальных сетях размещается много предложений помочь фонду или конкретному человеку.

Как поступать в такой ситуации?

Удостоверьтесь, что это на самом деле организация, не поленитесь перейти на их сайт и проверить документы, детальные отчеты о поступлениях и тратах. Посмотрите, сколько собрано и куда конкретно идут средства, задайте вопросы в поддержку с уточняющими вопросами, это же относится к частным лицам, плюс ко всему проверить через поиск фото того, кому требуется помощь, часто их просто копируют с одного источника.

2. Взломы аккаунтов и развод друзей

Пожалуй, самый распространенный вид мошенничества, когда от кого-нибудь из ваших друзей или родственников вдруг начинают приходить сообщения с просьбой дать денег в долг, под любым предлогом, причем очень настойчиво, с мольбами о помощи. Действует это не на всех, но процент успешности все же есть, близкие входят в положение и переводят деньги на предложенные аферистами кошельки. Происходит это либо путем регистрации злоумышленником странички-клона с аватаркой, именем и даже фотографиями жертвы, либо путем взлома странички жертвы с использованием специальных программ, что сложнее. Далее схемы похожи: мошенник отправляет всем друзьям сообщения с просьбой о переводе денег или размещает аналогичную информацию на стене взломанной страницы.

Как поступать в такой ситуации?

Важно не поддаваться первоначальному порыву, а постараться связаться с человеком по телефону или задать ему проверочный вопрос, ответ на который можете знать только он и вы. Если вы видите, что он не может ответить или уходит от ответа, его взломали. Обязательно постарайтесь связаться по телефону с тем, кого взломали, и поясните ситуацию, это даст возможность поменять пароль в аккаунте, тем самым перехватить управление и остановить дальнейшее вымогательство.

3. Внезапный выигрыш призов

В основном схема базируется на курсах, когда участника конкурса просто разводят на деньги, под предлогом оплатить доставку за выигранный приз. При этом схема проста: создается группа, которая некоторое время ведется как настоящая, выкладывается информация, добавляются друзья и участники, и при достижении определенного количества начинает проходить конкурс о розыгрыше ценного приза. Далее участнику приходит сообщение о выигрыше, а для получения приза необходимо оплатить доставку.

При переписке мошенники очень убедительны, часто прибегают к тому, что присылают фотографии призов с бумажкой, на которой написана ваша фамилия, что отвлекает внимание жертвы от главного.

Как поступать в такой ситуации?

Если вы получили сообщение о выигрыше, уточните, когда он проходил и есть ли видео, подтверждающее, что выиграли именно вы, и не платите за доставку.

Запомните главное – такие преступления раскрываются очень сложно в виду того, что злоумышленник может находиться в другом регионе или в другой стране. Даже если преступление раскроют и преступник будет задержан, у него может не оказаться материальных ценностей, на которые может быть наложен арест для возмещения причиненного вам имущественного вреда.