ГУ МВД России по Иркутской области

ОСТОРОЖНО, МОШЕННИКИ!

факты и комментарии

Прежде, чем заочно передавать (пересылать) кому бы то ни было Ваши деньги, прочитайте реальные истории из жизни, возможно это сохранит Ваш бюджет, убережёт нервы, здоровье и время.

Круглосуточный телефон дежурной части ГУ МВД 8 (3952) **216511**
Телефон доверия 8 (3952) **21-68-88**
Отдел по борьбе с мошенничествами 8 (3952) **216095; 212095**
Отдел участковых уполномоченных 8 (3952) **216284; 212079**

г. Иркутск 2018г.

Гражданке «К» 1937 г.р. (г.Усолье-Сибирское) на сотовый телефон позвонил неизвестный мужчина, который представился её внуком и сообщил, что на автомашине сбил женщину и для освобождения от ответственности ему нужны деньги, которые необходимо перечислить на указанные им номер счёта и телефон. Гражданка «К» через терминал самообслуживания отделения ПАО «Сбербанк России» перевела преступникам 70 тысяч рублей.

Как впоследствии оказалось, внук жив-здоров и ни в каком ДТП не участвовал.

Гражданке «Б» 1963 г.р. (г.Ангарск) на сотовый телефон позвонил неизвестный мужчина, который представился сотрудников полиции и пояснил, что её сын попал в ДТП – сбил человека; для «урегулирования» инцидента необходимые денежные средства, которые следует перевести на указанный неизвестным номер телефона. Гражданка «Б» через терминал самообслуживания перевела преступникам 30 тысяч рублей.

В последующем оказалось, что сын ни в каком ДТП не участвовал.

Никогда в подобных случаях не принимайте поспешных решений. Расчёт преступника строиться как раз на том, что бы не дать вам возможности разобраться в случившемся и обдумать ваши действия. Не поддавайтесь на уловки преступников – «Срочно… Быстрее … »

В разговоре с «родственником» у вас должна сложиться 100% уверенность, что это именно он. Если есть «проблемы со связью» (плохая слышимость, шум и т.д.), скажите, что перезвоните и наберите известный вам телефон вашего близкого человека. Не принимайте никаких решений пока чётко и ясно не услышите голос близкого человека и не поймёте, что это именно он.

Если у вашего «родственника» вдруг, не оказалось своего телефона (сломался, забыл и т.п.), перезвоните на предложенный номер и спросите его о том, что известно только вам двоим (о близких людях, о последней встрече, о его семье и т.п.).

Если вам по просьбе «родственника» звонит неизвестный (случайный свидетель, друг и т.п.), скажите, что не будете предпринимать никаких действия пока не переговорите с близким человеком лично. Если он получил «травму», уточните район происшествия и номер скорой помощи, после чего перепроверите информацию через диспетчерскую «03».

Главное, под любым предлогом (например – «нужно посмотреть сколько у меня есть денег»), возьмите паузу. Всё обдумайте, проверте, а потом только принимайте решение.

Если Вам с подобной информацией и предложением звонит «сотрудник органов внутренних дел» (например инспектор ГИБДД или следователь) помните, что прекращение уголовного либо административного преследования за денежное вознаграждение является тяжким должностным преступлением. В ГУ МВД России по Иркутский области проводится

активная, системная работа по выявлению «предателей» интересов службы, привлечению их к уголовной ответственности и увольнению, поэтому подобный факт представляется маловероятным.

Кроме того, сам факт передачи денег должностному лицу для «освобождения от ответственности», образует состав преступления (взятка) и подразумевает привлечение к уголовной ответственности.

Постарайтесь получить как можно больше информации от звонившего (кто он; его должность; место службы; фамилия, имя отчество; обстоятельства произошедшего (где, когда, при каких обстоятельствах); состояние потерпевшего и его данные; номера (в т.ч. бортовые) приехавших машин ГИБДД и т.п.). Запишите номер телефона с которого поступил звонок. Скорее всего преступник уклониться от «подробного» общения с вами.

Уточните в дежурной части ДПС ГИБДД (21-27-99 – область; 21-76-01 - Иркутск) имело ли место подобное ДТП. Либо позвоните «02» с этим же вопросом.

Сообщите о полученном звонке в дежурную часть ближайшего отдела (отделения) полиции (02), либо на телефон доверия ГУ МВД (3952 216888), либо вашему участковому уполномоченному, либо по любому другому известному вам номеру полиции. Вам разъяснят ваши действия и помогут.

Гражданину «С» 1989 г.р. (г.Иркутск) позвонил неизвестный мужчина, который назвался его знакомым, сообщил что у него в районе г.Черемхово сломалась машина и попросил занять денег. С помощью системы «Сбербанк Онлайн» гражданин «С» перевёл на счёт, указанный неизвестным 21 тысячу рублей. Как в последующем оказалось у реального знакомого все было в порядке, деньги попали к мошенникам.

Никогда не отправляйте деньги знакомым (родственникам) не убедившись на 100%, что это действительно ваш близкий человек (обязательно дозвонитесь до него по известному вам номеру, а не по тому, с которого был получен первоначальный звонок).

Не стесняйтесь перезванивать и переспрашивать, если у вас возникли подозрения по поводу тембра, интонации или других особенностей голоса вашего «знакомого». Если на ваши повторные звонки уже никто не отвечает, это скорее всего мошенники.

Попросите других ваших родственников, знакомых созвониться с вашим близким, который просит помощи. Посоветуйтесь с ними, уточните знают ли они какие-либо подробности о жизни (положении) этого человека.

Помните, что в реальной жизни дальние (малознакомые) вам люди навряд ли будут обращаться к вам с просьбой о финансовой помощи.

В большинстве случаев подобные звонки поступают из других регионов России (привязка к месту осуществляется по картам, через Интернет). Постарайтесь поподробнее расспросить вашего «знакомого» о том месте где он находится (задавайте наводящие вопросы о наличии там каких-либо зданий, сооружений, поселений и т.п.). Если вы проявите уверенность в

вопросах (даже плохо зная тот район), преступник скорее всего откажется от обсуждения этой темы.

Предложите вашему «знакомому» («родственнику») обратиться к сотрудникам полиции, либо вызвать помощь по тел. 112, либо тех. поддержку из ближайшего поселения. Скажите, что оплатите их услуги. При этом необходимо убедиться в легитимности организации, которая занимается решением технических (либо каких-то иных) проблем (через реквизиты, в т.ч. официальный телефон, факс, расчётный счёт; все это можно будет проверить через Интернет).

Или скажите «знакомому», что сами отправите к нему помощь (через указанные выше организации, а возможно и приедете лично). Преступники в таком случае сразу же отказываются от своих планов на ваши деньги.

Гражданин «З» 1974 г.р. (г.Ангарск) в Интернете, на одном из сайтов нашёл объявление о продаже лодочного мотора, позвонил по указанному номеру телефона и договорился с неизвестным о покупке; после чего в счёт предоплаты перевёл преступникам денежные средства в сумме более 100 тысяч рублей (уже на следующий день телефон «продавцов» стал недоступен, сайт удалён).

Гражданка «С» 1990 г.р. (Иркутск) заказала одежду на сайте gepur.com; через некоторое время ей на электронную почту пришли реквизиты для оплаты (как в последующем оказалось со взломанной страницы менеджера сайта). Гражданка «С» перевела денежные средства преступникам в сумме 32,5 тысячи рублей.

Не предпринимайте никаких действий пока не убедитесь в «порядочности» сайта. Разноцветный сайт, на котором представлены красивые меню и картинки, а также заверения в исключительной порядочности данного сайта и магазина - не более чем изображение на экране. Такой сайт может сделать любой студент.

1. С помощью сервисов типа http://leader.ru/secure/ несложно определить все данные о домене магазина - в частности, когда он зарегистрирован, и на кого. И если домен зарегистрирован недавно на «Васю Пупкина», или размещается у непонятного малоизвестного хостера где-то за границей - то это повод задуматься;

2. Стоит внимательно присмотреться к сайту - нет ли там ошибок (грамматических ошибок, нерабочих ссылок, разделов со статусов "на реконструкции"). Наличие множества подобных ошибок, равно как скажем неработоспособность поиска или половины ссылок вглубь сайта должно заставить серьезно задуматься;

3. Несложно узнать индекс цитируемости любого ресурса, например, с помощью сервиса «Яндекс». Кроме того, можно поискать ресурс в моделируемом каталоге поисковика (в случае Яндекса, это - http://help.yandex.ru/catalogue/?id=1111360). Индекс цитирования поддельного сайта будет около нуля;

4. Следует "пробить" URL магазина через крупные поисковые машины (в частности: Яндекс, Рамблер, Google). Анализируя результат несложно сделать выводы о репутации сайта - нередко в первых 3-5 результатах встречается описание проблем с данным магазином или жалобы обманутых клиентов. Кроме того, многие поисковики (например ЯндексМаркет) ведут свои рейтинги магазинов, аккумулируя положительные либо отрицательные отзывы;

5. Одним из факторов оценки является наличие на сайте множества сторонних баннеров, всевозможной рекламы, кучи кнопок счетчиков и рейтингов - крупные ресурсы таким вещами не занимаются, так как Интернет-торговля приносит им доход, несопоставимо больший дохода от подобной рекламы;

6. Для получения полной картины о товаре перед его приобретением через Интернет стоит не полениться, и изучить отзывы по нему на различных форумах и сайтах, посетить сайт производителя, или что лучше - поискать реального человека среди знакомых, разбирающегося в искомой категории товаров или имеющего такой товар.

7. Самое главное в фирме - это офис. С нормальным юридическим адресом (которым не является квартира!), телефоном, факсом, банковскими реквизитами. Причем это совершенно однозначный критерий - у любой реальной фирмы они есть, и эту информацию реальная фирма не скрывает. И наоборот - если офиса нет, и предлагается связь по ICQ, почте или скайпу (т.е. нет даже телефонов) - то это крайне настораживающий фактор. Еще более настораживающим является использование в качестве контактов магазина почтовых адресов на бесплатных сервисах типа mail.ru.

8. Пробуйте договориться об оплате после получения товара. Просите оформить отправку почтой с наложенным платежом, или запросите расчет наличными с курьером. Если продавец отказывается, скорее всего, он недобросовестен.

9. Используйте следующую схему защиты своих денежных средств - попытайтесь дозвониться до менеджера Интернет-магазина, и уточнить у него что либо (причем не важно, что именно). Если это не удается (нет контактов, хронически не отвечают телефоны, или отвечает и там сидит "девочка-попугай" с ответом на все вопросы "Смотрите на сайте, там все есть, ничего больше не скажу") - интернет магазин явно неблагонадежный.

Если связь есть – задайте второй вопрос: "А к вам можно подъехать (причина любая: оплатить товар по месту, уточнить что-то из его характеристик, подписать договор)? И тут нередко выясняется, что на звонки отвечает работающий по найму оператор, который не знает координат офиса и не видел в глаза своего работодателя. Это второй настораживающий фактор (причем необходимо учитывать и то, что у «создателей» фиктивных интернет-магазинов есть и готовый сценарий подобных бесед - "приезжайте конечно, наш офис в д.Малое Гадюкино, 150 км вертолетом на северо-запад от Нижнего Тагила" - т.е. расчет идет на то, что никто и никогда туда не поедет).

10. На сайте Федеральной налоговой службы России размещен электронный сервис «Проверь себя и контрагента», который позволяет оценить надежность будущего партнера, выявить фирмы-однодневки.

Пользуйтесь только услугами проверенных сайтов, с которыми уже имели дело ваши друзья и знакомые.

Гражданину «Ч» 1956 г.р. (Иркутский район) на сотовый телефон позвонил неизвестный мужчина и сообщил, что ему положена денежная компенсация за ранее приобретённые некачественные лекарственные препараты, для получения которой необходимо зарегистрироваться в системе «Сбербанк Онлайн» и сообщить, пришедшие по СМС коды. Гражданин «Ч» сделал все, что его попросил неизвестный после чего с его счёта были списаны все находящиеся там деньги – 3 тысячи рублей.

Гражданину «К» 1948 г.р. (г.Братск) на домашний телефон позвонил неизвестный мужчина, который представился сотрудником расчётно-кассового центра (г.Москва) и сообщил, что ему положена компенсация за ранее приобретённые препараты (БАДы). Для получения денег, необходимо заплатить налог, компенсировать траты на пересылку и использование, согласованных с налоговой инспекцией счетов.

В общей сложности гражданин «К» перечислил преступникам 720 тысяч рублей.

Никогда и никому не сообщайте пароли (коды), полученные от банка для проведения каких бы то ни было финансовых операций.

Не входите в одну и ту же реку дважды – если вас уже один раз обманули, представляется маловероятным, что у преступников проснулась совесть и они решили компенсировать вам потери.

Если позвонивший вам человек представился сотрудником какого-либо правоохранительного или надзорного органа (прокуратура, полиция, судебные приставы, налоговая служба, федеральная служба по защите прав потребителей и т.п.), помните, что вам может быть положена компенсация (за не полученный, либо не качественный товар) исключительно по судебному решению. А следовательно: вы должны были написать заявление (в установленной форме); вас должны были допросить (причём очно), признать потерпевшим; информировать о ходе и окончании следствия; возможно вызвать в суд для дачи свидетельских показаний; направить копию судебного решения. Но и это ещё не всё, преступники очень редко добровольно возмещают финансовые потери потерпевшим, поэтому уже вы сами должны были обратиться с заявлением и судебным решением в Федеральную службу судебных приставов по месту жительства для принудительного взыскания долгов.

Если всего вышеперечисленного вы не делали, то и никакую компенсацию за не полученный (либо не качественный товар) вы получить не можете.

Кроме того, расспросите подробно позвонившего вам человека кто он такой, какое ведомство представляет (где оно находиться - адрес), его фамилия, имя отчество, должность, номера рабочих (стационарных) телефонов; фамилия руководителя. Обязательно всё запишите. Перезвоните в аналогичное ведомство (прокуратура, полиция и т.п.), расположенное в Вашем населённом пункте (либо по любому, известному вам номеру полиции), расскажите всю ситуацию и данные звонившего. Вашу информацию проверят и обязательно сообщат с кем на самом деле вы имеете дело.

Если всё-таки решили получить от кого-либо денежные средства «заочно» через ваши банковские карты или иные счета, заведите для этого случая отдельную банковскую карту (счёт) с символической (минимально возможной) суммой денежных средств.

Гражданка «П» 1956 г.р. (г. Иркутск) в 2016 году услышала по радио рекламу о «чудесных» возможностях одного из народных целителей, позвонила по указанному номеру телефона и договорилась о проведении нескольких «лечебных» сеансов (заочно) за что перевела «целителю» денежные средства.

В 2017 году гражданке «П» позвонил неизвестный, который представился сотрудником прокуратуры г.Москвы и сообщил, что «целитель» с которым она общалась годом ранее на самом деле является мошенником и ей положена компенсация за потраченные денежные средства. Для получения компенсации необходимо провести ряд финансовых операций, что гражданка «П» и сделала.

В общей сложности гражданка «П» перевела преступникам 700 тысяч рублей.

Стоит очень критично относиться ко всем представителям нетрадиционной медицины. Перед тем, как обратиться за помощью к целителю, магу или колдуну, следует задуматься над сущностью проблемы и обдумать традиционные методы решения. Если человек твердо решает пойти к целителю, ему следует выбирать специалиста, который будет работать с ним в индивидуальном порядке.

Обычному человеку, не имеющему глубоких познаний в сфере лечения, достаточно трудно отличить профессионального врача от преступника с корыстными намерениями. При обращении к народному целителю больного должны насторожить следующие тревожные сигналы:

- возможность избавления от любого недуга, в том числе смертельных болезней, которые не поддаются лечению традиционными фармакологическими, психотерапевтическими или хирургическими методами;
- применение однотипных методов лечения от всех болезней;
- лечение и заговоры на будущее по фотографии;
- возможность получить не только лечебную помощь, но и услуги по наложению порчи, гаданию, покупке ритуальных принадлежностей и сувениров;

- рекомендации лекаря вернутся для коррекции многочисленных патологий, защиты от сглазов, снятия порчи и наговоров;

- обещания получить немедленный результат после оплаты первого взноса;

- многочисленные отрицательные отзывы других посетителей целителя;

- наличие ярких рекламных объявлений и баннеров, сайтов в социальных сетях, интернет-магазинов, коммерческих объявлений в СМИ;

- заявление со стороны «мага», который обличает других обманщиков. Истинные целители не занимаются черным пиаром и не изобличают других представителей народной медицине в обмане;

- наличие в кабинете у целителя обилия ненужных побрякушек для создания таинственного антуража и отвлечения клиентов, аксессуаров каббалистической символики, противоречащих друг другу религиозных символов;

- яркая одежда, множество вычурных украшений;

- непонимание сути ключевых лечебных и магических терминов, изобилие туманных фраз и стремление уйти от сути проблемы.

Гражданину «В» 1986 г.р. (г. Нижнеудинск) пришло СМС-сообщение о том, что его банковская карта заблокирована, а также номер телефона, по которому можно было бы уточнить информацию и решить возникшую проблему. По указанному номеру гражданину «В» ответила неизвестная женщина, которая представилась менеджером банка, сослалась на сбой программы, попросила назвать номер карты и код, пришедший по СМС. После чего со счёта гражданина «В» были списаны все находящиеся там деньги – 25 тысяч рублей.

«Гражданке «С» 1948 г.р. на сотовый телефон позвонил неизвестный мужчина, представился сотрудником «Департамента инвестирования» и сообщил, что ей необходимо получить банковские проценты со сберегательного вклада в ПАО «Восточный Экспресс банк», для этого нужно сообщить номер личного кабинета и код, полученный посредством СМС сообщения. Гражданка «С» выполнила инструкции неизвестного, после чего с её счёта были списаны все, находящиеся там деньги в сумме 42 тысячи рублей.

Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты (и ваших счетов) – это банк, обслуживающий ее, у которого есть официальные реквизиты и телефоны (которые пишутся на обороте карты).

Перезвоните в ваш банк по официальному телефону и выясните интересующие вас вопросы (в т.ч. по блокировке, начислению процентов и т.п.).

Перепроверите номер, с которого получен звонок (через официальный сайт банка, или той организации на которую ссылается незнакомый вам человек). Если вы не найдёте подобного телефона, скорее всего это мошенники.

Если у вас есть подозрения о том, что с вашей картой что –то не в порядке, если вы получили информацию о «бонусах» и «процентах», которые и не ожидали, не предпринимайте никаких действий, пока не убедитесь в реальности проблем (предложений) лично посетив ваше банковское учреждение. Любой консультант окажет вам помощь.

Если банки закрыты, дойдите до ближайшего банкомата и проверте порядок действия вашей карты, а также сумму, находящихся там денег (проценты обычно зачисляются на текущий счёт).

Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении. Во-первых, скорее всего это мошенники, во вторых - за это может взиматься дополнительная плата.

Гражданин «И» 1980 г.р. (Усть-Кут) на различный сайтах в сети Интернет разместил заявки на получение кредита. Через некоторое время ему позвонил неизвестный мужчина, который представился сотрудником ПАО «СКБ Банк» и сообщил, что заявка одобрена и для получения денег необходимо оплатить страховку и услуги курьера. Гражданин «И» через платёжный терминал самообслуживания и систему «Сбербанк Онлайн» перевёл на указанный ему счёт 25,5 тысяч рублей.

Кредит не получил. Телефоны «менеджера банка» не доступны. Деньги получены мошенниками.

На территории Иркутской области оказывают финансовые услуги более 50 банков. Их реквизиты, адреса и телефоны можно посмотреть в Интернете (например на сайте «Выберу.ру» или «Сравни.ру»).

Прежде чем размещать заявку на получение кредита на сайтах малоизвестных банковских учреждений или на специальных сайтах, которые рассылают заявки во все банки, попробуйте получить кредит в банках (либо отделениях) расположенных в вашем населённом пункте.

Если во всех банках, куда вы обратились лично, вам отказали в выдаче необходимой вам суммы, смотрите на вещи реально - представляется маловероятным, что какое-либо иное, уважающее себя финансовое учреждение, согласиться сотрудничать с вами.

Различные банки имеют различные условия выдачи кредита; бывает и страхование и курьерская доставка. Однако, дабы обезопасить себя от возможных неприятностей, постарайтесь найти такие условия, которые не предполагают выплату денег банку ещё до того, как банк сам выплатит вам кредит. Предложите банку вариант выплаты (либо отчисления) подобных расходов из суммы вашего кредита. Нормальное финансовое учреждение ведёт гибкую политику привлечения клиентов и скорее всего пойдёт вам на встречу, а вот мошенники нет.

Попросите направить вам на электронную почту (либо каким-то другим способом) договор оказания банковских услуг (открытия кредитной линии). Помните, что никакой официальный банк не выдаст вам никакого кредита если не будет подписан договор с всеми оговорёнными условиями (в т.ч. страховкой, курьером и т.п.). Банк не имеет право требовать от вас каких бы то ни было выплат пока не будет подписан договор.

Найдите в Интернете официальный сайт данного банка (либо координаты его филиалов в вашем городе (области)). Созвонитесь с консультантами по официальным телефонам учреждения, расскажите о полученном вами предложении, укажите номера телефонов с которых вам поступали звонки, уточните реальность предложенным вам условий.

Гражданка «П» 1973г.р. (Усть-Кутский район) на сайте «Авито.ру» нашла объявление о продаже автомашины, позвонила по указанному номеру и договорилась с неизвестным мужчиной о покупке, после чего в счёт предоплаты через систему «Сбербанк Онлайн» перевела преступнику денежные средства в размере 540 тысяч рублей (через день телефон «продавца» оказался недоступен, объявление с сайта удалено).

Гражданин «Я» 1984 г.р. (г.Железногорск-Илимский) на сайте «Авито.ру» нашёл объявление о продаже видеокарт и позвонил по указанному номеру, ему ответил неизвестный мужчина, который подтвердил наличие товара и предложил внеси предоплату на указанный им счёт. Гражданин «Я» через платёжный терминал перечислил «продавцу» 61 тысячу рублей, после чего телефон последнего стал недоступен, объявление с сайта удалено.

Никогда не переводите предоплату за товар, который хотели бы приобрести, неизвестным вам лицам.

Постарайтесь по возможности отказаться от «заочных» покупок по объявлениям физических лиц если не имеете возможности лично убедиться в наличии, законности и качестве товара.

Мошенники привлекают внимание к объявлениям низкой ценой. Посмотрите на другие предложения интересующего товара, ознакомьтесь с ценами. Не связывайтесь с продавцами, у которых цены более чем на 30% отличаются от среднерыночных.

Скажите продавцу, что хотели бы отправить «родственника» («знакомого») посмотреть товар перед покупкой и попросите адрес его местонахождения. Мошенник, скорее всего будет уклоняться от подобной встречи.

Популярный мошеннический приём — «срочно переведите деньги, иначе товар будет продан другому покупателю». Ответственный продавец всегда готов немного подождать оплату реальному покупателю.

В разговоре с продавцом и попросите предоставить больше информации о товаре, например, дополнительные фотографии или характеристики. Если

товар в наличии и продавец готов его продать, он не откажет в вашей просьбе. Хорошим доказательством наличия товара станет фото товара с хозяином и документом, подтверждающим его личность, а также актуальность даты продажи-покупки (получите и проверте логин продавца).

Если продавец не хочет делиться с вами на дополнительной информацией, он может оказаться мошенником. Если у вас возникло ощущение, что продавец плохо знает свой товар, то не спешите с покупкой и обратите внимание на другие аналогичные предложения.

Гражданке «К» 1997г. (г. Иркутск) на сотовый телефон позвонил неизвестный мужчина, представился сотрудником ООО «Эльдорадо» и сообщил, о том, что она выиграла приз в лотерею, которую проводила данная фирма. Мужчина также сообщил, что для получения выигрыша необходимо заплатить страховой взнос. Гражданка «К» перечислила преступникам на указанный ими счёт 3 тысячи рублей (никакого выигрыша не получила).

Гражданке «М» 1963 г.р. (г. Саянск) с одного из интернет сайтов пришло СМС сообщение о том, что она выиграла автомашину «Тойота Лэнд Крузер 200». Гражданка «М» перезвонила по указанному в СМС номеру, неизвестный мужчина пояснил, что для получения приза необходимо заплатить налог, что она и сделала переведя «организаторам лотереи» 75 тысяч рублей. Сразу после получения денег, телефоны преступников оказались недоступны.

Не стоит верить никаким сообщениям о чудесном выигрыше. Если Вы не участвовали ни в какой лотерее, то и выиграть Вы ничего не можете.

Любые просьбы о переводе средств для получения большого выигрыша свидетельствуют о мошеннических намерениях создателей проекта.

Свяжитесь с представительством компании на территории вашего города, выясните реальную информацию о проведении «лотереи» и её «победителях» (такую же информацию можно получить на официальном сайте организации). Если вы нигде не найдёте понятных и подробных сведений о «лотерее», то значит «участвуют» в ней и выигрывают (ваши деньги) исключительно преступники.

Постарайтесь выяснить как можно больше информации у человека, который вам позвонил (кто он, какую должность занимает, откуда (город) звонит, что за лотерея, когда она проводилась, где о ней было напечатано (сообщено), где оформлены официальные данные о победителях и т.п.). Если хоть на один вопрос нет ответа или он вызывает определённую заминку у человека, это скорее всего мошенник.

Гражданка «А» 1975г.р. (г.Иркутск) разместила на сайте «Авито.ру» объявление о продаже мебели. Через некоторое время ей на телефон позвонила неизвестная женщина и высказала желание эту мебель

приобрести, а также внести предоплату за будущую покупку. Для получения предоплаты гражданка «А» сообщила «покупателю» номер своей банковской карты и пришедший по СМС код, после чего преступники сняли со счёта гражданки «А» все имеющиеся там деньги – 6 тыс. рублей.

Гражданка «П» 1942 г.р. (г.Шелехов) на сайте «Авито.ру» разместила объявление о сдаче в аренду комнаты, ей на телефон позвонил неизвестный мужчина и сообщил, что хочет арендовать жилплощадь и внести за неё предоплату. Гражданка «П» прошла к банкомату и по подсказке потенциального «арендатора» произвела ряд операций (сообщила ему свой счёт и код (цифровой пароль)), после чего с её счёта на счёт преступников были списаны денежные средства в размере 68 тысяч рублей.

Никогда и никому не сообщайте пароли (коды), полученные от банка для проведения каких бы то ни было финансовых операций.

Старайтесь производить расчёты исключительно при визуальном контакте с покупателем. Помните, если человек, отозвавшийся на ваше объявление, больше интересуется не товаром, а способами расчёта, это скорее всего мошенник.

Постарайтесь разговорить покупателя на отвлечённые темы, например где он живёт, работает и т.п. Представляется маловероятным, что «нормальный» человек из Москвы захотел бы купить шкаф в Иркутске (если только это не эксклюзивный антиквариат). В большинстве случаев мошенники звонят из других городов. Если «покупатель» из другого города, это должно Вас насторожить. Задайте какой-либо вопрос о том районе, адрес которого он назовёт (если это ваш город). Если он начинает «плыть» в географии вашего города, при этом говорит, что живёт в соседнем районе, это скорее всего мошенник.

Если всё-таки решили проводить расчёты с покупателем «заочно» через ваши банковские карты или иные счета, заведите для этого случая отдельную банковскую карту (счёт) с символической (минимально возможной) суммой денежных средств.

В целом, для того, что бы обезопасить свои денежные средства:

Не распространяйте сведения о мобильных номерах и свои анкетные данные в Интернете, не указывайте их на страницах в соц. сетях. Особенно те, к которым привязаны банковские карты и мобильный банк.

Для работы с банковскими картами и системами мобильного и интернет-банка нужно использовать отдельное мобильное устройство, не предназначенное для разговоров и развлечения в Интернете.

Согласуйте с банком, что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, ограничьте круг операций, установите лимит, который можно переводить с помощью мобильного устройства.

Запретите перевод всего объема денежных средств с карты и счета.

Гражданину «Д» 1987 г.р. (г.Иркутск) в социальной сети «ВКонтакте» пришло сообщение со «страницы» знакомого – «Степан переведи пожалуйста деньги для погашения кредита». Гражданин «Д» посредством услуги «Сбербанк Онлайн» перевёл на счёт физического лица 15 тысяч рублей. Как позже оказалось, «страница» знакомого была взломана, деньги попали к мошенникам.

Гражданке «Б» 1958 г.р. (Заларинский район) в социальной сети «Одноклассники» пришло сообщение со «страницы» её знакомой о том, что в сети «Одноклассники» можно приобрести бонусы на подарки. Гражданка «Б» в ответном сообщении отправила «знакомой» данные своей банковской карты и коды, присланные ей в СМС сообщениях. После чего с её банковской карты были списаны все находящиеся там деньги – 7,5 тысяч рублей. Как позже оказалось страница знакомой была взломана преступниками.

Помните, что для преступников, специализирующихся на компьютерных технологиях, не составляет большого труда взломать не только «страницу» физического лица, но и практически любой сайт, который не развивает и не совершенствует системы безопасности (специальные программы автоматически перебирают все возможные слова (используемые в паролях) которые есть в словарях, как русских, так и английских).

Поэтому никогда не перечисляйте деньги вашим «знакомым» («родственникам»), основываясь исключительно на их просьбе, поступившей по эл. почте, посредством СМС сообщений, через социальные сети или мессенджеры типа «Вайбер» и «Ватсап».

Прежде чем предпринимать какие-либо действия, обязательно перезвоните вашему близкому человеку по известному вам номеру телефона (сотового, стационарного) и убедитесь, что ему действительно нужна помощь (помните, что ложное стеснение (либо «неудобство») могут стоить вам денег).

Ещё одним способом обезопасить себя может стать переписка (общение) с вашим «знакомым», до того, как вы соберётесь ему что-либо отправить. Подробно расспросите его о проблеме и причинах её возникновения, между делом упомяните общих знакомых, спросить о вещах, которые известны только вам и вашему близкому человеку (т.е. о вещах, которые нельзя узнать о вас из интернета). Общие фразы, недоговорённость, торопливость, являются признаками того, что вы скорее всего общаетесь с мошенником.

Если вам предлагают участие в каких-то специальных (бонусных, праздничных и т.п.) программах, перед тем как что то предпринять, обязательно ознакомитесь с условиями таких акций на официальном сайте организации (соц. сети). Если вы не найдёте подробной и понятной информации о проводимой акции, значит её и нет, а вы имеете дело с мошенниками.

Что бы не стать жертвой или невольным участником подобных неприятностей, примите меры к тому, чтобы обезопасить свой аккаунт. Нужно придумывать сложные пароли как минимум из 8 символов. Лучше, если это будут несуществующие слова, смысл которых понятен только пользователю. Можно добавить несколько цифр, ведь чем сложнее пароль, тем труднее хакеру взломать страницу.

Гражданину «Ш» 1994г.р. (г. Ангарск), водителю службы такси «Максим», на сотовый телефон пришло СМС сообщение о вызове такси на один из адресов города. Гражданин «Ш» перезвонил на номер, указанный в СМС, ему ответил неизвестный мужчина, который подтвердил заказ и попросил по пути следования к адресу заехать в магазин, купить продукты и пополнить счёт телефона с последующей отдачей денег при встрече. На всё вышеперечисленное, гражданин «Ш» потратил 5,5 тысяч рублей. По прибытию на адрес оказалось, что там никто такси не вызывал, номер телефона у хозяев другой, а тот, с которого поступал звонок, оказался недоступен.

Самый простой способ уберечь себя от подобного вида мошенничеств – не тратить деньги на неизвестных вам лиц.

Если вы в силу различных обстоятельств не можете просто отказаться от подобной услуги человеку «из телефона», сошлитесь на отсутствие в данный момент денежных средств, но ни в коем случае не покупайте ничего и не переводите деньги «на голос».

В описанном выше случае звонок поступил с сотового телефона, зарегистрированного в Оренбургской области. Подавляющее число подобного рода звонков (до 90%), поступает в наш регион из других субъектов Российской Федерации (в том числе из мест лишения свободы).

Если по специфике своей деятельности вы часто имеете дело с незнакомыми вам номерами, будет полезно выяснить для себя основные варианты первых трёх цифр (после 8-ки), которые используют сотовые операторы в нашем регионе. Номера с необычной конфигурацией указанных цифр должны вызывать у вас чувство настороженности, тем более если разговор будет идти о перечислении (одалживании) денег либо покупке каких-то вещей. Спросите вашего собеседника какому оператору принадлежит номер, а после ответа, добавьте (уверенно), что подобную конфигурацию данный оператор в нашем регионе не использует (даже если вы этого точно не знаете). Скорее всего ваш уверенный тон побудит преступника отказаться от своих намерений.

Гражданке «С» 1983 г.р. (г. Иркутск) продавцу-консультанту одного из павильонов ТРЦ «Сильвер-Молл» на стационарный телефон павильона поступил звонок от неизвестного мужчины, который представился директором данного павильона, сказал, что ему нужны

деньги для оплаты рекламы и попросил перечислить 20 тысяч рублей на счёт через мобильный банк, что гражданка «С» и сделала.

В последующем оказалось, что реальный директор с подобными просьбами никому не звонил. Деньги были перечислены мошенникам.

Расчёт преступников строиться на том, чтобы обескуражить собеседника активным монологом, напором, властным тоном и требованием решить вопрос незамедлительно. То есть не дать опомниться и подумать о логике и порядке своих действий.

Кроме того, будучи не плохими психологами, преступники рассчитывают на то, что продавец (тем более молодой и неопытный) не будет задавать лишних вопросов «руководителю», переспрашивать, либо перезванивать для уточнения каких-то нюансов.

Следовательно, для того, чтобы не попасться «на удочку» мошенников, вам необходимо их разочаровать своей рассудительностью и дотошностью.

Не стесняйтесь задавать своему «руководителю» уточняющие вопросы. Скажите, что переживаете за его деньги и поэтому хотели бы убедиться в полной их безопасности, а для этого ему нужно назвать некоторые вещи, которые точно знает ваш директор и не могут знать мошенники (например ваше имя отчество, число и год рождения, марка и номер его машины, когда он последний раз забирал у вас выручки и т.п.). Или например скажите – «Так вы же вчера брали деньги на рекламу!!» (даже если этого не происходило). Практически все подобные звонки поступают из других регионов России (телефоны преступники получают через интернет); используйте это обстоятельство, задав вопрос о месте расположения вашего павильона и его особенностях.

Сделайте вид, что потеряна связь и перезвоните вашему директору на известный вам номер телефона. Ничего не предпринимайте пока не дозвонитесь.

Перед тем, как отдать (переслать) заочно деньги, посоветуйтесь с любым из ваших коллег или со старшим продавцом, бухгалтером, администратором.

Помните, что реальный директор вас наверняка похвалит за бдительность и осторожность.

Гражданке «Ч» 1947 г.р., руководителю одной из обслуживающих население компаний (г.Усть-Илимск), на стационарный телефон организации позвонил неизвестный мужчина, который представился работником прокуратуры и попросил приехать в здание прокуратуры для уточнения отдельных вопросов, касающихся деятельности предприятия. По пути следования гражданке «Ч» повторно, но уже на сотовый телефон, позвонил этот же мужчина и попросил пополнить баланс двух телефонов (с последующим возвратом денег по прибытию в прокуратуру), что она и сделала через терминалы «МТС», перечислив на указанные ей номера 10 тысяч рублей.

Прибыв в прокуратуру, гражданка «Ч» выяснила, что никто её не вызывал, сотрудника с таким номером телефона в данной организации нет.

Выясните у звонившего его данные (фамилия, имя, отчество; звание и должность, номер кабинета и как можно подробнее – существо дела по которому вас вызывают).

Перезвоните в приёмную руководителя учреждения куда вас вызывают (прокуратура, ФСБ, другое контроль-надзорное ведомство) либо в дежурную часть (полиция, МЧС) и уточните есть ли у них такой сотрудник, а также (если есть) попросите его номер телефона (телефоны приёмных и дежурных частей легко узнать на официальных сайтах, а также в справочниках). Обязательно позвоните по данному вам номеру (под любой легендой, например уточнить порядок ваших действий).

С большой долей вероятности окажется, что там, куда вы позвоните либо нет такого сотрудника, либо с вами будет разговаривать совсем не тот, кто звонил первоначально.

Не предпринимайте никаких действий, пока не убедитесь в реальном существовании сотрудника (прокуратуры, полиции и т.п.), а также законности, обоснованности и реальности его требования (просьбы).

Уклоняйтесь (сошлитесь на отсутствие денег) от каких бы то не было просьб о перечислении денег, пополнении счетов телефонов, покупке подарков и т.п. Сообщите, что будете общаться исключительно по деловым и официальным вопросам.

Помните, что просьбы сотрудников правоохранительных либо контрольно-надзорных органов (подобные вышеуказанным) граничат либо с должностным преступлением, либо (как минимум) с дисциплинарным проступком. Сообщите о полученной вами просьбе любому из руководителей учреждения куда вас вызывают (телефоны есть на официальном сайте), либо в дежурную часть полиции (на территории обслуживания «02», или в дежурную часть главного управления МВД России по Иркутской области - 216511), либо в подразделение собственной безопасности (тел. 212162, 216929, 212144), либо по телефону доверия - 216888.