Информация
по предупреждению краж и мошенничества с использованием банковских карт, компьютерных и телекоммуникационных технологий

Ежедневно в Республике Бурятия регистрируется по несколько преступлений, связанных с кражей денежных средств с банковских карт или мошенничества с использованием электронных средств платежа. За 10 месяцев 2020 года зарегистрировано свыше 1100 преступлений по фактам мошенничества. Суммы украденных денежных средств составляют от нескольких тысяч до более миллиона рублей.

1. Сотовый телефон используется как средство передачи голосовой информации, например, «ваш сын попал в аварию..», «мама у меня проблемы..», «это из банка/соцзащиты и прочее..», либо для передачи СМС с ложной информацией: «мама, кинь мне на этот номер денег, потом все объясню», «ваша карта заблокирована подробности по телефону..», «с вашего счета списано 5000 рублей, подробности по телефону...».

В случае получения входящего звонка необходимо прекратить разговор, перезвонить близким, от чьего имени пришло сообщение, позвонить в банк по указанному на карте телефону, посетить ближайшее отделение банка и уточнить информацию о совершенных с картой операциях. При получении сообщения ни в коем случае не нужно перезванивать на указанные номера.

Должно насторожить, если у вас запрашивают сведения о карте клиента (её номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия), ПИН-код. Банки никогда не запрашивают по телефону эти данные.

Мошенники умело вступают в контакт, располагают к себе. Например, для решения проблем с банковскими картами могут предложить обратиться в банковское отделение или устранить ее по телефону. Такие слова усыпляют бдительность человека, подтверждают причастность говорящего к финансовой организации, и граждане, продолжая телефонный разговор, рискуют потерять свои деньги.

2. Мошенничество в виде ошибочной оплаты заключается в отправке сообщения о выполнении зачисления определенной суммы денег. После этого приходит сообщение от мнимого отправителя денег, которое уведомляет об ошибке и просит выполнить обратный перевод. Жертва мошенника, не проверив пополнение своего счета, выполняет перевод на указанный счет, тем самым теряя собственные средства.

3. Мошенники могут использовать ваше объявление в сети Интернет (например, сайт Avito) для получения от вас данных карты: например, «я по вашему объявлению на авито (о продаже, о сдаче в аренду), сообщите мне данные с вашей карты и код на обратной стороне я вам отправлю деньги...».

Для предотвращения мошенничеств рекомендуем не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным. По возможности не использовать в сети Интернет номера мобильных телефонов, привязанных к банковским картам или «Мобильному банку».

4. Мошенники также могут пересылать СМС-сообщения, сообщения через мессенджеры Viber, WhatsApp с вредоносной информацией: например, «здесь наши с тобой фото http:\\\\...», , «ваш аккаунт, страница «ВКонтакте» взломаны, пройдите регистрацию http:\\\\...», «вы выиграли автомобиль, подробности http:\\\\...». При получении похожего сообщения откажитесь от прохождения по указанной ссылке. Если вы прошли по ссылке, при этом к вашему мобильному устройству привязана банковская карта, срочно свяжитесь с банком, заблокируйте карту и приостановите обслуживание по счетам.

5. Распространены случаи мошенничества при продаже товаров в сети Интернет по предоплате, получения от интернет-магазина или продавца товара, не соответствующего заявленному. При заказе следует особое внимание уделить отзывам о данном интернет-магазине, продавце, проверить, когда был создан магазин, сайт. Если сайт существует меньше месяца, то стоит отказаться от покупки. При любом сомнении откажитесь от приобретения товара со 100% предоплатой через социальную сеть.

Рассмотрим другую ситуацию. Потерпевший сам ищет какой-либо товар в сети Интернет для покупки. В данном случае Вам никто не может гарантировать честность продавца. Поэтому если Вы желаете приобрести вещь, необходимо ознакомиться с рейтингом доверия продавца, который учитывается в приложении, почитать отзывы об интернет-магазине. Однако следует помнить, что и отзывы можно купить. Полицейские рекомендуют воздерживаться от покупок у лиц, проживающих за пределами региона. Ищите продавца, к которому вы можете приехать, осмотреть товар, убедиться в его наличии. Лучше, совершать покупки через официальные сайты компаний.

Пример: *Оперативниками сыскного отдела уголовного розыска Управления МВД России по г. Улан-Удэ задержана подозреваемая в мошенничестве*

Следствием установлено, что братчанка в марте текущего года на одном из популярных сайтов объявлений опубликовала объявление о продаже щенка йоркширского терьера. Связавшейся с ней улан-удэнке она рассказала, что может доставить собаку, но для этого необходимо сделать предоплату в сумме пяти тысяч рублей. Однако после получения денежных средств «продавец» заблокировала входящие сообщения от покупательницы и перестала отвечать на звонки.

В июле злоумышленница также опубликовала на сайте объявление о продаже щенка французского бульдога. Связавшись с покупательницей из Улан-Удэ, братчанка попросила перевести на банковский счет более 32 тысяч рублей за щенка и доставку. После получения денежных средств злоумышленница также заблокировала покупательницу и не отвечала на телефонные звонки.

Возбуждены уголовные дела по признакам преступления, предусмотренного ч. 2 ст.159 Уголовного кодекса Российской Федерации.

6. Широкое распространение в сети Интернет так же приобретают мошенничества с привлечением средств пользователей для их приумножения в

финансовых пирамидах, микрофинансовых организациях, рынках электронных валют.

Злоумышленники звонят гражданам и представляются сотрудниками компаний, занимающихся получением дохода на финансовом рынке, и предлагают сотрудничество. В дальнейшем все общение, как правило, переходит в мессенджеры.

На компьютер потерпевшего устанавливается программа удаленного доступа, после чего мошенник, выступая в роли брокера, получает доступ ко всем счетам потерпевшего. Он, якобы, проводит операции, покупает акции, обменивает валюту. Пострадавший видит, как вложенные деньги дают прибыль, однако вывода денежных средств в конечном итоге не происходит.

При этом период со дня совершения мошеннических действий до дня обращения в полицию может затянуться до одного года. И всё это время потерпевший полагает, что осуществляет деятельность на финансовом рынке.

Пример: *27 мая в отдел полиции Октябрьского района г. Улан-Удэ с заявлением о факте мошеннических действий обратился 30-летний местный житель.*

Мужчина рассказал, что в апреле для дополнительного заработка зарегистрировался на сайте брокерской компании, где ему предложили выгодно вложить деньги. Улан-удэнца заверили, что пущенные в оборот денежные средства за короткий срок принесут прибыль: об этом, в том числе, позаботится эксперт, который будет направлять клиента и поддерживать общение с ним через популярный мессенджер.

В течение месяца горожанин перечислял на указанный сотрудником фирмы счет крупные суммы. В общей сложности он перевел 1 250 000 рублей. Мужчина был убежден, что его сбережения, участвующие в финансовых сделках, приносят доход. По данным сайта, за месяц он дополнительно заработал 44 тысячи долларов.

Когда клиент решил вывести средства, аналитик фирмы потребовал для осуществления операции еще 4400 долларов. В этот момент гражданин понял, что стал жертвой обмана. Его личный кабинет на сайте организации был заблокирован, а сам эксперт перестал выходить на связь. В результате житель Улан-Удэ потерял как вложенные, так и, якобы, заработанные средства.

Зачастую граждане переводят достаточно крупные суммы денег лицам, которых ни разу не видели. Также, как и не видели какие-либо официальные документы организации, не знакомились с деятельностью трейдинговой организации в сети Интернет, не читали отзывы и сами не обладают познаниями в этой сфере деятельности.

Полиция рекомендует прежде чем, отдавать деньги совершенно незнакомым лицам, для начала получить достаточные познания в данной сфере, прочитать специальную литературу, пройти курсы, посетить финансовых консультантов, аналитиков и т.д.

7. Каждый человек может столкнуться с предложением оформить кредит или займ через социальные сети. В подобных случаях мошенники могут использовать информацию о поданной заявке, предложив оформить страховку для дальнейшего получения кредита.

8. В связи с активным распространением у населения банковских карт, расчет по которым на сумму до 1000 рублей возможен без введения пин-кода – увеличилось количество преступлений, при совершении которых злоумышленники, похищая (либо находя) банковскую карту, рассчитываются по ней в магазинах. Гражданам необходимо проявлять особую осмотрительность, а в случае утери карты принимать незамедлительные меры по ее блокировке.

То же самое касается сотовых телефонов с подключенной услугой «мобильный банк». Если Вы потеряли гаджет или сменили номер телефона, необходимо незамедлительно обратиться к в банк и отключить привязку банковского счета к сим-карте.

Чаще всего на уловки мошенников попадаются граждане в возрасте от 25 до 40 лет. Легко на уловки злоумышленников попадают пожилые люди – в силу своего возраста и доверчивости. Особенно, если речь идет о, якобы, попавших в беду родственниках.

Еще раз обращаем ваше внимание на меры по обеспечению собственной безопасности:

- Никогда, никому, ни при каких обстоятельствах нельзя передавать логин, пароль или реквизиты банковской карты (код безопасности, имя владельца, срок действия), ПИН-код.

- Если вы потеряли карту или у вас есть основания полагать, что третьи лица узнали ее реквизиты, незамедлительно обратитесь в банк и заблокируйте ее. После получения ответа от банка с выпиской по счету обратитесь в полицию.

- Чтобы уберечь SIM-карту, к которой привязана карта, оперативно уведомляйте банк при получении подозрительных сообщений и ни в коем случае не звоните по указанным в них номерам. Проинформируйте банк, если сменили номер или потеряли SIM-карту.

- Читайте отзывы о сайтах, страницах в социальных сетях, через которые планируете что-то приобретать.

Проявляя необходимую бдительность, вы сохраните свои денежные средства!

Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Если вы решили испытать счастье и выйти на связь с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения.

Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или т.н. «электронные кошельки».

Будьте бдительны и помните о том, что для того, чтобы что -то выиграть, необходимо принимать участие в розыгрыше. Все упоминания о том, что ваш номер является «счастливым» и оказался в списке участников лотереи, являются, как правило, лишь уловкой для привлечения вашего внимания.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего - необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату, зачастую путем внесения денежных средств на некий виртуальный кошелек посредством терминала экспресс-оплаты. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

Цель подобных сайтов – обмануть максимальное количество людей за короткий срок. Создать Интернет-сайт сегодня – дело нескольких минут, поэтому вскоре после прекращения работы сайт возродится по другому адресу, с другим дизайном и под другим названием.

Если вы хотите купить товар по предоплате помните, что серьезные Интернет-магазины не будут просить вас перечислить деньги на виртуальный кошелек или счет мобильного телефона. Поищите информацию о магазине в сети Интернет, посмотрите, как долго он находится на рынке. Если вы имеете дело с сайтом крупной или известной вам компании, убедитесь в правильности написания адреса ресурса в адресной строке вашего браузера. При необходимости потребуйте от администраторов магазина предоставить вам информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц. Убедитесь в том, что вы знаете адрес, по которому вы сможете направить претензию в случае, если вы будете недовольны покупкой.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер.

Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что – то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

	На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах? **НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.** *Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.*

Один из популярных способов мошенничеств, основанных на доверии связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами и выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Благоразумие поможет и здесь. Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая, однако, о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи. Воспользуйтесь Интернет-поиском. Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Посмотрите среднюю стоимость аналогичных товаров. Чересчур низкая стоимость должна вызвать у вас подозрение. Если продавец требует перечислить ему полную или частичную предоплату за приобретаемый товар на электронный счет, подумайте, насколько вы готовы доверять незнакомому человеку. Помните, что перечисляя деньги незнакомым лицам посредством анонимных платежных систем, вы не имеете гарантий их возврата в случае, если сделка не состоится.

Вы хотите приобрести авиабилеты через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.

Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.

Покупать авиабилеты через Интернет удобно. Вам не нужно никуда ехать и стоять в очередях. Вы выбираете рейс, дату, оплачиваете билет и получаете его спустя несколько секунд. Сегодня многие люди выбирают именно такой способ приобретения билетов на самолет.

Естественно, мошенники не могут оставить данную сферу без внимания. Создать Интернет-сайт по продаже авиабилетов – дело нескольких часов, на смену его названия, адреса и внешнего оформления требуется еще меньше времени. Как правило, обман раскрывается не сразу, некоторые узнают о том, что их билетов не существует, лишь в аэропорту. Это дает мошенникам возможность перенести свой Интернет-ресурс на новое место и продолжать свою преступную деятельность под другим названием.

Чтобы не испортить себе отдых или деловую поездку стоит внимательно отнестись к покупке авиабилетов через сеть Интернет. Воспользуйтесь услугами Интернет-сайта авиакомпании или агентства по продаже билетов, давно зарекомендовавшего себя на рынке. С осторожностью отнеситесь к деятельности неизвестных вам сайтов, особенно тех, которые привлекают ваше внимание специальными предложениями и низкими ценами. Не переводите деньги на электронные кошельки или счета в зарубежных банках. Не поленитесь позвонить в представительство авиакомпании, чтобы убедиться в том, что ваш рейс существует и билеты на него еще есть. Эти простые правила позволят вам сэкономить деньги и сберечь нервы.

Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

НИКОГДА не переходите по ссылке, указанной в сообщении.

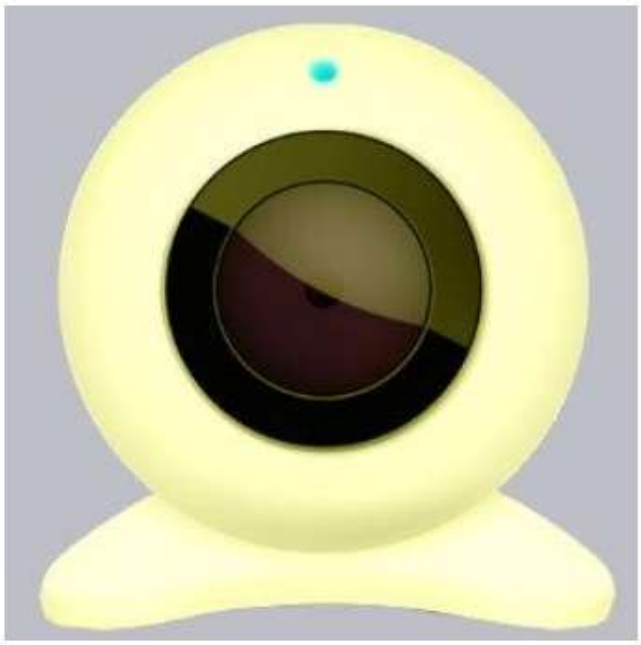
Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

Если вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или какой -нибудь программы, не спешите открывать её. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто -то из знакомых вам людей, будет не лишним дополнительно убедиться в этом, ведь сообщение могло быть отправлено с зараженного телефона без его ведома. Если отправитель вам не знаком, не открывайте его.

Помните, что установка антивирусного программного обеспечения на мобильное устройство - это не прихоть, а мера, позволяющая повысить вашу безопасность.



Общаетесь в интернете и имеете аккаунты в соцсетях?

НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

Многие люди сегодня пользуются различными программами для обмена сообщениями и имеют аккаунты в социальных сетях. Для многих общение в сети стало настолько привычным, что практически полностью заменило непосредственное живое общение.

Преступникам в наши дни не нужно проводить сложные технические мероприятия для получения доступа к персональным данным, люди охотно делятся ими сами. Размещая детальные сведения о себе в социальных сетях, пользователи доверяют их тысячам людей, далеко не все из которых заслуживают доверия.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Поэтому не следует раскрывать малознакомому человеку такие подробности вашей жизни, которые могут быть использованы во вред. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

Не забывайте, что никто лучше вас самих не сможет позаботиться о сохранности той личной информации, которой вы не хотите делиться с общественностью.