

Информация о практикуемых мошенниками способах хищений, совершаемых на территории Республики Алтай с использованием коммуникационных и информационных технологий

Сообщение «Ваша банковская карта заблокирована»:

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников. Например, предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда жертва звонит по указанному телефону, ей сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

Размещение объявления на сайтах о продаже имущества: законопослушный гражданин размещает объявление о продаже бывшего в употреблении мебельного шкафа на страницах магазина бесплатных объявлений в Интернете «Авито». Злоумышленник звонит по указанному в объявлении номеру, заверяет, что шкаф ему нравится и он поручил родственнику его забрать завтра- послезавтра, а деньги готов отправить уже сейчас на карту банка. Продавец диктует реквизиты карты или счета. Через 15-20 минут злоумышленник вновь перезванивает продавцу, сообщает, что стоит у платежного терминала и не может отправить деньги. Ему нужен СМС-код, который сейчас поступит на телефон продавца (потенциальной жертвы обмана). Если в силу неосведомленности продавец называет этот код, то через несколько секунд ему поступает СМС о снятии всех денег с его счета.

Звонок от службы безопасности банка: злоумышленник звонит на абонентский номер гражданина, представляется сотрудником службы безопасности банка, говорит о том, что по счету клиента, проходят подозрительные операции, для прекращения данных операций необходимо назвать номер карты и CVV2/CVC2 код (три цифры с обратной стороны карты), а так же код который придет по СМС - сообщению.

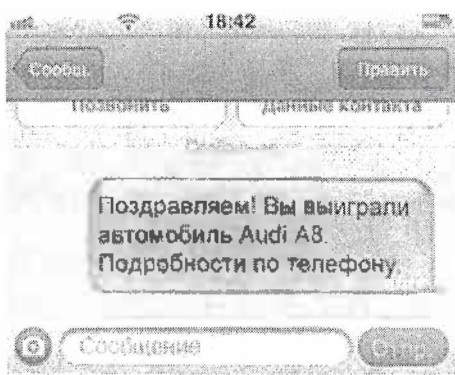
Помощь в оформлении кредита: злоумышленник размещает объявление о помощи в оформлении кредита. Жертва обращается за помощью, злоумышленник предлагает оплатить страховку за получение кредита в сумме от 5-10 %, после перевода денежных средств злоумышленник блокирует телефон.

Продажа товара по заниженной цене: злоумышленник на Интернет площадках, в социальных сетях размещает объявление о продаже товара по заниженной цене, после получения денежных средств злоумышленники оплаченный товар не отправляют.

Сайты, предлагающие быстрый заработок: потерпевший заходит на сайт, читает, что он предлагает быстрый доход, например, с 1000 рублей +5000 рублей в месяц. При этом на сайте присутствуют сотни положительных отзывов. Но: на таком сайте, скорее всего, отсутствуют контактные данные, либо они есть, но подставные. Нельзя переводить деньги на кошельки, указанные на таких сайтах.

Ваш родственник попал в беду: требование по телефону денег за решение разного рода проблем, в том числе за возможность избежать наказания за противоправное деяние, является одним из самых распространенных обманов. Звонить может как сам «родственник», так и человек, представляющийся адвокатом или сотрудником полиции. Причины могут называться разные: совершил ДТП, избил человека, задержан с наркотиками и т.д., но итог разговора всегда одинаков – для «решения» вопроса требуется определенная сумма денег. Деньги просят передать либо курьеру или перевести их через платежный терминал на конкретный телефонный номер.

Интернет-мошенничество - памятка для граждан

СИТУАЦИЯ 1	
	Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза? НИКОГДА не отправляйте деньги неизвестным лицам на их электронные счета. <i>Помните, что вероятность выиграть приз, не приняв участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.</i>

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. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

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. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша.

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.

СИТУАЦИЯ 2	
	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. <i>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 столкнетесь с мошенниками крайне высока.</i>

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-оплата. 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.

СИТУАЦИЯ 3	
	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. <i>Самым правильным решением в данной ситуации будет позвонить в банк, выпускающий и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.</i>

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

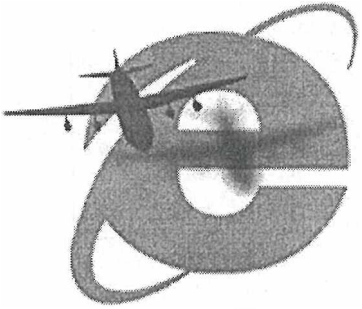
вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

СИТУАЦИЯ 4	
	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. <i>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.</i>

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.

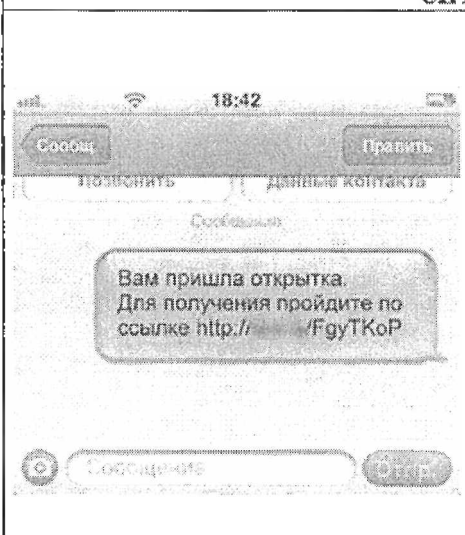
СИТУАЦИЯ 5	
	Вы хотите приобрести авиабилеты через Интернет? НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов. <i>Заказывайте билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.</i>

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. За последний год существенно увеличилось количество жалоб на обман при покупке электронных билетов. 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 относиться к покупке авиабилетов через сеть Интернет. Воспользуйтесь услугами Интернет-сайта авиакомпании или агентства по продаже билетов, давно

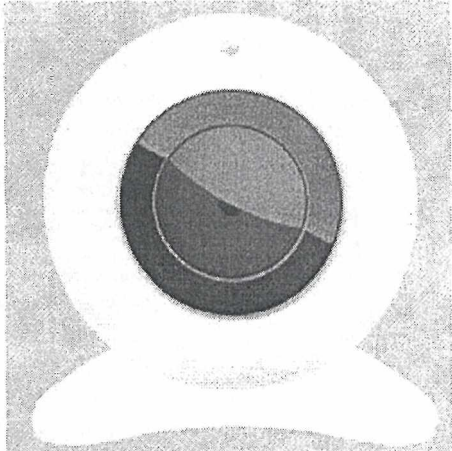
зарекомендовавшего себя на рынке. С осторожностью отнеситесь к деятельности неизвестных вам сайтов, особенно тех, которые привлекают ваше внимание специальными предложениями и низкими ценами. Не переводите деньги на электронные кошельки или счета в зарубежных банках. Не поленитесь позвонить в представительство 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.

СИТУАЦИЯ 6	
	Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы? НИКОГДА не переходите по ссылке, указанной в сообщении. <i>Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.</i> <i>Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.</i>

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.

СИТУАЦИЯ 7	
	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. <i>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.</i>

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.

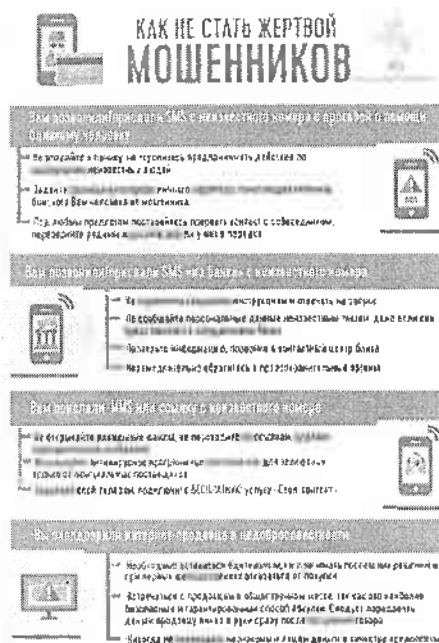
Преступникам в наши дни не нужно проводить сложные технические мероприятия для получения доступа к персональным данным, люди охотно делятся ими сами. Размещая детальные сведения о себе в социальных сетях, пользователи доверяют их тысячам людей, далеко не все из которых заслуживают доверия.

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.

ПАМЯТКА(Скачать)

Советы по определению Интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей



Информация НЦБ Интерпола МВД России

о самых распространенных видах мошеннических действий с использованием компьютерных технологий.

Уважаемые граждане! Если Вы относитесь к активным пользователям Интернета, то рекомендуем Вам обязательно прочитать этот материал!

Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Подобная преступная деятельность преследуется законом независимо от места совершения - в реальной или виртуальной среде.

Мошенники постоянно изыскивают все новые и новые варианты хищения чужого имущества. Кратко остановимся на самых распространённых.

«Брачные мошенничества»

Типичный механизм: с использованием сети Интернет

преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов. Направленные жертвами деньги преступники получают

на подставных лиц. После получения средств переписка под различными предложениями прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

Мы настолько привыкли покупать в интернет-магазинах, что часто становимся невнимательными, чем и пользуются мошенники. Обычно схема мошенничества выглядит так: создаётся сайт-одностраничник, на котором выкладываются товары одного визуального признака. Цена на товары обычно весьма привлекательная, ниже среднерыночной. Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные данные. Чаще всего такие интернет-магазины работают по 100% предоплате. Переписка о приобретении товаров ведётся с использованием электронных почтовых ящиков. По договорённости с продавцом деньги перечисляются, как правило, за границу через "Western Union" на имена различных людей. Конечно же, псевдо-продавец после получения денег исчезает!

«Крик о помощи»

Один из самых отвратительных способов хищения денежных средств. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

«Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для

кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотерее, а также сообщения о получении наследства.

«Нигерийские письма»

Один из самых распространенных видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взятки чиновникам и т.п.

«Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В распоряжении Бюро имеется информация о следующих недобросовестных брокерских компаниях: «MXTrade», «MMC1S» и «TeleTrade».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам-трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Важно! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «Н» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН-КОД КАРТЫ

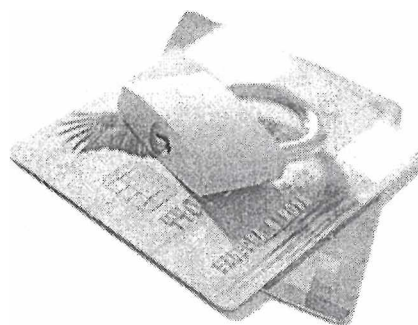
- ВЫУЧИТЬ ПИН-КОД ЛИБО ХРАНИТЬ ЕГО ОТДЕЛЬНО ОТ КАРТЫ И НЕ В БУМАЖНИКЕ
- НЕ ПЕРЕДАВАТЬ КАРТУ ДРУГИМ ЛИЦАМ – ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ
- ПОЛЬЗОВАТЬСЯ ТОЛЬКО БАНКОМАТАМИ НЕ ОБОРУДОВАННЫМИ ДОПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ
- ПО ВСЕМ ВОПРОСАМ СОВЕТОВАТЬСЯ С БАНКОМ, ВЫДАВШИМ КАРТУ



Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

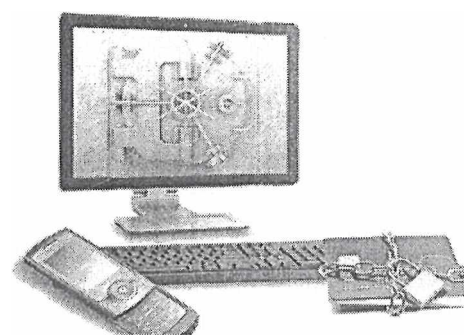
Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты Управления «Н» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сэкономят Ваши средства.



Будьте осторожны и внимательны!

Мошенники на атакуют владельцев карт



ПИН-КОД — КЛЮЧ К ВАШИМ ДЕНЬГАМ

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду, как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё — в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ВАША КАРТА — ТОЛЬКО ВАША

Не позволяйте никому использовать Вашу пластиковую карту — это все равно что отдать свой кошелек, не пересчитывая сумму в нём.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Помните: хранение реквизитов и ПИН-кода в тайне — это Ваша ответственность и обязанность.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Использование банкоматов без видеонаблюдения опасно вероятностью нападения злоумышленников.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.

БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата — если он долгое время находится в режиме ожидания или самопроизвольно перезагружается — откажитесь от его использования. Велика вероятность того, что он перепрограммирован мошенниками.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком — он обязан предоставить консультацию по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Мошенничество с использованием сайтов-дублеров благотворительных организаций

В сети интернет регулярно размещаются объявления от лица благотворительных организаций, детских домов, хосписов, приютов и др. с просьбой о материальной помощи.

Злоумышленники:

- Создают сайт-дублер, являющийся точной копией оригинального;
- Меняют реквизиты для перечисления денежных средств.

Запомните!

Прежде чем помочь какой-либо организации:

- Позвоните по телефону в указанную организацию;
- Уточните номер расчетного счета, либо посетите ее лично;
- Убедитесь в достоверности размещенной информации.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Памятка безопасности при онлайн-покупке товаров и онлайн-оплате услуг

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

Злоумышленники:

- Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем;
- Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина;
- Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен;
- После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

- неоправданно низкая цена на товар;
- электронная почта или мессенджеры в качестве способов коммуникации;
- оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;
- обязательная предоплата, зачастую более половины стоимости товара;
- отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт;
- сомнительный интернет-адрес.

Запомните!

- Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;
- Самый безопасный способ оплаты - после получения заказа;
- Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предлогами (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки).

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

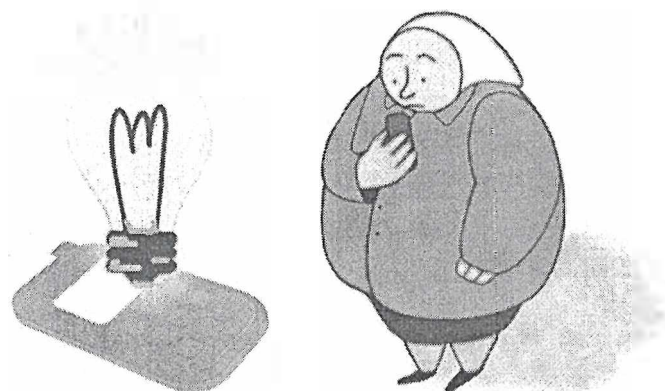
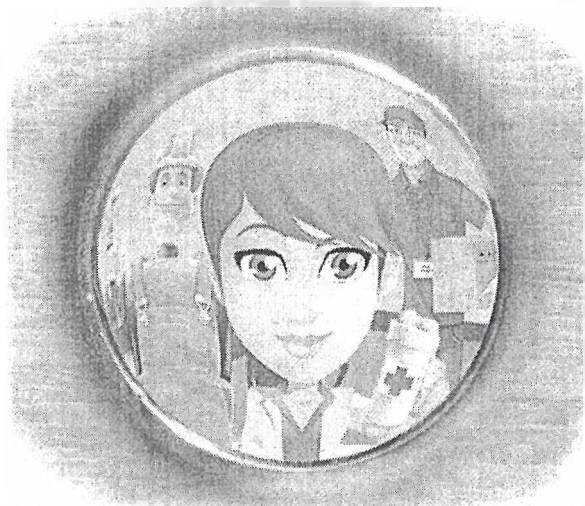


МВД РОССИИ ПРЕДУПРЕЖДАЕТ

будьте бдительны! звоните 02 или 102

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым

людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста!



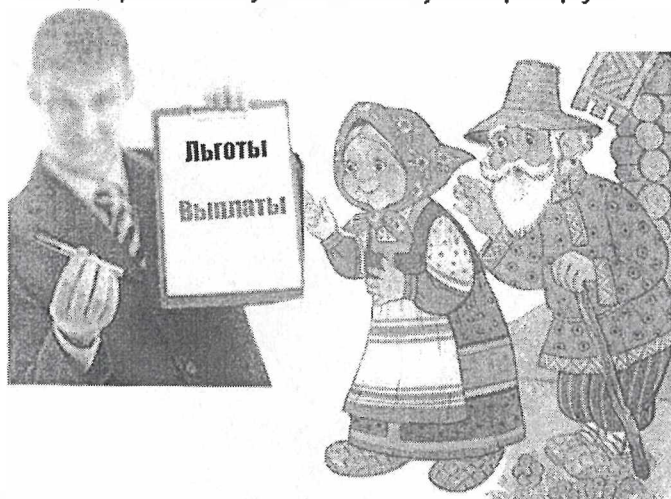
НЕ ДОВЕРЯЙТЕ,

если Вам звонят и сообщают, что Ваш родственник или знакомый попал в беду или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться.

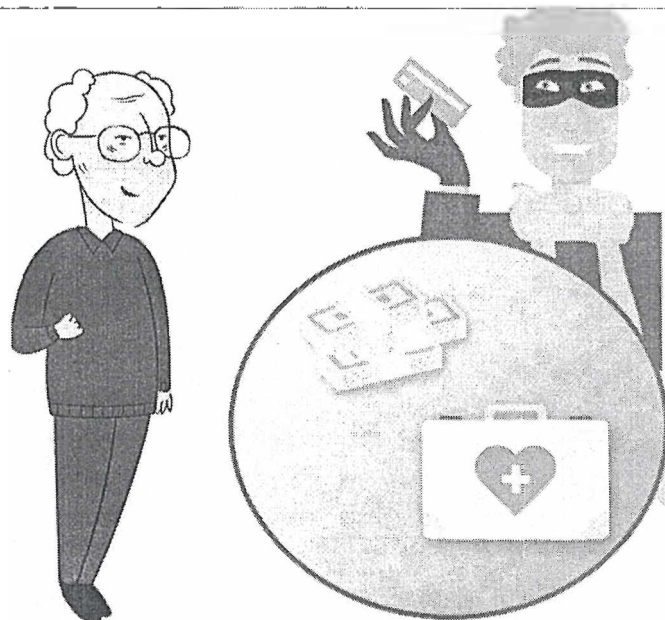
Это ОБМАН!

СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ

Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!



Не подписывайте никакие документы!



Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам?

НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!

Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

- Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;
- Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;
- Под надуманными предложениями просят сообщить PIN-код банковской карты, содержащиеся на ней данные;
- Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

- Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;
- Сотрудник банка может запросить у клиента только контрольное слово, ФИО;
- При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;
- Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;
- При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на обратной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

- Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;
- Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;
- Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.