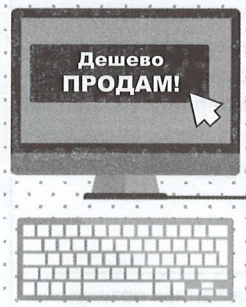
УМВД РОССИИ ПО ГОРОДУ АСТРАХАНИ ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО: МОШЕННИКИ!

Не Дайте себя обмануть!

02, 112, 400-116

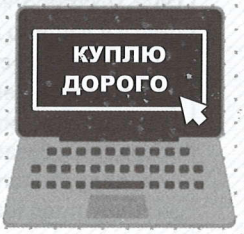
Объявления о продаже



Мошенники - продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

Объявления о покупке

Мошенники - покупатели спрашивают реквизиты банковской карты или СМС-код, якобы для перечисления денег за товар после чего похищают деньги с банковского счета.



Сообщения от друзей

Мошенники пользуются чужой страницей в социальных сетях, и под видом Вашего друга (родственника) под различными предлогами просят перечислить им деньги или сообщить данные Вашей карты, якобы для перечисления денег.

Блокировка банковской карты

Сообщения о блокировке банковской карты с номера, по которому нужно позвонить. Цель преступников узнать данные Вашей карты.

Махинации с банковской картой

Телефонные заказы товаров, оформление почтовых посылок на непроверенных интернет сайтах, после оплаты и получения которых, оказывается, что товар не соответствует заказанному. Телефон и интернет сайт мошенников после этого не доступны.

Незаконная банковская операция (несанкционированное списание)

Мошенники звонят с телефонных номеров с приставкой +7-495***; +7499******; 8-800**** и др. сообщают о том, что в настоящее время с Вашей Карты происходит незаконное списание средств. После, вводят в заблуждение и узнают данные Вашей карты или перечисляют с нее денежные средства.**

Вирус в телефоне

Поступает сообщение (в том числе от имени друзей) со ссылкой, которая оказывается вирусом. С помощью него мошенники получают доступ к банковской карте и снимают с нее деньги.

Наиболее часто совершаемые формы мошенничеств

• Сотовый телефон и ваше объявление в сети Интернет (сайт Avito) используется мошенником для получения от вас данных карты и привязки карты к мобильному телефону мошенника: - «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...»; - «я хочу отправить деньги вам на карту за товар на авито, предоплату за аренду, у вас карта привязана к мобильному банку, если нет идите к банкомату я вас проинструктирую как подключить мобильный банк». • Сотовый и проводной телефон используется как средство передачи голосовой информации, подвиды, типы: - «ваш сын, брат и т.д. и т.п. попал в аварию..», - «мама/папа у меня проблемы..», - «это из банка – ваша карта заблокирована или имеются проблемы со счетом». • Сотовый телефон используется для передачи СМС с ложной информацией: -«мама, кинь мне на этот номер денег, потом все объясню», -«ваша карта заблокирована подробности по тел..», -«с вашего счета списано 5000 рублей, подробности по тел...».	При получении сообщения не нужно перезванивать на указанные номера. Мошенники могут потребовать передать деньги курьеру, перечислить их на карту, номер мобильного телефона, попытаются получить от вас сведения о Вашей банковской карте, предложить пройти к банкомату и совершить какие-либо операции у банкомата, попросят сообщить коды которые приходят к Вам на телефон. В случае получения входящего звонка необходимо прекратить разговор, даже если собеседник вселяет уверенность в своей правдивости. Мошенники обладают психологическими приемами введения в заблуждение, либо обладают информацией о потерпевшем и его близких. Аналогичные случаи мошенничества встречаются и в сети Интернет, но сообщение о помощи передается посредством сообщения в социальной сети с ложной страницы родственника.
• Сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Типы сообщений: «здесь наши с тобой фото http:\\\\...», «ваш акакунт, страница «вКонтате» взломаны, пройдите регистрацию http:\\\\...», «вы выиграли автомобиль, подробности http:\\\\...” • Новый тип сообщений с вредоносной ссылкой: «я по вашему объявлению, согласны ли на обмен на это http:\\\\ foto3.inc...»	При получении данного сообщения откажитесь от прохождения по указанной ссылке и активации полученных ссылок. По возможности проверьте есть ли в сети Интернет в поисковых системах сведения о данных ссылках и возможных мошенничествах. Сообщите пользователям сети Интернет, что данная ссылка мошенническая. Удалите указанное сообщение если убеждены, что оно не нанесло вред Вашему устройству.
• Мошенничества при продаже товаров в сети Интернет по предоплате (распространенные виды: продажа Iphone, цифровой, бытовой техники, одежды, обуви, автомобилей, автозапчастей, продажа авиабилетов и путевок в санаторий). • Получение от интернет магазина, продавца товара не соответствующего заявленному.	Не стоит приобретать товары в интернет магазинах позиционирующих себя как российские, но имеющие сайты в доменных зонах .com .org .biz .net .info .tv .mobi. Особое внимание следует уделить отзывам в сети Интернет по данному интернет-магазину, продавцу. Проверить когда был создан магазин, сайт. Создан ли он год и более назад. Если сайт существует меньше месяца, то стоит отказаться от покупки. Можно проверить наличие офиса у данного магазина, удостовериться в сети Интернет, что такой дом существует, посмотреть его на карте, фото снимках, панорамах Яндекс, Гугл. В случае необходимости приобрести товар через социальную сеть необходимо тщательно проверить продавца, обязательно связаться с ним по телефону, расспросить подробности о товаре, потребовать фотографии товара в деталях, предложить отправить товар курьерской службой и наложенным платежом, обговорить возможность возврата товара, возможность самовывоза.
Сайты-«подделки», а так же фишинговые сайты	Единственной рекомендацией может быть проявление внимательности. Необходимо обратить внимание на адресную строку сайта, название сайта, есть ли какие-либо добавочные символы или названия в адресной строке, расположен ли сайт в доменной зоне «ru». Скопировать название сайта из адресной строки и проверить в поисковой системе. Не стоит доверять сайтам имеющим в названии знакомые слова, но расположенные в доменных зонах .com .org .biz .net .info .tv .mobi и других не связанных с российским интернет пространством. При покупке авиа, жд. билетов не ищите очень дешевые билеты на сомнительных сайтах, тем более расположенных в доменных зонах .com .org .biz .net .info .tv .mobi. Доступные по цене билеты желательно приобретать на официальных сайтах компаний перевозчиков.

Если вы стали жертвой мошенничества и заметили, что после разговора или проведения операции, покупки у вас происходит списание денежных средств, немедленно обратитесь в банк по **горячей линии** и потребуйте отменить все денежные операции, совершенные в период общения с мошенниками и осуществите возврат денежных средств. Это же необходимо сделать в случае перечисления денежных средств на абонентские номера сотовой связи либо на электронные средства платежа (ЯндексДеньги, Вебмани, Киви и т.д.).