За последние несколько лет стали распространенными преступления, связанные с обманом людей, особенно престарелого возраста.

Эта категория людей очень доверчива ко всякому роду просьбам (например: дать человеку попить, поесть, позвонить и т.д.), вследствие чего люди пускают незнакомцев в свой дом, квартиру. Находясь в жилище злоумышленники сразу же ориентируются в обстановке и пользуясь тем, что хозяин чем-то отвлелечен быстро проводят осмотр комнат и, как правило, находят сбережения людей в разных местах их хранения.

УМВД России по Рязанской области в целях предотвращения мошенничеств и хищений рекомендует:

- не приглашать в жилище незнакомых людей, кем бы они не представлялись – газовщиками, соцработниками, работниками пенсионного фонда, распространителями льготных товаров.

Проверьте документы, служебное удостоверение, подтверждающие профессиональную принадлежность. Когда злоумышленники, представляясь сотрудниками газовой службы, проникают к вам в жилище, то один отвлекает разговорами, второй в это время может попытаться похитить деньги из квартиры.

Также злоумышленники могут представляться сотрудниками социальной службы и, говоря о якобы будущей денежной реформе, предлагают переписать номера купюр, обещая их потом обменять на банкноты нового образца. Гражданин сам достает деньги и невольно показывает их место хранения, после этого хозяина квартиры отвлекают, и второй злоумышленник получает возможность похитить сбережения.

Подобные ситуации следует пресекать. Постарайтесь запомнить внешность людей, которые показались Вам подозрительными. Не оставляйте без внимания и заботы своих пожилых родственников, регулярно рассказывайте им о различных способах обмана и совершения краж.

С появлением широко оснащенных различными функциями гаджетов самыми распространенными видами преступлений стали мобильное и Интернет-мошенничество. **УМВД России по Рязанской области обращает особое внимание граждан: будьте острожны и бдительны! Не указывайте номера телефонов, привязанных к банковской карте, на страницах социальных сетей! Вашими данными могут воспользоваться мошенники!**

УМВД России по Рязанской области рекомендует ознакомиться с более подробной информацией, связанной с мобильным и интернет-мошенничеством:

1. Мошенничества, совершаемые с использованием мобильной и проводной связи:

а) сотовый и проводной телефон используется как средство передачи голосовой информации, где злоумышленник сообщает информацию типа:

- «ваш сын попал в аварию..»;

- «мама/папа у меня проблемы..»;

- «это из банка/соцзащиты и пр..».

б) сотовый телефон используется для передачи СМС с ложной информацией, где злоумышленник может сообщить следующее:

-«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...».

в) Самый популярный тип мошенничества: 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 за...»;

- «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…».

При получении подобных сообщений или звонков не нужно перезванивать на указанный номер. 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.

При малейшем сомнении в правдивости полученной информации следует перезвонить близким, от имени которых пришло сообщение, позвонить в банк по указанному на карте, либо в договоре телефону посетить ближайшее отделение банка.

Помните! Сотрудники банков никогда не запрашивают по телефону сведения о карте клиента, её номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия, и тем более пин-код. Если собеседник пытается получить от Вас такую информацию или просит сообщить коды от банка, пришедшие на Ваш абонентский номер, прекратите с ним разговор.

Гражданам, имеющим престарелых родственников, следует их проинструктировать и разъяснить последним, какие виды мошенничества существуют и как вести себя при получении звонков и сообщений мошеннического характера, а именно: не вести диалоги с мошенниками, прекратить разговор и позвонить родственникам. Если пожилой человек получает пенсию на банковскую карту, то предложите свою помощь в снятии с карты денежных средств, либо предложите родственнику передать карту Вам. Во многих случаях в ходе общения с престарелыми людьми сообщники мошенников находятся в районе проживания пожилого человека, либо у его дома, подъезда. При получении мошеннического звонка необходимо немедленно сообщить о данном факте в полицию.

Если при мошенничестве, в ходе телефонного разговора преступником была получена информация о банковской карте, то необходимо позвонить по телефону указанному на карте и заблокировать карту. В день совершения мошенничества необходимо обратиться в банк с заявлением о возврате денежных средств на карту, так как банк обязан возвратить денежные средства, если операция была оспорена владельцем карты в день операции.

УМВД России по Рязанской области рекомендует: для предотвращения подобного рода мошенничества не распространяйте в сети Интернет сведения о

мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, в подаваемых в сети объявлениях не указывать рядом с номером телефона Имя и Фамилию, адрес жительства и другую личную информацию.

В целях профилактики мобильного мошенничества не стоит использовать в сети Интернет номера мобильных телефонов, к которым привязаны банковские карты и номера, используемые для работы в «Мобильном банке».

Последнее время получают распространение мошенничества, совершенные в отношении пользователей сети Интернет, продающих товары на сайтах бесплатных объявлений. Это происходит следующим образом:

Продавцу поступает звонок от якобы покупателя. Мошенник под видом покупателя сообщает, что желает приобрести товар, но проживает в другом городе и предлагает оплатить товар путем перечисления денежных средств на карту продавца. Для этого он просит продавца назвать номер, владельца и срок действия карты, код на обратной стороне, а также сотовый номер привязанный к карте, либо по умолчанию использует номер указанный в объявлении. После получения этих сведений мошенник использует данные о карте для оплаты покупок в сети Интернет.

Другой вариант: на телефон продавца поступают коды от банка, мошенник просит сообщить их якобы для перевода денег. В этот момент мошенник подключает к телефону потерпевшего, либо к своему телефону услугу «Мобильный банк» и похищает деньги с карты.

Третий вариант когда мошенник, выступающий в роли «покупателя» предлагает продавцу пройти к банкомату и, якобы произведя некоторые операции, получить деньги.

Во всех трех указанных случаях мошенник похищает денежные средства продавца. Не поддавайтесь влиянию злоумышленникови не ведитесь на их уловки: **никому не сообщайте реквизиты карты!**

г) сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Подобные сообщения могут выглядеть следующим образом :

- «здесь наши с тобой фото http:\\\\...», ,

- «ваш акакунт, страница «вКонтате» взломаны, пройдите регистрацию http:\\\\...»,

- «вы выиграли автомобиль, подробности http:\\\\...”,

- а также **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.

Вредоносные программы создаются и усовершенствуются мошенниками регулярно. При работе с телефоном Вы можете столкнуться с видом вредоносных программ, не требующих Вашей активности, и программы самостоятельно могут быть загружены на Ваше мобильное устройство через уязвимость операционной системы.

В случае заражения мобильного устройства рекомендуется определить угрозы и последствия получения доступа хакера к Вашему мобильному устройству.

Признаками заражения мобильного устройства могут быть: блокирование операционной системы, блокирование входящих СМС сообщений, отправка искусственно сгенерированных мобильным устройством сообщений. Зараженный мобильный телефон следует немедленно выключить, а сим-карту перевыпустить у оператора сотовой связи, телефон сохранить для последующего изучения полицией, если было совершено мошенничество, либо передать в сервисный центр, если деньги похищены не были.

Если к данному мобильному устройству привязана банковская карта, а также банковские услуги «Мобильный банк», «Онлайн Банк», «Интернет-банк», то необходимо незамедлительно связаться с банком, заблокировать карту и приостановить обслуживание по счетам. Если с помощью телефона это сделать не удается, то следует обратиться в ближайшее отделение банка. Если же мобильное устройство используется для доступа к страницам в социальных сетях,

то необходимо с другого устройства либо компьютера выйти в социальную сеть и сменить привязанный номер телефона.

Зараженное мобильное устройство также является источником распространения вредоносной информации по контактам, содержащимся в телефоне. Для предотвращения рассылки необходимо уведомить максимальное количество знакомых о Вашей проблеме и о возможно приходящих от Вашего имени вредоносных сообщениях.

В случае если с Вашего телефона или банковской карты похитили денежные средства, необходимо в день совершения хищения обратиться в банк с требованием вернуть денежные средства, заблокировать ваш счет, запретить перевод денежных средств с вашего счета на другие счета, приостановить обслуживание счетов на которые были перечислены ваши денежные средства. После получения ответа от банка, с выпиской по счету обратиться в полицию.

Одним из распространенных мобильных мошенничеств также является использование дубликата сим-карты для доступа к системам дистанционного управления банковским счетом. Признаком использования дубликата Вашей сим-карты является блокирование доступа мобильной связи. В этом случае необходимо срочно обратиться к мобильному оператору и перевыпустить сим-карту. В случае подтверждения мобильным оператором факта несанкционированной замены Вашей сим-карты необходимо написать претензию в сотовую компанию и обратиться в полицию.

Чтобы не стать жертвой подобных мошенничеств, необходимо следовать следующим рекомендациям:

- Для работы с банковскими картами, системами «Мобильный банк», «Банк-онлайн», «Интернет-банк» и др. использовать отдельное мобильное устройство, не предназначенное для разговоров и развлечения в сети Интернет;

- Не указывать номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах соцсетей;

- Приобрести и установить на мобильное устройство лицензионное антивирусное программное обеспечение из официальных источников;

- Указать в договоре (в иной форме согласовать) с банком, что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, а также ограничить круг операций, установить лимит, который можно переводить с помощью мобильного устройства.

- Запретить перевод всего объема денежных средств с карты или счета.

2. Мошенничества, совершаемые в сети Интернет и с помощью сети Интернет:

а) мошенничества при продаже товаров в сети Интернет по предоплате (распространенные виды : продажа Iphone, цифровой, бытовой техники, одежды, обуви, автомобилей, автозапчастей);

б) получение от интернет магазина, продавца товара не соответствующего заявленному;

Развитие данных видов мошенничества обусловлено человеческими факторами, такими как желание сэкономить, отсутствие близко расположенных магазинов с таким товаром, полное отсутствие предложений на рынке. Основными приобретаемыми товарами являются предметы роскоши: дорогая цифровая техника, автомобили, шубы, брендовые вещи. Желание сэкономить зачастую приводит к потере всех денежных средств, в связи с чем УМВД России по Рязанской области рекомендует приобретать вещи за их реальную стоимость и не искать предложений с 30-50 % выгодой, так как это противоречит в целом принципам рынка, либо присланный товар окажется неисправным или подделкой, либо не удовлетворяющим запросам покупателя. 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 и проверить дату регистрации магазина. Если сайт существует меньше месяца, то стоит отказаться от покупки. Можно проверить наличие офиса у данного магазина, посмотреть его на карте, фото снимках, панорамах Яндекс и Гугл, а также убедиться, что на предполагаемом здании есть вывеска магазина, либо имеются офисные помещения. На снимках так же можно узнать названия, телефоны близко расположенных организаций, позвонить им и выяснить достоверность информации. В интернет справочниках найти телефоны

администратора офисного центра и убедиться, что такой магазин или индивидуальный предприниматель реально существуют и осуществляют свою деятельность в данном здании. Полученную информацию следует использовать при общении по телефону с сотрудниками магазина. Если магазин или продавец отказываются звонить по телефону предлагают другие способы общения такие как Viber, Skype, WhatsApp и другие, либо телефона магазин не имеет, следует отказаться от покупки. В ходе общения по телефону можно сообщить, что находитесь в городе продавца, магазина или магзина предложите забрать товар самовывозом и оплатить наличными в офисе. В случае категоричного отказа следует отказаться от покупки.

При приобретении таких дорогостоящих вещей как, к примеру, автомобиль, дорожная техника, строительные материалы, рекомендуется потратить деньги на дорогу до города продавца и удостовериться в наличии продавца и товара, либо найти в городе продавца знакомых и попросить их проверить достоверность предложения в сети Интернет. Если же такой возможности нет, следует оплатить услуги юриста, сотрудника автофирмы, занимающейся в городе продавца продажей и скупкой авто и за символическую плату предложить ему встретиться с продавцом и осмотреть авто и документы. То же касается и приобретения стройматериалов и металла, обратитесь к услугам юриста в городе продавца. Любые присланные Вам по Интернету фотографии, сканы документов и автомобиля мошенники с легкостью подделывают.

В настоящее время большинство интернет-магазинов работаю по 100% предоплате, при соблюдении указанных рекомендаций можно совершить удачную покупку.

Настоятельно рекомендуется не осуществлять «слепые» покупки в социальных сетях. Администрация соцсетей исключила разделы объявлений с сайтов и не несет ответственность за совершаемые с использованием сети действия пользователей.

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 наложным платежом, обговорить возможность возврата товара и возможность самовывоза.

Также следует обратить внимание и проверить отзывы и оставленные комментарии в группе и на странице продавца. Если несколько пользователей сети размещают сплошь хвалебные отзывы и рекомендации, то стоит просмотреть страницы этих пользователей, не являются ли они «фейковыми», есть ли у них на страницах личные фотографии, большое количество друзей. Данную информацию можно просмотреть и на странице магазина. Страница продавца должна быть активной, на ней регулярно должны размещаться личные фотографии, обновляться альбомы, должны быть сведения о месте учебы и работы, а в друзьях должны быть «живые» и активные пользователи. Можно уточнить, где находится продавец, в каком городе, предложить забрать товар якобы вашим знакомым, находящимся в данном городе и оценить реакцию продавца. Если в сети Вы общаетесь с продавцом магазина, то потребуйте сообщить сайт магазина в сети Интернет, юридический и фактический адрес. При любом сомнении откажитесь от приобретения товара со 100% предоплатой через соцсеть.

Широкое распространение в сети Интернет приобретают мошенничества с привлечением средств пользователей для их приумножения в финансовых пирамидах, кооперативах, микрофинансовых организациях, биржах, букмекерских конторах, рынках электронных валют. **Правоохранительные органы настоятельно рекомендуют не вступать в какие-либо отношения с такими организациями и лицами, предлагающими такие услуги**, так как многие компании и интернет-сайты данных компаний находятся за рубежом, организации работают по законам других государств, либо изначально мошеннические и вернуть затраченные на данные проекты деньги практически невозможно.

в) сайты - «подделки» , а также фишинговые сайты

Этот вид мошенничества предполагает, что жертва посчитает сайт знакомым и приобретет на нем товар или услугу, либо укажет данные своей банковской карты.

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.

Проверьте неоднократно сайты, в разделах которых планируете указать данные о своей банковской карте, по дате создания сайта, по телефонам указанным на сайте, по отзывам в сети Интернет, следует уточнить нет ли сайта в различных блек листах сети Интернет.

Помните! Мошеннику достаточно номера карты и кода на обратной стороне карты (CVV код состоящий из четырех цифр) для покупок и оплаты услуг в сети Интернет. Такие данные как срок действия карты, он может подобрать, а имя и фамилию владельца узнать от вас либо из сети Интернет с ваших личных страниц.

Если вы стали жертвой подобного сайта и заметили это после проведения операции, связанной с покупкой, заблокируйте карту и обратитесь в банк в день проведения операции для её отмены и возврате денежных средств.

Кроме того, при покупке авиа/ждбилетов 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.

Чтобы не стать жертвой мошенников, проявляйте бдительность! Разъясняйте своим близким, родственникам, знакомым, что при любом таком звонке либо посещении жилища незнакомыми лицами необходимо обратиться в дежурную часть полиции. Объясните родным, что лучше самим связаться с родственниками, чтобы выяснить произошло ли у них что-либо. Не предоставляйте никому данные своей банковской карты.

Если вы стали жертвой злоумышленников, незамедлительно обращайтесь в полицию по телефону 02 (102 – для мобильных операторов) или по телефону дежурной части УМВД России по Рязанской области (4912) 27-08-60.

Материал взят с сайта УМВД России по Рязанской области: https://62.мвд.рф