**Осторожно мошенники: Управление МВД России по городу Таганрогу советует, как не попасться на удочку злоумышленников**

Преступления против собственности и борьба с ними стали одной из самых актуальных проблем правоохранительных органов. Мошенничество, как один из видов преступления против собственности, по своей форме «мошеннических обманов»

чрезвычайно разнообразно.

Межмуниципальное управление МВД России «Волгодонское» рекомендует быть особенно бдительными в следующих ситуациях. Итак, самыми распространенными на сегодняшний день являются мошеннические схемы:

**Виды мошенничеств в сетях сотовой и проводной связи и в сети Интернет**

1. Мошенничества совершаемые с использованием мобильной и проводной связи:

а) сотовый и проводной телефон используется как средство передачи голосовой

информации, подвиды, типы:

- «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:

-«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...»;

Самая актуальная схема мошенничества:

в) 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».

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.

При сомнении в правдивости полученной информации следует перезвонить

близким от имени кого пришло сообщение, позвонить в банк по указанному на карте, либо в договоре телефону, посетить ближайшее отделение банка. Банк никогда не запрашивает по телефону сведения о карте клиента её номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия, а тем более пин-код, если собеседник пытается получить от вас такую информацию, либо просит сообщить коды которые пришли на Ваш телефон от банка, прекратите с ним разговор. Гражданам имеющим престарелых родственников, соседей, знакомых необходимо разъяснить им, какие способы мошенничества существуют, 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.

Для предотвращения мошенничеств так же рекомендуем не распространять 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 сотового телефона Имя и Фамилию, адрес жительства и другую личную информацию. Не использовать в сети Интернет номера своих мобильных телефонов к которым привязаны банковские карты и номера мобильных телефонов, которые используются для работы в «Мобильном банке».

Последнее время получают распространение мошенничества совершенные в отношении пользователей сети Интернет продающих товары на сайтах бесплатных объявлений. 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 карты, владельца карты, срок действия карты, код на обратной стороне, а так же 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.

Последнее время получают распространение мошенничества совершенные в отношении пользователей сети Интернет продающих товары на сайтах бесплатных объявлений. 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 карты, владельца карты, срок действия карты, код на обратной стороне, а так же 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 когда на телефон продавца поступают коды от банка и мошенник просит сообщать 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, в трех указанных случаях мошенник похищает денежные средства продавца.

г) 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. Вредоносные программы создаются и усовершенствуются мошенниками регулярно и при работе с телефоном Вы можете столкнуться с видом вредоносных программ

которые не требуют Вашей активности и самостоятельно могут быть загружены на Ваше мобильное устройство через уязвимости операционной системы. В случае заражения мобильного устройства рекомендуем 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. Сим-карту перевыпустить у оператора, а 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, банковские услуги такие как «Мобильный банк», «Онлайн Банк», «Интернет-банк», то необходимо срочно связаться с банком заблокировать карту и приостановить обслуживание по счетам. Если с помощью телефона это не удается сделать, то необходимо обратиться в ближайшее отделение банка. Если мобильное устройство используется для доступа к страницам.

**Будьте бдительны! О всех подозрительных лицах и звонках сообщайте по тел.: 02, 102 или в дежурные части Управления МВД России по городу Таганрогу:**

| Наименование подразделения | Почтовый индекс, адрес дежурной части территориального органа МВД России | Телефон дежурной части (с указанием телефонного кода) |
|---|---|---|
| ДЧ У МВД России по г. Таганрогу | 347900, Ростовская обл. г. Таганрог пр. Александровская, 45 | 8-8634-632-220<br>8-8634-632-500<br>102 (с мобильного) |
| ДЧ ОП № 1 У МВД России по г. Таганрогу | 347900, Ростовская обл. г. Таганрог пр. Чехова, 78 | 8-8634-632-366 |
| ДЧ ОП № 2 У МВД России по г. Таганрогу | 347900, Ростовская обл. г. Таганрог ул. Александровская, 166 | 8-8634-632-321 |
| ДЧ ОП № 3 У МВД России по г. Таганрогу | 347900, Ростовская обл. г. Таганрог ул. П. Осипенко, 64 | 8-8634-632-220 |