Терсенову М.А.
19.07.19

УМВД России по Тюменской области

УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ГОРОДУ ТЮМЕНИ
(УМВД России по г. Тюмени)
Полиция
ул. Ватутина, 34, г. Тюмень, 625013
«18» 07 2019 года № 91/2-14018
на № _____ от _____

Прокурору г. Тюмени
старшему советнику юстиции
Э.Р. Гиматову

ул. Даудельная, д. 1 г. Тюмень,625002
(для Терсенова М.А.)

О направлении ответа

Уважаемый Эдуард Рафикович!

Во исполнение пункта 3 комплексного плана мероприятий по профилактике совершения мошенничеств с использованием информационных технологий и средств мобильной связи на 2019 год направляю в Ваш адрес типовой урок по профилактике мошенничеств в информационном пространстве.

Телефонные мошенничества – один из самых распространённых видов преступной деятельности в настоящее время.

Начиная с 2015 года, наблюдается ежегодный рост количества совершенных преступлений указанной категории, вот почему так остро стоит вопрос об ответных мерах реагирования со стороны правоохранительных органов. Большинство схем дистанционных мошеннических действий основаны на использовании средств сотовой связи.

Основной целью любого мошенничества является хищение материальных ценностей. В случае телефонных и интернет мошенничеств – денежных средств.

В 2018-2019 годах участились случаи мошенничеств в сети Интернет, на различных сайтах (Авито, Юла, Дром, Вконтакте и т.д.). Граждане размещают объявление, о продаже какого либо товара, а мошенник под видом покупателя звонит на указанный абонентский номер в объявлении. В ходе телефонного разговора злоумышленник поясняет, что желает приобрести данный товар и хочет оплатить его сразу. В результате чего просит сообщить ему номер банковской карты, в дальнейшем говорит, что у него карта другого банка и платежи не проходят. В результате чего просит сообщить CVV код и СМС пароли, после чего также производит снятие денежных средств, с карты продавца. Для перевода денежных средств, независимо карта какого банка, не нужно сообщать СМС пароли и CVV код.

Имеются факты когда, мошенники на различных сайтах, в сети Интернет размещают объявления о продаже какого либо товара, но цена при этом указана

Дата 19.07.2019

значительно ниже рыночной. После того как покупатель звонит злоумышленнику, который в ходе телефонного разговора поясняет, что у него имеется интересующий товар и доставить он его может в любой субъект РФ. Мошенники просят перевести предоплату, после того как продавец перевел денежные средства, мошенники перестают выходить на связь. В данных случаях необходимо пояснять, что оплата за данный товар будет производиться при получении товара.

Так же имеются факты мошенничества, когда злоумышленники взламывают аккаунт в социальной сети «Вконтакте», после чего делают рассылку другим аккаунтам, находящимися в друзьях пользователя, с просьбой занять денежные средства. В данных случаях необходимо перезвонить своему знакомому и уточнить по данному факту, а не производить преждевременных переводов.

Банковская карта заблокирована!

Вы получили SMS сообщение о том, что ваша банковская карта заблокирована, где указан номер телефона, на который нужно перезвонить для уточнения подробностей.

Номер может быть указан городской или мобильный. Это один из самых популярных способов мошенничества. Не доверяйте сообщениям о блокировке вашей банковской карты. Не называйте никакой личной информации по телефону. Перезвоните в свой банк по известному вам номеру перепроверьте информацию.

В последнее время участились случаи получения абонентами сообщений с номера, маскирующегося под короткий сервисный номер Сбербанка 900 **(номер выглядит как 9ОО) с текстом «Вы совершили покупку на сайте OZON на сумму 9 950 руб**, если вы не совершали данную покупку срочно свяжитесь со службой безопасности по номеру 8-800-333-10-16». Потерпевшие связывались по телефону, указанному в сообщение, после чего под предлогом отмены покупки неизвестное лицо просило продиктовать СМС-сообщение от банка, код в смс и после чего списывались денежные средства со счетов потерпевших. Для отмены покупки не нужно сообщать СМС пароли и CVV код.

Вам положена компенсация. Злоумышленники звонят на стационарный телефон, как правило пожилым людям и поясняют, что последние приобретали какие-либо лекарственные препараты, которые по результатам исследования признаны вредоносными, в связи с чем последним положена компенсация, но для этого необходимо отправить страховой взнос в денежном эквиваленте. После отправки страхового взноса потерпевшим, как правило, злоумышленники обещают отправить выплату в ближайшее время, после чего связь с потерпевшим прерывается.

Ваш сын/дочь попал(а) в беду. Поступает телефонный звонок как правило в ночное время или рано утром. Человек представляется вашим сыном/дочерью и поясняет, что он находится в полиции и передает трубку «следователю», после «следователь» рассказывает обстоятельства произошедшего и предлагает

урегулировать вопрос за определенную сумму денег. Деньги просит или передать курьеру (как правило, ими являются водители такси), либо, удерживая потерпевшего на связи просит дойти до терминала и перевести денежные средства на абонентские номера сотовых операторов (как правило «МТС», «Билайн»).

Сотрудник банка. Поступает телефонный звонок с ip-телефонии с абонентских номеров номерная емкость которых начинается с 8800, 8495, 8499 и т.д. неизвестный человек представляется сотрудником службы безопасности банка, и под предлогом несанкционированного снятия денежных средств, узнает номер банковской карты, просит назвать CVV код, пароль из смс-сообщения. После чего крадет денежные средства с банковских счетов. В настоящее время, данный вид мошенничества очень распространен. Не называйте никому пароли из смс-сообщений, CVV коды.

Будьте бдительны при совершении действий с банковскими картами и соблюдайте элементарные правила безопасности, чтобы не стать жертвой мошеннических действий:

- НИКОГДА И НИКОМУ не сообщайте трёхзначный код на обратной стороне Вашей банковской карты, это ключ к Вашим деньгам. Если человек просит Вас сообщить код – ЭТО МОШЕННИК.
- Если Вам поступил звонок от «сотрудника банка», который сообщил Вам о блокировке Вашей банковской карты или подозрительных операциях с Вашими деньгами, прекратите разговор и позвоните на горячую линию Вашего банка, Вам только что позвонил МОШЕННИК.
- НИКОГДА не сообщайте смс-коды от банка другим людям. Смс-код от банка – ключ к Вашим деньгам, человек, который его спрашивает – ЭТО МОШЕННИК.
- Если по Вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты и смс-код, чтобы перевести деньги, прекратите разговор и ни в коем случае не сообщайте код – ЭТО МОШЕННИК.
- Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. НИКОГДА не выполняйте действия с банкоматом «под диктовку» другого человека - ЭТО МОШЕННИК.
- Если Вам поступило смс-сообщение с информацией о блокировке Вашей банковской карты и номером телефона, по которому нужно перезвонить, обратитесь на горячую линию Вашего банка, не перезванивайте, - ЭТО МОШЕННИК.
- Если Ваш друг или родственник пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные Вашей карты, чтобы перечислить их Вам, свяжитесь с ним любым другим способом и проверьте, скорее всего, Вам пишет МОШЕННИК.
- Если Вам позвонили от имени близкого человека или представителя власти, сообщили о несчастном случае и требуют деньги, прекратите разговор и позвоните близкому. Человек, который выманивает Ваши деньги – ЭТО МОШЕННИК.

- НИКОГДА не перечисляйте денежные средства в качестве предоплаты за товар (услугу) непроверенным лицам, чаще всего предоплату за несуществующий на самом деле товар просит внести МОШЕННИК.
- Всегда проверяйте Интернет-магазин, на котором планируете произвести покупку. Если цена за товар или услугу значительно ниже средней, этот сайт может быть создан МОШЕННИКОМ.
- Если Вам предлагают получить компенсацию за приобретенный товар, препарат (биологически активную добавку и др.) от представителя власти и при этом просят перевести деньги, прекратите разговор – ЭТО МОШЕННИК.
- Не доверяйте Вашу банковскую карту третьим лицам, не оставляйте её без присмотра, не записывайте ПИН-код в легкодоступных местах, в паспорте, на самой карточке – так ими легко может воспользоваться МОШЕННИК.

В случае потери или хищения Вашей банковской карты немедленно обратитесь в банк.

С уважением,

Врио начальника
подполковник полиции С.Н. Абышев