Информация

«О профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий»

В последнее время не только в Тюменской области, но и в России, в целом, широкое распространение получили так называемые «дистанционные мошенничества», совершаемые с использованием мобильной связи и сети Интернет, что касается нашего района, то за прошедший период 2021 года было зарегистрировано 16 таких преступлений, в 2020 года таких преступлений было 18. Общая сумма ущерба причиненного гражданам Аромашевского района в результате совершенных дистанционных мошенничеств составила 2 700 000 рублей.

В течение 2021 года сотрудниками ОП № 1 МО МВД России «Голышмановский» в рамках ОПМ «Профилактика» и всероссийской акции «Нет Мошенничеству» проводились профилактические беседы с гражданами Аромашевского района на предмет предупреждения о возможных мошеннических действиях. В ходе беседы гражданам раздавались буклеты, на которых отражена информация о способах совершения мошенничеств, а так же инструкции по действиям в случаях совершения данных преступлений. Сотрудники полиции постоянно напоминают о том, что ни в коем случае нельзя подходить к банкомату и вообще выполнять какие-либо манипуляции с использованием информации о своих картах и счетах под диктовку неизвестных лиц по телефону.

Не смотря на проводимую работу, преступлений данной категории не становится меньше, злоумышленники с каждым разом придумывают все новые и новые способы обмана и завладения денежными средствами граждан.

На сегодняшний день в районе распространены мошенничества, совершаемые с номеров 499 и 495, которые граждане воспринимают как «горячие линии» банков. Злоумышленники сообщают, что являются сотрудниками службы безопасности банков, и что с их счета произошло несанкционированное списание денежных средств, либо говорят, что карта заблокирована. Просят назвать реквизиты карты, код безопасности (с обратной стороны карты) и пароль доступа, пришедший по СМС. Таким образом, получают полный доступ к счёту и похищают деньги.

Так же в последнее время мошенники стали звонить со стационарных номеров, которые зарегистрированы на отделы полиции Тюменской области и других субъектов, представляются сотрудниками полиции и уверяют, что ранее с ними связывались сотрудники банка и что нужно выполнять все их указания. Помните, что этого делать нельзя, так как мошенники используют программы для подмены номеров, сами сотрудники полиции звонить вам по таким вопросам не станут. Так, например одной из жительниц с. Аромашево позвонили мошенники, представились сотрудниками банка стали убеждать, что с ее счетов происходят несанкционированные списания денежных средств, гражданка назовем ее «Регина», помня, что это могут быть мошенники стала говорить им, что она им не верит, тогда ей позвонили со стационарного номера отдела полиции № 4 г. Тюмени представились сотрудником полиции и убедили

Регину, в том что ей действительно звонят с банка, и что нужно выполнять их указания. После этого Регина поверила мошенникам и перевела все свои денежные средства на продиктованный ими счет.

Кроме этого, граждан обманывают при сделках купли-продажи, которые заключаются через интернет. Злоумышленники выставляют объявления, потерпевшие перечисляют оплату или аванс за товар, объявления тут же исчезают, а телефоны «липовых» продавцов оказываются недоступны. Либо обратная история: потерпевшие размещают объявления, а им звонят мошенники, якобы, для того, чтобы перевести аванс. Люди сами сообщают коды и пароли доступа к счету и в результате лишаются средств.

Имеют место взломы страниц в социальных сетях, когда приходят письма от имени знакомых с просьбой занять деньги. Достоверность такого письма нужно обязательно перепроверить у знакомого или близкого человека, который входит в круг друзей вашего аккаунта и от имени которого пришло сообщение.

Новым способом мошенничества является завладение данными на сайте «Госуслуг», в данному случае мошенники звонят и представляются сотрудниками МФЦ (Госуслуги) поясняя, что их аккаунт в приложении Госуслуги подвергся атаке, и нужно сбросить пароль, так же просят выполнить действия по сбросу пароля и сообщить пароль пришедший в СМС, после чего получают доступ ко всем Вашим данным, могут оформить как микрозайм, так и лизинг. Например, в России имеется случай, когда индивидуального предпринимателя, ввели в заблуждение, получили доступ к аккаунту на сайте «Госуслуг» и оформили на него автомобиль в лизинг.

Противоправные деяния совершаются с использованием большого количества сим-карт и телефонов. При этом мошенниками используются различные платежные системы. Они действуют с территории других регионов. Будучи хорошими психологами, мошенники в телефонной беседе под различными предлогами уговаривают людей перевести деньги с их банковских карт на счет некоего абонентского номера через те или иные платежные системы (экспресс-переводы, онлайн-сервисы) или же передать их лично в руки неустановленному лицу. К сожалению, основной причиной распространенности телефонного мошенничества по-прежнему остается доверчивость граждан. Чаще всего жертвами становятся женщины и люди пожилого возраста.

Еще одним распространённым видом мошенничества становится «инвестиции», в сети интернет появляются рекламы о быстром заработке с помощью брокерских компаний. Примером послужит житель нашего села, назовем его «Сергей» который в сети интернет увидел рекламу «Газпром инвестиции» перейдя по ссылке он попал к мошенникам, которые убедили его, что после нескольких месяцев инвестирования, в дальнейшем ему не придется работать. Открывали брокерский счет за который Сергей перевел 12 000 рублей, ему присылали логин и пароль от личного кабинета, где он видел баланс и действия производимые с акциями. Сергея убедили, что для получения прибыли необходимо внести большую сумму денежных средств, Сергей по указанию мошенников в приложении «Сбербанк Онлайн» оформил кредит на сумму 1 миллион рублей и перевел их на неустановленные счета, указанные мошенниками. В течение 2 месяцев Сергей перевел мошенникам чуть меньше 2х миллионов. Однако когда захотел осуществить вывод денежных средств, то

мошенники, которые представлялись брокерами, сказали, что вывод пока не возможен, требуется оплатить комиссию в сумме 700 000 рублей. После этого Сергей понял, что связался с мошенниками и обратился в полицию.

Хочу обратиться к жителям Аромашевского района, нужно быть бдительными и обязательно перепроверять поступившую информацию. Прекратить разговор со звонившим и самим позвонить на «горячую линию» банка. Обращаю особое внимание – никогда сотрудники банков инициативно не звонят клиентам. Код с обратной стороны карты (CVC) нельзя никому сообщать ни при каких условиях! В социальных сетях использовать более сложные, многоступенчатые пароли, чтобы страницу не взломали. При продаже-покупке через Интернет нужно внимательно изучать страницу продавца. Ни при каких обстоятельствах нельзя передавать посторонним лицам сведения о своих счетах и банковских картах, а также не совершать никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону. При возникновении любых вопросов либо сомнений необходимо проконсультироваться непосредственно в отделении банка, позвонить на горячую линию кредитной организации, уточнить сведения по телефону доверия полиции, обратиться в ближайшую дежурную часть или даже к сотруднику полиции, которого вы увидели на улице. Будьте бдительны. Не отдавайте свои деньги мошенникам!