Дистанционные мошенничества

По данным уголовного розыска Отделения МВД России по Улаганскому району за 9 месяцев 2020 года зарегистрировано 15 преступлений связанных с мошенничеством с использованием мобильной связи, незаконное списание денежных средств со счетов банковских карт, по ст.159 «Мошенничество».

Проблема раскрытия данного вида преступления, в основном из-за того, что преступники зачастую находятся в других регионах России. Доверчивые граждане сами предоставляют всю информацию о своих картах и счетах, передают пароли и подключают самостоятельно услуги мобильный банк к номерам мобильных телефонов, которые им говорят преступники.

В большинстве случаев жертвами мошенников становятся люди преклонного возраста, но и молодежь, потеряв бдительность, не редко попадается на удочку злоумышленников.

Причинами, по которым в капканы мошенников попадаются доверчивые граждане, во первых, является потеря бдительности - я никого не обманываю и меня никто не обманывает, а во-вторых, срабатывает человеческий фактор – раз есть заинтересованное лицо, нельзя его потерять, а поэтому, почему бы и не согласиться на его условия, которые на первый взгляд кажутся безопасными.

Весьма распространенный способ дистанционного мошенничества – использование социальных сетей и услуг интернет – магазинов.

Чаще «покупаются» на предложения обманщиков на сайте Аvito. Размещая объявление о продаже, например, транспортного средства, граждане должны быть готовы к тому, что не только потенциальных покупателей может заинтересовать данное объявление, но и преступников. Очень часто преступные элементы под предлогом покупки вашего товара, предлагают перевести на вашу банковскую карту предоплату. Они просят сообщить им номер вашей карты, на которую обязуются перечислить денежные средства. После того как вы сообщили номер карты, на ваш телефон начинают приходить СМС- сообщения с паролями, которые лжепокупатели просят также сообщить им, для того чтобы перевести деньги на вашу карту. Ни в коем случае этого делать нельзя!!! Для перевода денег на банковскую карту никакие пароли не нужны.

Также преступники представляясь сотрудниками банков сообщают ложные сведения о том, что клиент оставлял заявку на получение кредита, но данную заявку последний не оставлял и сообщает, что пользуется услугами банка «Сбербанк». Далее клиента переключают якобы на специалиста ПАО «Сбербанк» и тот сообщает, что его личный кабинет Сбербанк Онлайн пытаются взломать. Далее просят подойти к банкомату, диктуют по телефону комбинации цифр, которые граждане по своей неосведомленности вводят, и тем самым привязывают чужой номер телефона к своему личному кабинету в Онлайн, после чего мошенники получают все коды доступа к счетам и вкладам, и переводят ваши сбережения на свои счета.

Еще одна схема обмана- для личного обогащения злоумышленники довольно успешно используют вредоносные программы. Заразить вирусами персональные компьютеры или мобильные устройства своих потенциальных клиентов они пытаются разными ссылками в социальных сетях. Дельцы такого рода, выставляя на виртуальную витрину различные товары и услуги, делают заманчивое предложение и предлагают перейти по ссылке. Один клик мышкой, и у вас тот самый злополучный вирус. Если к вашему сотовому телефону привязан «Мобильный банк» с функцией «Быстрый платеж», вредоносная программа автоматически переправит ваши денежные средства с банковской карты на номер телефона злоумышленников. А владелец сотового телефона и банковской карты не знают, что их материальные средства «уплывают» в неизвестном направлении до тех пор, пока не воспользуются своим счетом. Тогда они бьют тревогу, обращаются в банк и узнают, что деньги ушли исключительно по их собственной наивности.

Отделение уголовного розыска

ОМВД России по Улаганскому району