Как не стать жертвой «мобильного» мошенничества.

Злоумышленники могут обратиться к Вам:

- Под видом сотрудников полиции, о нарушении их близкими родственниками законов, с целью передачи Вами денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившейся ситуации. В этой ситуации не продолжайте разговор, не позволяйте себя убедить. Вам звонит мошенник. Обратитесь в полицию!

- О блокировке банковской карты путем рассылки SMS-сообщений, а так же о переводе денежных средств за покупку товара по объявлению и последующего информирования о необходимости дальнейшего введения ряда команд с банкомата. Вам звонит мошенник! Никому нельзя сообщать реквизиты своей банковской карты, в том числе сотруднику банка, об этом всегда информируют банк при получении пароля к карте, в последствие необходимо лично обратиться в ближайшее отделение банка, с целью выяснения возникших проблем с банковской картой.

- О сообщении Вам, якобы, из поликлиники или больницы, что у Вас или у Ваших родственников обнаружили страшный диагноз и чтобы вылечить болезнь необходимо перевести деньги за лекарства. Прервите разговор, Вам звонит мошенник! Медицинское учреждение принимает денежные средства после заключения соответствующего договора в письменном виде, при Вашем личном присутствии. Свяжитесь с Вашим родственником, позвоните в больницу. Не переводите денежные средства мошенникам. Обратитесь в полицию!

- получения СМС-сообщений с неизвестных номеров о выигранном призе, с просьбой положить деньги на телефон, или вернуть деньги, так как они были переведены ошибочно. Это обман. Человек не может выиграть приз, не участвуя в лотереях. Не отвечайте на такие сообщения, не переводите денежные средства.

Как не стать жертвой мошенников в сети Интернет.

Злоумышленник, с целью хищения Ваших денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира) по заниженной цене и оставляет свои контактные данные.

После того, как Вы собираетесь приобрести товар, связываетесь с мошенником, он сообщает, что для покупки необходимо внести предоплату (на расчетный счет, Яндекс-деньги, счет Веб-мани и т.д.).

Наиболее часто встречающимися площадками для размещения подобных объявлений является сайты социальных сетей «В контакте», «Instagram», «Одноклассники», также такими сайтами могут выступать ресурсы бесплатных объявлений «Авито», «Юла» и «avto.ru». Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отправит товар сразу после того, как удостоверится в оплате товара. Злоумышленник может выслать копию паспорта (поддельную).

Также, распространенным способом мошенничества в сети Интернет, является создание сайтов Интернет-магазинов. Злоумышленник по электронной почте высылает договор, который заполняет заказчик, после чего просит внести предоплату за товар.

Как не стать жертвой мошенничества с банковскими картами при использовании услуги «Мобильный банк»:

В случае потери мобильного телефона с подключенной услугой «Мобильный банк» или мобильным приложением «Сбербанк Онлайн», следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» и/или «Сбербанк Онлайн».

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью отключения услуги «Мобильный банк» от старого номера и подключения на новый.

Не следует оставлять свой телефон без присмотра, чтобы исключить несанкционированное использование мобильных банковских услуг другими лицами.

Не подключайте к услуге «Мобильный банк» абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.

При пользовании банковскими картами:

С целью избежать несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения к Вам какого-либо лица лично, по телефону, в сети Интернет, через социальные сети или другим способом, которое под различными предлогами пытается узнать полные данные о вашей банковской карте: шестнадцатизначном номере, сроке ее действия, трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты и т.д. (паролях или другой персональной информации), будьте осторожны - это явные признаки противоправной деятельности. При любых сомнениях рекомендуется прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

Не следует прислушиваться к советам третьих лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обратитесь к сотрудникам филиала банка или позвонить по телефонам, указанным на устройстве или на обратной стороне карты.

Во избежание использования карты другим лицом, следует хранить ПИНкод отдельно от карты, не писать его на карте, и не сообщать его другим лицам (в том числе родственникам).

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по SMS/MMS/, электронной почте/мессенджерам (Вайбер, ВацАп и др.), в том числе от имени Банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.

ОеМВД России по Тарусскому району