ПРОКУРАТУРА ИНФОРМИРУЕТ
население Куйтунского района
о мерах безопасности при совершении банковских операций по картам/счетам, а также о предупреждении совершения преступлений с использованием злоумышленниками информационно-коммуникационных технологий

С каждым днем всё актуальнее становятся вопросы, связанные с хищением, совершенном с использованием современных информационно-коммуникационных технологий.

Наиболее распространенным способом совершения хищения денежных средств у физических и юридических лиц из банков и кредитных организаций происходит с использованием информационно-коммуникационных технологий в сети «Интернет», с помощью средств сотовой связи.

Мошенники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников с целью получения персональных данных пользователя, номера банковских карт, паспортных данных, логины и пароли.

Как правило, у граждан, юридических лиц похищаются денежные средства под предлогом совершения каких-либо банковских операций, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются работниками банками, звонят с неизвестных номеров.

Существуют следующие схемы способов совершения преступлений с использованием информационно-телекоммуникационных технологий:

1. злоумышленник звонит или отправляет СМС-сообщение на телефоны, сообщая, что банковская карта или счет мобильного телефона потерпевшего в результате осуществления на его карте/счете сомнительных операций неизвестными лицами, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника, или просит предоставить персональные данные.
2. потерпевшему поступает звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет злоумышленника;
3. потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ, либо переходит по ссылке на неизвестную интернет-страницу, осуществляет перечисление денежных средств за несуществующий товар злоумышленникам.

С целью пресечения совершения преступления, каждому гражданину необходимо критически относиться к таким сообщениям и не выполнять просьбы.

В случае возникновения подобной ситуации гражданам необходимо самостоятельно связаться с оператором банка, сотовой связи и узнать о совершении

блокировки карты, номера телефона, подключения услуг или совершения иных операций. Данные действия поспособствуют предотвращению хищения денежных средств, а также установлению злоумышленника.

Приобретая товары в Интернет-магазинов или по объявлениям необходимо обращать внимание на:

- *Требование предоплаты.* В большинстве случаев при переводе денег в счет предоплаты, покупатель лишается гарантий их возврата или получения товара. Если же всё же решили совершить покупку по предоплате, то необходимо убедиться в безопасности совершения такой покупки, в надежности продавца путем ознакомления в системе «Интернет» с отзывами о продавце, проверки рейтинга продавца в платежных системах;
- *Отсутствие контактной информации и сведений о продавце.* Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном то, такой магазин может представлять опасность. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем иные организации;
- *Излишняя настойчивость продавцов.* Если в процессе совершения покупки менеджер магазина начинает торопить совершить заказом и оплатить его, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи — это явный признак мошенничества, поскольку злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все условия сделки.

Так, отсутствие возможности курьерской доставки и самовывоза товара, низкая цена товара, отсутствие у магазина «истории», а также подтверждение личности продавца путем направления отсканированного изображения паспорта, также свидетельствуют о подозрительности продавца, магазина.

При совершении мошеннических действий потерпевшему следует незамедлительно обратиться в правоохранительные органы и написать заявление о свершившемся противоправном деянии, либо позвонить с мобильного телефона по номерам 102 и 112, с городского телефона по номерам 02 и 102