О противодействии преступлениям, совершаемым с использованием современных информационно-коммуникационных технологий

Хищение, совершенное с использованием современных информационно-коммуникационных технологий является общественно опасным деянием, причиняющим значительный имущественный вред гражданам. Наблюдается значительный рост преступлений, связанных с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций, совершаемых в виде дистанционного мошенничества.

Злоумышленники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Они преследуют цель - получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных о банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками или представителями правоохранительных органов.

В подавляющем большинстве случаев преступники используют следующие основные схемы обмана. Так, злоумышленник звонит или отправляет смс-сообщение на телефон, сообщая что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, 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.

Может поступить 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 мошенника.

Потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ. В таких случаях важно быть внимательным и не использовать непроверенные сайты, в том числе сайты-двойники.

При возникновении подобных ситуаций необходимо оперативно самостоятельно связаться с оператором банка, сотовой связи с целью блокировки карты, номера телефона, отключения услуг и т.д. Данные действия способствуют незамедлительному установлению злоумышленника и предотвращению совершения преступления.

Важно помнить! Ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код.

Исключите разговоры с неизвестными лицами по поводу состояния Ваших банковских счетов. При необходимости получить кредит или воспользоваться иными банковскими услугами обращайтесь непосредственно в офисы банковских организаций или пользуйтесь официальными сайтами и приложениями проверенных банков.