Хищение с использованием современных информационно-коммуникационных технологий

Хищение, совершенное с использованием современных информационно-коммуникационных технологий является общественно опасным деянием, причиняющий имущественный вред гражданам и разрушающий нравственные устои общества.

Наблюдается значительный рост преступления, связанные с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций. Совершаемых 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. Цель злоумышленников – 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 об их банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками.

Анализ способов совершения преступлений с использованием информационно-телекоммуникационных технологий показал, что в основном распространенно используются 3 схемы:

Схема –злоумышленник звонит или отправляет СМС-сообщение на телефоны, 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; Схема-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; Схема-потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ. С целью перечисления совершения преступления, необходимо критически относиться к таким сообщениям и не выполнять просьбы. При возникновении подобной ситуации необходимо самостоятельно связаться с оператором банка, сотовой связи и узнать о совершении блокировки карты, номера телефона, отключения услуг и т.д. Данные действительно поспособствуют незамедлительному установлению злоумышленника и перечислению совершения преступления.

Помните, что ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код!