Несмотря на проводимую правоохранительными органами разъяснительную работу с гражданами, значительного снижения количества преступлений в сфере информационно-телекоммуникационных технологий (так называемые «телефонные мошенничества») на территории Глушковского района не происходит.

Следует признать, что расследование таких преступлений представляет определённую сложность по причине значительных временных затрат для получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.).

В связи с развитием информационно-телекоммуникационных технологий совершенствуются и технические средства, используемые преступниками, меняются способы совершения таких преступлений и уничтожения следов преступления.

Наиболее распространённой схемой, используемой мошенниками, является «звонок из службы безопасности» какого-либо банка. По такой схеме хищение денежных средств в гражданина осуществляется под предлогом предотвращения их "списания" со счёта банковской карты либо активации бонусной программы возврата денежных средств.

С этой целью преступники в ходе, например, телефонного разговора с потерпевшим, путём обмана получают от последнего его персональные данные и с их помощью осуществляют переводы или совершают покупки со счёта банковской карты.

Имеет место и такая разновидность «телефонного мошенничества» как "звонок от лица сотрудника правоохранительного органа". Такие преступления могут совершаться при наличии у преступников сведений (базы данных) о клиентах кредитных организаций. В таком случае мошенники обращаются к гражданину по фамилии, имени, отчеству и сообщают о возбуждении уголовного дела в отношении данного лица либо его родственника, и для «решения вопроса» получают сведения, необходимые для использования в системах дистанционного банковского обслуживания и списания денежных средств с банковского счёта.

Следует отметить, что без получения персональных данных от самого гражданина невозможно осуществить хищение денежных средств с банковской карты. Практически во всех случаях хищение денежных средств происходит путём завладения злоумышленниками в результате обмана идентификационных данных банковской карты гражданина или получения доступа к личным кабинетам мобильных банковских приложений гражданина. В связи с этим гражданам необходимо пресекать разговоры с преступниками, ни в коем случае не сообщая им персональные данные и данные банковских карт, в том числе указанные в смс-сообщениях коды. Важно знать, что ниработники коммерческих банков и их служб безопасности, ни работники правоохранительных органов не могут звонить по телефону и не могут требовать выполнения действий с банковскими картами и движением денежных средств, в том числе с целью сохранности денежных средств. Если такой звонок поступил на Ваш телефон - это мошенники. Немедленно прекратите с ними разговор.

Заместитель прокурора района
О.А. Мищенко