Дистанционное мошенничество

Рост прогресса в сфере информационно-телекоммуникационных технологий (далее – ИТТ) дает злоумышленникам изобретать новые и новые способы хищения денежных средств у граждан, что в свою очередь влияют на статистические сведения, в сторону их увеличения.

С учетом, высокой латентности (скрытности) данного вида преступлений, связанной с использованием ИТТ, многообразием их приемов и методов, обусловленных межрегиональным характером, правоохранительные органы ведут не равную борьбу с таким видом мошенничеств.

Довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае преступное лицо, с помощью взлома персональной страницы в социальных сетях, обращается от лица потерпевшего с просьбой о помощи, а именно о переводе денежных средств на банковский счет, либо просят реквизиты карт, чтобы перевести деньги.

Мошенничество через «Интернет-магазин», преступники берут с будущей жертвы предоплату или полную сумму за определенный товар, но не исполняют своих обязательств. Благодаря фальшивых интернет-сайтов, мошенники собирают реквизиты банковских карт потерпевших и далее используют для операций по обналичиванию. Или же потерпевший сам переводит на номера банковских карт (номера сотовых телефонов) денежные средства.

Еще один вид интернет-мошенничества «фишинг», целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Мошенники при помощи рассылок через различные мессенджеры от лица банка дают потенциальной жертве ссылку на страницу, на которой предлагается вести определенные конфиденциальные данные.

При телефонном мошенничестве, как правило, от имени сотрудников банков России, мошенники сообщают потенциальной жертве о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимой блокировки банковской карты. Далее, мошенники, войдя в доверие, просят предоставить определенные данные карты владельца или сообщить смс-код, поступивший на его телефон. После чего, как правило, происходит списание денежных средств с банковского счета.

Наиболее активно действуют мошенники, путем совершения звонков на мобильные средства граждан, с применением психологических уловок по получению доступа к персональным данным и сведениям о реквизитах держателя банковских карт, когда на счета поступают значительные суммы денежных средств (заработная плата, премии, иные выплаты). В целях предотвращения мошеннических действий, лучше всего не брать трубку с неизвестных абонентов телефонов, либо через мобильное приложение установить программу по определению номера телефона.

Прокуратура Оконешниковского района