Мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием дистанционным способом совершается преступником как правило без физического контакта с потерпевшим. Злоумышленник может находиться в другом регионе, городе России и даже за рубежом.

Рост прогресса в сфере информационно-телекоммуникационных технологий (далее – ИТТ) дает злоумышленникам возможность изобретать новые и новые способы хищения денежных средств у граждан, что ведет к увеличению роста преступности.

Довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае преступник 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.

При мошенничестве через Интернет-магазины преступники берут с будущей жертвы предоплату или полную сумму за определенный товар, но не исполняют своих обязательств по отправке этого товара.

Благодаря фальшивым интернет-сайтам, мошенники собирают реквизиты банковских карт потерпевших и далее используют их для операций по обналичиванию денежных средств. 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 блокировке 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.

Если гражданин попал на уловку мошенников, то действовать ему нужно незамедлительно. С помощью звонка в банк или личного посещения ближайшего филиала банка, обратиться к оператору и сообщить о мошеннических действиях, через сотрудника банка заявить о приостановлении транзакции. Банк, в сЁвою очередь должен заблокировать это действие на определенный период времени (на время проверки). Взять в банке письменную распечатку о движении денежных средств по счету, с указанием даты, времени снятия денежных средств и номер счета, на который переведены деньги. Одновременно потерпевшему необходимо обратиться в полицию с заявление о преступлении и предоставить копию распечатки из банка о движении денежных средств по счету.

При совершении мошенничества с использованием ИТТ используется совершенно иной механизм следообразования. Установить лиц, причастных к совершению таких преступлений возможно только благодаря комплексу следственных действий и оперативно-розыскных мероприятий, с использованием технических средств и взаимодействием с службами безопасности банков.

В последнее время мошенники наиболее активно действуют путем совершения звонков на мобильные телефоны граждан, с помощью психологических уловок получая доступ к персональным данным и сведениям о реквизитах держателя банковских карт.

09.02.2021