**МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

         В связи с развитием информационно-телекоммуникационных технологий (далее – ИТТ) злоумышленники изобретают все новые и новые способы хищения денежных средств у граждан, о чем свидетельствует рост числа возбужденных уголовных дел в сфере мошенничества.

         Мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием дистанционным способом совершается, как правило без физического контакта с потерпевшим, лицами, находящимися в другом регионе и даже за рубежом.

         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.

         Совершая мошенничество через «Интернет-магазины», 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.

         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 свою очередь должен заблокировать это действие на определенный период времени (на время проверки).

         Также необходимо 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 заявлением о преступлении и предоставить копию распечатки с банка о движении денежных средств по счету.

         Ответственность за мошенничество с использованием электронных средств платежа предусмотрена ст.159.3 УК РФ. Преступное деяние наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

         При этом наказание за то же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, предусмотрено в том числе в виде лишением свободы на срок до пяти лет, а если деяние совершено в особо крупном размере - до десяти лет лишения свободы.

         Статьей 159.6 УК РФ предусмотрена ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

         Наказание по данной статье грозит от штрафа в размере до ста двадцати тысяч рублей до принудительных работами на срок до двух лет.

         То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, в том числе лишением свободы на срок до пяти лет.

         Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные, лицом с использованием своего служебного положения; в крупном размере; с банковского счета, а равно в отношении электронных денежных средств, наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей.

         Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.