**Осторожно, мошенники!**

Мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием дистанционным способом совершается, как правило без физического контакта с потерпевшим, находясь на значительном расстоянии, в другом городе, субъекте Российской Федерации и даже за её пределами.

Активное развитие информационно-телекоммуникационных технологий (далее – ИТТ) позволяет злоумышленникам изобретать новые способы хищения денежных средств у граждан, что в свою очередь влияет на статистические сведения, в сторону их увеличения.

С учетом, высокой латентности (скрытности) данного вида преступлений, связанных с использованием ИТТ, многообразием их приемов и методов, обусловленных межрегиональным характером,ежегодно отмечается рост преступлений указанной категории.

В настоящее время преобладают следующие способы дистанционных хищений:

- хищение посредством использования подложных объявлений на интернет-площадках;

- с использованием SIP-телефонии. Под SIP-телефонией понимается система звонков через сеть Интернет с использованием протокола IP на обычные телефонные сети передачи голосовой информации (подвижной или стационарной).

- мошенники представляются сотрудниками полиции или других правоохранительных органов, работникамиразличных банковских организаций;

- создание злоумышленниками ложных интернет-сайтов (близнецов), похожих на сайты известных банков, интернет-магазинов, которые пользуются у потребителей доверием, через которые происходит хищение реквизитов платёжных карт;

- распространение злоумышленниками в сети «Интернет» и социальных сетях предложений заработать на процентах и на так называемых «биржах», «инвестиционных компаниях», обещая получить быстрый заработок.

- поддельные биржевые площадки для инвестирования.

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 фальшивым интернет-сайтам, 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). 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 с банка о движении денежных средств по счету.

Ответственность за использование чужого доверия с целью завладения денежными средствами, привязанными к платежной карте, предусмотрена  
ст. 159.3 УК РФ.

Согласно ч. 1 ст. 159.3 УК РФ под мошенничеством с использованием платежных карт понимается хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Это деяние наказывается штрафом 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.

Согласно ч. 1 ст. 159.6 УК РФ под **мошенничеством в сфере компьютерной информации** понимается 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.

За данное преступление предусмотрена ответственность в виде штрафа 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 арестом на срок до четырех месяцев.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по  
ст. ст. 272, 273 или 274.1 УК РФ.