Дистанционные виды мошенничеств:

1. Несанкционированное списание денежных средств с банковских карт клиентов ПАО «Сбербанк России» посредством распространения вредоносного программного обеспечения, как правило, путем распространения смс-сообщений, с содержащимися в них ссылками на интернет-ресурсы и коротким текстом «Сохрани это фото», «Выгодный обмен» и т.д.

2. «СМС-Рассылка» - сообщается, что владелец абонентского номера стал обладателем приза, после этого под различными заманчивыми предложениями заставляют отказаться от приза, оплатить налог за приз и получить его в виде денежных средств. После перевода потерпевшими денежных средств, связь с преступниками прекращается. Также к данному виду относится сообщение о блокировании банковской карты, после звонка на телефон, с которого приходило смс-сообщение, мошенники убеждают провести операции у банкомата под их диктовку, в результате жертва не запоминает цифры которые нажимает и денежные средства переводит на неустановленный счет мошенника, либо просят продиктовать с лицевой и оборотной стороны реквизиты карты, а после совершают дистанционный (посредствам интернет сети) перевод денежных средств на различные счета и покупки.

3. «Продажа/покупка» - такой вид преступления получил свою популярность благодаря распространению сайтов бесплатных объявлений таких как «Авито», «ДРОМ», где злоумышленники за привлекательную цену продают различные товары (мебель, вагоны-бытовки, автомобили, стройматериалы и прочее), за которые, чтобы на них посмотреть или успеть купить по выгодной цене просят произвести предоплату, где после перевода денежных средств абонентский номер продавца отключается. Также может производится звонок человеку, продающему что-либо (различные товары), где сообщается, что находятся за пределами города, что желают приобрести товар и просят данные банковской карты, для перевода денежных средств. Часть владельцев карт, предают данные и сообщают кроме номера, срок действия карты и цифры с тыльной стороны карты, которые как раз таки и позволяют произвести в интернет сети операции, без использования карты. К данной категории также относятся объявления о приеме на работу, где люди в последующем в счет будущей зарплаты или под предлогом неудобства будущего начальника принимающего на работу куда-либо выехать просят произвести оплату на баланс сотового телефона.

4.«Интернет магазин» - в данном случае создается интернет страница, как правило, магазин бытовой техники и на выгодных условиях предлагается товар, который в последующем, после перевода денежных средств на заранее оговоренные счета, товар не поставляется, сайт перестает действовать.

Кроме вышеперечисленного, зафиксированы случаи, где взломанные в социальных сетях страницы пользователей, производивших ранее оплату по карте, замечали списание денежных средств, случается это по ошибке самих

же пользователей которые после производства оплаты оставляют номера карт и привязывают их к своим страницам. Еще один вид мошенничества в соц.сетях, когда злоумышленники взламывают страницу пользователя и осуществляют массовую рассылку пользователям, находящихся у него в «друзьях» сообщений с просьбой занять денежные средства (как правило суммы не большие от 2000 до 5000 рублей).

5) В последнее время начали набирать популярность мошенничества в сфере кредитования и социальной защиты, а именно:

- В сфере кредитования: Злоумышленник размещает рекламу на различных интернет сайтах с текстом об оформлении кредита. Далее лицо, нуждающееся в деньгах, оставляет заявку на сайте, после чего ему перезванивают (как правило с Московских номеров +7495….) и сообщают о том, что кредит одобрен и для его получения необходимо в счет страховки перевести денежные средства (30% от суммы) на указанный счет. После того как потерпевший перевел необходимую сумму, ему говорят, что пакет документов будет передан курьеру компании «DHL». Через некоторое время перезванивает, якобы, курьер и убеждает перевести денежные средства за доставку в сумме 7-8 тыс. рублей, если же потерпевший отказывается, то ему предлагают вариант по возврату денежных средств поп страхованию. Злоумышленник сообщает, что для того что бы получить обратно денежные средства, необходимо, что бы на балансе счета потерпевшего находилась сумма 7-8 тыс. рублей, а так же в момент возврата денег, необходимо находиться у банкомата для введения кода активации перевода. На самом же деле потерпевший не замечает как привязывает свою карту к абонентскому номеру злоумышленника, после чего происходит списание денег с карты потерпевшего.

- В сфере соц. защиты: Злоумышленник звонит на городской телефон. Далее начинает перечислять множество продукций, изготовителей которых осудили за мошеннические действия, и теперь их пользователям полагается компенсация, но для ее получения необходимо перевести денежные средства в счет страховки, либо за судебные издержки. После того как потерпевший переводит указанную сумму, ему сообщают, что сумма компенсации увеличилась и для ее получения необходимо доплатить. После вновь совершенного перевода, потерпевшему снова сообщают, что сумма компенсации увеличилась и так продолжается пока жертва не поймет, что ее обманули.