Межрайонной прокуратурой проанализирована практика совершения преступлений с использованием средств связи и мобильных приложений.

В последнее время отмечен такой способ хищения, как «отмена подозрительных операций».

Так, потерпевшему звонят неустановленные лица, представляются сотрудниками банка и сообщают, что службой безопасности зафиксированы подозрительные заявки на получение кредита в другом городе от его имени. Преступники уточняют, делал ли потерпевший такие запросы. После ответа «нет», поступает предложение:

- предоставить доступ к компьютеру или телефону с личным кабинетом;
- установить программу для удалённого управления устройством потерпевшего;
- перевести уже имеющиеся денежные средства в «защищённую ячейку» по реквизитам, которые сообщит злоумышленник. После выполнения действий денежные средства с карты потерпевшего похищаются.

Также на территории страны распространены следующие виды и способы совершения преступлений бесконтактным способом:

- злоумышленники представляются оператором сервиса электронных платежей «Яндекс.Деньги», после чего требуют перевести средства на биткойн-кошелек под угрозой публикации компрометирующих видео. В письме злоумышленник называет себя программистом, которому удалось взломать компьютер потерпевшего, получить полный доступ к его данным, в том числе к камере. Сообщает о том, что сделал интимные видео и фото, требует перевода денежных средств, под угрозой осуществления рассылки материалов списку контактов «жертвы»;
- заказ якобы от «Яндекс.Такси». Приходит заказ, а затем сообщение в чат о том, что это тестовый заказ «Яндекс.Такси», который надо выполнить для улучшения клиентского приложения. В действительности сообщение поступает с сайта-двойника и денежные средства переводятся мошенникам;
- мошенничество с использованием приложения BlaBlaCar. Злоумышленник под предлогом предоплаты за поездку отправляет фишинговую ссылку, после перехода на которую происходит списание денежных средств (фишинг - тактика рассылки электронных писем и попытка обманом заставить получателей перейти по вредоносной ссылке или скачать «зараженное» приложение);
- случай с родственниками и близкими. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (совершил ДТП, хранение оружия или наркотиков и т.д.). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас так делать нельзя, так как он боится потерять погоны. Деньги необходимо привезти в определенное место или передать какому-либо человеку (например, водителю такси). Если абонент согласился привезти деньги, то ему называют адрес, куда приехать, либо просят адрес места жительства, куда отправить курьера (водителя);

- розыгрыш призов. На мобильный телефон абонента звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Перезвонившему отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения; грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.), просит реквизиты карты, на которую отправить выигрыш. Предложение самостоятельно забрать выигрыш не принимается, таковы правила рекламной акции. В дальнейшем с использованием полученных сведений происходит списание денежных средств с карты;

- СМС-просьба. Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер недоступен, положи на него определенную сумму и перезвони»;

- платный код. Поступает звонок якобы от сотрудника службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников;

- штрафные санкции оператора. Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды;

- ошибочный перевод средств. Абоненту поступает СМС-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина или женщина сообщают, что ошибочно перевели деньги на его счет и просит вернуть их обратно тем же «Мобильным переводом». В действительности СМС-сообщение приходит с номера-двойника, а не из банковской организации. Денежные средства перечисляются преступникам;

- предложение получить доступ к СМС переписке и звонкам абонента. Пользователю предлагается изучить содержание СМС-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер.

Учитывая появление новых способов хищений, совершаемых бесконтактным способом, гражданам предлагается использовать указанную информацию в целях самозащиты от мошенников.

Старший помощник
межрайонного прокурора