«Новые способы дистанционного мошенничества».

Общество, трансформируясь в цифровое, становится более зависимым от информационных ресурсов (интеграция процессов в онлайн режим, развитие электронной коммуникации и т.д.), используемых злоумышленниками.

Используя доверчивость граждан, преступники вынуждают их оформлять кредиты, осуществлять переводы денежных средств. Для достижения своих целей мошенники, используя специальные программные средства, подменяют абонентские номера, которые определяются мобильным устройством как входящий вызов.

В ходе телефонного разговора злоумышленники представляются сотрудниками операторов сотовой связи и сообщают о том, что абонентский номер в ближайшее время будет заблокирован, затем просят набрать комбинацию цифр или символов, изменяя таким образом настройки сим-карты. Как следствие устанавливается переадресация всех звонков и смс-сообщений. Это позволяет получить доступ к государственным услугам, личным кабинетам, в том числе банков. Воспользовавшись данными возможностями, осуществляют списание денежных средств со счетов граждан, а также оформляют кредиты.

Еще одним способом получения доступа к государственным услугам является звонок из пенсионного фонда. Злоумышленники звонят и говорят о том, что якобы неправильно посчитан стаж или сумма пенсионных накоплений, естественно она занижена. С целью исправления ошибки рекомендуют подойти в ближайшее отделение пенсионного фонда, заполнить заявление. Выясняют какое отделение находится рядом, предлагают записаться на прием. В дальнейшем называют время и дату, вымышленную фамилию сотрудника, который будет осуществлять прием. Затем с целью якобы подтверждения факта записи просят продиктовать код, который поступает на госуслуги. Назвав его, мошенники таким образом получают доступ к личным кабинетам портала государственных услуг. А далее осуществляют списание денежных средств со счетов граждан, а также оформляют кредиты.

Чтобы не стать жертвой необходимо соблюдать следующие правила:

1. Не сообщать никому по телефону данные банковский карт, а также сведения из смс-сообщений,
2. Не загружать в мобильный телефон приложения и программы из непроверенных источников,
3. Не осуществлять переводы денежных средств, не удостоверившись в подлинности намерений звонившего и его личности.

Управление по надзору за следствием,
дознанием и оперативно-розыскной деятельностью