О новых способах дистанционного мошенничества

Под влиянием злоумышленников доверчивые граждане оформляют кредиты и переводят денежные средства мошенникам.

Для введения в заблуждение мошенники с использованием специальных программных средств подменяют абонентский номер, который определяется мобильным устройством как входящий.

Мошенники представляются службой поддержки государственных услуг, сообщают о взломе их личного кабинета, затем просят набрать определенную комбинацию цифр и символов, таким образом меняя настройки сим-карты, устанавливая переадресацию смс-сообщений и звонков на номер злоумышленника.

Получая информацию из сообщений, преступники открывают доступ к государственным услугам, личным кабинетам в банки и совершают операции по списанию денежных средств.

Чтобы не стать жертвой преступников необходимо запомнить и соблюдать следующие правила:

– не сообщать никому, в том числе лицам, представившимися сотрудниками банковских организаций, данные банковских карт, а также сведения из смс-сообщений для входа в онлайн-банк или совершения финансовой операции;

– не осуществлять поспешные переводы денежных средств, лицам, представившимся родственниками, без проверки данной информации;

– не загружать на мобильные устройства приложения и программы из непроверенных источников;

- проявлять бдительность при осуществлении онлайн-покупок, не переходить для покупок по ссылкам.

Если доверившись злоумышленнику Вы сообщили данные своих банковских карт и другую значимую информацию, необходимо незамедлительно позвонить на горячую линию банка по номеру телефона, указанному на обороте банковской карты, установить блокировку на совершение банковских операций и обратиться в правоохранительные органы.