

В последнее время в г. Симферополе увеличился рост уголовных дел о хищениях, совершаемых дистанционным способом. Особенно усматривается высокий рост дистанционных мошенничеств, где в качестве средств их совершения используются мобильная связь и различные методы социальной инженерии.

Зачастую мошенники звонят в мессенджерах Viber, WhatsApp, Telegram и пр. либо через социальные сети «ВКонтакте», «Одноклассники», где размещают рекламу с логотипом банков.

Как правило мошенники звонят под видом сотрудников банка и сообщают о том, что с карты пытаются снять деньги, о попытке оформлении кредитов, о выигрыше и прочее. В ходе разговора мошенники пытаются узнать номер карты, трехзначный CVV-код, коды из СМС или просят установить стороннее приложение на мобильное устройство или перейти по ссылке для удаленной помощи и сохранности средств, сообщают легенду о неправомерном списании, либо о попытках списания, денежных средств с банковского счета и предлагают перевести денежные средства на «безопасный» счет.

Также осуществляются звонки от предполагаемых сотрудников полиции, следственного комитета, представляясь которыми говорят о получении доступа к банковским данным и помощи в уголовном деле.

При поступлении звонков с неизвестных номеров от лиц, представляющихся сотрудниками банков или государственных структур и при отсутствии подтверждающих данных, не следует вступать с ними в общение и переговоры. Злоумышленники используют специальные методы воздействия.