Прокуратурой Фрунзенского района выявлен факт регистрации ряда сообщений о преступлениях, о совершении возможных мошеннических действий в отношении граждан с использованием кредитных карт.

Обстоятельства проводимых проверок свидетельствуют о совершении однотипных действий, что требует акцентирования внимания граждан в целях недопущения аналогичных деяний. В настоящее время по материалам проводится доследственная проверка. Вместе с тем, изложенные ниже обстоятельства, затрудняют принятие решения при отсутствии данных, подтверждающих факт обмана.

Так, например, с целью получения путем обмана доступа к банковским картам граждан в мессенджере Viber пользователям рассылают сообщение, что по их банковской карте прошла операция, которую они не совершали.

В сообщении говорится, что по карте прошла покупка на определенную сумму в интернет-магазине. В целях пресечения несанкционированного снятия денежных средств, необходимо позвонить по номеру, указанному в сообщении.

После того, как гражданин перезванивает по указанному номеру телефона, возможные злоумышленники пытаются обманным путем заполучить данные с карты — обычно требуют назвать фамилию имя и отчество, а также назвать номер (в том числе частично- последние четыре цифры) карты, код CVV2, указанный на обратной стороне карты для идентификации клиента. После этого происходит списание денежных средств с банковского счета гражданина.

В отдельных случаях злоумышленники просят найти ближайший банкомат и далее следовать инструкциям. Как правило, инструкции сводятся к необходимости ввести набор цифр. При получении СМС сообщения просят предоставить сведения по указанному в сообщении коду. При этом, гражданин как правило не задумывается, что он фактически совершает перевод денежных средств на иной банковский счет самостоятельно или предоставляет злоумышленникам всю необходимую для этого информацию.

Также злоумышленники могут использовать размещенные гражданами в сети Интернет объявления о реализации какого-либо товара. Перезвонив, предлагают оплатить товар с использованием банковской карты, после чего предлагают найти банкомат и, далее происходит аналогичный «инструктаж».

Следует отметить, что не стоит никому называть любые данные своей банковской карты, тем более по телефону, а также незамедлительно выполнять любые требования неизвестных с использованием данных банковской карты. Также отмечено, что банковские учреждения не используют мессенжеры, не требую предоставить пароли.

В любом случае необходимо, при наличии сомнений, обращаться по телефону, указанному на обратной стороне банковской карты.

О совершении подобных действий необходимо обращаться в органы полиции в связи с наличием признаков состава преступления, предусмотренного ст.159 УК РФ.