**Как не стать жертвой обмана**

По-прежнему большинство регистрируемых преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, составляют хищения с банковских счетов, осуществляемые с получением от жертвы в телефонном разговоре либо в процессе иного общения конфиденциальных данных (персональных, номеров и других параметров платежных карт, счетов и т.д.).

Технологически банки предусматривают защиту, предполагающую участие клиента в процессе подтверждения операции (например, подтверждение операции кодом, направляемым клиенту посредством смс-сообщений), поэтому мошенники стараются узнать коды или пароли.

Одним из часто встречающихся предлогов, используемых злоумышленниками, является внесение предоплаты или полной оплаты за товар, информация о котором размещается пользователями на популярных сайтах частных объявлений. Совершая звонок на абонентский номер, указанный в объявлении, неизвестный выражает намерение немедленно оплатить товар, для чего просит сообщить ему информацию, указанную на банковской карте, а также код подтверждения операции, якобы необходимый для перевода денежных средств. На самом деле, с использованием данной информации производится списание денежных средств со счета самого продавца товара.

**Как не стать жертвой обмана:**

1. Для совершения перевода денег с карты на карту не требуется никаких данных, кроме номера карты получателя. Не следует сообщать другим лицам остальные реквизиты банковской карты, в особенности трехзначный код, нанесенный на оборотной стороне карты.

2. Код подтверждения операции, поступающий клиенту посредством смс- сообщения, необходим для подтверждения операций, совершаемых самим держателем карты. Сообщать его кому-либо, даже сотруднику банка, не следует ни в каком случае. Информация об этом содержится в каждом смс-сообщений, содержащем код подтверждения.

Начальник Отдела МВД России по Купинскому району А.В.Горин