ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Прокуратура Астраханской области

Махинации с банковскими картами– это преступление, за которое подлежит нести уголовную ответственность согласно статье 159.3 УК Российской Федерации «Мошенничество с использованием электронных средств платежа».

Мошенники на «Авито».

При использовании сайта/приложения «Авито» риск столкнуться с мошенниками также не исключен. И рискуют главным образом именно средства на банковской карте.

Пользователей услугой должно насторожить следующее:

- Продавец просит предоплату товара без его предварительного осмотра. В последнее время такое случается редко, поскольку администраторы сайта контролируют подобные сделки.

- Покупка товара с запросом о пин-коде. На такую уловку могут попасться как покупатели, так и продавцы. Мошенники под видом тех или иных просят продиктовать им не только номер карты, но и пин-код, чтобы провести процесс оплаты якобы через свои ресурсы. Все это должно насторожить другую сторону и отказаться от предоставления лишних данных.

Посредством Мобильного банка

Мобильные приложения, касающиеся банковских услуг, очень удобны в использовании и упрощают финансовые действия: оплату, перевод средств другим людям, пополнение счета и т.п. Но они могут нести угрозу денежным средствам.

Мошенничество через Мобильный банк осуществляется путем заражения приложения вирусом-трояном. Вирус подменяет оригинальное окно ввода логина и пароля на фальшивое, а после введенные данные держателя карты переходят в распоряжение мошенников.

Этот вирус позволяет мошенникам получать доступ не только в Мобильный банк потерпевшего, но и к его смс с одноразовыми паролями. Кроме того, троян может преграждать путь смс из банка о совершенных транзакциях на номер владельца карты, в результате чего последний долгое время не подозревает о финансовых махинациях.

Звонок от лже-оператора или метод вишинга.

Такой вид махинации с банковскими картами широко распространен от «лица» Сбербанка.

Сперва на номер телефона держателя карты приходит смс с номеров похожих на 900 или 9000 о том, что для подтверждения перевода денег необходимо ввести код, иначе операция совершится самостоятельно (при этом, разумеется, владелец не проводил никаких действий с деньгами). Через некоторое время после смс абоненту звонит псевдо-оператор Сбербанка и говорит, что для отмены перевода денег им необходимо предоставить данные карты. Многие люди в панике и по незнанию предоставляют мошенникам всю запрашиваемую информацию и через считанные минуты остаются без средств на карте.

Такой способ именуется вишингом. Он рассчитан на неопытных доверчивых людей, которые способны без подозрений передать «банковским работникам» пин-код, в то время как эти данные являются строго конфиденциальной информацией. Потеряв и забыв пин-код владелец карты не может его восстановить ему остается только перевыпустить карту или проводить операции по ее счету в отделении, предоставив паспорт сотрудникам банка. Поэтому официальный работник Сбербанка у вас никогда не будет запрашивать по телефону пин-код.