О противодействии мошенничеству с использованием реквизитов банковских карт

С развитием технологий глобальных информационных сетей, электронной торговли и дистанционного обслуживания появилось большое количество различных преступлений, в том числе связанных с незаконным использованием реквизитов платёжных карт для оплаты товаров или услуг.

Речь идёт об операциях, когда карта физически не участвует в их проведении: покупки в магазинах сети Интернет, бронирование гостиничных номеров, аренда автомобилей или приобретение авиабилетов. Зачастую для подобных операций достаточно знать только основные карточные реквизиты: её номер и срок действия.

Мошенники получают персональные данные держателей и реквизиты их карт посредством так называемых «фишинга» и «фарминга»:

Фишинг (**«выуживание»)** — получение от клиентов банков обманным путем реквизитов их банковских карт. Для их выведывания злоумышленники связываются с держателями карт по телефону и применяют разнообразные уловки.

Часто это происходит путём имитации деятельности реально существующего банка от лица его подразделений. Под различными, внешне благовидными, но вымышленными предлогами, мошенники предлагают сообщить им реквизиты действительных платежных карт и ПИН-коды.

В случае направления мошеннических СМС-сообщений держателей информируют о якобы блокировке карт, окончании сроков их действия, изменении ПИН-кодов и просят перезвонить, как правило, на номер мобильного телефона, с которого было отправлено сообщение. Дальнейшие действия мошенников направлены на побуждение держателей передать им сведения о реквизитах карт или совершить выгодные действия вплоть до самостоятельного перевода средств на мошеннические счета.

Фарминг («автоматизированный» фишинг) заключается в том, что пользователь Интернета обманным путём направляется на мошеннический сайт, который является фальсификацией сайта реальной кредитно-финансовой организации или мошеннического торгово-сервисного предприятия (ТСП). Не подозревая об обмане, пользователь Интернета вводит на сайте запрашиваемые данные: пароли, реквизиты карт, ПИН-коды, тем самым передавая их в руки мошенников. В случаях с ТСП держатели карт могут стать жертвами мошеннических транзакций за не приобретаемые в действительности товары и услуги.

В 2012 году участились случаи СМС-мошенничества, совершаемого с использованием наименования Центрального банка Российской Федерации. На мобильные телефоны клиентов банков, действующих на территории Владимирской области, Краснодарского края, Свердловской и Самарской областей, г. Москвы и других городов поступали многочисленные СМС-сообщения от имени «Центробанк России», «CentroBank», «Служба безопасности Банка России» и т.п. с информацией о блокировке карты клиента и указанием номера телефона для связи.

Официальное разъяснение Центробанка РФ в связи с этим следующее: «Подразделения системы Банка России не вправе рассылать подобные сообщения, так как Банк России не вмешивается в оперативную деятельность кредитных организаций и договорные отношения с их клиентами, за исключением случаев, предусмотренных

федеральными законами». Указанные сообщения являются элементом мошенничества.

В связи с вышеизложенным обращаем ваше внимание на следующее:

1. Банк никогда не запрашивает по телефону у клиентов информацию об их персональных данных, номерах платежных карт, а также не осуществляет рассылку электронных писем и СМС-сообщений с просьбой проверить эту информацию.

2. Убедительно просим всех сотрудников и клиентов:

- не отвечать на подозрительные звонки и тем более не обсуждать по телефону какие-либо относящиеся к банковским картам сведения;
- не звонить по указанным в СМС-сообщениях телефонам, не раскрывать свои персональные данные и реквизиты банковской карты;
- принять решение о возможном обращении в правоохранительные органы и службы безопасности мобильных операторов с просьбой оградить вас от преступных посягательств;
- соблюдать меры предосторожности при покупках на незнакомых сайтах в сети Интернет напрямую или при переходах по ссылке с другого сайта;

- поделиться содержанием данной Памятки с вашими родственниками и знакомыми.

Ещё раз напоминаем держателям карт одно из основных правил безопасности: никто не имеет права интересоваться вашим ПИН-кодом, он должен быть известен только держателю карты, ни в коем случае не следует сообщать его третьим лицам, даже представителям Банка и родственникам!

Дирекция безопасности

Департамент карточных и
дистанционных технологий