ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ ПРИ ПОЛЬЗОВАНИИ БАНКОВСКИМИ КАРТАМИ

Банковские карты – удобное современное средство платежа, с помощью которого граждане каждый год оплачивают товары и услуги на триллионы рублей. Но технологиями в финансовой сфере научились пользоваться и мошенники. По предварительным данным, только за 2016 год с банковских карточек ими было украдено более 1,6 млрд рублей. Чаще всего жертвами мошенников становятся люди с низким уровнем образования, а также граждане преклонного возраста.

Простейшие правила кибербезопасности следует помнить и соблюдать всем без исключения, ведь преступники делают ставку именно на нашу невнимательность, доверчивость и легкомыслие.

Вот несколько самых элементарных норм безопасности, которыми всегда надо руководствоваться при пользовании банковской картой:

- никогда не сообщайте незнакомцам данные своей карты (ее номер, пин-код, кодовое слово и т.д.), даже если они представляются работниками банка или госструктур;

- как только речь заходит о деньгах, например, вам предлагают какие-то призы, выплаты, компенсации, сообщают о блокировке карты или списании денег с нее и предлагают помочь решить эту проблему, проявите бдительность и не забывайте, что бесплатный сыр бывает только в мышеловке;

- помните также, что Центральный банк Российской Федерации (Банк России) не работает с гражданами: не принимает вклады и не дает кредиты, не открывает и не закрывает банковские счета, не блокирует карты, не выплачивает никакие компенсации, выигрыши. Кроме того, Банк России не рассылает SMS-сообщения. Поэтому, если вы получили сообщение якобы от имени Банка России, – просто проигнорируйте его и ни в коем случае не перезванивайте по указанному в нем телефонному номеру.

Какие схемы используют кибермошенники?

Телефонные звонки

Граждане могут получать звонки от мошенников, которые представляются сотрудниками Банка России, Прокуратуры, суда, Министерства здравоохранения, Министерства финансов и других учреждений и сообщают о положенном возмещении ущерба от действий мошенников в прошлом, например, о компенсации за купленные медицинские товары, услуги психологов и экстрасенсов, участие в финансовых пирамидах и т.д. Для получения обещанной компенсации мошенники, как правило,

предлагают что-то оплатить: подоходный налог, налог на прибыль, банковский сбор, обязательную страховку, госпошлину, комиссию за перевод денег и т.п. Кроме того, преступники требуют предоставления паспортных данных и банковских реквизитов. Очевидно, что после перевода денег никаких компенсаций не следует.

Письменные уведомления

Похожая схема мошенничества - поддельные уведомления о выплатах и компенсациях. Гражданин получает по почте на бланке с некими реквизитами уведомление о том, что судом принято решение о выплате компенсации за приобретение в мошеннических организациях лекарств, биодобавок, медицинских приборов или за оплату услуг экстрасенсов и психологов. В фальшивом уведомлении указывается контактное лицо и номер телефона. Для большей убедительности мошенники предупреждают свою жертву о том, что в случае игнорирования письма компенсация перейдет в пользу государства. Человек, поверивший такому письму, попадает к сети к аферистам, которые далее действуют по схеме, аналогичной первой.

СМС-сообщения

Мошенничества с использованием СМС-сообщений - также одна из наиболее распространенных схем, в которых аферисты прикрываются именем Банка России. Вы можете получить СМС-сообщение с текстом примерно следующего содержания: «Ваша банковская карта заблокирована. Информация по телефону: 00000000000. ЦБ РФ». В качестве отправителя может быть указан короткий номер 900, а также номера с кодом 8800. Вместо «ЦБ РФ» может быть указано «Служба безопасности ЦБ» или «Centrobank».

Владелец карты, позвонивший по указанному в сообщении номеру, попадает в фальшивую службу безопасности якобы Банка России или крупного коммерческого банка. Его убеждают, что в системе произошел сбой и предлагают либо подойти к ближайшему банкомату и провести операции, которые ему укажут, либо сообщить данные своей карты для того, чтобы ее можно было разблокировать (возможны и другие варианты). Если человек выполнит указания мошенников, с его карты будут списаны деньги.

Что делать, если вы столкнулись с мошенничеством?

Если с банковской карты без вашего согласия списаны деньги, следует незамедлительно позвонить в банк, выпустивший карту, сообщить о мошеннической операции и заблокировать карту. Номер телефона указан на обороте карты, на официальном сайте банка и в договоре о выпуске и обслуживании карты. Затем нужно обратиться в отделение банка, запросить выписку по счету и написать заявление о

несогласии с операцией, экземпляр заявления с отметкой банка о приеме оставить у себя. Также нужно обратиться в правоохранительные органы с заявлением о хищении.

В соответствии с законом, заявление рассматривается банком не более 30 дней со дня его получения, при осуществлении международных операций – не более 60 дней. Банк информирует держателя карты о результатах рассмотрения заявления способом, определенным договором о выпуске и обслуживании карты. По требованию держателя карты банк обязан предоставить письменный ответ.

Можно ли рассчитывать на компенсацию?

После получения заявления клиента банк проводит служебное расследование, по результатам которого принимает решение о возмещении ущерба. На него можно рассчитывать, если держатель карты не нарушал условия ее использования, в том числе соблюдал меры по безопасности, и обратился в банк не позднее дня, следующего за днем получения от банка уведомления о совершении операции. Но следует иметь в виду, если кража денег с карты стала следствием неосмотрительности держателя карты (например, держатель карты сообщил преступникам свои персональные данные), банк может не возвращать деньги.