Рекомендации
по профилактике краж денег с банковских карт граждан

Федеральным законом от 29.11.2012 № 207-ФЗ в Уголовный кодекс РФ внесен ряд изменений в области уголовной ответственности за специфические виды мошенничества, в том числе за мошенничество с использованием платежных карт.

По итогам 2019 годанаблюдается негативный рост мошеннических действий, совершаемых с помощью средств мобильной связи и сети «Интернет». Так, увеличилось совершение преступлений с использованием электронных средств платежа на 473,9% (с 46 до 264 фактов). Зафиксирован рост мошенничествав сфере кредитования, при получении выплат, в сфере компьютерной информациина 31,5% (с 2747 до 3611 фактов).

Кроме того, увеличилось совершение хищений с банковских счетов, в отношении электронных денежных средств на 195,7% (с 655 до 1937 фактов).

Наиболее распространенными и популярными видами мошенничества с использованием банковских карт являются:

1. Средством мошенничества является телефон. Например, клиент получает звонок от «сотрудника» службы безопасности банка, который сообщает о попытке незаконного списания денежных средств со счета. Подставной сотрудник просит перезвонить по указанному им сотовому телефону, что и делает жертва. Поскольку указанный номер является фиктивным, ни в коем случае нельзя сообщать данные своей карты или отправлятьСМС-сообщения с информацией о карте.

2. Похищение реквизитов пластиковой карты с помощью специальных устройств. Устройство считывает данные картыи позволяет мошенникам получить код доступа к банковской карте. В результате мошенник получает все необходимые данные для создания «карты-клона», что позволяет похитить денежные средства с банковского счета потерпевшего.

3. Создание поддельного сайта банка, имитирующего работу настоящего. Мошенники осуществляют рассылку электронных писем клиентам кредитной организаций, заманивая их на поддельный сайт, где просят указать данные о карте, а именно: номер карты, ПИН-код. Например, преступник от имени банка рассылает сообщения о том, что в системе банка, обслуживающего данное лицо, будут производиться изменения, в виду этого просит сообщить данные карты (номер, ПИН-код) или пройти по ссылке «указанной ниже» и заполнить анкету. В результате лицо, переходя по ссылке, попадает на поддельный сайт банка и указывает данные карты.

В существующей ситуации одним из направлений борьбы с преступлениями в сфере использования платежных карт является их предупреждение.

Предупреждение совершения данных категорий преступлений состоит, прежде всего, в повышении безопасности платежных карт и повышении контроля за их использованием.

Для профилактики мошеннических действий с банковскими картами граждан необходимо довести до граждан следующую информацию:

- наличные денежные средства предпочтительно снимать в банкоматах, стоящих на территории банков;

- обратить внимание на возможное расположение на банкомате посторонних конструкций или предметов. Рядом с клавиатурой не должно быть лишних объектов, все элементы должны быть одного цвета и из одного материала. При возникновении подозрений, лучше воспользоваться другим устройствам;

- необходимо держать карту подальше от посторонних лиц и не передавать третьим лицам;

- нельзя хранить записанный ПИН-код рядом с картой или записывать его на саму карту, желательно держать эти цифры в памяти. Если посторонние лица узнали ваши персональные данные, необходимо немедленно оповестить банк и заблокировать карту;

- в случае возникновения какой-либо проблемы с банкоматом (например, застряла карта), необходимо немедленно позвонить в банк для разрешения возникшей ситуации (на номер телефона указанный на банкомате);

- при совершении платежей, нельзя упускать карту из виду. Необходимо требовать от продавца предоставить портативный терминал для совершения оплаты;

- при расчете через Интернет лучше создать виртуальную карту либо открыть новый расчетный счет и получить новую карту, которая будет использоваться исключительно для совершения покупок в сети, и переводить на нее денежные средства самостоятельно, не аккумулировать на ней значительных денежных средств;

- устанавливать ограничение суммы на операцию в банкомате и покупку в торговой точке;

- мошенники часто прибегают к таким видам уловок, как отправку SMS-сообщений на телефон с просьбой перезвонить по указанному номеру или отправить ответное сообщение с определенной комбинацией цифр. При таком случае необходимо обратиться в службу технической поддержки своего банка для того чтобы проверить информацию о состоянии своего счета (например, если Вы получили сообщение с незнакомого номера с просьбой перезвонить или направить в ответ сообщение с каким-либо текстом или комбинацией цифр, этого делать не стоит. Необходимо позвонить на номер телефона горячей линии указанный на банковской карте);

- лучше установить СМС-оповещение на телефон. Это позволит быть в курсе действий, происходящих с платежной картой, а также появиться возможность вовремя заблокировать карту, в случае совершения не

санкционированных списаний, и совершение иных преступленных действий;

- в случае утраты сотового телефона или сим-карты, а также в случаях смены номера телефона, необходимо уведомить об этом банк, и путем подачи письменного заявления отключить услугу «Мобильный банк» (оператор сотовой связи передаст номер сим-карты другому абоненту, в случае если гражданин определенное время ею не пользуется, а банк, не будучи уведомлен об этом, продолжит направлять СМС-оповещения с данными по операциям с карты, на номер телефона, который уже не принадлежит гражданину);

- не доверять сайтам, где перед получением товара, оказания услуг или помощи в трудоустройстве необходимо осуществить предоплату;

- не участвовать ни в каких акциях и розыгрышах призов на интернет сайтах, особенно на сайтах социальных сетей «Вконтакте», «Одноклассники». Не указывать никакой информации о своих банковских картах;

- если в переписке Вас просит друг/подруга/просто знакомый, который есть в списках Ваших друзей «Вконтакте», дать взаймы, то не следует переводить денежные средства на указанный в переписке номер банковской карты. Необходимо позвонить или иным способом связаться с этим человеком, удостоверяясь, что ведете переписку именно с Вашим другом, его страничка может использоваться посторонним лицом – мошенником.

Что делать, если произошел факт хищения денежных средств?

Следует срочно обратиться в банк для получения подробной выписки о движении ваших средств (с указанием адресата получения переводов) и заблокировать карту. У сотового оператора необходимо получить детализацию соединений по номеру, на которой подключена услуга «Мобильный банк», и с этими документами обратиться в полицию.