***Прокуратура Иркутского района информирует!***

С каждым годом число пользователей банковских карт неуклонно растет, а также неуклонно растет количество краж денежных средств с банковских карт, при этом мошенники вынуждены изобретать все более изощренные способы хищения денег у граждан.

Самые распространенные приемы данного вида преступления следующие.

На сотовый телефон абонента приходит смс — сообщение о том, что его банковская карта заблокирована, и ему предлагается схема действий. Такое СМС вполне может получить любой владелец банковской карты. Ее номер мошенники узнают из украденных банковских баз данных, баз данных интернет-магазинов. Далее идет текст такого примерно содержания: «Причина – представлены неверные данные». Звонивший оператор дает инструкции по телефону. Он просит подойти к банкомату и позвонить уже оттуда. Согласно инструкции мошенника, потерпевший следует к банкомату и по схеме переводит деньги на указанные реквизиты.

В настоящее время актуальна услуга «Мобильный банк», но при смене сим-карты абонентского номера граждане зачастую забывают ее отключать. Через определенное время замененный номер продается, а новому собственнику приходят SMS-сообщения о пополнении счета подключенной карты, и он снимает с нее деньги. Чтобы не попадать в подобные ситуации, при смене сим-карты обязательно отключайте услугу «Мобильный банк» на старом абонентском номере.

Также участились случаи хищения денежных средств с банковских карт с помощью глобальной сети Интернет. Как правило, при использовании Интернета на мобильных устройствах, необходимо устанавливать антивирусную программу. В тех случаях, если данная программа не установлена, или не обновлена, в телефон может попасть специальный запрограммированный вирус с целью хищения денег с Вашей карты (в том случае, если подключена услуга «мобильный банк»).

Таким образом, чтобы не стать жертвой мобильного мошенничества, необходимо соблюдать несколько простых правил:

 - не используйте ваш мобильный телефон для доступа к Интернет-банку (как вариант, можете с персонального компьютера с установленной антивирусной программой заходить в Интернет-банк, а на телефон получать банковские СМС-уведомления);

- если вы потеряли или перестали пользоваться SIM-картой, то отключите на ней «Мобильный банк»;

- никому нельзя сообщать информацию, напечатанную на обеих сторонах Вашей банковской карты;

- установите на смартфон/планшет антивирусную программу;

- устанавливайте приложения только из официальных источников. Это Google Play для Android устройств и  AppStore для устройств Apple (iPhone / iPad);

- не производите в банкомате с картой никаких действий по рекомендациям незнакомых людей.