ПАМЯТКА

«ЧТО НУЖНО ДЕЛАТЬ, ЧТОБЫ РИСК ПОТЕРИ ОТ ДЕЙСТВИЙ МОШЕННИКОВ СВЕСТИ К МИНИМУМУ ПРИ ОБРАЩЕНИИ С ПЛАТЕЖНЫМИ КАРТАМИ»

Чтобы свести потери от мошенников к минимуму, необходимо соблюдать простые правила обращения с платежными картами, а именно:

- никогда и никому (даже родственникам) не сообщайте ПИН-код, Помните: операция, совершенная с вводом ПИН-кода признается выполненной держателем карты;

- если не можете запомнить ПИН-код и записываете его, то держите его отдельно от карты. Никогда не записывайте ПИН-код на карте;

- никогда не передавайте карту для использования другим людям. Давая карту для оплаты, следите, чтобы кассир совершал операции у вас на глазах, перед вводом ПИН-кода проконтролируйте сумму операции на чеке;

- вводя ПИН-код, прикрывайте свободной рукой клавиатуру, следите, чтобы рядом не было посторонних «наблюдателей». При совершении операции через банкомат не прибегайте к помощи либо советам третьих лиц, свяжитесь со своим банком - он обязан предоставить консультационные услуги по работе с картой;

- перед тем, как воспользоваться банкоматом, обратите внимание на предмет наличия на нем дополнительных устройств, накладок на клавиатуру или прорезь для приема карт. Если возникают сомнения - откажитесь от использования такого банкомата. Не используйте неисправный банкомат;

-для оплаты через Интернет используйте одноразовую «виртуальную карту» или заведите дополнительную карту. Перечисляйте на нее денежные средства под расчет предполагаемой операции;

- используйте на своем компьютере антивирусное программное обеспечение и не открывайте почтовые сообщения с исполняемыми файлами. Лучше вообще не открывать подозрительные сообщения и не переходить по гиперссылкам, отправленных с незнакомых адресов;

- можно воспользоваться услугами, которые предлагают банки: можно установить суточный/месячный лимит на совершение операций, блокировку операций по территориальному признаку, заблокировать отдельные услуги;

- учитывая, что в большинстве случаев жертвы сами сообщают данные своих карт мошенникам, будьте бдительны, не сообщайте эту информацию третьим лицам, чем бы они не объясняли такую необходимость.

Кроме того, не забывайте, что сейчас операции переводу денежных средств или по оплате товаров и услуг можно совершать с использованием устройств мобильной связи: телефонов, смартфонов, - это так называемый «мобильный банкинг». В данном случае для минимизации рисков хищения денежных средств следует также бережно обращаться не только с картой, но и с мобильным телефоном. Рекомендуем:

- установить на устройство мобильной связи антивирусное программное обеспечение, базы которого будут регулярно обновляться;

- не передавайте мобильный телефон для использования третьим лицам;

- если вы сменили номер телефона мобильной связи, обязательно сообщите об этом в свою кредитную организацию.

В случае утери мобильного телефона нужно незамедлительно заблокировать карты, которые привязаны к вашему «мобильному банку».