О мерах по предупреждению хищений денежных средств при использовании банковских карт

Хищение с банковских карт в связи с развитием средств коммуникации и электронного обмена данными в настоящее время является наиболее распространенным способом завладения чужими денежными средствами.

Использование банковской карты значительно упрощает операции с деньгами, вместе с тем внедрение инновационных способов расчета, открывает широкие возможности не только для добропорядочных граждан, но и для злоумышленников.

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из следующего.

Сотрудники банка никогда по телефону или в электронном письме не запрашивают:

-     персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);

-      реквизиты и срок действия карты;

-     пароли и коды из СМС-сообщений для подтверждения финансовых операций или их отмены;

-      логин, ПИН-код и СVV-код банковской карты.

Сотрудники банка также не предлагают:

-     установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

-      перейти по ссылке из СМС-сообщения;

-      включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

* под их руководством перевести для сохранности денежные средства на «защищенный счет»;
* зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать сообщение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

* подключения к общедоступным сетям Wi-Fi;
* использование ПИН-кода или СVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);
* сообщения кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или СVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

Перед использованием банкомата осмотрите его и убедитесь, что все операции, совершаемые предыдущим клиентом, завершены; что на клавиатуре и в месте для приема карт нет дополнительных устройств; обращайте внимание на неисправности и повреждения.

В случае смены номера мобильного телефона или его утери свяжитесь с банком для отключения и блокировки доступа к СМС-банку и заблокируйте сим-карту, обратившись к сотовому оператору.

При возникновении малейших подозрений насчет предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.