Возросшее число фактов хищений денежных средств с банковских карт является следствием недостаточной осведомленности граждан в области информационных технологий и пренебрежительного отношения к элементарным правилам безопасности.

Для предотвращения противоправных действий по снятию денег с банковского счета необходимо знать, что сотрудники банков никогда по телефону или в электронном виде на запрашивается персональные данные, реквизиты и срок действия карт, пароли или коды СМИ-сообщений для подтверждения финансовых операций или их отмены, логин ПИН-код и CVV-код банковских карт.

Также работники банков не предлагают установить программы удаленного доступа на мобильное устройство; перейти по ссылке на 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 под «защищенный счет»; зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Банк может инициировать общение 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 отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовыми учреждениями. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии.

Держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

- подключения к общедоступным сетям Wi-Fi;
- использовать ПИН-код или CVV-код при заказе товаров и услуг через сеть «Интернет», а также по телефону;
- сообщения кодов третьим лицам.

При использовании банкоматов необходимо отдавать предпочтение тем, которые установлены в защищенных местах.

Перед использованием банкомата необходимо осмотреть его и убедиться, что все операции, совершаемые с предыдущим клиентом, завершены; что на клавиатуре и в месте приема карт нет дополнительных устройств; обращать внимание на неисправности и повреждения.

При совершении операций не следует прислушиваться к советам незнакомых людей и принимать их помощь.

При использовании мобильного телефона необходимо соблюдать ряд правил:

при установке приложений обращать внимание на полномочия, которые они запрашивают, быть особенно осторожными, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;

отключить в настройках возможность использования голосового управления при заблокированном экране.

Принимая сервисы СМС-банка, следует сверять реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.

При оплате услуг картой в сети «Интернет» требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные. Поэтому особое внимание нужно обращать на необходимость использования только проверенных сайтов. Внимательного прочтения текстов СМС-сообщений с кодами подтверждений, проверку реквизитов операции.

Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» рекомендуется оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции для данного вида карты, в том числе с использованием других банковских карт, выпущенных на имя держателя.

Когда банк считает подозрительными операции, совершаемые от имени клиента, он может по своей инициативе заблокировать доступ к сервисам СМС-банка или онлайн-кабинета. Если операции совершены держателем карты, для быстрого возобновления доступа к денежным средствам достаточно позвонить в контактный центр банка.

В случае смены номера мобильного телефона или его утери следует связаться с банком для отключения и блокировки доступа к СМС-банку и блокирования сим-карту путем обращения к сотовому оператору.

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