ПРОКУРАТУРА
ЯРОСЛАВСКОЙ ОБЛАСТИ

Как предупредить хищение денежных средств при использовании банковских карт?

Необходимо помнить, что 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 или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин, ПИН-код и CVV-код банковских карт.

Сотрудники банка не предлагают:

- установить программы удаленного доступа на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);
- 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 СМС-сообщения или электронного письма.

Банк инициирует 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.

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

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН-кода и CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);
- сообщения кодов третьим лицам.

При использовании банкоматов следует отдавать предпочтение тем, которые установлены в защищенных местах (в госучреждениях, офисах банков, крупных торговых центрах).

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

При совершении операций не следует прислушиваться к советам незнакомых людей, а также пользоваться их помощью.

При оплате услуг картой в сети «Интернет» (особенно при привязке к регулярным платежам или аккаунтам) необходимо учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные.

Необходимо использовать только проверенные сайты, внимательно читать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операции.

В целях 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 карты.

По подозрительным операциям, совершаемым от имени клиента, банк может по своей инициативе временно заблокировать доступ к сервисам СМС-банка и онлайн-кабинет. В случае совершения держателем карты операций для быстрого возобновления доступа к денежным средствам достаточно позвонить в контактный центр банка.

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 малейшем подозрении предпринимаемых попыток совершения мошеннических действий следует незамедлительно уведомлять об этом банк.

Прокуратура Ярославской области