

**О мерах по предупреждению хищений денежных средств
при использовании банковских карт**

Результаты анализа сообщений о фактах хищений денежных средств с банковских карт свидетельствуют о возросшем числе подобных преступлений, которым, как показывает практика, способствуют недостаточная осведомленность людей в области информационных технологий и порой их пренебрежительное отношение к элементарным правилам безопасности.

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 банковской карты);
- реквизиты и срок действия банковской карты;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин, ПИН-код и CVV-код банковских карт.

Сотрудники банка также **никогда** 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 общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне банковской карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку. Следует помнить, что развитие технологий позволяет в настоящее время с использованием специальных программ использовать так называемые «виртуальные телефонные номера» и производить подмену официально используемых банками для связи с клиентами абонентских номеров. По этой причине в случае возникновения малейших сомнений относительно того, действительно ли входящий звонок осуществляет работник банка, рекомендуется прерывать разговор и самостоятельно перезванивать на официально используемый номер, указанный на оборотной стороне банковской карты.

Для связи с представителями банков следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны «горячей линии», группы или чат-боты в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store.

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

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН-кода или CVV-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 CVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

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

Перед использованием банкомата рекомендуется осмотреть его и убедиться, 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.

При совершении операций с использованием банкомата не рекомендуется прислушиваться к советам незнакомых людей и не принимать их помощь.

При использовании мобильного телефона следует соблюдать следующие правила:

- при установке приложений следует обращать внимание на полномочия, которые они запрашивают и быть особенно осторожным, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;
- рекомендуется отключать в настройках возможность использования голосового управления при заблокированном экране;
- при применении сервисов СМС-банка необходимо 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» (особенно при привязке к регулярным платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные.

По этой причине следует использовать только проверенные Интернет-сайты, внимательно читать тексты поступивших СМС-сообщений с кодами подтверждений, проверять реквизиты 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 карты.

Когда банк считает подозрительными операции, которые совершаются от имени клиента, он может по своей инициативе временно заблокировать доступ к сервисам СМС-банка и 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 срочно связаться с банком для отключения и блокировки доступа к СМС-банку и заблокировать сим-карту, обратившись к сотовому оператору.

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

Прокуратура района