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

В прокуратуре Тоджинского района проанализировано состояние преступности в сфере хищения денежных средств с банковских карт.

Результаты анализа свидетельствуют о возросшем числе подобных преступлений, которым, как показывает практика, способствует недостаточная осведомленность граждан в области информационных технологий и правил 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 карты);

реквизиты и срок действия карты;

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

логин, ПИН-код и CVV-код банковских карт.

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-сообщений 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 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;

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 мобильного телефона соблюдайте следующие правила:**

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

отключите в настройках возможность использования голосового управления при заблокированном экране.

Применяя сервисы СМС-банка, сверяйте 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. Поэтому необходимо использовать только проверенные сайты.

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 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, а при необходимости правоохранительные органы.