**Памятка о мерах по предупреждению хищений денежных средств при использовании банковских карт**

Прокуратурой района по итогам 2020 года проанализирована эффективность профилактики преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Всего в 2020 году совершено 1042 (+988) таких преступлений. Значительный рост обусловлен совершением хищений с банковских счетов граждан, в том числе дистанционным способом.

Для предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить из того, 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);
* пароли или коды из смс-сообщений для подтверждения финансовых операций 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;
* 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 инициирует общение с клиентом только для консультаций по финансовым продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотней стороне карты, на сайте банка. Иные номера не имеют никакого отношения к банку.

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 и по телефону;
* сообщения кодов третьим лицам.

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

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.

При использовании мобильного телефона соблюдайте следующие правила:

* при установке приложений обращайте внимание на полномочия, которые они запрашивают. Будьте 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 необходимо всегда учитывать высокую вероятность перехода на поддельный сайт, созданный мошенниками для компрометации клиентских данных. Поэтому необходимо использовать только проверенные сайты, внимательно читать тексты 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.

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.