Проведенным в прокуратуре края анализом установлено, что в 2020 г. на 69,2% (с 5479 до 9271) возросло число преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, при этом в разы (с 48 до 3396) увеличилось количество таких преступлений с использованием расчетных (пластиковых) карт.

Возросшему числу хищений денежных средств при использовании гражданами банковских карт способствует недостаточная осведомленность в области информационных технологий и пренебрежительное отношение к элементарным правилам безопасности.

В этой связи для предотвращения противоправных действий гю снятию денежных средств с банковского счета необходимо исходить из следующею.

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(три цифры на обороте карты)банковских карт.

Сотрудники банка также не предлагают:

-установить программы удаленного доступа на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

- перейти по ссылке из СМС-еообщения:
- 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 консультации 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 отношении к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением.

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

- подключения к общедоступным сетям WI-FI;

использование ПИН-кода или CVVкода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);

- сообщения кодов третьим лицам;
- переход по ссылкам и установку приложений/обновлений, пришедших по СМС и электронной почте;
- оставление своего телефона без присмотра, чтобы исключить возможность несанкционированного использования услуги «Мобильный банк». В этой связи следует установить на мобильном телефоне пароль доступа к устройству.

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

Совершая операции, не прислушивайтесь к сове гам незнакомых людей и не принимайте их помощь.

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.

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.