«Осторожно, мошенники!»

Для предупреждения противоправных действий по дистанционному хищению денежных средств важно запомнить следующее.

Сотрудники банка по телефону или в электронном письме не запрашивают:

- персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);
- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка также не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) 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 «защищённые» или «безопасные» счёта;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

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

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

При использовании сотовых телефонов (смартфонов) соблюдайте следующие правила:

- при установке мобильных приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и иных уведомлений, доступ к сети «Интернет»;
- отключите в настройках возможность использования голосового управления при заблокированном экране;
- не переходите по ссылкам из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислашим);
- не перечисляйте денежные средства знакомым, родственниками и близким лицам на их просьбы о переводе денежных средств из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их прислашим);

При использовании интернет-сервисов, в то числе для покупки и продажи товаров и оказания услуг (Авито, Юла и т.п.) запомните ряд простых правил:

- используйте средства общения, предоставленные данными сайтами;
- не переходить на «индивидуальное» общение с посторонними лицами с использованием личных номеров телефонов;
- не передавайте свои персональные данные, в том числа адрес проживания, контактные телефоны, банковские реквизиты и коды подтверждения банковских операций;
- используйте только порядок и формы оплаты, получения товаров, предусмотренные данными интернет-сервисами.

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

Для минимизации возможных хищений при проведении операций с использованием сети «Интернет» рекомендуется:

- оформить виртуальную карту с установлением размера индивидуального лимита, ограничивающего операции, в том числе с использованием других банковских карт;
- внимательно читать тексты СМС-сообщений и иных уведомлений с кодами подтверждений, проверять реквизиты операций. Если реквизиты не совпадают, то такой пароль вводить нельзя.

Когда банк считает совершаемые от имени клиента операции подозрительными, 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 утери или смены номера телефона, привязанного к банковской карте, необходимо:

- связаться с банком для отключения услуги СМС-уведомления;
- заблокировать сим-карту, обратившись к сотовому оператору.

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

Соблюдение приведенных мер и рекомендаций позволит предотвратить случаи дистанционного хищения денежных средств.

Управление по надзору за следствием,
дознанием и оперативно-розыскной деятельностью