**Новосибирская транспортная прокуратура информирует**

Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает возможность осуществления противоправных деяний, связанных с использованием информационных технологий. В последнее время число преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, возрастает. Наиболее распространены хищения денежных средств, мошенничества, кражи с банковского счета и иные. В связи с этим, чтобы избежать негативных последствий для себя и своих близких, необходимо быть предельно бдительными и помнить основные правила безопасного поведения и общения посредством информационно-телекоммуникационных технологий.

Существует ряд простых правил, при соблюдении которых, Вы можете обезопасить себя:

- Никому не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам.

- Сообщать кодовое слово или код клиента банка можно только в том случае, если вы обратились в контакт-центр и разговариваете с сотрудником банка.

**Как безопасно пользоваться интернет-банком?**

Используйте сложный пароль блокировки экрана и качественную антивирусную программу. Не храните в телефоне реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты.

Избегайте входа в систему мобильного банкинга с чужих устройств.

При утрате телефона немедленно обратитесь в банк для блокировки карты и в офис мобильного оператора для блокировки SIM-карты.

Не переходите по ссылкам из SMS-сообщений, даже если в сообщении утверждается, что оно из банка.

ВАЖНО!

Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

ПОМНИТЕ!

При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.

Что делать, если вам позвонили из банка, и интересуются вашей платежной картой? Разумнее всего прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты).

Также можно обратиться в отделение банка лично. Помните, что самый распространенный способ совершения хищений денежных средств с карт граждан – побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

**Как безопасно совершать платежи в интернете?**

Используйте на устройстве антивирус с активной защитой онлайн- платежей. Совершайте оплату только посредством использования защищенных соединений. Защищенное или зашифрованное подключение можно распознать по значку в виде замочка в начале адресной строки браузера и префиксу https:// (не просто http, а с буквой s на конце) перед адресом сайта.

Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладку браузера. Не проводите финансовые операции с общественного WI-FI в кафе, транспорте или гостиницах. Не сохраняйте свои данные о карте в браузере.

**Безопасность учетных записей**

Завладев логином и паролем от учетной записи электронной почты, социальной сети, портала госуслуг и других сервисов, мошенники получают возможности для извлечения материальной выгоды. И это не только списание средств с банковской карты. Войдя в чужую учетную запись, мошенники могут рассылать контактам пользователя сообщения с просьбой о переводе небольшой, как правило, суммы денег, или публиковать на странице информацию компрометирующего характера.

**Как не оказаться в подобной ситуации?**

Для каждой учетной записи использовать разные логины и пароли. Использовать сложные пароли, состоящие из букв и цифр. Создавать и хранить их поможет менеджер паролей. Для максимальной защиты учетной записи рекомендуется использовать двухэтапную аутентификацию (для входа в аккаунт кроме логина и пароля необходимо ввести одноразовый код или подтвердить действие на электронных устройствах, подключенных к вашему аккаунту).