Прокуратура Автозаводского района г. Тольятти разъясняет:
«Будьте осторожны! Интернет-мошенничество»

Важнейшая проблема, с которой сталкиваются многие граждане – это дистанционное мошенничество, связанное с получением мошенниками удаленного доступа к банковской карте и интернет-мошенничеством. Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов», «подключения к социальной программе» или иных надуманных предлогов 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. 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).

Мошенниками могут быть запрошены у жертвы следующие данные:

- ПИН-код карты – четырехзначная комбинация цифр, выдаваемая в конверте одновременно с изготовленной банковской картой. Его можно изменить, обратившись в отделение банка или позвонив на горячую линию.

- Код безопасности (CVV2 или CVC2) – комбинация цифр, указанная на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Проверочный код необходим только для совершения платежей в интернете. При онлайн-оплате он вводится вместе с номером карты, именем держателя карты и сроком окончания действия карты.

- Одноразовый пароль банка для подтверждения оплаты онлайн – комбинация цифр, отправляемых банком в смс-сообщении или push-уведомлении для подтверждения операций с денежными средствами.

Ни в коем случае не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!!!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности!!!

Одним из самых распространенных видов интернет-мошенничества является так называемый «фишинг». Мошенники совершают определенные действия, направленные на получение доступа к денежным средствам на банковской карте потенциальной жертвы, при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования.

Распространенным способом мошенничества является мошенничество в социальных сетях. Мошенники взламывают персональную страницу пользователя в социальных сетях или мессенджере и либо всем подряд отправляют сообщения с просьбой помочь и срочно перевести денег либо анализируют переписку и находят самых близких людей, тех, кто точно не откажет.

После первого перевода мошенники могут связаться с жертвой, сказать, что-то пошло не так, попросить повторить перевод и так пока на карте не закончатся деньги или жертва не догадается об обмане, но выманивать могут не только деньги, но и реквизиты карт якобы для того, чтобы перевести деньги жертве (спросят номер карты, срок действия, трехзначный код безопасности и пароли из смс), однако деньги жертве разумеется не придут, зато с карты средства будут списаны.

Что же делать, если вам пришло сообщение с просьбой о помощи от одного из знакомых или родственников? Необходимо немедленно связаться с ним по телефону, уточнить отправлял ли он это сообщение и не предпринимать ничего, пока он не подтвердит это лично. Тем более ни в коем случае нельзя сообщать реквизиты своей карты (три цифры на оборотной стороне, срок действия, пароль из смс).

Кроме того, нужно позаботиться и о пароле для своего аккаунта в соцсетях и мессенджерах. Он защищает не только вашу безопасность, но и безопасность ваших родных и близких.