Мошенничество с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

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.

К примеру, в августе 2021 года в МО МВД России «Зеленчукский» зарегистрировано сообщение гражданина Л., который сообщил, что в июле 2021 года, ему поступил звонок с абонентского номера 8-985-637-80-28 от неизвестного мужчины, который представился сотрудником «Сбербанка России» и сообщил, что с банковской карты гражданина Л. посторонние лица совершают попытки оформить кредит на имя гражданина Л., в связи с чем последнему необходимо обналичить заемные денежные средства в ближайшем банкомате «Сбербанка России» и совершить досрочное погашение указанного кредита, внеся денежные средства на банковские карты, привязанные к определенным номерам телефонов, которые «сотрудник» «Сбербанка России» продиктует.

Гражданин Л., зайдя в приложение «Сбербанк Онлай» обнаружил, что на его имя оформлен кредит на сумму 250 000 рублей с совершил все указанные мошенником действия, после чего мошенник сообщил, что кредит погашен.

Позже гражданин Л. обнаружил, что кредит не был погашен и он стал жертвой мошеннических действий неизвестного лица, представившегося сотрудником «Сбербанка России».

Кроме того, в августе 2021 года зарегистрировано еще 2 факта совершения мошенниками аналогичных преступлений в отношении иных лиц.

По всем указанным фактам мошенничества следователями СО МО МВД России «Зеленчукский» возбуждены уголовные дела, которые находится в настоящее время в производстве.

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.

Еще одним крайне распространенным видом интернет-мошенничества являются фальшивые интернет-магазины. Мошенники берут с покупателя предоплату за товар и не выполняют своих обязательств.

Важно отметить, что популярность сайта в поисковике вовсе не гарантия вашей безопасности. В действительности мошенники активно продвигают свои сайты с использованием вебмаркетинга. И зачастую фальшифки стоят даже выше ссылок на оригинальный сайт и внешне он на первый взгляд ничем не отличается от оригинала. Платежные страницы на таких сайтах только маскируются под оплату товаров и услуг, на самом деле потенциальная жертва переводит деньги на карты мошенников или на номера мобильных телефонов, с которых впоследствии мошенники снимут деньги. Кроме того на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты гражданин-покупатель даже может получить подтверждение по почте, но товаров и услуг доставлено и оказано не будет.

Признаки отличия поддельных сайтов от настоящих:

-Внимательно изучите адресную строку. Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы один символ.

-Сайт новый и о нем нет никакой информации в интернете.

-Тексты на сайте могут содержать ошибки и неработающие ссылки.

-Дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка.

-Вместо названия магазина на аутентификационной странице символы P2P, PEREVODNAKARTU или CARD2CARD, то есть информация о переводе средств с карты на карту.

-Сумма на аутентификационной странице банка может быть изменена.

После введения корректных данных сайта для одноразового пароля жертве сообщают, что пароль неверный и просят ввести новый пароль на самом деле, чтобы провести новую операцию.

Заметив любой из этих признаков, звоните по телефону, который указан на вашей карте и пользуйтесь только проверенными интернет-площадками.

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.