

-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 жертвы 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 обратной 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.