

Мошенники не дремлют – Банк России просит сохранять бдительность

Банк России просит жителей Тамбовской области не поддаваться панике из-за коронавируса, оставаться внимательными при совершении покупок в интернете и не вестись на новые легенды мошенников, играющих на обостренных чувствах людей в кризисной ситуации

Довольно часто мошенники активизируются во время стихийных бедствий, техногенных катастроф и эпидемий. Например, они призывают людей делать пожертвования якобы для помощи пострадавшим. Часто обманщики маскируются под официальные организации.

«Легенды могут быть самыми разными. В текущей ситуации махинаторы могут предлагать купить медицинские маски, супердезинфицирующее средство, лекарства, вакцину и даже амулеты, которые защищают от любых болезней», – рассказал заведующий сектором отдела информатизации Отделения Тамбов ГУ Банка России по ЦФО Вадим Киселев.

В действительности обманщики используют ситуацию в своих интересах – украсть деньги с карты либо получить доступ к персональным данным, сообщениям и банковским приложениям человека, который попался на их крючок.

В некоторых случаях мошенники даже не призывают переводить деньги или что-то покупать. Они просто направляют письмо или сообщение, в которых дают ссылку на сайт с якобы самыми актуальными рекомендациями.

На самом деле это фишинговые сайты, которые собирают личные данные и платежные реквизиты пользователей. Вместо рекомендаций по борьбе с коронавирусом человека, скорее всего, ждет вредоносная программа. Она проникнет в телефон, планшет или компьютер и получит доступ к конфиденциальным данным – например, к паролю от онлайн-банка.

Если вам предлагают внести пожертвование на счет какой-либо известной организации, необходимо зайти на ее официальный сайт и убедиться, что она действительно проводит сбор денег. На сайте должны быть указаны реквизиты организации или ссылки на страницы, где деньги можно перевести безопасным способом. В случаях, когда организация или интернет-магазин вам неизвестны, стоит сначала поискать информацию и отзывы о них в интернете.

Эксперты Банка России напоминают, чтобы не попасться на уловки преступников, необходимо соблюдать и другие правила кибербезопасности:

- Не переходите по ссылкам из писем незнакомых отправителей.
- Проверьте адресную строку сайта — часто фишинговые сайты отличаются от официальных всего одной-двумя буквами.
- Используйте отдельную карту для онлайн-платежей и кладите на нее нужную сумму непосредственно перед покупкой.
- Установите на все свои устройства антивирус и регулярно обновляйте его. Хороший антивирусный пакет включает защиту от спама и фишинговых писем. Он сам распознает подозрительных адресатов.
- Если преступники уже получили данные вашей карты, заблокируйте ее и попросите банк выпустить новую.