«Поддержите разработку вакцины от коронавируса»

Валентина, Сыктывкар

Вчера получила письмо от Всемирной организации здравоохранения. В теме было написано «Разработка вакцины от коронавируса». Я заинтересовалась, открыла письмо. В нем говорилось, что ученые всего мира активно работают над вакциной и лекарством от коронавируса, а ВОЗ курирует эту работу. Но разработка очень дорогая, поэтому всем неравнодушным людям предлагается поддержать исследования. Было написано, что пожертвовать можно любую сумму, даже совсем небольшую. И дальше ссылка на сайт, где это можно сделать. Я решила не оставаться в стороне и перевести 300 рублей. Перешла по ссылке, ввела данные карты, сумму и нажала «оплатить». Списали 300 рублей. А потом еще несколько раз подряд разные суммы, пока все деньги на карте не кончились. Получается, это были аферисты, а никакая не Всемирная организация здравоохранения?

Совет эксперта по противодействию мошенничеству:

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

Легенды могут быть самыми разными. В случае с коронавирусом махинаторы также предлагают купить медицинские маски, супердезинфицирующее средство, лекарства, вакцину и даже амулеты, которые защищают от любых болезней.

В некоторых случаях мошенники даже не призывают переводить деньги или что-то покупать. Они просто направляют письмо или сообщение, в которых дают ссылку на самые актуальные рекомендации, как защититься от коронавируса, от имени авторитетных организаций.

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.

Махинаторы создают специальные фишинговые сайты, которые собирают личные данные и платежные реквизиты пользователей. Такая информация позволяет им обнулить чужие счета.

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.

Чтобы не попасться на уловки преступников, необходимо соблюдать и другие правила кибербезопасности:

- Не переходите по ссылкам из писем незнакомых отправителей.

- Проверяйте 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.