«Пришла рассылка от популярного видеосервиса, оказалось — мошенники»

Василиса, Кемерово

Во время пандемии стала пользоваться одним популярным сервисом для видеоконференций. А недавно с его официального адреса пришло очень странное письмо.

В нем было сообщение о какой-то компенсации в связи с COVID-19, и тут же ссылка на незнакомый сайт. Ради интереса кликнула по ссылке и попала на страницу некоего фонда финансовой поддержки. Там написано, что мне положена компенсация, размер которой можно узнать, если ввести четыре последних цифры моей банковской карты. Ну я ввела наобум. Сайт показал, что мне положено 30 000 рублей. Все понятно — развод.

Читаю дальше: получить деньги можно только оплатив небольшую комиссию. Разумеется, тоже с банковской карты — тут же форма для заполнения всех реквизитов. На этом я уже остановилась: но кто-то ведь поведется и сольет данные своей карты мошенникам.

Не понимаю, как все это оказалось в официальной рассылке сервиса? Адрес, с которого пришло письмо, тот же, с которого обычно получаю от них все письма и уведомления. В общем заскриншотила все и разослала знакомым, чтобы не попались на этот обман. В сам сервис тоже пожаловалась.

Совет эксперта по противодействию мошенничеству:

Мошенники все чаще используют известные сервисы, чтобы от их имени вводить пользователей в заблуждение и затем обворовывать. Рассылают фейковые «уведомления» в онлайн-календарь, задействуют банковскую СМС-рассылку в своих схемах.

Цель всегда одна и та же: выманить у человека конфиденциальную информацию — полные реквизиты банковской карты, включая срок действия и трехзначный код с обратной стороны.

Эти данные дают злоумышленникам доступ к счету, с которого они могут украсть все деньги.

В случае с Василисой аферисты воспользовались растущей популярностью сервиса видеоконференций. Создавая в нем новый аккаунт, пользователь может ввести довольно длинный текст в полях «Имя» и «Фамилия». Мошенники вбивают туда целые фразы. Например, вместо имени — «Вам положена компенсация в связи с COVID-19», а вместо фамилии — ссылку на фишинговый сайт.

После регистрации сервис предлагает новому пользователю пригласить для участия в видеоконференциях до десяти знакомых. Для этого надо указать их электронную почту, и им придет приглашение. Аферисты вбивают адреса, которые оказались в сети, например из-за утечки персональных данных.

В итоге люди получают письмо от известной компании—с ее настоящего адреса и с фирменным оформлением. Но только вместо имени и фамилии друга или коллеги, который приглашает присоединиться к видеочатам, они видят текст обманщиков и ссылку на их сайт. Подобное письмо на бланке и с официального сайта видеосервиса с предложением компенсации получила и Василиса.

Мошенники могли пообещать что угодно: государственную выплату, выигрыш в конкурсе, возмещение за отмененный из-за пандемии рейс и многое другое. Или предложить «скидку» при подписке на сам сервис видеоконференций и оставить ссылку на его сайт-клон, где тоже требовалось бы указать данные банковской карты.

Если бы Василиса поверила сообщению и ввела на мошенническом сайте реквизиты карты, лишилась бы денег со счета. При этом вернуть украденную сумму через банк не вышло бы: ведь в этой ситуации она сама передала бы конфиденциальную информацию посторонним. Пришлось бы обращаться в полицию.

Чтобы не попасться на уловки обманщиков, соблюдайте правила безопасности:

- Если вам пришло письмо от сервиса, в котором вы не зарегистрированы, сразу переносите сообщение в папку «Спам». И не переходите по ссылкам из этого письма — так вы можете загрузить на свое устройство вирус, который крадет данные.

- Не вводите на сомнительных сайтах информацию о карте, ПИН-коды, пароли и коды из уведомлений от банка, а также данные паспорта и других документов. Сначала убедитесь, что страница не фишинговая.

- Не доверяйте «письмам счастья» и рекламе о внезапном обогащении или компенсациях. Если вам обещают «возмещение от государства», сначала проверьте в СМИ и на официальных сайтах ведомств, действительно ли принят закон или постановление о каких-либо выплатах. В идеале стоит найти этот документ и внимательно его изучить.

- Установите антивирусы на всех гаджетах, которыми пользуетесь.