«Новое уведомление в календаре: получите деньги»

Ольга, Сочи

Недавно мне пришло странное уведомление в Google-календарь: «На сегодня заплонирован вывод 110 230 руб получение» и какая-то ссылка.

Понятно, что это спам: написано все с ошибками и вообще вывода денег я не планировала. Но я была в запаре и на автомате перешла по ссылке.

Открылся странный сайт. Там было написано, что на мой счет идет перевод, но надо оплатить комиссию, и тогда деньги зачислятся на карту. Была приписка — если я не заплачу комиссию, мой счет заблокируют. Я сразу позвонила в банк, мне сказали, что это мошенники.

Моему коллеге в этот же день пришло похожее уведомление в календарь, только ссылка открылась другая. В сообщении было указано, что он выиграл 130 000 рублей. Чтобы получить их, надо сделать платеж со своей карты на 200 с чем-то рублей. На сайте были отзывы разных людей, которые уже получили деньги.

Он перешел по ссылке «выполнить платеж». Открылась форма, которую надо было заполнить. Ввести номер карты, имейл и тд. Он не стал ничего вводить, и так ясно, что это лохотрон.

Обычно такой спам приходит в почту. Мы не поняли, как оно попало в календарь и как блокировать эти сообщения?

Совет эксперта по противодействию мошенничеству:

Ольга столкнулась со спамерами, которые рассылают ссылки на фишинговые сайты через популярные сервисы и пытаются выманить чужие деньги. Если бы она или ее коллега ввели данные своих карт, мошенники смогли бы получить доступ к их счетам и вывести все средства, что на них были.

Киберпреступники решили действовать через Google-календарь — онлайн-сервис для планирования встреч, событий и дел. Злоумышленники воспользовались тем, что приглашать человека на встречу через календарь может кто угодно — достаточно знать e-mail. Спам-фильтры не считают такие приглашения подозрительными и не блокируют их. Пользователь не ожидает подвоха, ведь в его календарь может приходить по несколько реальных приглашений в день и он привык к подобным уведомлениям.

Спам-мошенники используют не только Google-календарь, но и другие социальные сервисы, в том числе и популярные мессенджеры, через которые можно свободно рассылать сообщения пользователям.

Чтобы не попасть в ловушку спам-мошенников, следуйте важным правилам:

- Установите антивирусы на всех гаджетах, которыми пользуетесь.

- Отключите автоматическое добавление мероприятий в календарь. В этом случае они не будут туда попадать, пока вы не примите приглашение.

- Не принимайте приглашения на встречи от людей, которых вы не знаете.

- Не переходите по ссылкам из писем и уведомлений от неизвестных отправителей. Это могут оказаться вредоносные ссылки с опасным вирусом, который крадет секретные данные с гаджета.

- Не вводите данные карты на подозрительных сайтах. Всегда проверяйте адресную строку браузера. Адрес безопасного ресурса начинается с https://, и в адресной строке есть значок в виде закрытого замка.

- Больше рекомендаций о том, как отличить безопасный сайт от фишингового, — в тексте «Безопасные покупки в интернете».