«Введите номер СНИЛС и получите 120 000 рублей!»

Тимур, Железногорск

В инстаграме вылезла реклама о том, что государство начало выплачивать всем деньги по номеру СНИЛС — до 120 000 руб! Якобы ввели такой новый закон. Причем пост выглядит как новость от известного ТВ-канала с фоткой ведущей из студии. И под ним много комментариев от людей, которые уже получили деньги.

По ссылке «Подробнее» открылся сайт какого-то фонда и написано, что сегодня они выплатили людям уже несколько миллионов рублей. Надо ввести номер СНИЛС и тогда узнаешь, сколько денег тебе полагается. Я поверил и ввел свой номер СНИЛС. Дальше появились строки с суммами от разных страховых и внизу написано, что могу получить 115 000 руб.

Я нажал кнопку ПОЛУЧИТЬ ДЕНЬГИ и тут началось самое интересное. Сайт сообщил, что надо заплатить с карты какую-то комиссию 200 рублей за подключение к базе. Я оплатил, и потом с меня просят еще 500 рублей за идентификацию личности и проверку личных данных.

Вот тогда до меня уже дошло, что это какой-то развод на деньги. И вдруг получаю смс от банка, что с карты попытались снять еще 1000 рублей. Хорошо, что на моей карте не было больше денег. На всякий случай карту заблокировал. Люди, не ведитесь!

Совет эксперта по противодействию мошенничеству:

Мошенники активно используют социальные сети, чтобы выманивать персональные данные, платежную информацию и деньги пользователей. Преступники подделывают аккаунты известных СМИ и популярных блогеров, чтобы распространять фейковые рекламные посты от их имени. Это могут быть объявления о социальных выплатах, конкурсах с денежными призами и другие «аттракционы невиданной щедрости».

Чтобы предложение выглядело максимально правдоподобно, злоумышленники нередко сопровождают пост фальшивым видео с участием медийного лица — умело смонтированной нарезкой из роликов с ним.

И все ради того, чтобы пользователь перешел на мошеннический сайт и оплатил «небольшую комиссию». Потеря 200–300 рублей, возможно, не так страшна. Но человека просят ввести секретные данные банковской карты: номер, имя владельца, срок действия и трехзначный CVC/CVV-код с обратной стороны карты. После этого преступники получают доступ к его счету и могут украсть остальные деньги.

Опасность ситуации, в которой оказался Тимур, еще и в том, что преступники могут использовать номер СНИЛС и в других мошеннических схемах. Например, зная данные паспорта и СНИЛС, попытаться оформить займы на его имя.

Чтобы избежать неприятностей, следуйте важным правилам финансовой безопасности:

- Всегда перепроверяйте информацию из социальных сетей. Если государство назначает какие-либо выплаты и компенсации — об этом обязательно напишут ведущие издания. Посмотрите, есть ли что-то по теме в разделах новостей в поисковых системах. В идеале стоит найти ссылку на сам закон или постановление и изучить его.

- Не доверяйте конкурсам, опросам и другим обещаниям внезапного обогащения, в особенности если организаторы требуют что-либо оплатить.

- Не спешите переводить деньги неизвестным получателям по первому требованию и никогда не переходите по ссылкам от незнакомцев.

- Не вводите на сомнительных сайтах конфиденциальные данные, в том числе информацию о карте, ПИН-коды, пароли из СМС, а также данные паспорта и других документов.

- Не храните крупные суммы денег на карте, которую используете для повседневных трат. Лучше завести отдельную карту для покупок в интернете и каждый раз класть на нее ровно столько, сколько нужно заплатить.

- Подключите СМС-оповещения или push-уведомления об операциях по карте. В этом случае вы сразу же узнаете о платеже, который вы не совершали, и сможете заблокировать карту и опротестовать операцию.

- Установите антивирус на всех своих гаджетах — это поможет защитить их от вредоносных программ.

Если вы столкнулись с подозрительным объявлением в социальной сети, пожалуйтесь ее администрации. Чем больше жалоб от пользователей, тем быстрее эту рекламу удалят. И меньше шансов, что кто-то пострадает от действий преступников.