

Не так давно в социальных сетях появились объявления примерно такого характера: государство начало выплачивать деньги по номеру СНИЛС – до 120 тысяч рублей, в связи с вступлением в силу нового закона. Для пущей убедительности такой пост выглядит как новость от известного ТВ-канала с фото не менее известной ведущей из студии. И под ним, как водится, много восторженных комментариев от людей, которые уже якобы получили деньги.

Дальше – интересней. Проходя по ссылке «Подробнее» открывается сайт некоего фонда и сведения о том, сколько миллионов рублей выплачено людям на текущую дату. Тут же предложение ввести свой номер СНИЛС и узнать, какая сумма полагается вновь прибывшему на сайт «счастливчику».

Жителю города Железногорска Тимуру К. щедрые благотворители пообещали выплатить 115 тысяч рублей.

«Я нажал кнопку «Получить деньги». Сайт сообщил, что надо заплатить с карты комиссию 200 рублей за подключение к базе. Я оплатил, и тут же следом меня просят перевести еще 500 рублей за идентификацию личности и проверку личных данных. Тогда я уже начал понимать, 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 я ее заблокировал...».

Ситуацию комментирует заместитель управляющего отделением по Курской области Банка России Александр Устенко:

«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 так далее.

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 этой ситуации 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».

Правила финансовой безопасности

Всегда перепроверяйте информацию из социальных сетей. Если государство назначает какие-либо выплаты и компенсации — об этом, первым делом, сообщают официальные источники и пишут 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 стоит хранить крупные суммы денег на карте, которую используете для повседневных трат. Лучше завести отдельную карту для покупок в интернете и 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» - отмечает Александр Устенко.