# «Вам письмо от Портала Госуслуг и денежная компенсация!»

Мария, Ростов-на-Дону

Пришло на почту письмо от портала госуслуг, но почему-то в спам. Открываю — пишут, что мне положена социальная компенсация, далее коды какого-то постановления и даже ФИО сотрудника, к которому можно обратиться за подробностями. Ниже ссылка, по которой надо активировать письмо, чтобы запросить выплату.

Письмо оформлено один в один как официальная рассылка портала и написано таким казенным языком. Я уже почти нажала на ссылку, но вдруг вспомнила свою знакомую. Ей как-то тоже пришло сообщение о компенсации. Она обрадовалась, зашла на какой-то сайт, ввела там данные своей карты, чтобы получить деньги — а их у нее списали вместо того чтобы начислить.

Решила приглядеться повнимательнее. Оформлено все красиво, а вот в содержании письма какая-то каша: ссылаются то на номер приказа, то на номер постановления. Предлагают по всем вопросам обратиться к «оператору из Центрального РОСП», я погуглила — это судебные приставы. Причем тут соцвыплаты?

Покопалась еще: забила в поиск прямо номер этого прекрасного постановления — а там куча отзывов от других людей. Пишут, что им приходят такие же письма и что это мошенники. Хорошо, что я вовремя остановилась. И других хочу предостеречь.

**Совет эксперта по противодействию мошенничеству:**

Мошенники постоянно рассылают подобные «письма счастья» от имени известных организаций. Они рассчитывают, что человек обрадуется внезапным выплатам, потеряет бдительность и перейдет по ссылке.

Но делать этого ни в коем случае нельзя. Кликнув по ссылке, пользователь рискует скачать опасный вирус, который украдет персональные и платежные данные с его устройства.

Либо человек попадает на фишинговый сайт, замаскированный под официальный Портал госуслуг или какой-либо другой известный ресурс. Там пользователя часто просят ввести номер СНИЛС, ИНН, паспортные данные или другую информацию, чтобы якобы «подать заявку на социальную компенсацию» или «проверить размер выплат».

Мошенники под любым предлогом стремятся выманить конфиденциальную информацию. И затем могут использовать ее, например, чтобы оформить кредит на чужое имя.

Для получения обещанной социальной выплаты человеку предлагают ввести полные реквизиты карты — включая срок действия, три цифры с оборота, коды и пароли из банковских уведомлений. Якобы эти данные нужны «для перевода денег» или «для оплаты небольшой комиссии».

Если владелец карты укажет эту информацию, то преступники получат доступ к его счету и смогут украсть все, что там есть. А банк ничего не компенсирует клиенту, ведь он добровольно сообщил секретные данные аферистам.

Обезопасить свои деньги и данные помогут правила кибербезопасности:

- Никогда не переходите по ссылкам из сомнительных сообщений — лучше сразу их удаляйте, не вводите секретную информацию на подозрительных сайтах. Как отличить официальные ресурсы от подделок, читайте в тексте «Безопасные покупки в интернете».

- Перепроверяйте информацию. Получив письмо от имени известной организации о внезапных компенсациях, конкурсах и других аттракционах невиданной щедрости, постарайтесь найти сообщение в первоисточнике. Зайдите на официальный сайт организации, позвоните туда, поищите информацию о выплатах в ведущих СМИ.

- Установите антивирусы на всех своих гаджетах — это поможет защитить их от вредоносных программ и спама.