

Россиянам рассказали, как определить письмо с вредоносным ПО на электронной почте

Электронные письма от злоумышленников можно вычислить по нескольким признакам, предупреждает руководитель группы спам-анализа «Почты Mail» Дмитрий Моряков. По его словам, насторожить должны вложения в таких форматах, как zip, rar, doc, xls, а также exe, scr и js. Эти файлы часто связаны с [вредоносным ПО](#). Моряков советует избегать открытия подозрительных вложений, особенно если они сопровождаются призывами вроде «посмотреть срочно» или «подтвердить данные».

Эксперт отмечает, что злоумышленники иногда используют уловки вроде грамматических ошибок или замены букв в адресах отправителей. Например, букву «о» могут заменить на цифру «0». Ещё один сигнал опасности — адрес отправителя, который выглядит легитимно, но содержит мелкие искажения. Если вы замечаете такие признаки, это может быть социальной инженерией — методикой, которая основывается на манипуляции психологией человека.

Чтобы защититься от мошенничества, Моряков рекомендует не открывать подозрительные вложения, избегать перехода по сомнительным ссылкам и не вводить личные данные. Использование антивирусного и антифишингового ПО, а также регулярное обновление программ помогут снизить риск вредоносных атак.