Эксперты предупреждают россиян о рисках, связанных с вредоносными вложениями в электронных письмах. Злоумышленники часто используют определенные типы файлов для распространения вирусов и других угроз. Такие вложения могут быть в форматах zip, rar, doc, xls, а также exe и других исполняемых файлов.

По словам специалиста Дмитрия Морякова из «Почты Mail», стоит насторожиться, если файл имеет необычные расширения или сочетания форматов. Особенно опасными считаются архивы, а также файлы с расширениями .exe, .scr, .bat, .vbs и .js, которые часто связаны с вредоносным ПО. Он также добавил, что файлы форматов pdf и docx реже используются в мошенничествах, поскольку пользователи научились их распознавать.

Еще один признак мошенничества — это странный отправитель, искаженные адреса или ошибки в тексте письма. Мошенники могут использовать психологические приемы, требуя от получателя срочно открыть файл или подтвердить информацию. Эксперт советует не открывать вложения от незнакомых отправителей и не переходить по сомнительным ссылкам.

Для защиты от таких угроз рекомендуется использовать антивирусные программы и антифишинговое ПО, а также регулярно обновлять системы безопасности.