

Дополнительные меры по повышению защищенности информационной инфраструктуры

В целях обеспечения устойчивого функционирования автоматизированных рабочих мест, имеющих доступ в сеть «Интернет», и предотвращения реализации угроз безопасности информации, связанных с фишингом необходимо:

Внимательно проверять адреса отправителя, даже в случае совпадения имени с уже известным контактом;

Проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

проверять ссылки, содержащихся в электронном письме, даже если письмо получено от другого пользователя (известного Вам пользователя) информационной системы;

особо внимательного отношения к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

пересылать письма, которые могут содержать вредоносное содержание (ссылку или вложение) на почту virus1979@internet.ru.