Внимание! Работникам образовательной организации.

В целях обеспечения устойчивого функционирования автоматизированных рабочих мест, имеющих доступ в сеть «Интернет»\. И предотвращении реализации угроз безопасности информации, связанных с фишингом (электронные письма, содержащие вредоносные вложения в виде ссылок на вредоносные файлы, маскирующиеся под документы Microsoft Word или PDF), необходимо регулярно применять следующие дополнительные меры защиты информации.

- **Проверка адреса отправителя, даже в случае совпадения имени с уже известным контактом;**
- **Проверка писем, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;**
- **Проверка ссылок, содержащихся в электронном письме, даже если письмо получено от другого пользователя информационной системы;**
- **Внимательного отношения к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;**
- **Осуществлять проверку всех поступающих на почту вложений с использованием средств антивирусной защиты. Обновить базу антивирусной защиты до актуальных версий.**
- **Использовать для работы с электронной почтой учетные записи пользователей операционной системы с минимальными возможными привилегиями.**