# Правила обращения с входящей электронной корреспонденцией

Чтобы снизить потенциальные риски и обеспечить безопасность на рабочих местах, просим вас с осторожностью относиться к письмам от незнакомых и подозрительных адресатов. Прежде чем открывать такое сообщение, убедитесь, что вы следуете правилам работы с электронными сообщениями:

1. Если вы получили письмо от незнакомого или подозрительного отправителя, проверьте его адрес. Официальные сообщения обычно отправляются с адресов, заканчивающихся на доменах известных организаций. Вы можете выполнить дополнительную проверку, связавшись с получателем по другим каналам и сравнив адреса. Обращайте внимание на опечатки и другие ошибки в адресах - они могут указывать на мошенничество.
2. Всегда обращайте внимание на тему письма. Она должна соответствовать содержанию и относиться к вам. Злоумышленники могут использовать темы, которые кажутся привлекательными или важными, чтобы обманом заставить вас открыть вложение или перейти по ссылке.
3. Если письмо содержит непонятные вопросы или предложения, это может указывать на попытку мошенничества.
4. Прежде чем перейти по ссылке, убедитесь, что она ведет на нужный вам сайт и не содержит странных символов, таких как #, $, &. Подозрительные ссылки могут представлять опасность.
5. Не загружайте на свои устройства подозрительные документы Microsoft Office, прикрепленные к электронным письмам, полученные от неизвестного отправителя. Многие вирусы и шпионские программы распространяются через вложения и ссылки в письмах.

# Если письмо соответствует вышеуказанным критериям, сообщите о нем на [электронный адрес: oz](mailto:ozi@cit.gov35.ru)[i@cit.gov35.ru](mailto:i@cit.gov35.ru)