



# **Task 2:** Analyze a Phishing Email Sample



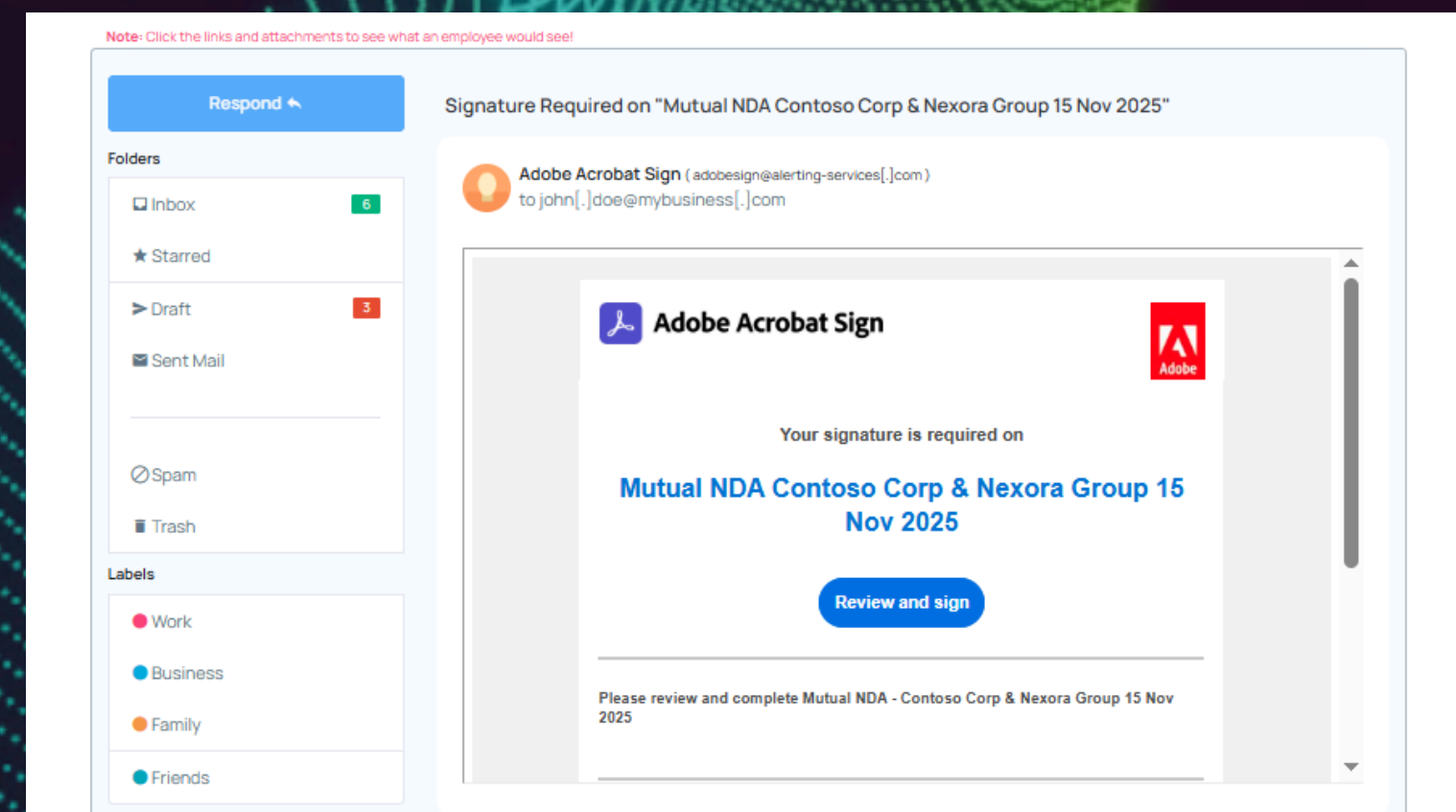




# 1.OBTAIN A SAMPLE PHISHING EMAIL (MANY FREE SAMPLES ONLINE)

## Email Overview

- Email Subject: *Signature Required on 'Mutual NDA Contoso Corp & Nexora Group 15 Nov 2025'*
- Sender Display Name: *Adobe Acrobat Sign*
- SenderEmailAddress: *adobesign@alerting-services[.]com*
- Recipient: *john[.]doe@mybusiness[.]com*







## 2.EXAMINE SENDER'S EMAIL ADDRESS FOR SPOOFING.

### Suspicious Indicators:

- Adobe Sign's legitimate domain is: @adobesign.com or @adobe.com
- Sender used: @alerting-services.com (unrelated domain)

This is clear spoofing designed to trick victims into clicking the "Review and sign" button.

- Generic domain name is not an Adobe-owned service
- The attacker purposely uses a trusted brand (Adobe Sign) in the display name







### 3.CHECK EMAIL HEADERS FOR DISCREPANCIES (USING ONLINE HEADER ANALYZER).

Using the MXToolbox Email Header Analyzer, I found multiple discrepancies indicating phishing:

- Sender domain not authorized: The domain used to send the email is not permitted to send messages on behalf of Adobe.
- Domain does not match sender identity: The “From” name claims Adobe Sign, but the actual sending domain is different.
- Received-from IP is not an Adobe server: The originating IP address does not belong to Adobe’s legitimate mail servers.

These authentication failures clearly show the email is spoofed and fraudulent.







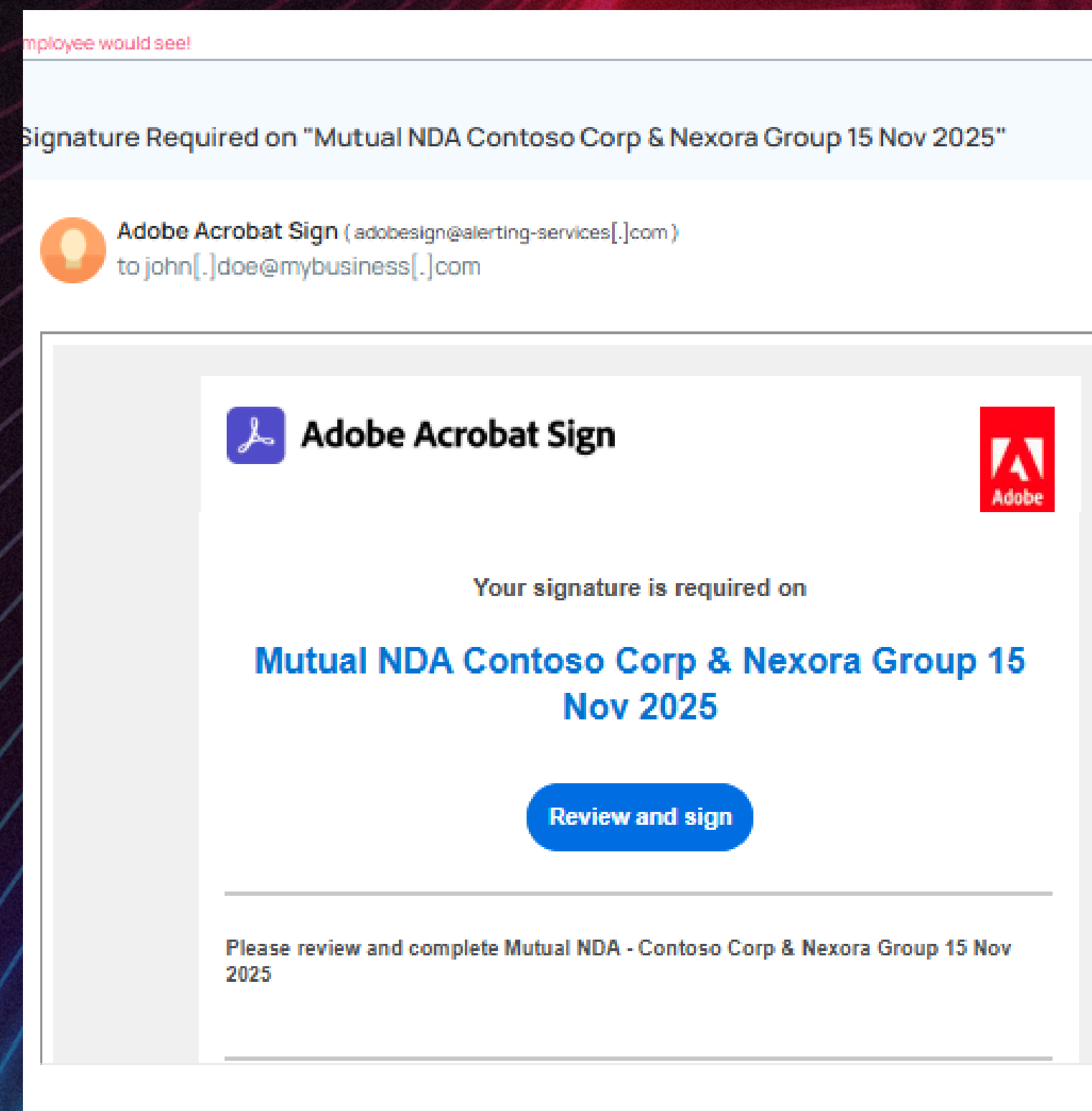
## 4.IDENTIFY SUSPICIOUS LINKS OR ATTACHMENTS.

In the email:

Button: “Review and sign”

Indicators:

- The button text pretends to be Adobe Sign
- Hovering over the link (in a real email) would show a non-Adobe URL





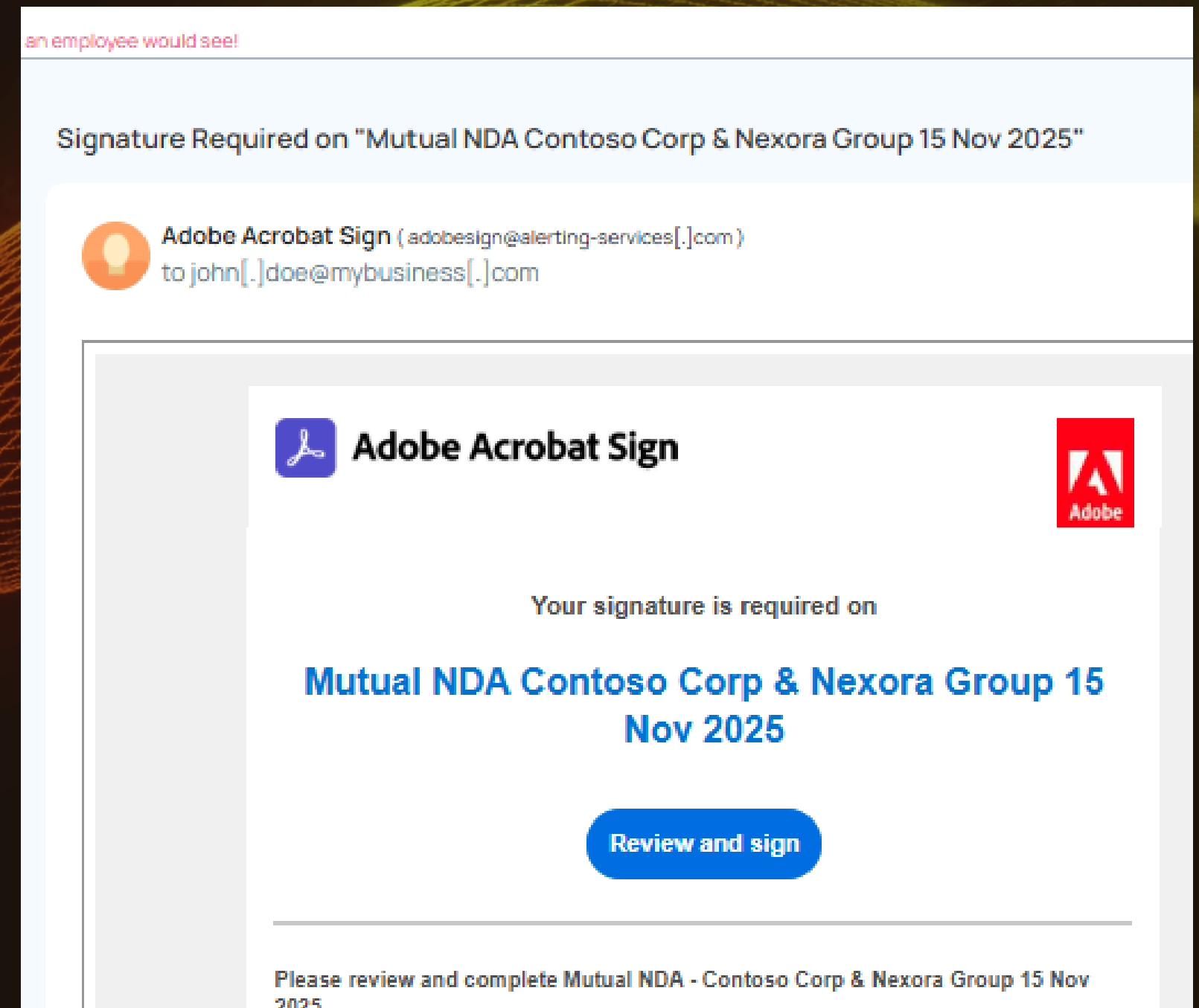


## 5. LOOK FOR URGENT OR THREATENING LANGUAGE IN THE EMAIL BODY.

Examples:

“Your signature is required”

- A time-sensitive legal request (NDA)
- Creates pressure so the victim acts quickly without thinking
- Urgency to bypass critical thinking.



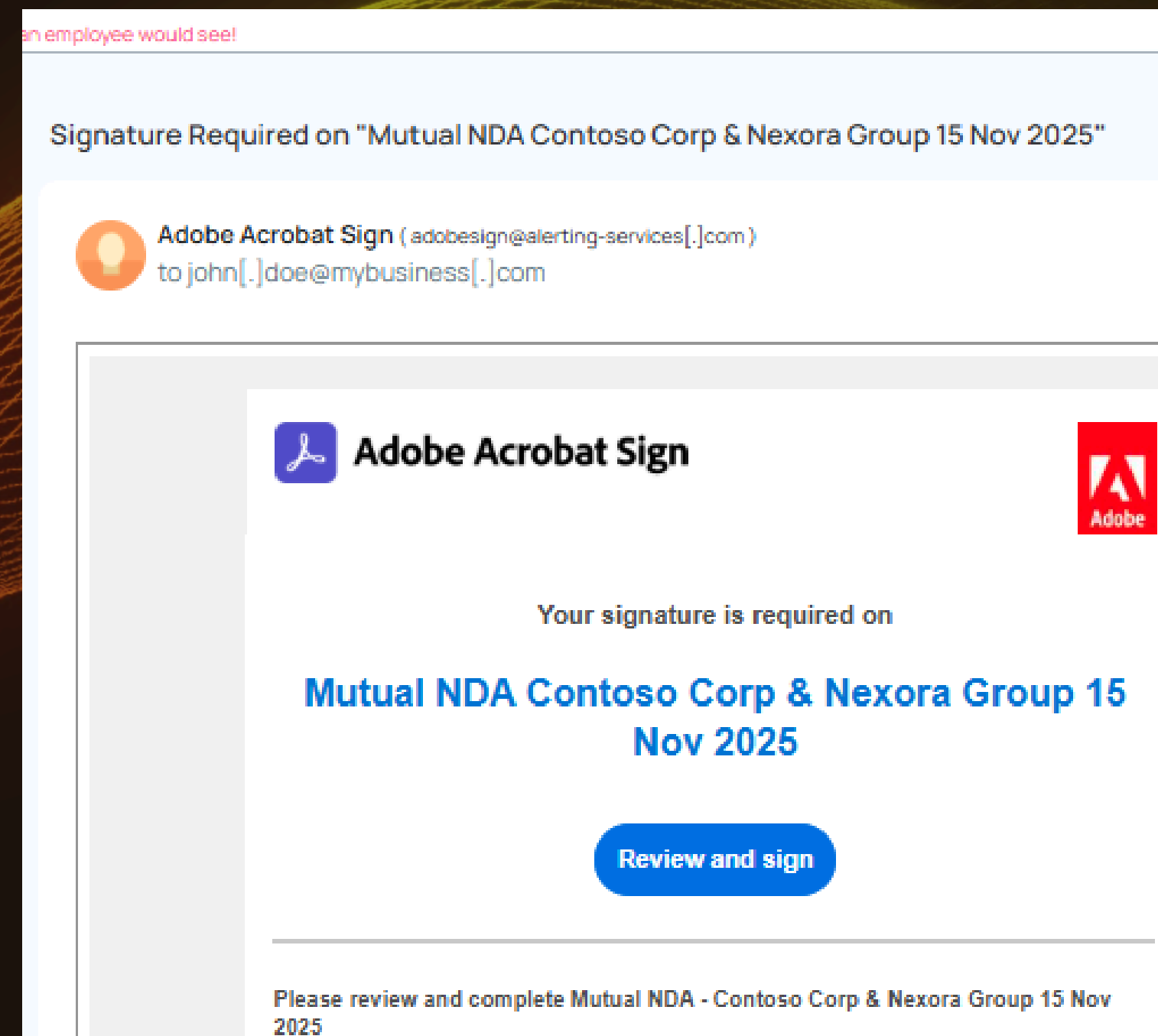


## 6. NOTE ANY MISMATCHED URLS (HOVER TO SEE REAL LINK).

Real Adobe Sign links always use:

- <https://secure.adobesign.com/>
- <https://documentcloud.adobe.com/>

The email uses a button with an unknown link, which is a suspicious trick.





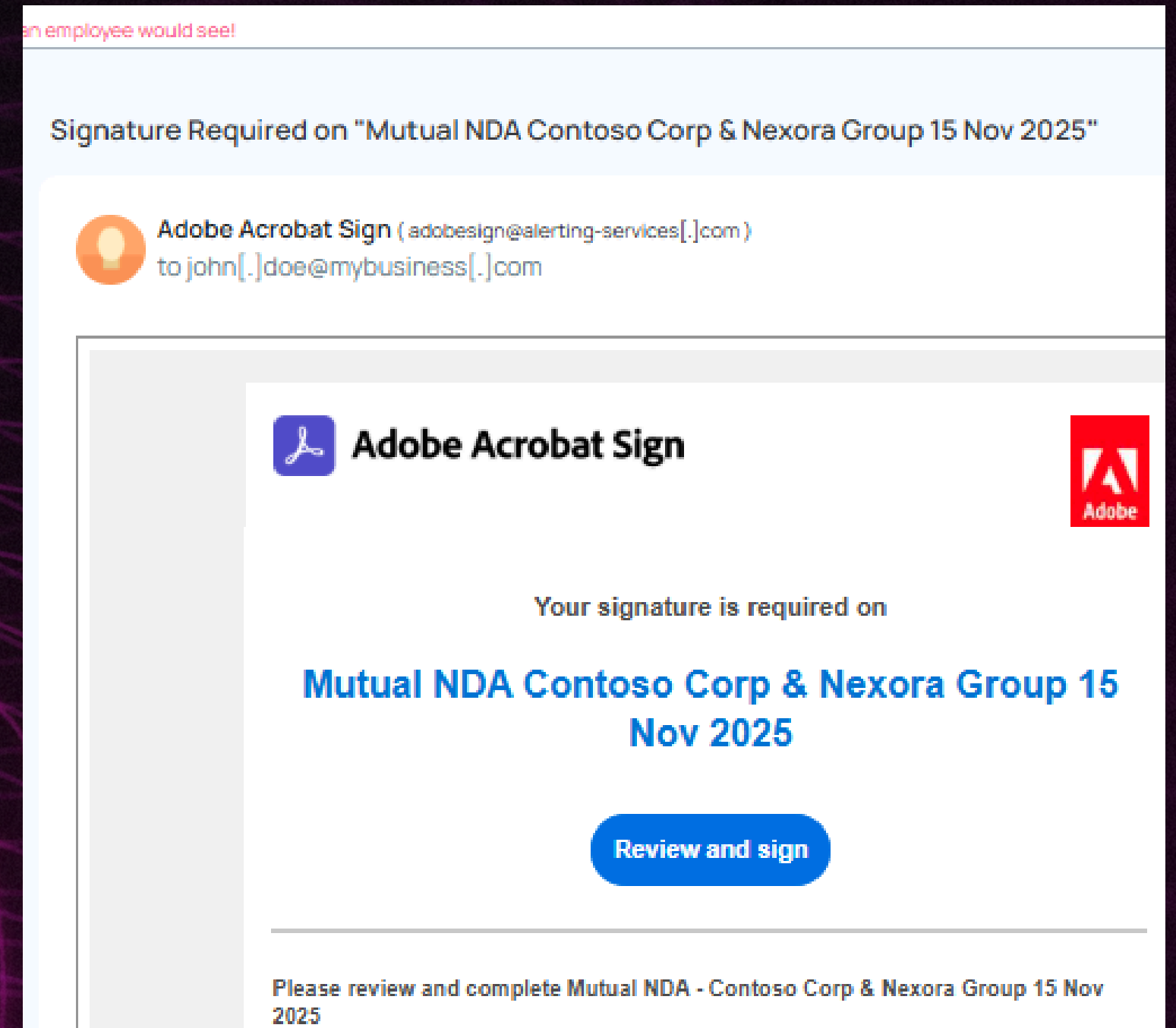


## 7. VERIFY PRESENCE OF SPELLING OR GRAMMAR ERRORS

The email looks professional, however it contains subtle issues:

- Odd phrasing: “Please review and complete Mutual NDA - Contoso Corp & Nexora Group 15 Nov 2025”
- Layout not consistent with real Adobe notifications
- Generic placeholder names (e.g., “John Doe”)

Real Adobe emails use standardized, consistent templates







## 8.SUMMARIZE PHISHING TRAITS FOUND IN THE EMAIL.

The email shows several signs of phishing. The sender's email address is fake, the message creates unnecessary urgency, and the link directs to a suspicious website instead of Adobe. Parts of the email also look unusual or poorly written. The header analysis shows it failed important security checks. Together, these signs clearly prove that the email is a phishing attempt.







# THANK YOU