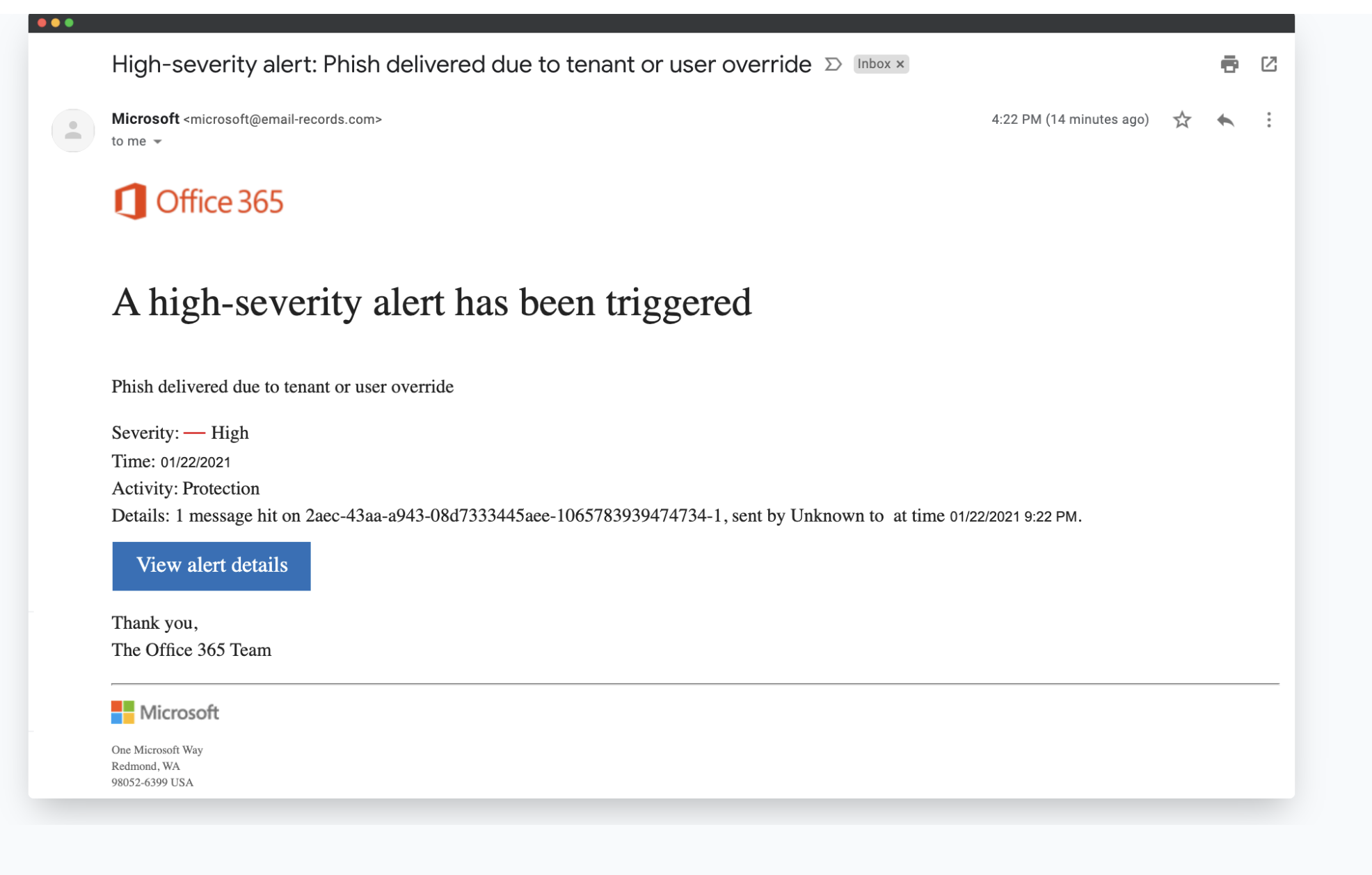
TASK – 2 Email Phishing Analysis



2. Examine Sender's Email Address for Spoofing:

* The sender address is [microsoft@email-records.com](mailto:microsoft@email-records.com).
* Analysis: This is not an official Microsoft domain (should be something like @microsoft.com or @office.com).
* Conclusion: This is a classic case of domain spoofing, meant to deceive the recipient by resembling a real Microsoft address.

3. Check Email Headers for Discrepancies (using online header analyzer)

* Copying the full raw email headers and paste them into an online email header analyzer (like Trustifi or MXToolbox).
* Check if “From” and “Return-Path” domains match.
* Verify SPF and DKIM authentication results.
* Examine the email’s journey—does it come from Microsoft’s servers?
* Analysis for this sample: Since the domain is already fake, these checks would likely reveal a failed or missing authentication and show the email did not originate from a Microsoft IP. As the example is taken from an online source there is no full details about the header function.

4. Identify Suspicious Links or Attachments

* Observation: There is a prominent “View alert details” button.
* Hovering over the button to reveal the true destination URL.
* Analysis: The real link will likely not go to an official Microsoft website; phishing links often lead to credential-stealing pages.

## 5. Look for Urgent or Threatening Language in the Email Body

* Phrases used:
  + “A high-severity alert has been triggered.”
  + “Phish delivered due to tenant or user override.”
* Analysis: The message is designed to induce urgency and worry, prompting the user to click the button quickly without thinking.

## 6. Note Any Mismatched URLs (Hover to See Real Link)

* Hover your mouse over any links to compare displayed text to the actual URL.
* Suspicious signs: If the link’s visible text claims to go to Microsoft but the actual destination is unrelated, it’s a phishing trait.
* In this case: The message tries to look like it's from Office 365/Microsoft but will almost certainly link somewhere else.

## 7. Verify Presence of Spelling or Grammar Errors

* Observation: This email is more sophisticated and contains professional-looking text (common in higher-quality phishing), but the generic “sent by Unknown to at time…” is awkward and suspicious.
* Analysis: Phishing emails often contain formatting issues or awkward language, either due to automation or because the attacker is not a native speaker.

## Summarizing Phishing Traits Found in the Email:

Phishing Traits in our Sample:

* Sender domain is spoofed and not official Microsoft.
* Email header and domain likely fail authentication.
* Email uses urgent, alarming language to provoke fast action.
* Suspicious button likely links to a phishing site.
* Generic email body lacking user-specific info and with formatting issues.
* Possible mismatched URL on the action button.
* Signs of poor data integration ("sent by Unknown...").