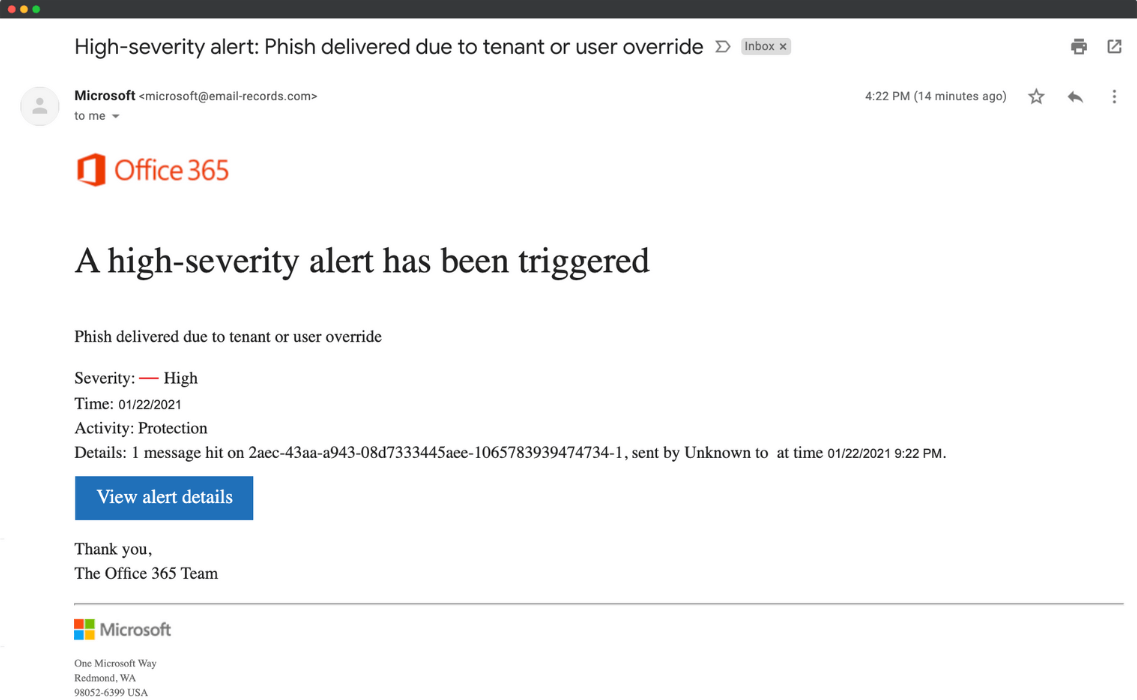
Sample phishing email

TASK-2



* **Spoofed Sender Address**

Appears as microsoft@email-records.com, which is not an official Microsoft domain.

* **Suspicious Email Headers**

Shows "sent by Unknown", indicating poor routing.

* **Suspicious Link or Button**

The "View alert details" button likely leads to a malicious or fake site (common phishing bait).

* **Urgent or Threatening Language**

Phrases like "High-severity alert" and "Phish delivered" are designed to create panic.

* **Mismatched or Inconsistent Details**

Body shows time as 9:22 PM but email received at 4:22 PM. Vague terms like “1 message hit” with no clear reference.

* **Generic Content (No Personalization)**

Email does not address you by name. Real alerts from Microsoft include personal info.

* **No Obvious Spelling or Grammar Errors**

Language is mostly correct but lacks the professionality expected from Microsoft.