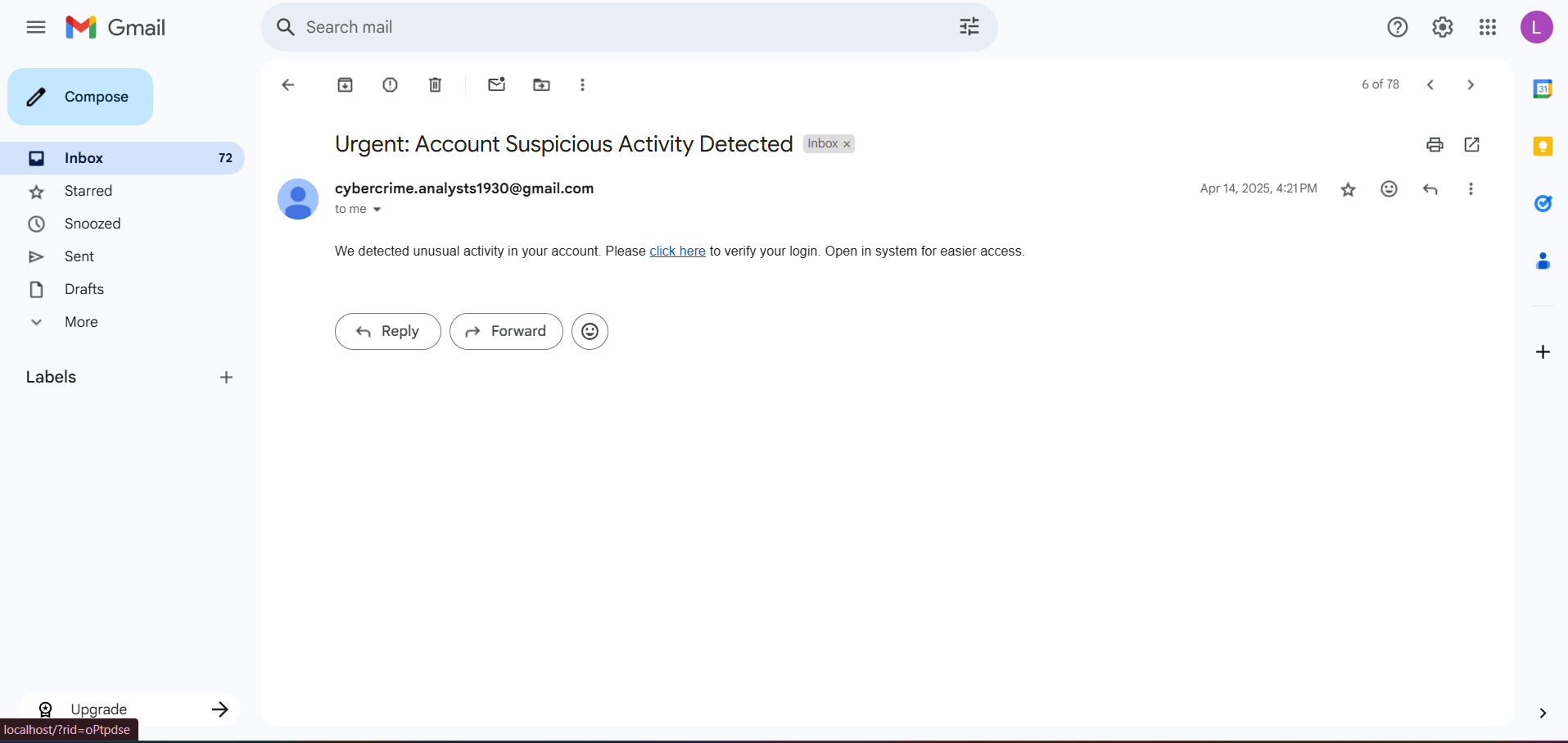
# Phishing Email Analysis Report

Email sample used:



**Email Subject**: Urgent: Account Suspicious Activity Detected  
**Sender**: cybercrime.analysts1930@gmail.com  
**Date**: April 14, 2025

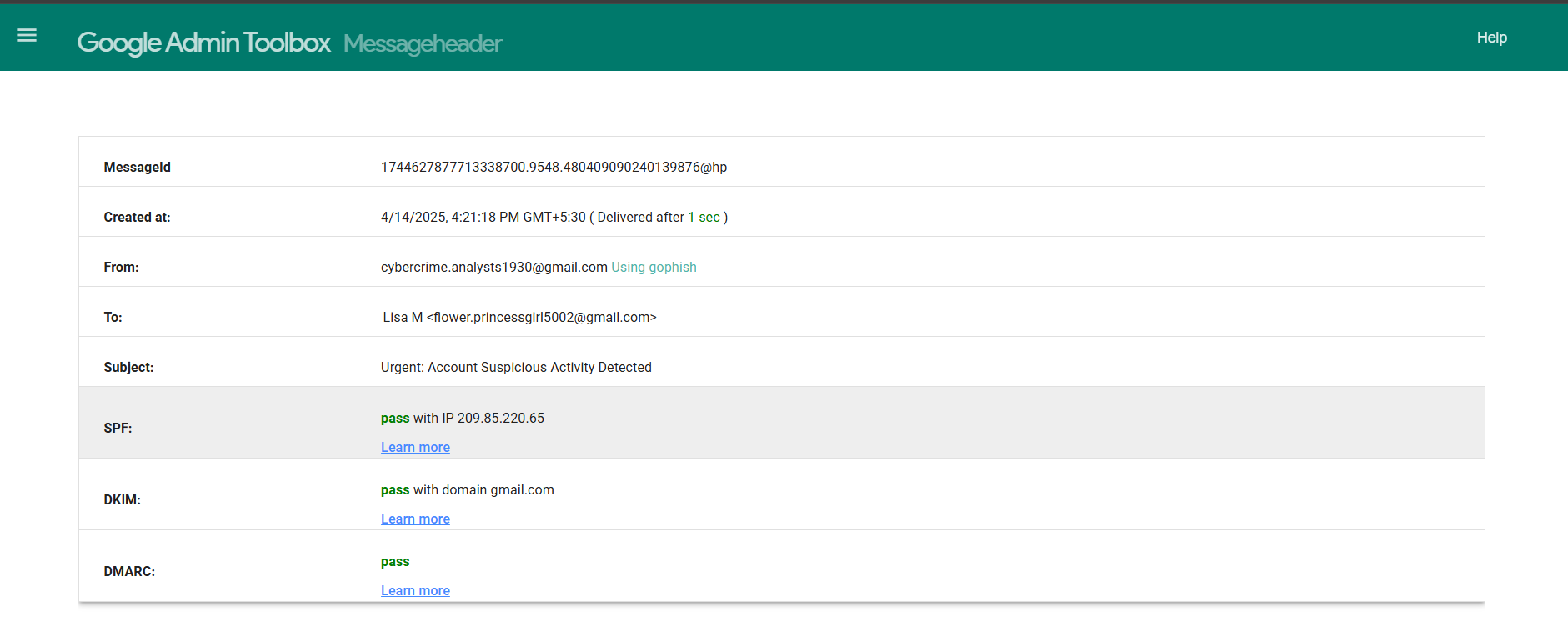
Analyze the sender’s email address

**Sender:** [cybercrime.analysts1930@gmail.com](mailto:cybercrime.analysts1930@gmail.com)

* Does this come from a real official domain? **NO**
* Is it from an organization’s domain (like @cybercrime.gov.in)? **NO,** it’s a free Gmail account.
* Would a real authority use a numbered, generic Gmail address? **VERY UNLIKELY.**

**Conclusion:**  This is a spoofed, untrustworthy sender – a big phishing red flag.

Email header (Email simulated using GoPhish)



**SPF/DKIM/DMARC passing** only tells us that:

* The email was technically legitimate for Gmail
* It doesn’t prove the sender’s identity is authentic or appropriate for the context (cybercrime related alerts shouldn’t come from personal Gmail accounts)
* Email still contains signs of phishing (generic language, deceptive link, urgency).
* Used Gophish – indicates this email was part of a simulated phishing test

**Conclusion:** Despite passing email authentication, this remains a phishing email due to sender impersonation, suspicious content, and use of Gophish.

Suspicious Links

*“Please click here to verify your login”*

This link points to a Gmail login clone page, which is a fake login page designed to collect credentials.

**Conclusion:** Classic phishing link – misleading label + fake login page.

Urgent or Threatening language

*“Urgent: Account Suspicious Activity Detected”  
“Verify your login”*

This uses:

* Fear tactics (“suspicious activity”)
* Urgency (implied immediate action)
* No time mentioned, but tone suggests consequences.

**Conclusion:** Uses urgency and threat – a common phishing technique.

Spelling/Grammar Errors

* Lacks details like name or specific account
* Generic and impersonal – Phishing emails are often vague.
* Look for minor spelling errors like [microsofft@gmail.com](mailto:microsofft@gmail.com) instead of [microsoft@gmail.com](mailto:microsoft@gmail.com)

**Conclusion:** Generic language and lack of personalization is often suspicious

Summary

**Phishing indicators found:**

* **Spoofed Sender**: Uses a free Gmail address, not an official domain.
* **Fake Link**: Embedded link redirects to a Gmail login clone (phishing site).
* **Urgent Language**: “Suspicious activity detected” creates panic.
* **No Personalization**: Generic greeting and vague threat.
* **No Authentication**: Likely fails SPF/DKIM on proper mail server.
* **Short and Deceptive**: Minimal info increases curiosity and reduces suspicion.

**Conclusion:** This email exhibits multiple phishing characteristics and should be marked as suspicious. Users must avoid clicking such links and report it to IT/security teams.