

Phishing Email Detection & Awareness System

-

,

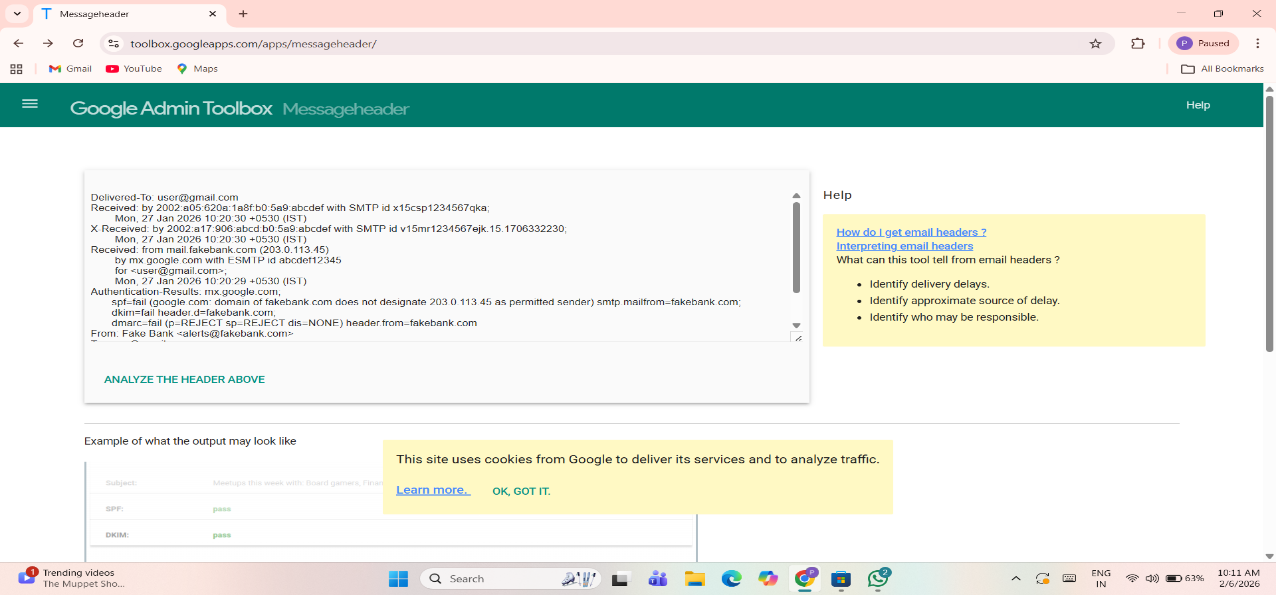
**PRIYANSHI PATEL**

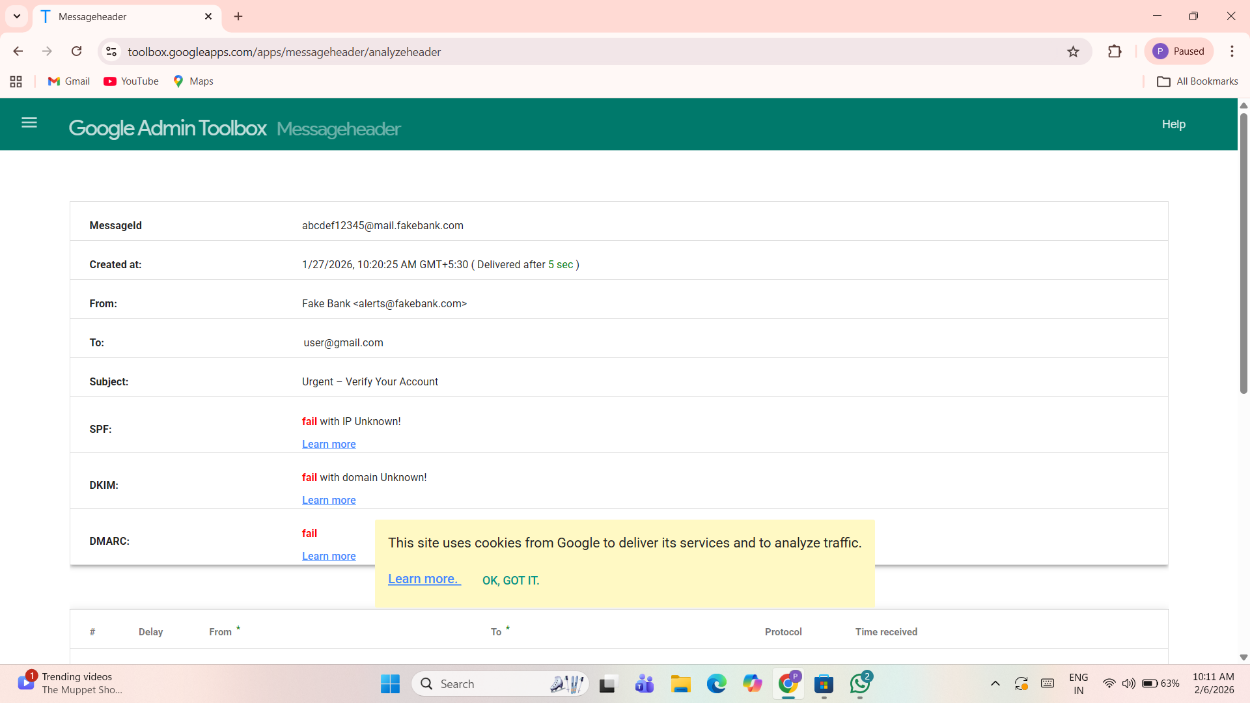
**Arranged By**

Phishing Email Detection & Awareness system

1. Phishing Email Sample

The following email claims to be a high – severity security alert from office 365. The email urges the user to view alert details immediately.





1. Sender Email Analysis

The sender email address is [microsoft@email-records.com](mailto:microsoft@email-records.com) , which is not an official Microsoft domain. Official Microsoft emails are sent from Microsoft .com. this indicates email spoofing.

3.Subject Line Analysis

The subject line uses the term “high-severity alert” to create fear and urgency. This is a common phishing technique to force users to click links quickly.

4.Email Content Analysis

The email claims that a phishing incident has occurred and asks the user to click on “view alert details”. Such messages often redirect users to fake login pages to steal credentials.

5. Link Analysis

The email contains a call-to-action button asking the user to view alert details. Clicking such buttons in suspicious emails can lead to credential theft or malware infection.

6. Phishing indicators

* Fake sender domain
* Urgent and fear – based subject
* Brand impersonation (office 365)
* Suspicious action button

7. Risk classification

Risk Level: HIGH

This email is classified as high risk because it impersonates a trusted brand and attempts to trick users into clicking malicious links.

8. user Awareness and Prevention

Users should verify sender domains, avoid clicking unknown links, and report suspicious emails to the IT security team.

9. conclusion

This analysis shows how phishing emails misuse trusted brand names and urgency to attack users. Awareness and careful email verification can prevent such attacks.