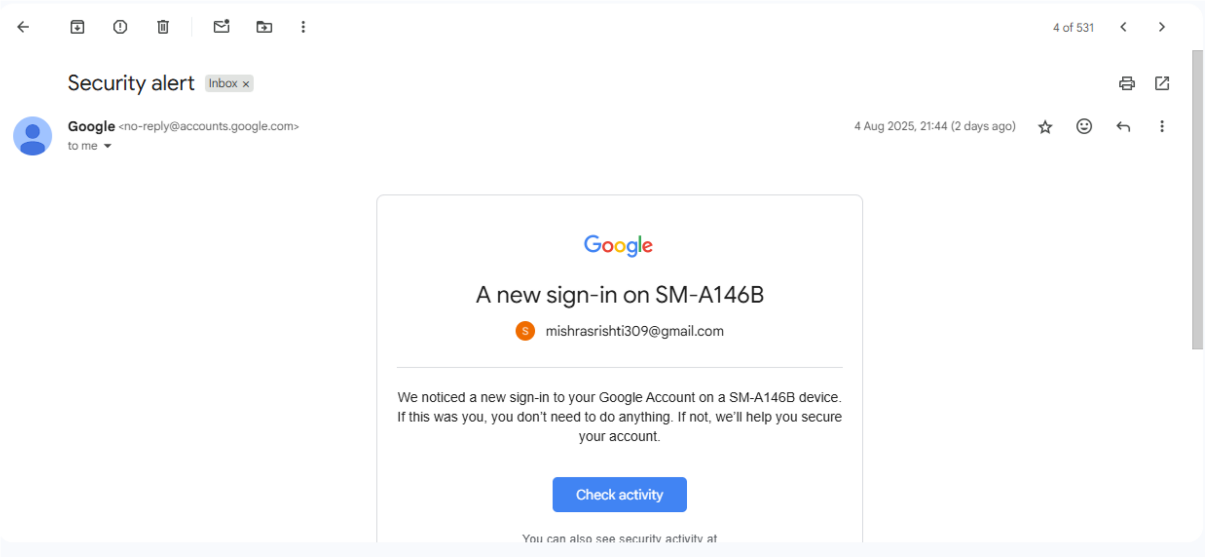
Task 2

1. Analyze a Email Sample



Security alert

Google <no-reply@accounts.google.com>

4 Aug 2025, 21:44 (2 days ago)

Google

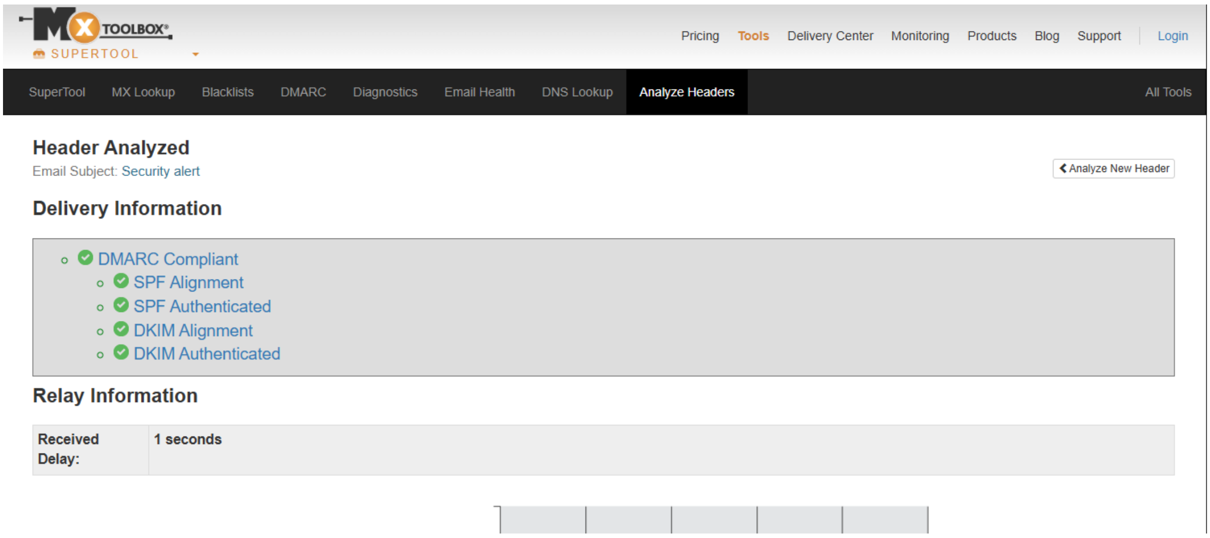
A new sign-in on SM-A146B

S mishrasrishti309@gmail.com

We noticed a new sign-in to your Google Account on a SM-A146B device. If this was you, you don't need to do anything. If not, we'll help you secure your account.

You can also see security activity at

2.Analyse header using mx toolbox



Header Analyzed

Email Subject: Security alert

Delivery Information

- ✓ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✓ DKIM Authenticated

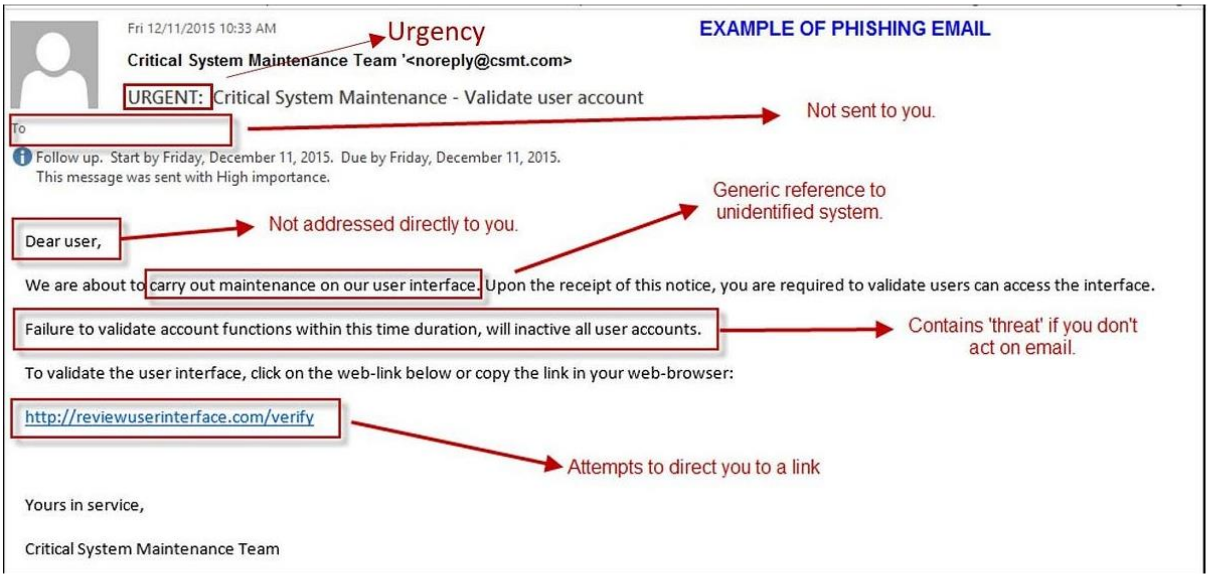
Relay Information

Received Delay:	1 seconds

In the above scenario SPF, DKIM and DMARC all passed ,so its not phishing attempt.

If **SPF**, **DKIM**, and **DMARC** all fail, or if the IP is from an unexpected region, **it's very likely a phishing attempt**.

3.Example of phishing email:-



EXAMPLE OF PHISHING EMAIL

Fri 12/11/2015 10:33 AM

Critical System Maintenance Team '<noreply@csmt.com>

URGENT: Critical System Maintenance - Validate user account

To

Follow up. Start by Friday, December 11, 2015. Due by Friday, December 11, 2015.
This message was sent with High importance.

Dear user,

We are about to carry out maintenance on our user interface. Upon the receipt of this notice, you are required to validate users can access the interface.

Failure to validate account functions within this time duration, will inactive all user accounts.

To validate the user interface, click on the web-link below or copy the link in your web-browser:

http://reviewuserinterface.com/verify

Yours in service,

Critical System Maintenance Team

Urgency

Not sent to you.

Generic reference to unidentified system.

Not addressed directly to you.

Contains 'threat' if you don't act on email.

Attempts to direct you to a link

Summary of Phishing Traits Found in the Email

- **Spoofed Sender Address:** Domain mimics a legitimate one (e.g., paypa1.com instead of paypal.com).
- **Suspicious Links:** URLs redirect to fake websites designed to steal credentials.
- **Generic Greeting:** Uses "Dear Customer" instead of your name — lacks personalization.

- **Urgent or Threatening Language:** Creates pressure with messages like “Account will be suspended in 24 hours.”
- **Spelling and Grammar Errors:** Words like “limeted” and awkward sentence structure reduce credibility.
- **Mismatched URLs:** Hovered links do not match the visible link text.
- **Unusual Attachments:** Includes suspicious HTML file or forms designed to capture sensitive data.
- **Fake Account Notifications:** Claims of access restrictions without any real verification.
- **Lack of Security Signs:** No official branding, secure HTTPS links, or verified contact info.