Task 2: Identifying Phishing Emails

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Saved email file (text), free online header analyzer.

We have Our Suspected Phishing Email as Follow:

```
From: paytm-security@paytmsupport.co.in
Subject: Action Required: Paytm Account Blocked

Dear User,

We have detected unusual activity on your Paytm wallet.
To ensure your security, we have temporarily suspended your Paytm services.
Please verify your identity immediately to restore access.

Click below to verify:
http://paytm-verifywallet.com/login

If you fail to verify within 12 hours, your account will be permanently disabled.

Thank you,
Paytm Support Team
```

We Could Identify and Verify the above Email Using:

1.Senders Email Address Check:

- Displayed email: paytm-security@paytmsupport.co.in
- Legitimate domain: @paytm.com
- Spoofing indicators: Uses a lookalike domain paytmsupport.co.in instead of the real paytm.com
- Red flag: Official Paytm support never uses .co.in domains for security emails

2. Analysing Email Header Through Email Header Analyser tool (Mx Toolbox)

- Return-Path: reply@customersupport-mail.xyz
- SPF/DKIM/DMARC: SPF Failed, DKIM Missing, DMARC Policy Reject
- Origin IP: Registered in Eastern Europe (unusual for Indian service)
  Header reveals forged sender and failed authentication

3. Suspicious Links or Attachments:

- Displayed Link: http://paytm-verifywallet.com/login
- Not an official Paytm domain
- Uses HTTP (not secure), and impersonates Paytm
- WHOIS data: Domain registered 2 days ago, owner hidden with privacy proxy
    - Clearly a phishing link designed to steal credentials
    - We can also hover over a link to check its URL if disguised

4. Urgent or Threatening Language:

- "Action Required"
- "Account Blocked"
- "Verify within 12 hours or permanent disablement"
    - Typical pressure tactics used in phishing to trigger panic

6. Mismatched URLs:

- Hovering over the link confirms: http://paytm-verifywallet.com/login ≠ https://paytm.com/
- No SSL certificate, hosted on suspicious IP
    - Mismatch between visible brand and real link destination

7.Spelling/Grammar Errors:

- Generic greeting (“Dear User”)
- Phrase like “Paytm services suspended” is unnatural wording
- Signature: “Paytm Support Team” (Paytm uses more formal branding)
    - Minor language inconsistencies that break authenticity

Conclusion:

This email is a classic phishing attempt targeting Paytm users. It uses spoofed domains, urgent language, a suspicious login link, and failed email authentication to trick users. It should be deleted immediately and reported to Paytm at cybercell@paytm.com.