

# Phishing Email Analysis Report

## 1. Email Metadata

- Subject: "Syllabus for the mid term" - Sender: Jaimol Thomas - Received via: siimindia.com (suspicious intermediary domain) - Date: Sat, Sep 20, 3:08 PM

## 2. Observed Phishing Indicators

- The email was flagged as SPAM by Gmail ("This message is similar to messages that were identified as spam in the past"). - Sender domain mismatch: Email appears from 'jaincollege.ac.in' but sent via 'siimindia.com'. - Unexpected attachment: PDF file named "Document (4).pdf" with a generic name is suspicious. - Generic message body: Only states "Syllabus of the mid term is attached below." with no personalization or context.

## 3. Risks Identified

- The attachment could contain malicious content (e.g., malware, phishing form). - The intermediary sending domain increases risk of spoofing. - Lack of detailed or personalized content suggests automated phishing attempt.

## 4. Recommended Actions

- Do not open the attached PDF until verified through a security tool (e.g., VirusTotal). - Verify the sender by contacting the institution (Jain College) through official channels. - Report this email to your organization's IT/security team or mark it as phishing in Gmail. - Delete the email after reporting if confirmed suspicious.

## 5. Conclusion

Based on the analysis, this email shows multiple phishing characteristics such as domain mismatch, suspicious attachments, and generic wording. It should be treated as potentially malicious.