Task 2: Analyze a Phishing Email Sample

# Objective

Identify phishing characteristics in a suspicious email sample to improve awareness of email-based threats.

# Tools Used

• Email dataset (SpamAssasin.csv)  
• Python (for data inspection)  
• Manual analysis

# Sample Email Analyzed

• Sender: tim.one@comcast.net (Tim Peters)

• Date: Fri, 06 Sep 2002 13:35:55 -0400

• Subject: [Spambayes] Deployment

• Body Summary: The email discusses Python tokenizer modules and coding practices. It seems like a collaborative technical discussion.

• Label: 0 (Indicating Ham/Not Spam)  
• URLs: 0 (No links present)

# Phishing Indicators Check

|  |  |
| --- | --- |
| Checkpoint | Findings |
| Spoofed Sender | Sender looks genuine, uses full name and ISP (comcast.net). Not obviously spoofed. |
| Header Issues | No visible red flags; full headers not available in this dataset. |
| Suspicious Links/Attachments | No links or attachments present. |
| Urgent/Threatening Language | No urgency or threats detected. |
| Mismatched URLs | No URLs to evaluate. |
| Grammar/Spelling Errors | Well-written technical content, no errors. |
| General Tone | Collaborative and informative — likely a discussion from a mailing list. |

# Conclusion

In Task 2, I analyzed a sample email for phishing indicators using structured email data. The sample reviewed showed no traits of phishing — it had a genuine sender, no suspicious links or attachments, and a professional tone.  
  
I learned how to:  
- Examine sender authenticity.  
- Use header data (if available) to check legitimacy.  
- Detect signs like urgency, grammar issues, or mismatched URLs.  
- Identify signs of spoofing or malware delivery attempts.  
  
This task improved my phishing awareness and email threat analysis skills.