**1. Obtain a Sample Phishing Email**

You can download safe examples from:

* **SpamAssassin public corpus**:  
  [https://spamassassin.apache.org/publiccorpus](https://spamassassin.apache.org/publiccorpus/)
  + Example: spam.tar.bz2 or phishing.tar.bz2
* **PhishTank** (for links only):  
  <https://www.phishtank.com/>

Once downloaded, open a .eml file in:

* **Thunderbird**
* **Outlook**
* Or analyze raw text content

🖼️ Screenshot Tip: Open the email in a viewer and take a screenshot of the suspicious parts.

**2. Examine the Sender's Email Address**

**Legitimate email?**  
If the sender claims to be from PayPal but the domain is something like:

css

CopyEdit

paypal-support@xyz123.ru

That’s a red flag.

**3. Analyze Email Headers**

Use an online tool:

* https://mxtoolbox.com/EmailHeaders.aspx
* https://toolbox.googleapps.com/apps/messageheader/

Check for:

* Return-Path mismatch
* Received headers showing unexpected source IPs or routing

🖼️ Screenshot Tip: Highlight mismatched "From" and "Return-Path".

**4. Check Links and Attachments**

* Hover over any links: real URLs should match the brand (e.g., paypal.com, not paypa1.com)
* Attachments: .exe, .zip, .html, .scr = suspicious

**5. Look for Urgent or Threatening Language**

Phishing emails often use pressure tactics:

“Your account will be suspended in 24 hours unless you verify…”

🧠 These appeal to fear or urgency.

**6. Spelling and Grammar Issues**

Professional companies rarely make typos like:

“You accont has been supended. Click hear to resolve.”

**7. Summary of Traits Found**

| **Trait** | **Found in Sample?** | **Notes** |
| --- | --- | --- |
| Spoofed sender address | ✅ | paypal-support@fake.ru |
| Suspicious link | ✅ | http://login.paypa1-security.com/verify |
| Grammar/spelling errors | ✅ | “click hear to secure” |
| Threatening tone | ✅ | “Your account will be locked in 24 hours” |
| Unusual attachment | ❌ | No attachment present in this sample |

