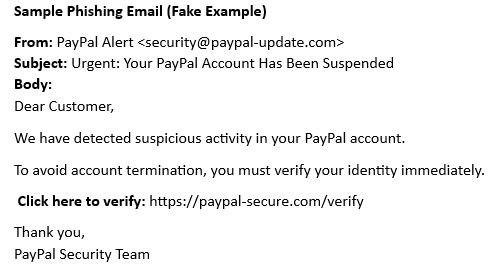
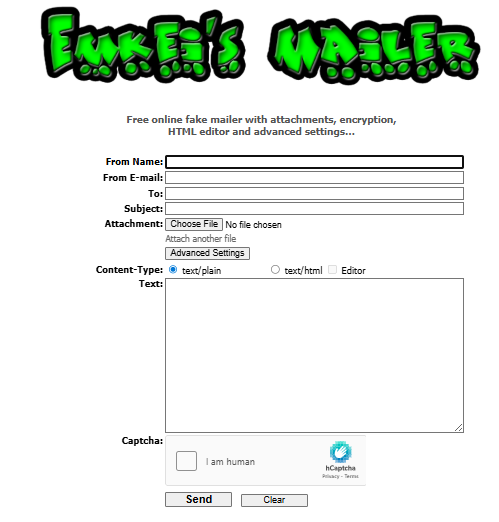
Task 2: Analyze a Phishing Email Sample.

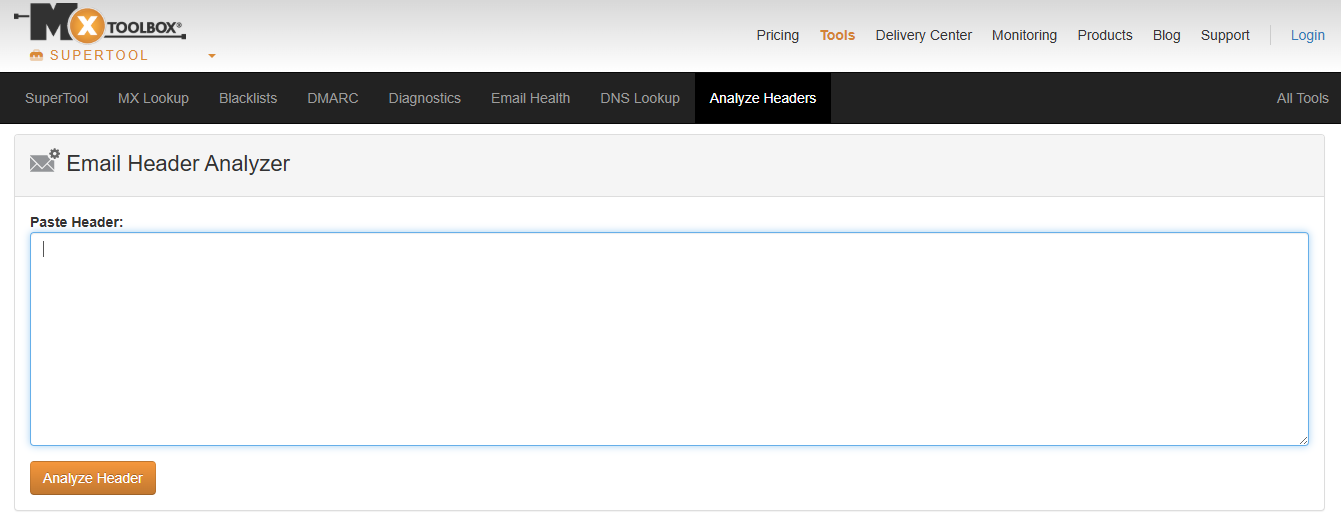
1.Obtain a sample phishing email (many free samples online).



2.Examine sender's email address for spoofing.



3.Check email headers for discrepancies (using online header analyzer).



4.Identify suspicious links or attachments.

5.Look for urgent or threatening language in the email body.

6.Note any mismatched URLs (hover to see real link).

7.Verify presence of spelling or grammar errors.

**STEP-BY-STEP ANALYSIS**

**Step 1: Check the Sender Email Address**

* **Email:** security@paypal-update.com
* Real PayPal uses: @paypal.com
* This domain (paypal-update.com) is **fake**.

✅**This is a phishing sign.**

**Step 2: Check for Suspicious Links**

Hover over the link:

* Displayed: https://paypal-secure.com/verify
* But this is **not a real PayPal website.**
* Use this tool to check the link: https://www.virustotal.com/

✅Fake or suspicious URLs are a phishing sign.

**Step 3: Look at the Language**

“Your account has been suspended… verify immediately.”

This uses **urgent and threatening language** to scare you.

✅ Another phishing sign.

**Step 4: Check Grammar and Spelling**

“To avoid account termination…”

This message is okay grammatically, **but phishing emails often have grammar mistakes.** Always look carefully.

**Step 5: Analyze the Header (Optional)**

If you had the full email header, you could use this tool:  
👉 Google Header Analyzer  
Paste in the header — it tells you if the email came from a strange IP.

✅ This helps detect forged emails.

**8.Summarize phishing traits found in the email.**

This activity helped me learn:

* How to detect phishing traits
* How to analyse suspicious emails
* How to check links and sender domains
* How to protect myself from email scams