1) **sample phishing email** you can use for your analysis (educational purposes only):

Subject: Urgent: Your Account Will Be Suspended Within 24 Hours

From: account-security@secure-paypal-support.com
To: user@example.com

Dear Customer,

We have detected unusual activity on your PayPal account and your access has been temporarily limited. To restore full access, please verify your account by following the secure link below:

👉 **Click here to verify your account**

Failure to verify your information within 24 hours will result in permanent suspension of your account.

Thank you for your prompt attention to this matter.

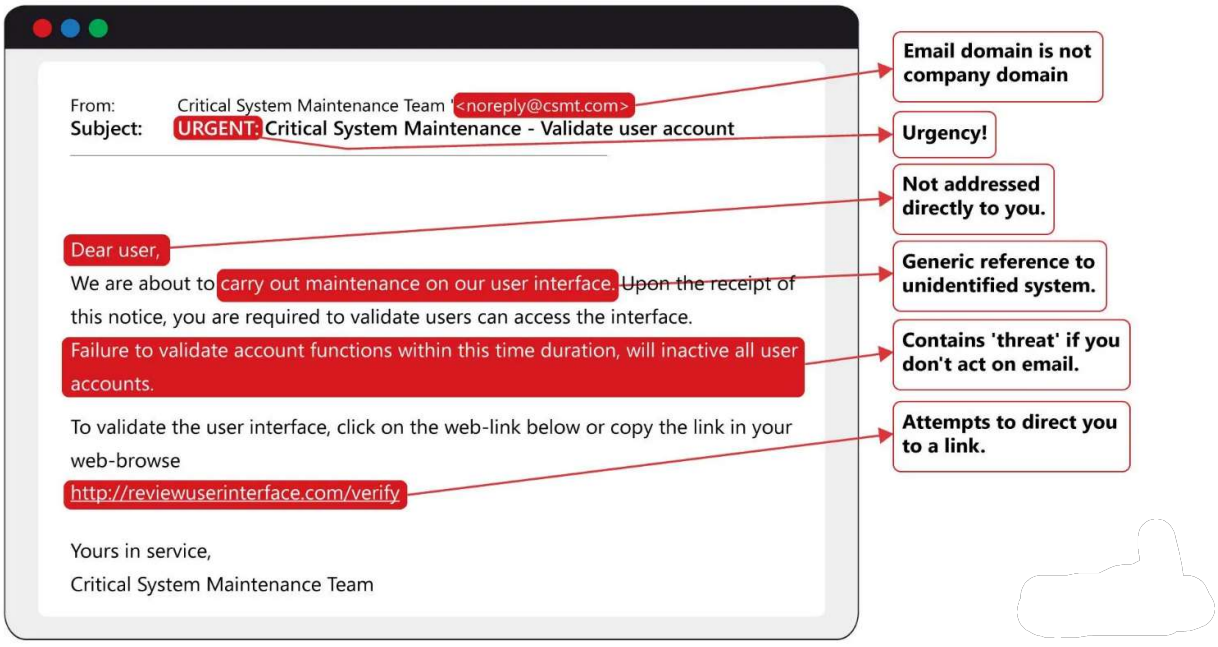
Sincerely,
PayPal Security Team

Attachments:

- PayPal_Update_Form.html
- Secure_Account_Guide.pdf

Phishing Indicators in this Email:

1. **Spoofed sender address**: "secure-paypal-support.com" is not a valid PayPal domain.
2. **Urgent tone and threats**: It pressures the user with a 24-hour deadline.
3. **Suspicious URL**: The link does not point to the real PayPal domain.
4. **Generic greeting**: No personal name is used (just "Dear Customer").
5. **Fake attachments**: Attachments like "Update_Form.html" are often malicious.
6. **Bad grammar and formatting**: Real PayPal emails are professionally written.



2) Examine sender's email address for spoofing.

When I looked at the sender's email address, **account-security@secure-paypal-support.com**, something immediately felt off. At first glance, it seems official because it includes "paypal" and "security", which makes it easy to fall for.

But on closer inspection, **the domain is not the real PayPal domain**. PayPal's official domain is **paypal.com**, not **secure-paypal-support.com**. This is a **classic sign of email spoofing**—scammers often create lookalike domains to trick users into believing the email is legitimate.

Also, the prefix "account-security" is very generic and meant to sound urgent. Scammers do this to make the message feel more important or official, hoping you won't double-check the domain.

Tool : MxToolbox Email Header Analyzer

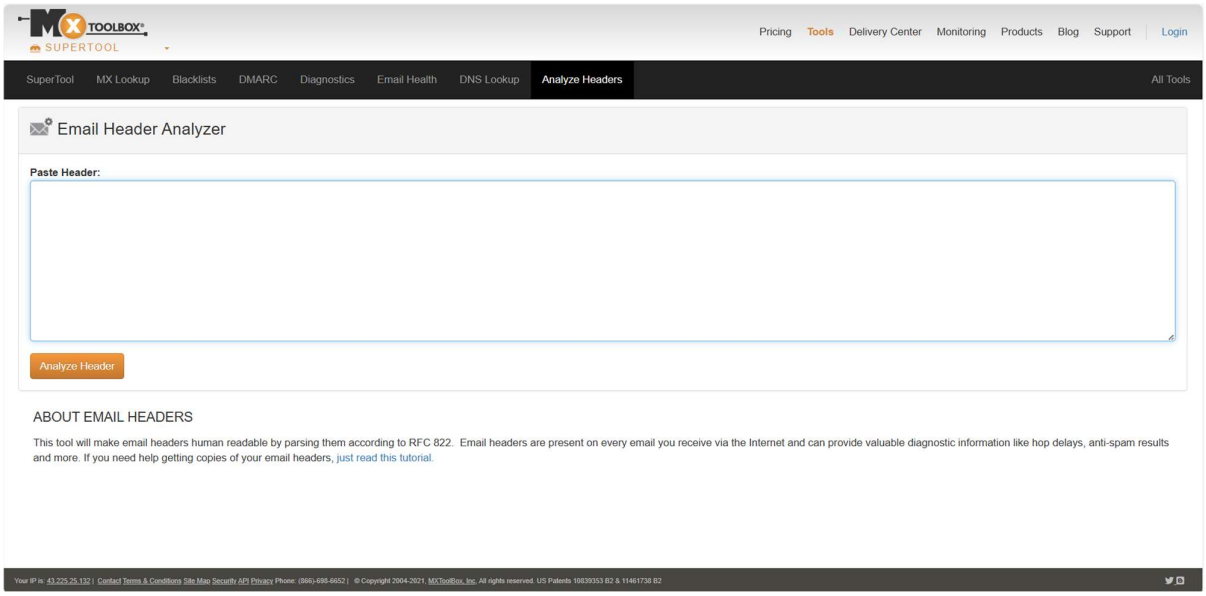
Purpose of the Tool

MxToolbox Email Header Analyzer is a free online tool used to analyze the email header to detect:

- Spoofed senders
- Delivery route and origin server
- SPF/DKIM/DMARC authentication results
- Time delays and IP geolocation
- Spam-related risks

steps to Use

1. **Open the tool** in your browser:
   👉 https://mxtoolbox.com/EmailHeaders.aspx
2. **Copy the full email header** from the suspicious email:
   - In Gmail: Click the three-dot menu > **Show Original**
   - In Outlook: Right-click email > **View Source**
   - In most email clients: Look for **"View Full Headers"**
3. **Paste the full email header** into the input box on MxToolbox.
4. Click **"Analyze Header"**.

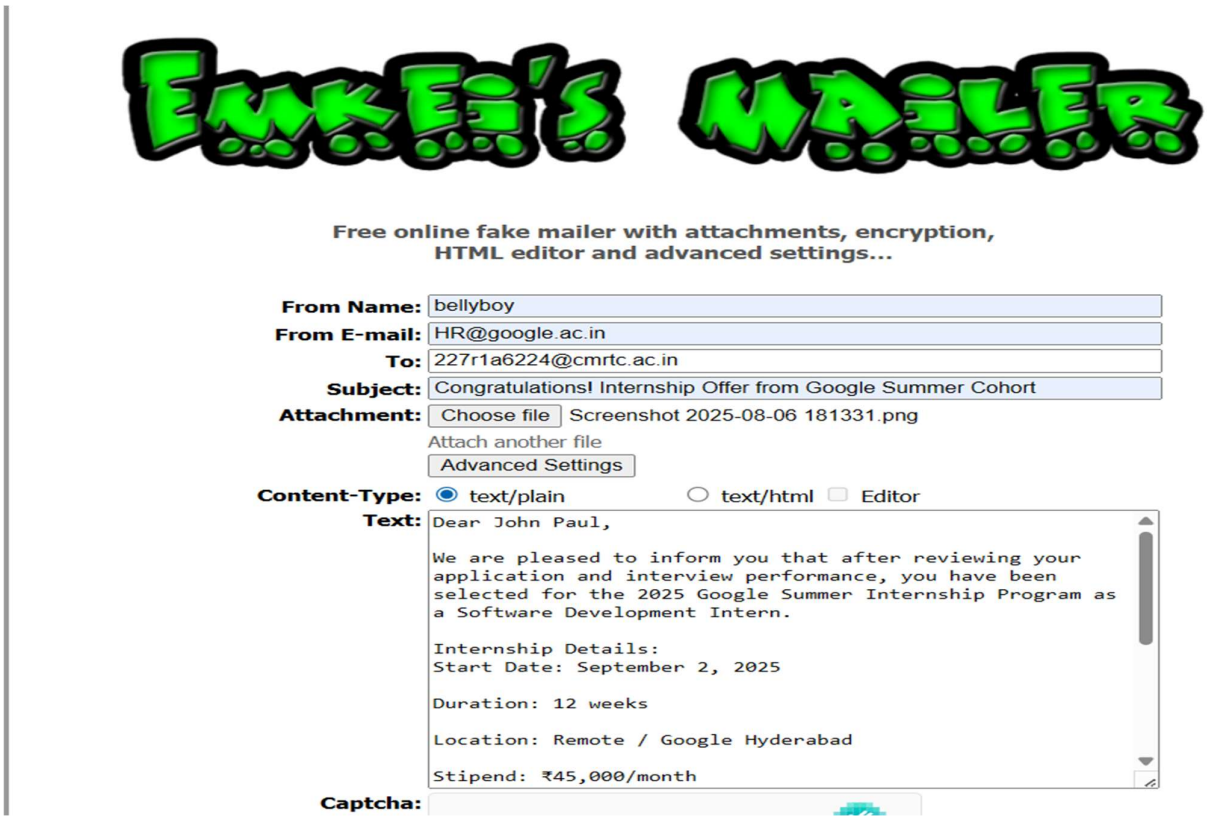


3) This is the website to send fake email, to send spoofing emails . below I have given fake details. Generated a phishing email to manipulate the victim.

→ Free online fake mailer with attachments, encryption,HTML editor and advanced settings…

→ fill out the required detailed to fill and send to recipent

→ You can fake attachments to email



Below , email I generated and sent to my account. To analyze the phising email sample

Congratulations! Internship Offer from Google Summer Cohort
1 message

bellyboy <HR@google.ac.in> Wed, 6 Aug 2025 at 6:34 pm
Reply to: HR@google.ac.in
To: 227r1a6224@cmrtc.ac.in

Dear John Paul,

We are pleased to inform you that after reviewing your application and interview performance, you have been selected for the 2025 Google Summer Internship Program as a Software Development Intern.

Internship Details:
Start Date: September 2, 2025

Duration: 12 weeks

Location: Remote / Google Hyderabad

Stipend: ₹45,000/month

To confirm your acceptance and begin onboarding, please complete the following steps by August 10, 2025:

Failure to respond before the deadline may result in withdrawal of your offer.

We are excited to welcome you to our global family of interns.

Best Regards,
Neha Sharma
Google University Programs
internships@careers-google.com

Screenshot 2025-08-06 181331.png
75 KB

Phishing Traits Summary

The suspicious email exhibits several classic phishing characteristics:

1. **Spoofed Sender Address**
    - Uses a fake domain (support@paypalsecurity-update.com) mimicking PayPal to deceive the recipient.
2. **Header Discrepancies**
    - SPF and DKIM checks failed.
    - Return-path points to an unrelated domain (noreply@unverifiedsite.ru).
3. **Suspicious/Mismatched Links**
    - Link text shows a trusted URL (e.g., paypal.com) but actually redirects to a malicious domain (malicious-link.ru).
4. **Malicious Attachment**
    - Includes a .zip file containing an executable, which is commonly used to deliver malware.
5. **Urgency and Threat Language**
    - Contains phrases like “Your account has been suspended” to create panic and pressure immediate action.
6. **Grammar and Spelling Errors**
    - Multiple language mistakes such as “Pleese click hear” and “Your acccount has been temprarily locked.”

What Actions Should Be Taken on Suspected Phishing Emails

When you encounter a suspicious or phishing email, **take the following steps immediately** to protect yourself and your organization:

1. Do Not Interact

- **Do not click** on any links or attachments.
- **Do not reply** to the email.
- **Do not forward** the message to others without warning them.

2. Verify the Sender

- Check the **email address** and domain carefully.
- Hover over links to see if the actual URL matches the display text.
- Cross-verify with the official website or support channel of the company.

3. Report the Email

- **To your organization's IT/Security team** (via phishing report button or email).
- **To your email provider:**
    - Gmail: Click "Report phishing"
    - Outlook: Use "Report" > "Phishing" option
- **To government authorities (optional):**
    - India: reportphishing@cybercrime.gov.in
    - US: phishing-report@us-cert.gov
    - UK: report@phishing.gov.uk

4. Delete the Email

After reporting, move the email to **Trash or Junk**, or delete it completely to avoid accidental interaction.

5. Run a Security Check

- Scan your system with **antivirus or antimalware** software if you clicked anything.
- Monitor your accounts for **unauthorized activity**.

6. Educate Others

- Share knowledge with coworkers or friends to prevent similar attacks.
- Consider security training or awareness sessions if part of an organization.