**Step 1: Choose the Email sample and find suspicious things**

**My Fake Email Sample : Government Refund Mail**

**Subject:** Income Tax Refund Available – Action Required

**From:** itdepartment@gov-refund.in

**Body:**

Dear Taxpayer,

You are eligible for an income tax refund of ₹5,700.  
Please fill out the attached form to claim your refund.

Attachment: TaxRefundForm.zip

Best Regards,  
Income Tax Department

**Subject:** Income Tax Refund Available – Action Required  
**From:** itdepartment@gov-refund.in  
**Attachment:** TaxRefundForm.zip

**Phishing(Suspicious) Indicators:**

1. Fake sender domain (gov-refund.in)
2. Attachment ( it could contain malware)
3. No official government formatting or signature
4. Tries to tempt with “refund” money

**Short Explanation:**This is a fake government refund email pretending to be from the Income Tax Department. It tries to trick users into downloading a malicious file.

Step 2: Examine the Sender’s Email Address

Check if the **sender’s email domain** looks official.

* Genuine government emails end with .gov.in (e.g: helpdesk@incometax.gov.in)
* Here it’s @gov-refund.in, which is **fake**.

**Explanation:** Attackers use similar looking domains to fool people (this is called *email spoofing*).

**Step 3: Check for Attachments or Links**

There is an **attachment** named TaxRefundForm.zip.

**Explanation:** Phishing emails often include ZIP or EXE files that contain malware. Never open such files from unknown sources.

**Step 4: Look for Urgent or Tempting Language**

Phrases like *“You are eligible for a refund”* or *“Please fill out the form to claim”* create a **sense of urgency** or greed.

**Explanation:** Phishing relies on emotional manipulation like either scaring or exciting the victim so they act quickly.

**Step 5: Analyze Email Formatting**

Notice:

* No official **logo** or **digital signature**
* No **contact number** or **official template**

**Explanation:** Government agencies always use standard formats, seals, or e-signatures. Their emails don’t look casual like this one.

**Step 6: Check Grammar and Structure**

Even if the grammar looks okay here, many phishing emails contain:

* Minor grammatical errors
* Poor formatting
* Generic greetings like “Dear Taxpayer” instead of your name

**Explanation:** Attackers often send mass emails, not personalized messages.

**Step 7: Analyze Header (if it’s available)**

If this was a real email file, you could:

* Copy the **email header**
* Go to MXToolbox Email Header Analyzer
* Paste the header and check the **real sender IP/domain**

**Explanation:** This helps verify whether the email was truly sent from a government domain.

Final Report :

**Phishing Email Analysis Report**

**Email Subject:** Income Tax Refund Available – Action Required  
**Sender:** itdepartment@gov-refund.in  
**Attachment:** TaxRefundForm.zip

**Phishing Indicators:**

1. Fake sender domain (gov-refund.in instead of official incometax.gov.in)
2. Malicious attachment (ZIP file)
3. Missing official logo or government signature
4. Emotional manipulation like “You are eligible for a refund”
5. Generic greeting (“Dear Taxpayer”)

**Conclusion:**  
This email is a phishing attempt designed to trick users into downloading malware and sharing personal details. It should be reported and deleted immediately.