**Task 2: Analyze a Phishing Email Sample**

**Step 1: Analyze the Sender’s Email**

* **Email shown:** goog...@protected-download.com
* **Suspicious?** ✅ Yes.
  + This is **not** a legitimate Google domain.
  + **"protected-download.com"** is not associated with Google services.

### ****Step 2: Check the Email Header (if available)****

If you're doing this practically:

* Export the raw header (in Gmail: click the 3 dots → “Show Original”).
* Paste it into: https://mxtoolbox.com/EmailHeaders.aspx
* Look for:
  + SPF/DKIM/DMARC failures
  + Return-path mismatch
  + IP address geolocation (often from foreign or unknown servers)

### ****Step 3: Identify Suspicious Links****

* The email says **“Click Here”**, but doesn’t show the **real URL**.
* Likely a **masked or shortened link**, which is a **phishing red flag**.
* If you hover (without clicking), you’d often see something like:  
  http://malicious-site.com/fake-google-pdf

### ****Step 4: Check for Urgent or Misleading Language****

* Subject: **“has a document for your review”** — vague and creates urgency.
* **No context** or sender name — just a button and a link.
* This is a **common phishing tactic** to trick users into clicking quickly.

### ****Step 5: Mismatched Branding****

* The **Google logo** is used to mimic authenticity.
* But the **email address and link domain** do not match real Google domains.
* This is classic **brand impersonation** — a strong phishing sign.

### ****Step 6: Spelling or Grammar****

* No obvious grammar mistakes, but the message is very **minimal and unnatural**.
* Legitimate services usually have:
  + Greeting with your name
  + Proper message formatting
  + Sender details

**Step 7: Create the Report**