**Task 2**

**🔍 Objective**

You must take a suspicious or sample phishing email and **analyze** it to identify all possible **phishing indicators** — such as spoofed sender addresses, mismatched URLs, fake login links, poor grammar, and emotional manipulation.  
The goal is to learn how phishing works and how to detect it.

**🧠 Concepts Covered**

* Phishing
* Email spoofing
* Email header analysis
* Social engineering
* Threat detection

**🧰 Tools Required**

* Any **email sample** (you can search for “sample phishing email” online)
* A **text editor** or email client (like Gmail, Outlook)
* An **online email header analyzer**  
  Example:
  + https://mxtoolbox.com/EmailHeaders.aspx
  + https://www.gaijin.at/en/tools/email-header-analyzer
* Browser (to hover and check suspicious links)

**🧪 Steps to Perform the Experiment**

**Step 1: Obtain a Sample Phishing Email**

* Search online for *“phishing email samples”* or *“phishing email examples for study”*.
* Choose one example that looks real — for instance, a fake PayPal or bank alert email.
* Save the email (copy text and headers) into a text file called phishing\_email\_sample.txt.

**Step 2: Examine the Sender’s Email Address**

* Check if the sender’s email domain looks suspicious.  
  Example:
  + Legitimate: support@paypal.com
  + Fake: support@paypa1-secure.com (note the number “1”)
* Record your findings in your report under *“Sender Analysis.”*

**Step 3: Analyze Email Headers**

* Copy the email’s full header text and paste it into a **header analyzer** (like MXToolbox).
* Note details like:
  + The actual sending IP address
  + Any “Received From” mismatches
  + Differences between “From” and “Return-Path” fields
* Summarize suspicious elements (e.g., forged relay servers, fake domains).

**Step 4: Inspect Links or Attachments**

* Hover over all links in the email (without clicking).
* Compare displayed vs. actual URLs:  
  Example: https://paypal.com vs https://paypa1-login.net.
* Check if any attachments have unusual extensions (.exe, .zip, .html).
* Document your observations in a *“Links and Attachments Analysis”* section.

**Step 5: Check for Urgent or Threatening Language**

* Look for pressure tactics such as:  
  “Your account will be suspended in 24 hours!” or “Confirm immediately to avoid penalty!”
* These emotional triggers are signs of phishing.
* Note such sentences in your *“Content Analysis.”*

**Step 6: Identify Spelling or Grammar Errors**

* Poorly written messages often indicate phishing.
* Highlight misspellings, odd capitalization, or unprofessional tone.

**Step 7: Summarize All Phishing Indicators**

Create a summary table or list in your report, for example:

| **Indicator Type** | **Example Found** | **Explanation** |
| --- | --- | --- |
| Spoofed Sender | support@paypa1.com | Misspelled domain |
| Urgent Language | “Your account will be blocked” | Psychological trick |
| Mismatched URL | https://paypal-secure-login.net | Fake domain |
| Grammar Errors | “Your account is been suspended” | Unprofessional text |