**Step-by-Step Instructions:**

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

Use a known example from a trusted source. Here's one from the **Anti-Phishing Working Group (APWG)** or use the one below:

**Sample Phishing Email**

sql

CopyEdit

From: PayPal Support <support@paypa1.com>

To: user@example.com

Subject: Urgent: Account Suspended Due to Unauthorized Activity

Dear Customer,

We noticed suspicious activity in your account. To protect your information, your account has been temporarily suspended. You must verify your identity immediately to restore access.

Click the link below to verify your account:

https://paypal-security.com/verify

Failure to do so within 24 hours will result in permanent suspension.

Thank you,

PayPal Security Team

Attachment: Secure\_Account\_Verification.zip

**Step 2: Analyze the Email Components**

**1. Sender’s Email Address (Spoofing)**

* Actual sender: support@paypa1.com
* **Phishing clue**: The domain "paypa1.com" uses the number **1** instead of letter **l** — a common spoofing tactic.

**2. Email Headers (Optional but Useful)**

* Use a tool like MxToolbox Email Header Analyzer
* Look for:
  + Mismatched Return-Path
  + Received: lines showing odd source domains or IP addresses
  + SPF/DKIM failures

**3. Suspicious Links**

* Link in email: https://paypal-security.com/verify
* **Phishing clue**: Not a real PayPal domain; deceptive link mimicking legitimacy.

**4. Attachment**

* File: Secure\_Account\_Verification.zip
* **Phishing clue**: ZIP attachments often contain malware or credential-stealing files.

**5. Urgent or Threatening Language**

* “Failure to do so within 24 hours will result in permanent suspension.”
* **Phishing clue**: Scare tactics to rush user actions without thinking.

**6. Mismatched URLs (Hover Technique)**

* In real emails, hovering reveals whether the link is genuine.
* If displayed text says "paypal.com" but link is something else, that’s a red flag.

**7. Spelling or Grammar Errors**

* “You must verify your identity immediately to restore access.” (Overly aggressive tone)
* “PayPal Security Team” – suspicious phrasing (usually "PayPal Customer Support")

**Sample Report Template**

**Phishing Email Analysis Report**

**Subject:** Urgent: Account Suspended Due to Unauthorized Activity  
**Sender:** support@paypa1.com

**Phishing Indicators Identified:**

| **Indicator Type** | **Description** | **Risk** |
| --- | --- | --- |
| **Spoofed Sender** | Uses "paypa1.com" instead of "paypal.com" (note the number 1) | High |
| **Suspicious Link** | Link leads to "paypal-security.com", not a real PayPal domain | High |
| **Threatening Language** | “Failure to do so within 24 hours…” to pressure user | Medium |
| **Malicious Attachment** | ZIP file attachment potentially contains malware | High |
| **Spelling/Grammar** | Awkward phrasing; not professionally written | Low |
| **Header Issues** | (Optional) Return-path/IP address may not match legitimate servers | Medium (if analyzed) |

### ****Outcome****

This exercise demonstrates **awareness of phishing tactics** and the ability to conduct a **structured email threat analysis**. Key takeaways include:

* Recognizing domain spoofing and deceptive URLs
* Evaluating sender authenticity and link safety
* Identifying social engineering tactics (urgency, threats)
* Understanding risks from unexpected attachments

**Conclusion:**

The email contains multiple red flags indicative of phishing, including domain spoofing, malicious attachments, fake URLs, and urgency-driven language. Users should not interact with any part of the message and should report it to their security team or email provider.