Task 2: Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found.

### Analysis Based on Your Checklist

#### 1. **Sender's Email Address (Spoofing Check)**

security@exaample.com – This is not a legitimate domain. It uses a common spoofing technique.

#### 2. **Email Header Discrepancies**

When the header is analyzed (e.g., via Google's Message Header Analyzer), you may find:

* **Return-Path** doesn’t match PayPal's domain
* SPF/DKIM/DMARC authentication may **fail** or be missing.
* **Received from** IP might be from an unrelated location or suspicious server.

#### 3. **Suspicious Links or Attachments**

The link text is **“Click here to restore your account”**, but hovering reveals:  
http://example-security-verification.com/verify – clearly not a domain.

#### 4. **Urgent or Threatening Language**

Words like:

* “**Urgent**”
* “**Suspended”**
* “**Failure to respond within 24 hours**”  
  This pressure creates fear, a common tactic to lower user caution.

#### 5. **Mismatched URLs**

Displayed link seems to say “restore your account,” but real link points to a **non-PayPal site**, often a fake login page to steal credentials.

#### 6. **Spelling or Grammar Errors**

Example email may be relatively clean, but many phishing emails contains:

* Odd phrasing (“restore your account immediately by clicking…”)
* Missing commas or unnatural tone

#### 7. **Summary of Phishing Traits Found**

* **Fake sender address** mimicking a real brand (example.com)
* **Threatening urgency** (“permanent suspension”)
* **Suspicious external link** not belonging to elink
* **Mismatched URLs** (hover reveals a fake domain)
* **Header analysis shows domain spoofing and failed authentication**
* **Lack of personalization** (e.g., "Dear Customer" instead of real name)

**Conclusion**

This email contains **multiple signs of phishing**, including **spoofed sender**, **fake URL**, **urgent tone**, and **header manipulation**. It should be **reported and deleted** immediately without clicking any links.

Relevant Screnshots























