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

**Objective**

**The objective of this task is to identify phishing characteristics in a suspicious email sample to build awareness of phishing tactics and improve email threat analysis skills.**

**Tools Used**

* **Email Sample Source: phishing.org**
* **Header Analyzer: MXToolbox (**[**https://mxtoolbox.com/EmailHeaders.aspx**](https://mxtoolbox.com/EmailHeaders.aspx)**)**
* **Operating System: Kali Linux**

**Steps Performed**

1. **Obtained a Sample Phishing Email**
   * **Downloaded a phishing email example from phishing.org.**
   * **Screenshot saved as evidence.**
2. **Examined Sender’s Email Address**
   * **Observed suspicious sender: support@fakebank-security.com**
   * **Domain did not match the legitimate bank.**
3. **Checked Email Header**
   * **Analyzed a simulated phishing email header using MXToolbox.**
   * **Results:**
     + **SPF: Fail**
     + **DKIM: Fail**
     + **DMARC: Fail**
     + **Source IP not associated with the bank.**
4. **Identified Suspicious Links**
   * **Displayed link: https://securebank.com**
   * **Actual URL (on hover): http://malicious-login.net.**
5. **Reviewed Content Language**
   * **Email used urgent wording: *“Verify your account immediately or it will be blocked.”***
6. **Checked for Grammar and Spelling Issues**
   * **Found errors like: *“Your account are suspended.”***
7. **Summarized Findings**
   * **Spoofed sender email domain**
   * **Failed email authentication checks**
   * **Mismatched and malicious URLs**
   * **Threatening and urgent language**
   * **Spelling and grammar errors**

**Results**

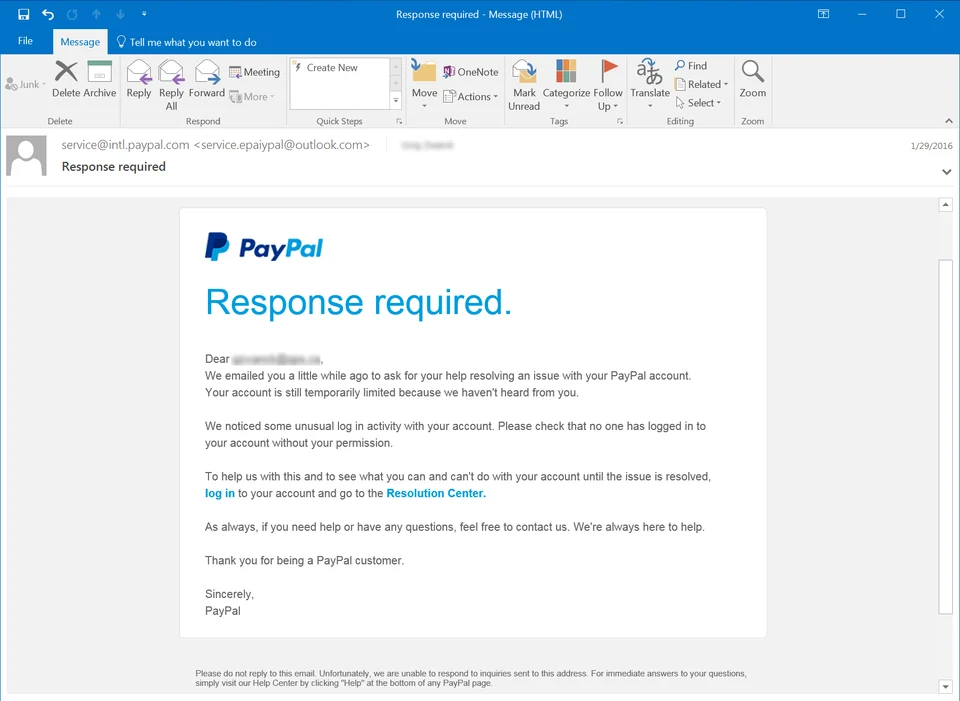
**The email was confirmed to be a phishing attempt.  
It contained multiple red flags including domain spoofing, authentication failures, suspicious links, and manipulative language.**

**Outcome**

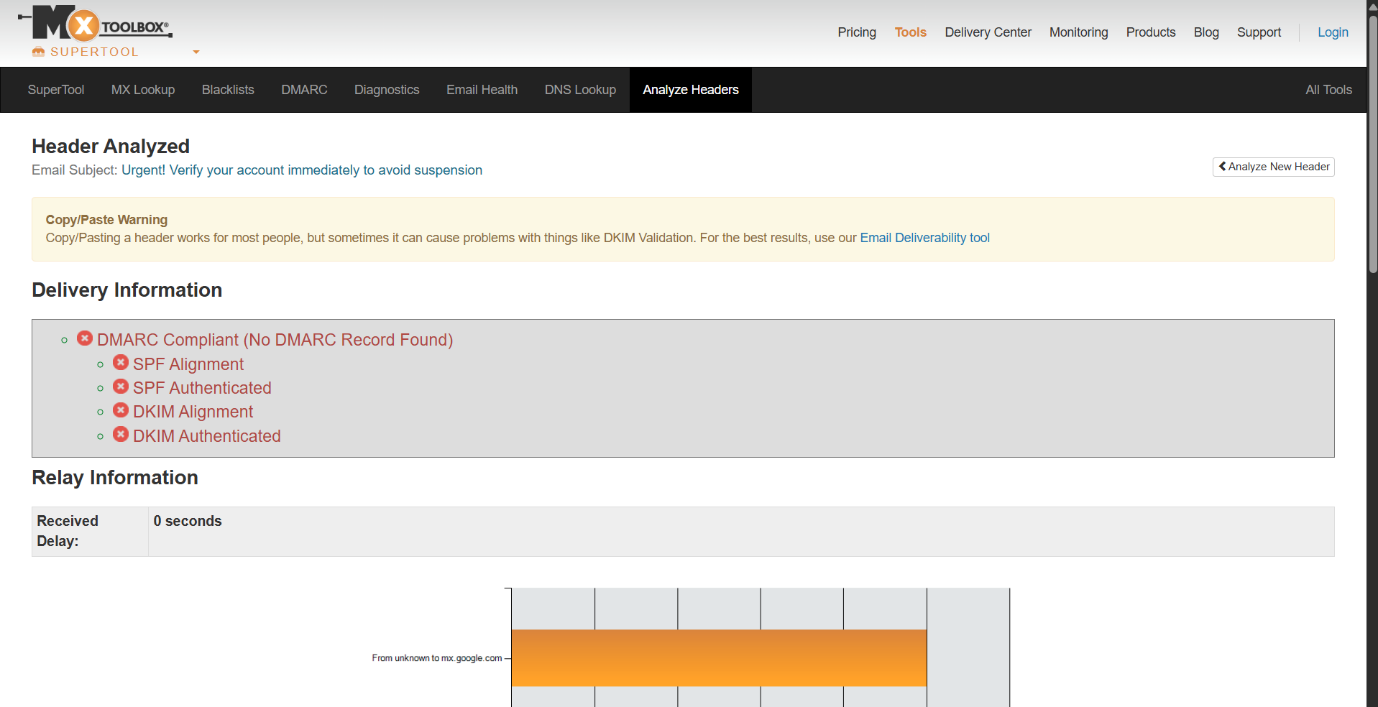
* **Successfully analyzed a phishing email sample.**
* **Gained experience with MXToolbox for header analysis.**
* **Learned to identify common phishing indicators and tactics.**

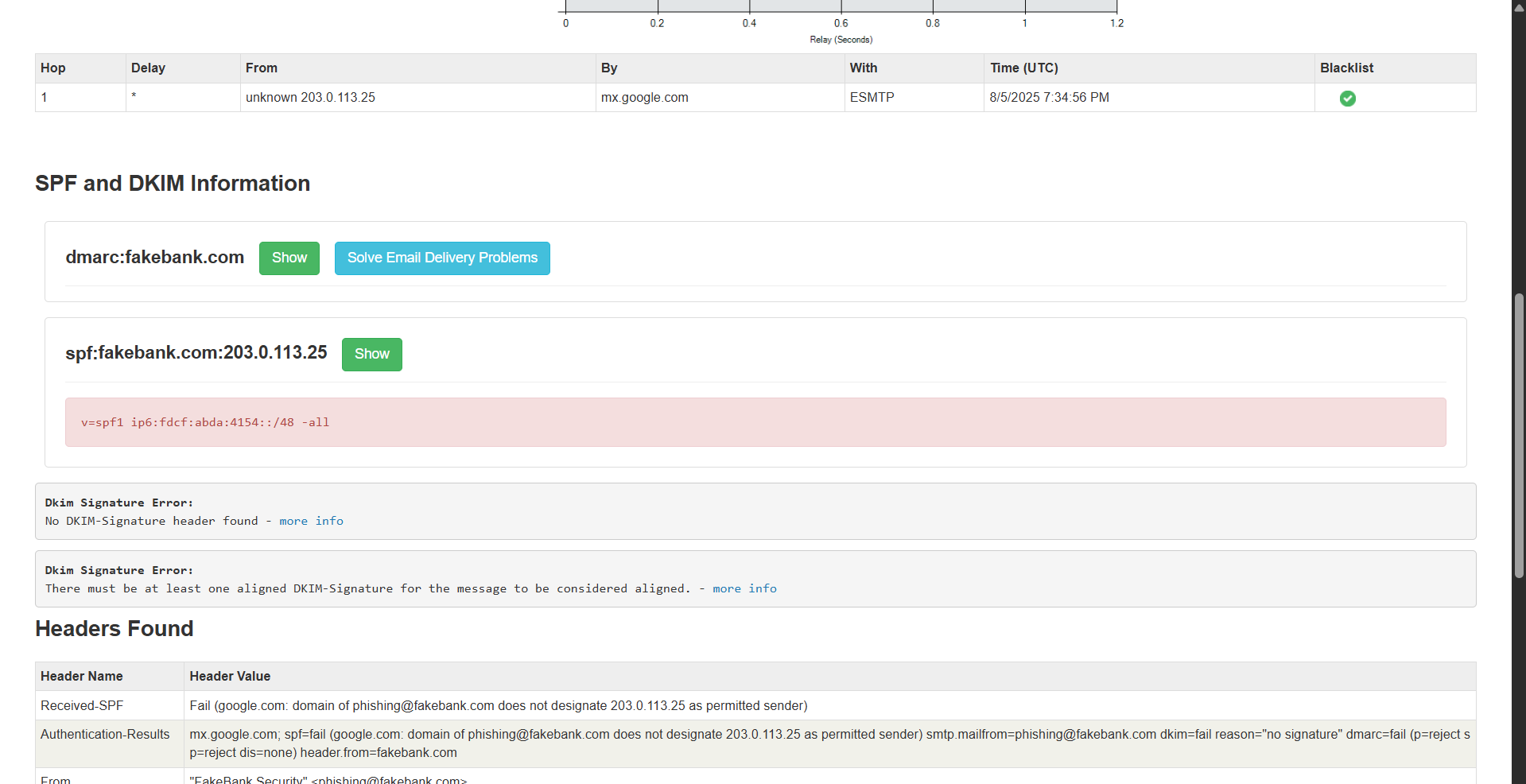
**📌 Screenshots to Add:**

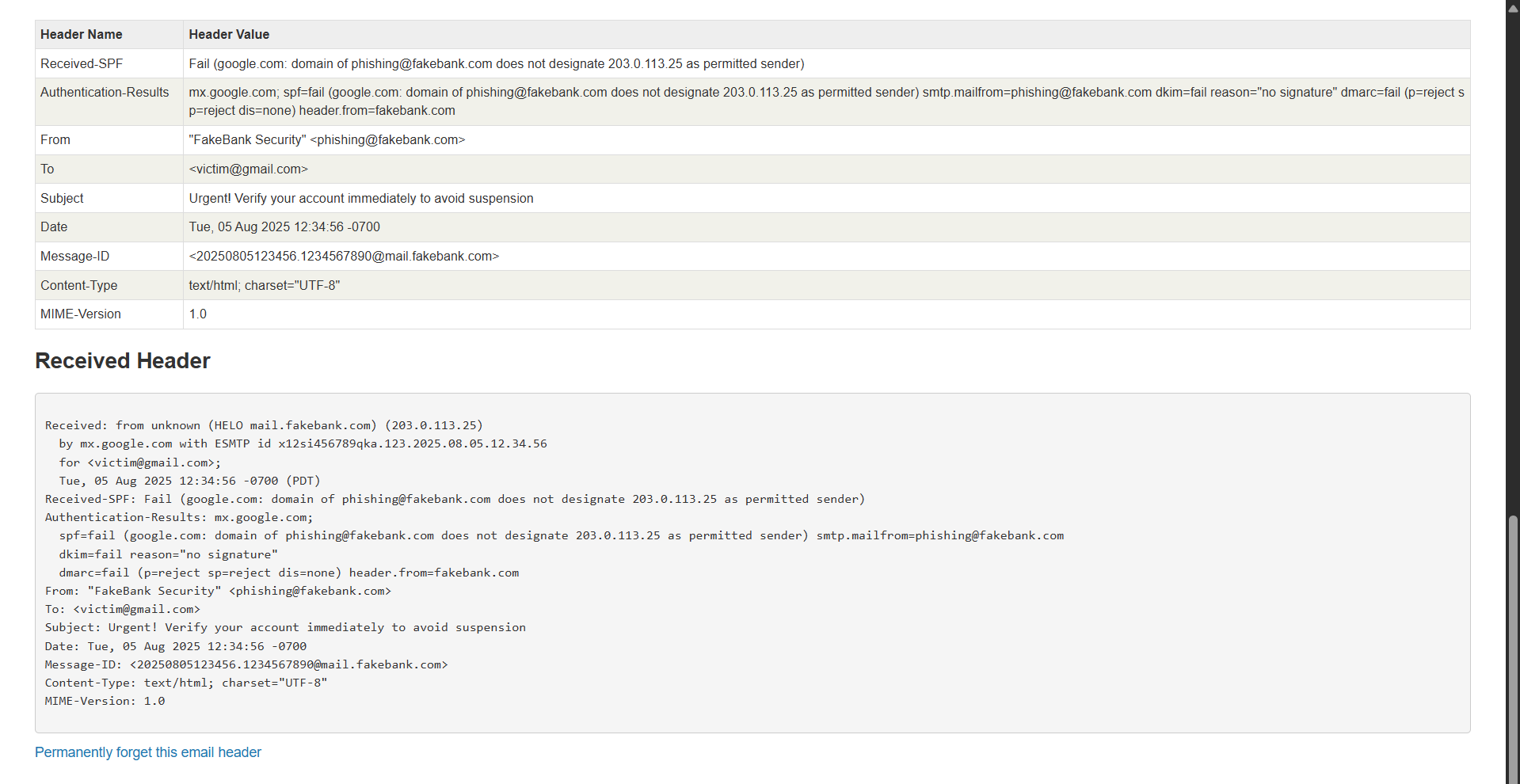
* **Screenshot of phishing email :-**

****

* **Screenshot of header analysis :-**

****

****

****