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

**# Objective**

**Identify phishing characteristics in a suspicious email sample to understand how phishing attempts are carried out and how to detect them.**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# 🛠 Tools Used**

**- Email Sample Source: phishing.org**

**- Header Analyzer: MXToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)**

**- OS Used: Windows**

**--------------------------------------------------------------------------------------------------------------------------------------**

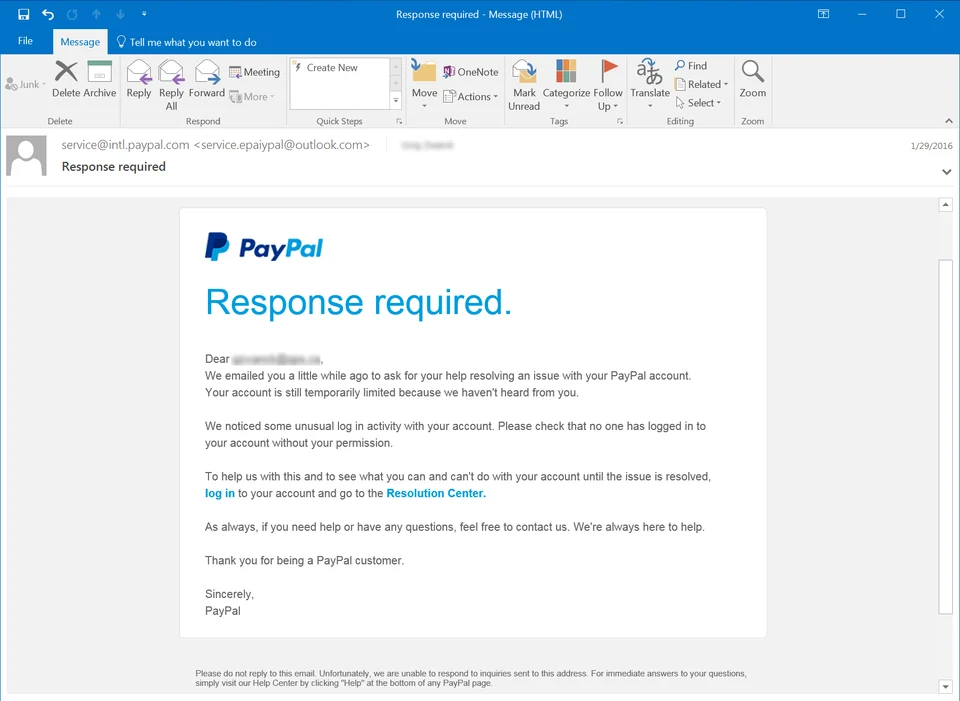
**# Steps Performed :-**

**1. Obtain a Sample Phishing Email**

**- Downloaded a phishing email example from phishing.org.**

**- Saved the screenshot for analysis.**

**Screenshot of Email Example:**

****

**--------------------------------------------------------------------------------------------------------------------------------------**

**2. Analyze the Sender's Email Address**

**- Observed that the sender address was `phishing@fakebank.com`, which does not match the legitimate bank domain.**

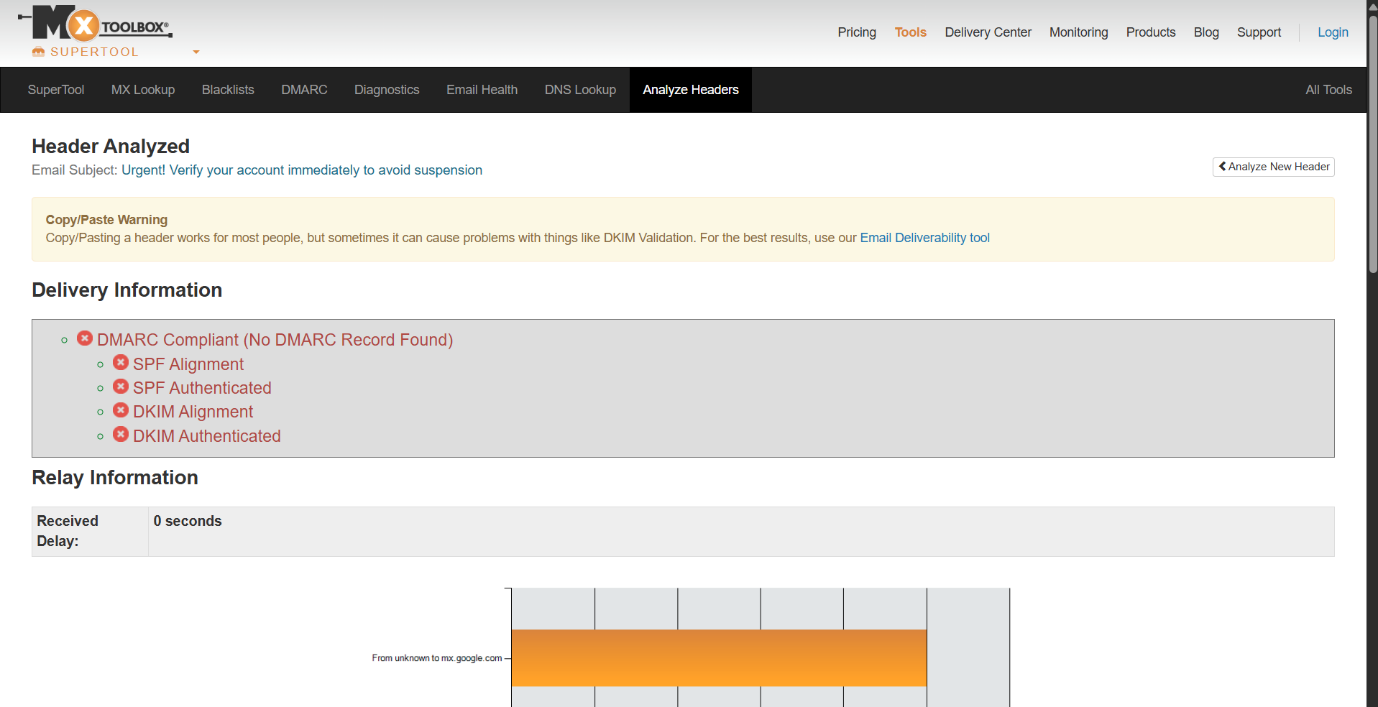
**--------------------------------------------------------------------------------------------------------------------------------------**

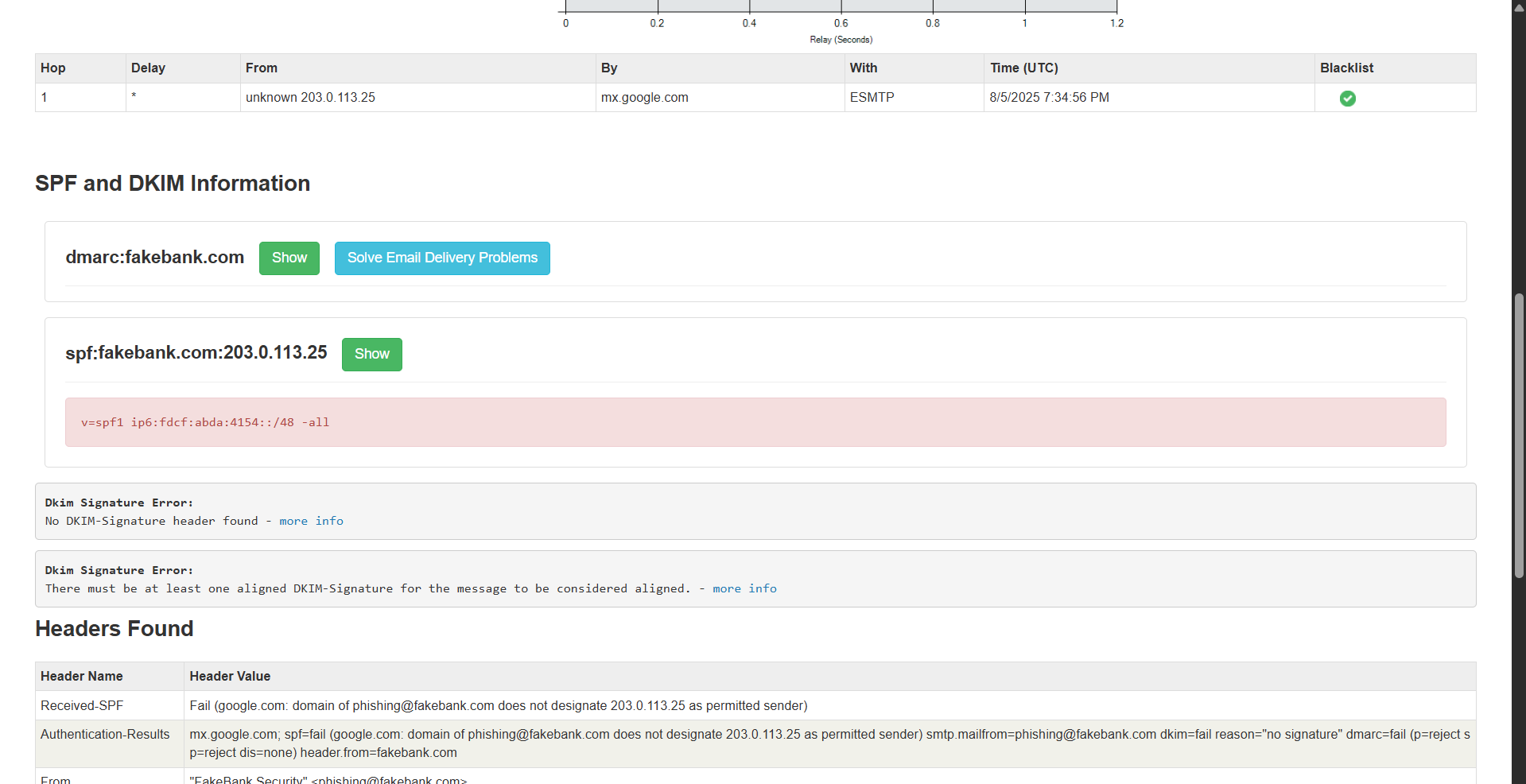
**3. Perform Email Header Analysis**

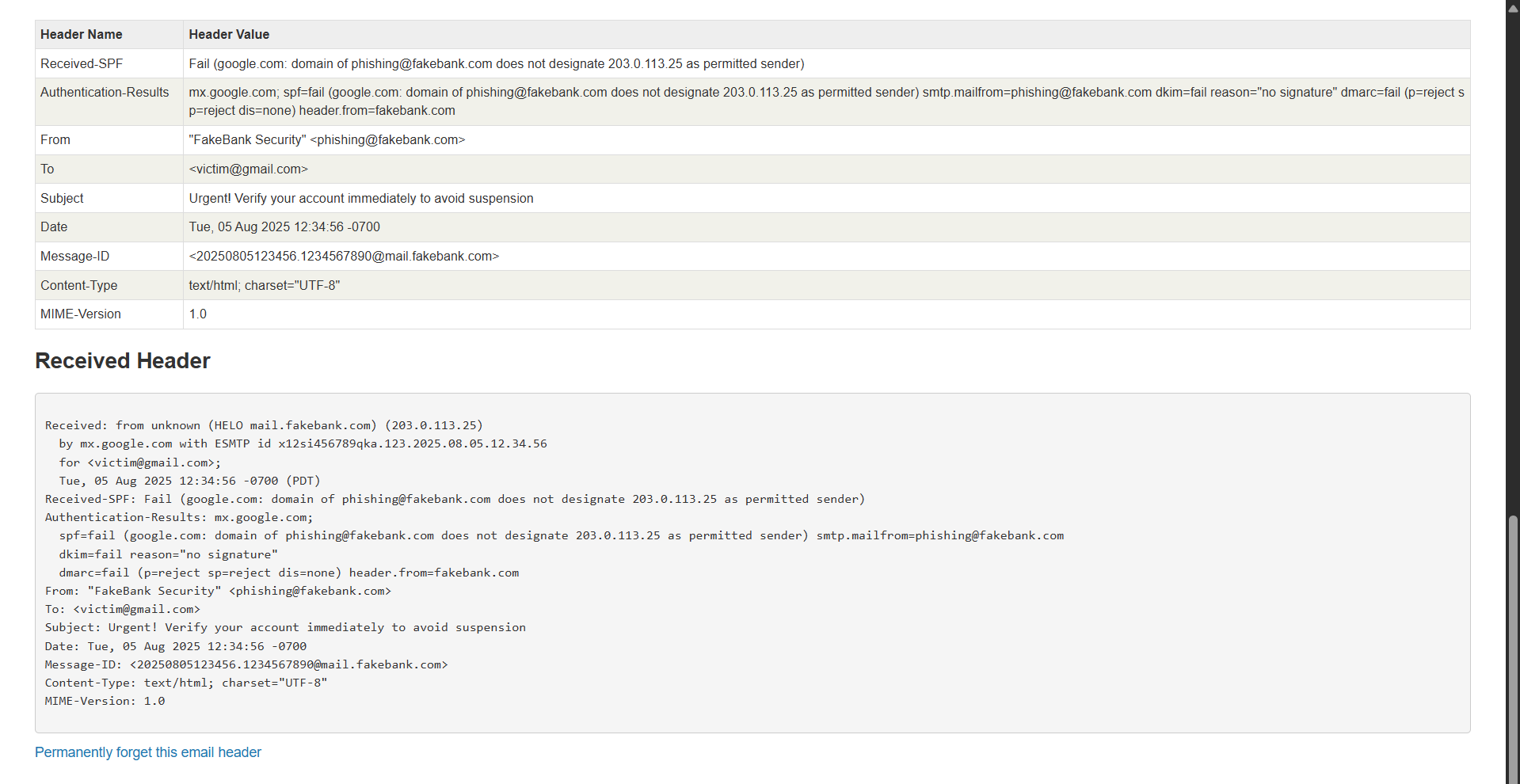
**- Used MXToolbox to analyze a simulated phishing email header.**

**- Observed multiple red flags:**

**Header Analysis Screenshot:**

****

****

****

**--------------------------------------------------------------------------------------------------------------------------------------**

**4. Identify Suspicious Elements**

**- Urgent Language: “Verify your account immediately to avoid suspension.”**

**- SPF/DKIM/DMARC Failures: Authentication checks failed.**

**- Suspicious Links: Displayed link claimed to be a bank, but hovered URL redirected to `http://malicious-site.com`.**

**- Grammar Issues: Minor errors indicating lack of professionalism.**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# Results**

**- Confirmed that the email was a phishing attempt.**

**- Detected multiple indicators:**

**- Spoofed sender domain**

**- Failed email authentication checks (SPF, DKIM, DMARC)**

**- Suspicious, mismatched URL**

**- Urgent and threatening language**

**- Grammar/spelling errors**

**--------------------------------------------------------------------------------------------------------------------------------------**

**# Outcome**

**- Gained awareness of how phishing emails attempt to deceive users.**

**- Learned how to use MXToolbox for header analysis.**

**- Developed skills to identify phishing indicators quickly and effectively.**