Phishing Email Analysis Report

**STEP 1: Set Up Your System**

**Operating System :**

Use **Windows 10/11** or **Kali Linux**

Windows is fine if you just need to analyze text-based emails and headers.

**1. Objective**

The objective of this task is to analyze a suspicious phishing email to

identify red flags such as spoofed sender addresses, suspicious hyperlinks,

misleading content, and unauthorized headers. The analysis helps develop

awareness of phishing tactics and improve skills in email threat detection.

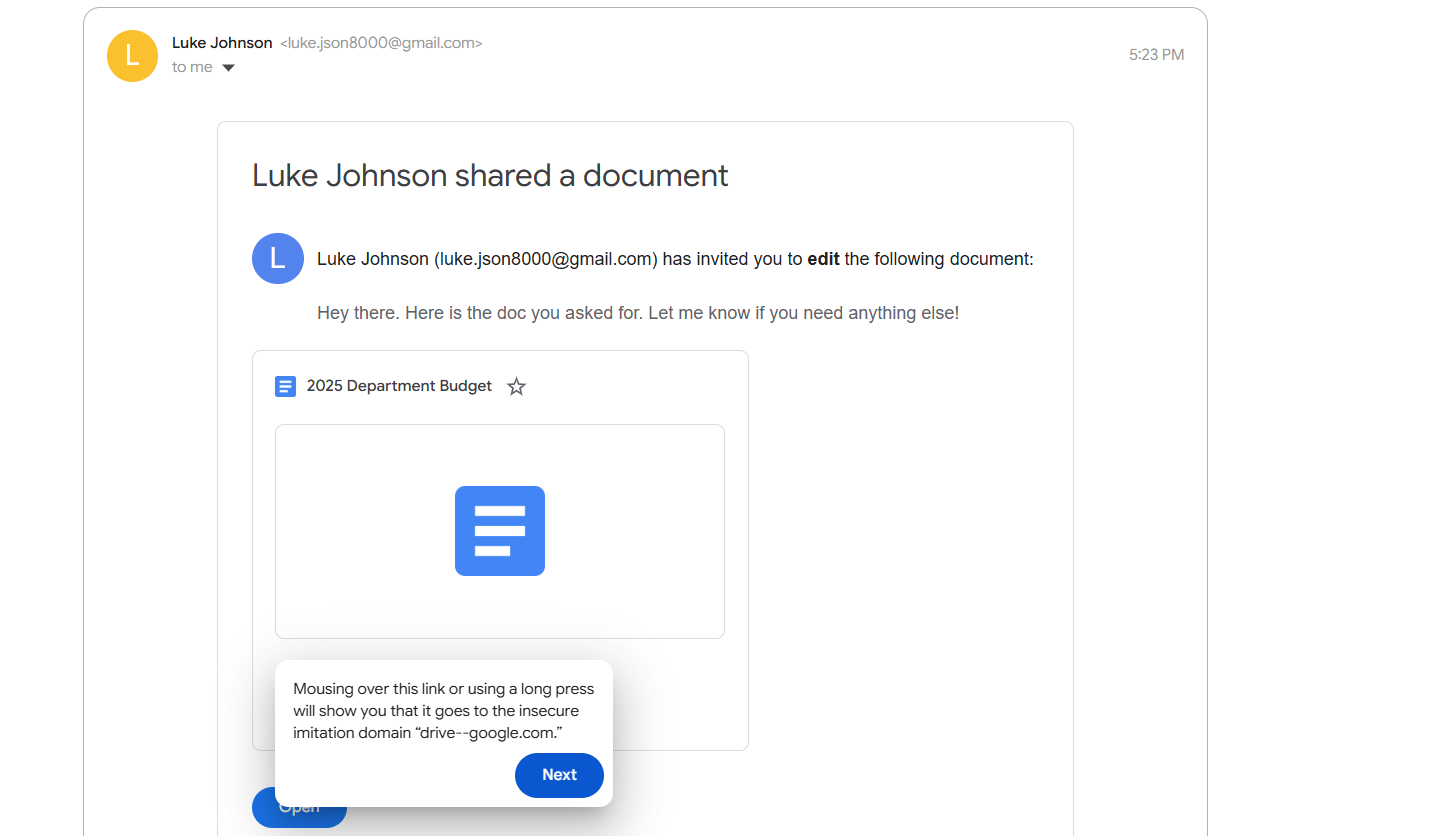
| **Category** | **Tool / Platform** |
| --- | --- |
| Email Sample | Google Phishing Quiz / Sample Phishing Sites |
| Header Analyzer | MXToolbox, Google ToolboxHeader Parser |

**STEP 2: Download or Get a Sample Phishing Email**

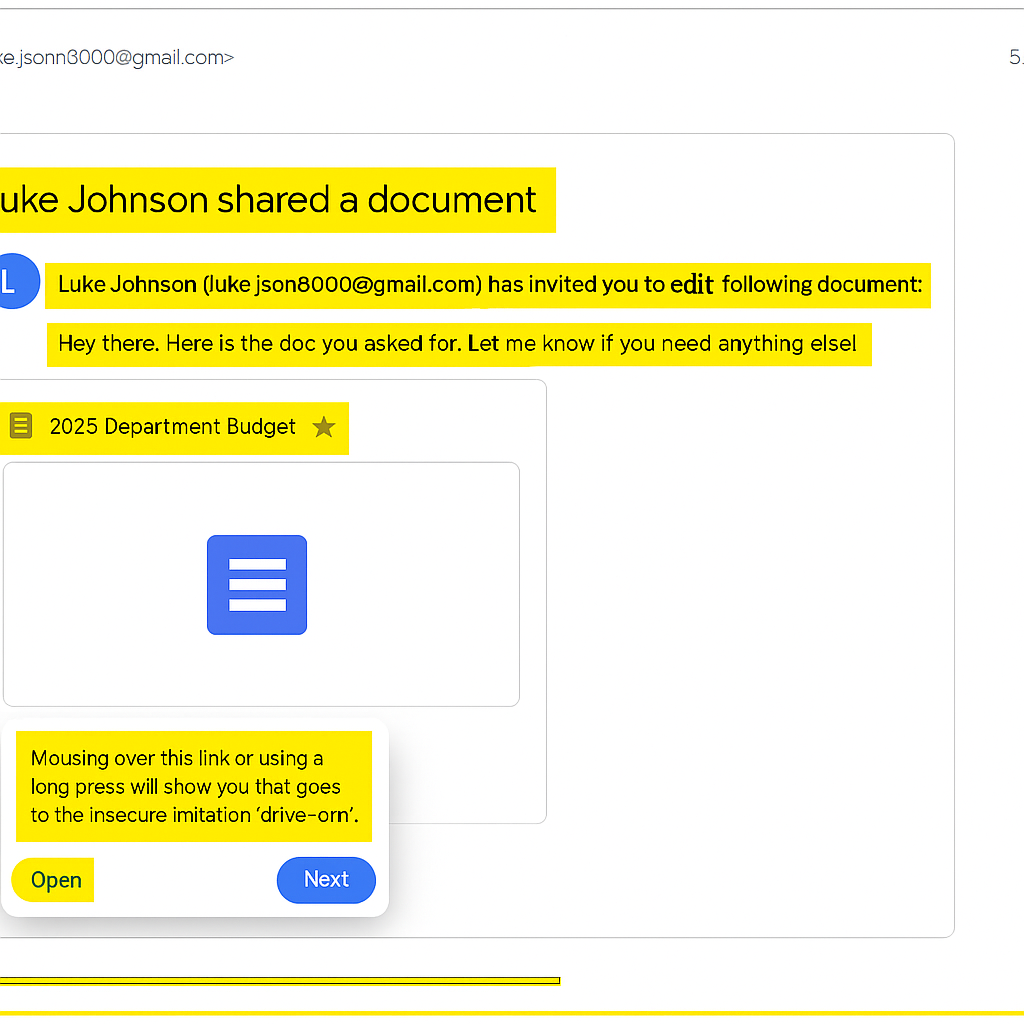
Use a **sample phishing email** from:

# https://phishingquiz.withgoogle.com/

## https://www.emailtray.com/blog/top-10-examples-of-phishing-emails/



**STEP 3: Analyze the Email for Red Flags**



* **STEP 4: Analyze Email Header**

Use one of these online tools:

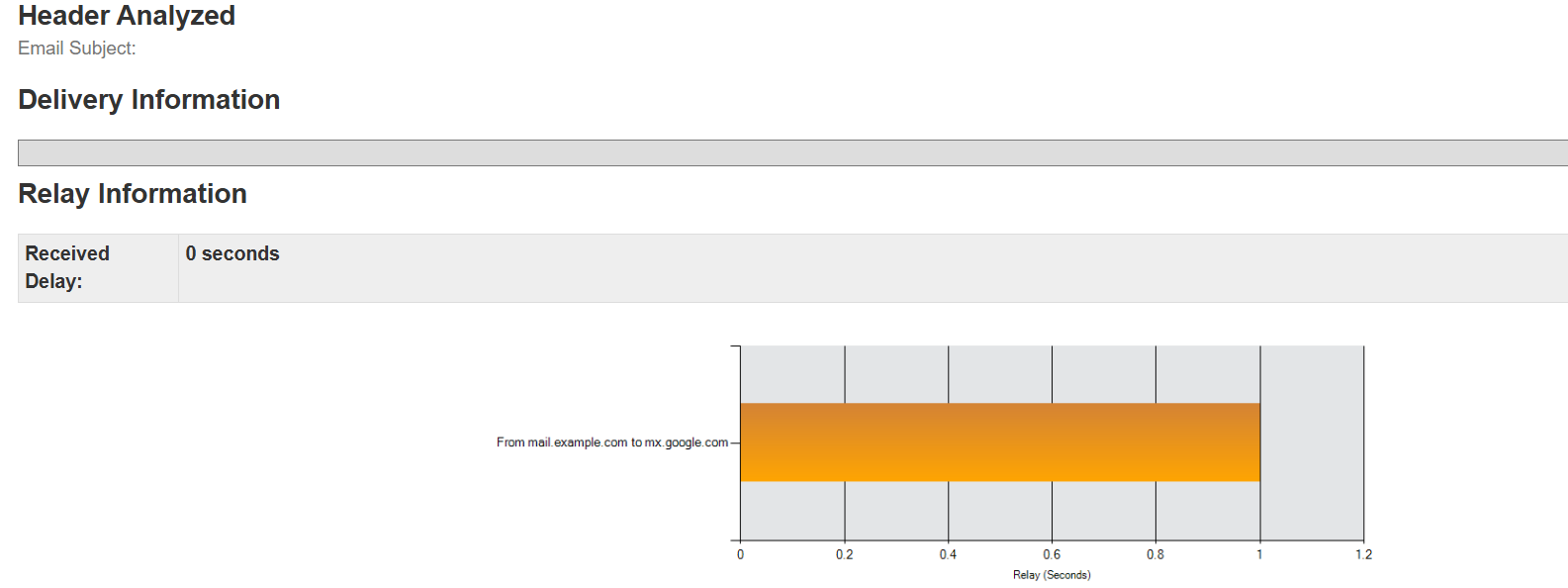
## https://mxtoolbox.com/EmailHeaders.aspx

## https://tools.wordtothewise.com/header\_analyzer

Paste the raw email header (from the sample), and analyze:

SPF, DKIM, Return Path

IP address origin



* **SPF and DKIM** 