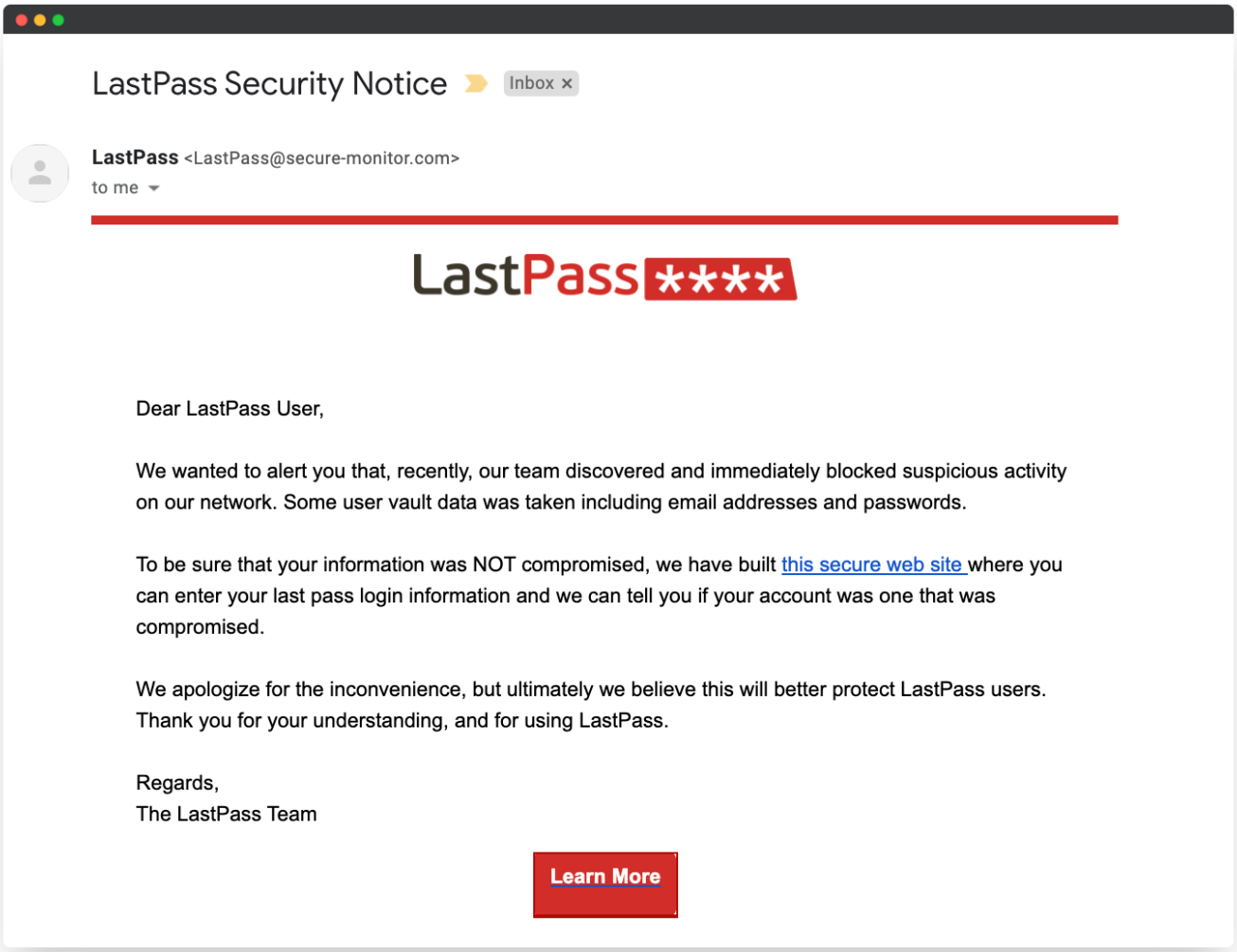
Task 2:

Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.



Phishing Indicators Found in the Sample Email

1. Suspicious Sender Email

- From: LastPass@secure-monitor.com
- Does **not match** the official LastPass domain (lastpass.com)
- Likely spoofed to look legitimate.

2. Urgent and Fear-Inducing Language

- "We wanted to alert you… vault data was taken including email addresses and passwords."
- As it creates panic to prompt the user to take quick action without thinking.

3. Fake Security Link

- Text: *"this secure web site"*
- Hovering shows a misleading URL not related to lastpass.com
- Trick to get users to enter their credentials into a fake site (credential harvesting).

4. Request for Sensitive Information

- "Enter your LastPass login information…"
- Legitimate services never ask users to log in through email links, especially for data breach confirmation.

5. Spelling & Grammar Issues

- “this secure web site” – spacing is off; it should be "website" (one word).
- Minor inconsistencies like this are common in phishing emails.

6. Generic Greeting

- “Dear LastPass User”
- No personal name — phishing attempts often avoid personalization.

Email Header Analysis

Received Header

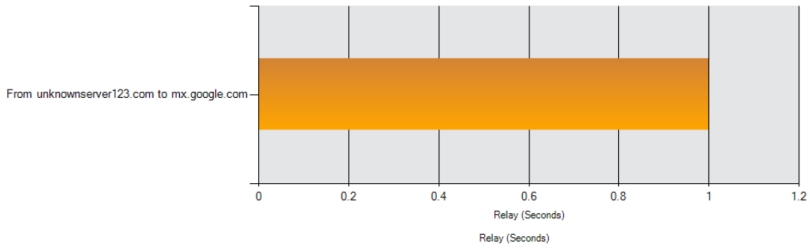
```
Return-Path: <bounce@secure-monitor.com>
Received: from unknownserver123.com (unknownserver123.com. [182.23.56.100])
        by mx.google.com with ESMTPS id z18si2458671qka.45.2025.08.05.12.45.23
        for <victim@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 05 Aug 2025 12:45:23 -0700 (PDT)
Received-SPF: fail (google.com: domain of bounce@secure-monitor.com does not designate 182.23.56.100 as permitted sender) client-ip=182.23.56.100;
Authentication-Results: mx.google.com;
       dkim=fail (bad signature) header.i=@secure-monitor.com;
       spf=fail (google.com: domain of bounce@secure-monitor.com does not designate permitted sender);
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=secure-monitor.com
From: LastPass <LastPass@secure-monitor.com>
To: <victim@gmail.com>
Subject: LastPass Security Notice
Date: Mon, 5 Aug 2025 12:45:17 -0700
Message-ID: <LastPassNotice239s@secure-monitor.com>
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
```

Delivery Information

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	**0 seconds**



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknownserver123.com 182.23.56.100	mx.google.com	ESMTPS	[Mon, 05 Aug 2025 12:45:23 -0700 (PDT)]	