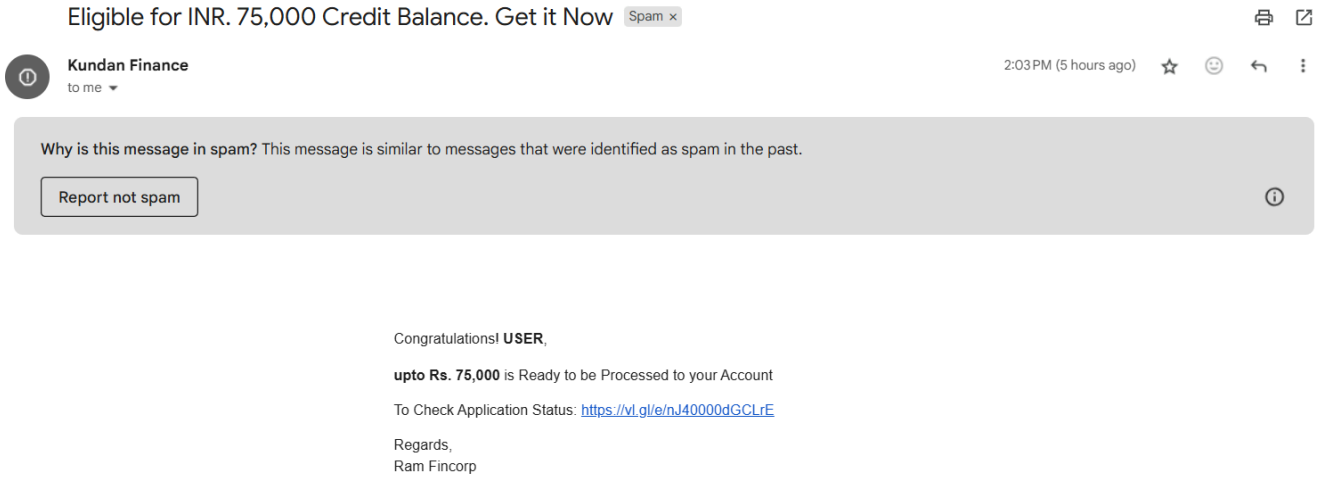
ELEVATE LABS CYBER SECURITY INTERNSHIP

Task 2: Analyze a Phishing Email Sample.

1) Obtain a sample phishing email



This is a spam mail I have received from Kundan Finance. But the regards are given by one named “Ram Fincorp”. This seems to be suspicious. This could be a phishing email.

2) Examine sender's email address for spoofing

Original Message

Message ID	<risfrw1750790770433854 3@blmail.buddyloan.com>
Created at:	Wed, Jun 25, 2025 at 2:03 PM (Delivered after 0 seconds)
From:	Kundan Finance <notifications@blmail.buddyloan.com> Using NetcoreCloud Mailer
To:	yallanurukishansai@gmail.com
Subject:	Eligible for INR. 75,000 Credit Balance. Get it Now
SPF:	PASS with IP 193.58.123.60 Learn more
DKIM:	'PASS' with domain blmail.buddyloan.com Learn more
DMARC:	'PASS' Learn more

The mail address domain of the sender is shown as buddyloan.com. This doesn’t match with the name of the sender, which raises a suspicion of fraud.But the SPF,DKIM, DMARC check is PASSED. Let’s analyze the header.

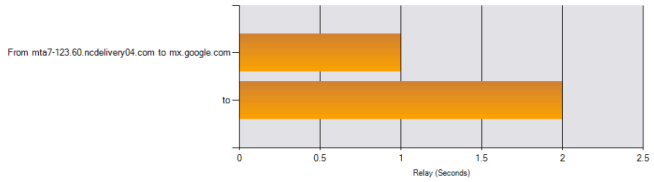
3) Check email headers for discrepancies

Delivery Information

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

Relay Information

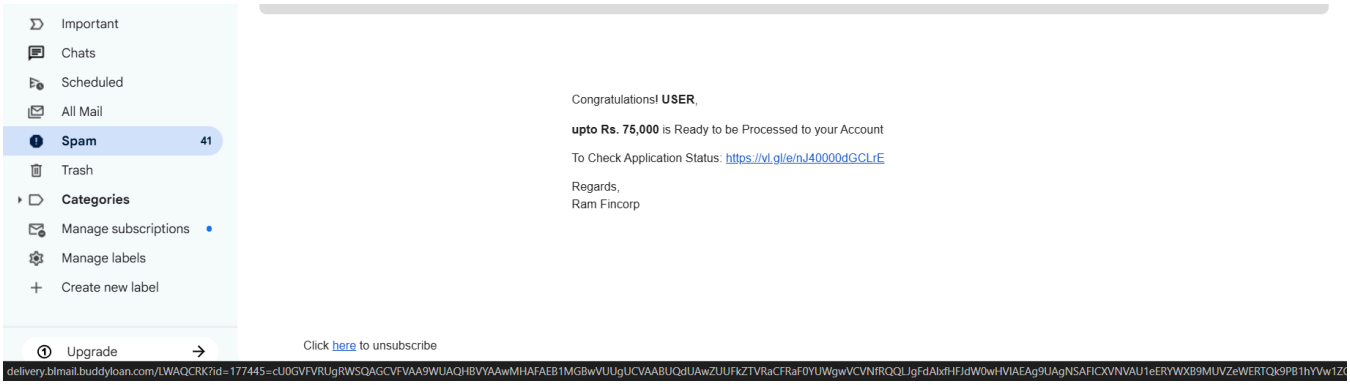
Received Delay:	**1 seconds**



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mta7-123.60.ncdelivery04.com 193.58.123.60	mx.google.com	ESMTPS	6/25/2025 8:33:58 AM	✓
2	1 Second		2002:a05:6000:188c:b0:3a6:c964:80d6	SMTP	6/25/2025 8:33:59 AM	

As the analyzer analyzed the email header, it shows that DKIM is not authenticated. This says that the sender domain is not authenticated. This is a sign of phishing.

4) Identify suspicious links or attachments.



The given link is looking like a short link, which could be redirected to any other website which it is not supposed to be.

5) Look for urgent or threatening language in the email body.

The phrase *“Ready to be Processed to your Account”* creates a false sense of urgency, prompting immediate action.

6) Note any mismatched URLs

As the mouse is hovering on the link, it shows as a link from buddyloan.com but it is not matching with the given link.

7) Verify presence of spelling or grammar errors.

The phrase *“upto Rs. 75,000”* is grammatically incorrect; it should be **“up to ₹75,000”**. Also, "USER" instead of your name is unprofessional and suspicious.

8) **Summarize phishing traits found in the email.**

The email, allegedly from "Kundan Finance" but signed off as "Ram Fincorp," raises multiple red flags indicating a potential phishing attempt. The sender's email domain is shown as **buddyloan.com**, which does not match the sender's name, suggesting spoofing despite SPF, DKIM, and DMARC initially appearing valid. However, header analysis reveals **DKIM authentication failure**, undermining the trustworthiness of the sender. The email contains a **suspicious shortened link**, which may redirect users to a malicious site. The message employs **urgent language** such as "Ready to be Processed to your Account," prompting immediate action. On hovering, the **displayed URL mismatches the actual redirect**, further indicating deception. Additionally, **grammatical issues** like "upto" instead of "up to" and the use of a generic greeting like "USER" point to a mass phishing attempt. Collectively, these traits—sender mismatch, DKIM failure, suspicious links, urgency, and language errors—strongly indicate that this is a **phishing email**.