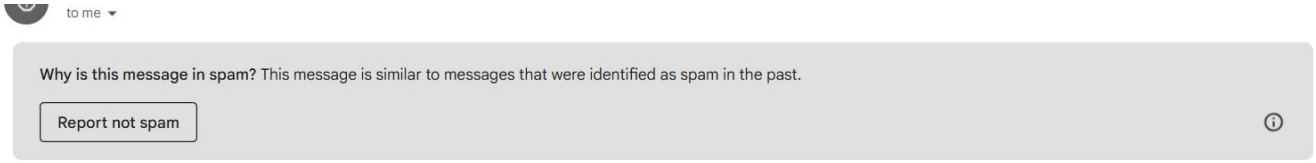
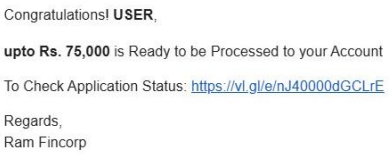
ELEVATE LABS CYBER SECURITY INTERNSHIP

Mothe Anurag Reddy

Task 2: Analyze a Phishing Email Sample.

1) Obtain a sample phishing email





This is a spam mail I have received from aFinance. 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.

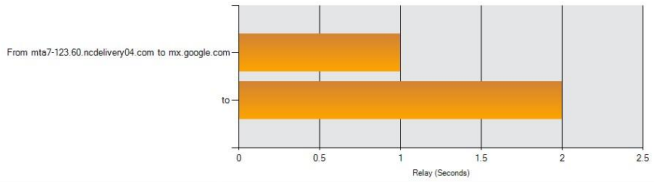
3) Check email headers for discrepancies

Delivery Information

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

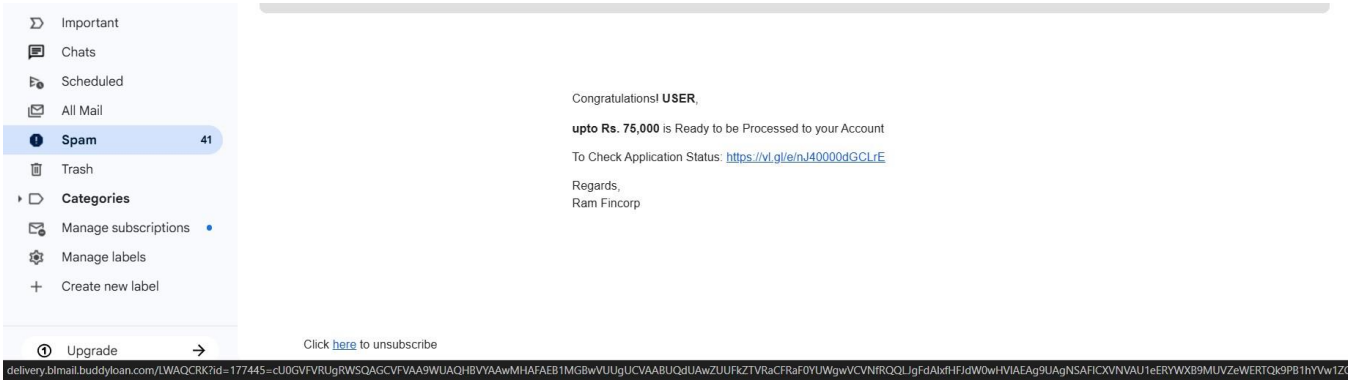
Relay Information

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.

I got an email that said it was from "Finance Bank," but it was signed as "Ram Fincorp," which was already confusing. The email came from a **buddyloan.com** address, which doesn't match the sender's name. At first, it looked like the email passed basic security checks, but after checking the headers, I saw that DKIM actually failed. That's a red flag.
The email also had a shortened link that seemed suspicious. When I hovered over it, the actual link was different from what was shown, which usually means it could be trying to trick me. The message sounded urgent, saying something like "Ready to be processed to your account," clearly trying to rush me into clicking.

It also had some grammar mistakes, like using "upto" instead of "up to," and it addressed me as "USER" instead of my name, which makes it feel like a mass message. Overall, the mismatched details, failed authentication, sketchy link, and poor language make it feel like a phishing email.