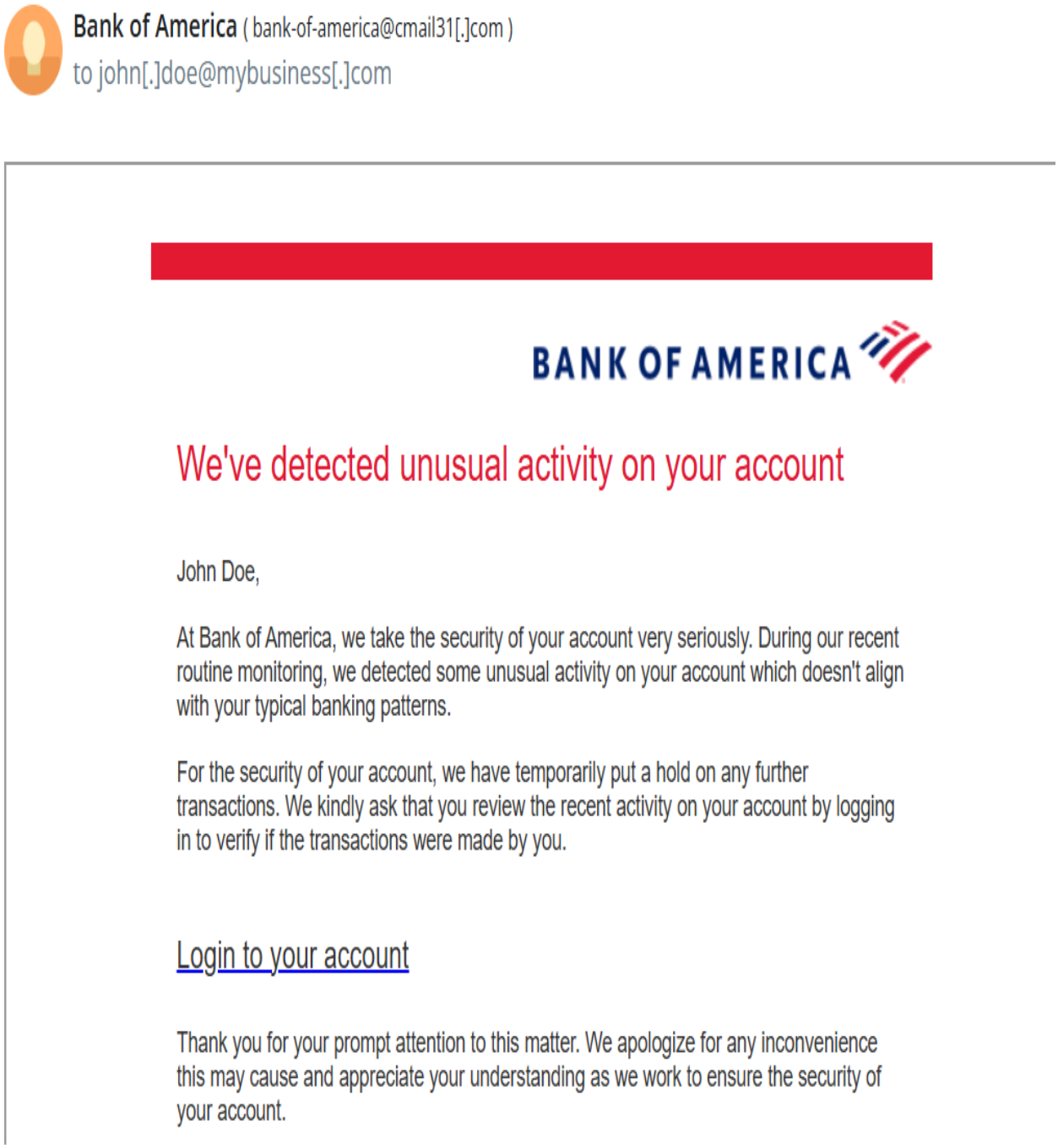
✧ Shailesh_task2

1. Obtain a sample phishing email (many free samples online).



Bank of America (bank-of-america@cmail31[.]com)
to john[.]doe@mybusiness[.]com

BANK OF AMERICA

We've detected unusual activity on your account

John Doe,

At Bank of America, we take the security of your account very seriously. During our recent routine monitoring, we detected some unusual activity on your account which doesn't align with your typical banking patterns.

For the security of your account, we have temporarily put a hold on any further transactions. We kindly ask that you review the recent activity on your account by logging in to verify if the transactions were made by you.

Login to your account

Thank you for your prompt attention to this matter. We apologize for any inconvenience this may cause and appreciate your understanding as we work to ensure the security of your account.

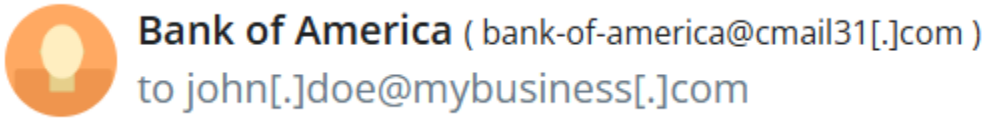
Bank of America (bank-of-america@cmail31[.]com)
to john[.]doe@mybusiness[.]com

For the security of your account, we have temporarily put a hold on any further transactions. We kindly ask that you review the recent activity on your account by logging in to verify if the transactions were made by you.

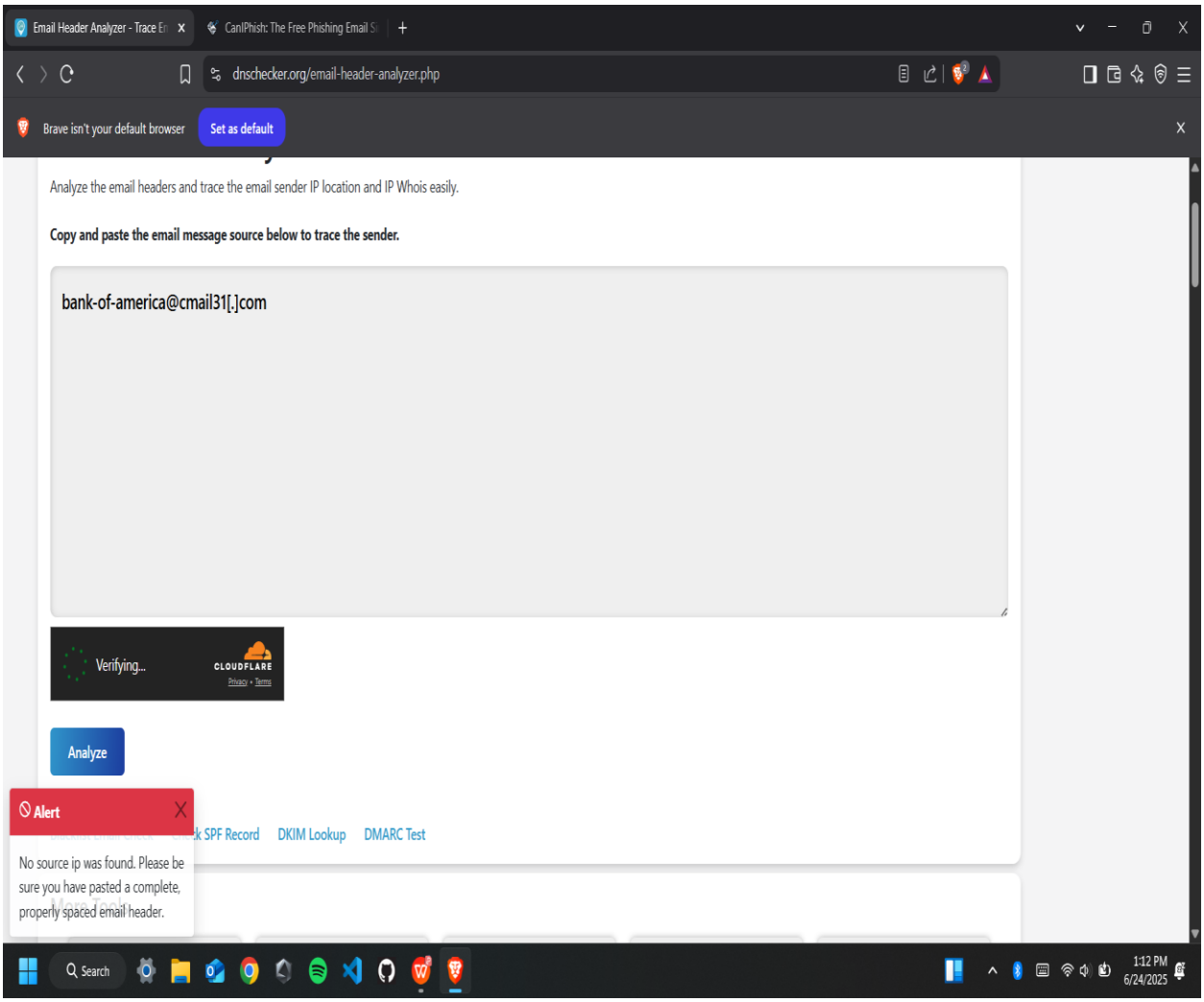
Login to your account

Thank you for your prompt attention to this matter. We apologize for any inconvenience this may cause and appreciate your understanding as we work to ensure the security of your account.

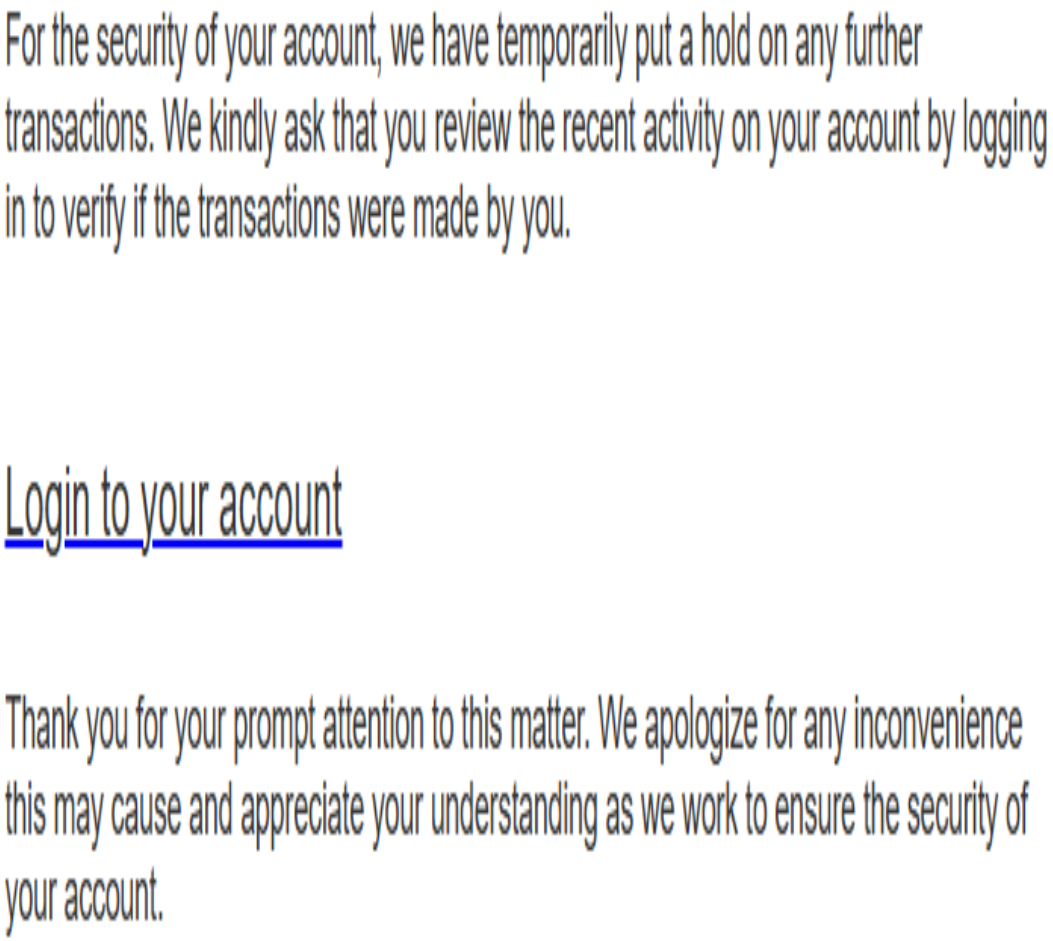
2. Examine sender's email address for spoofing



3.Check email headers for discrepancies (using online header analyzer)



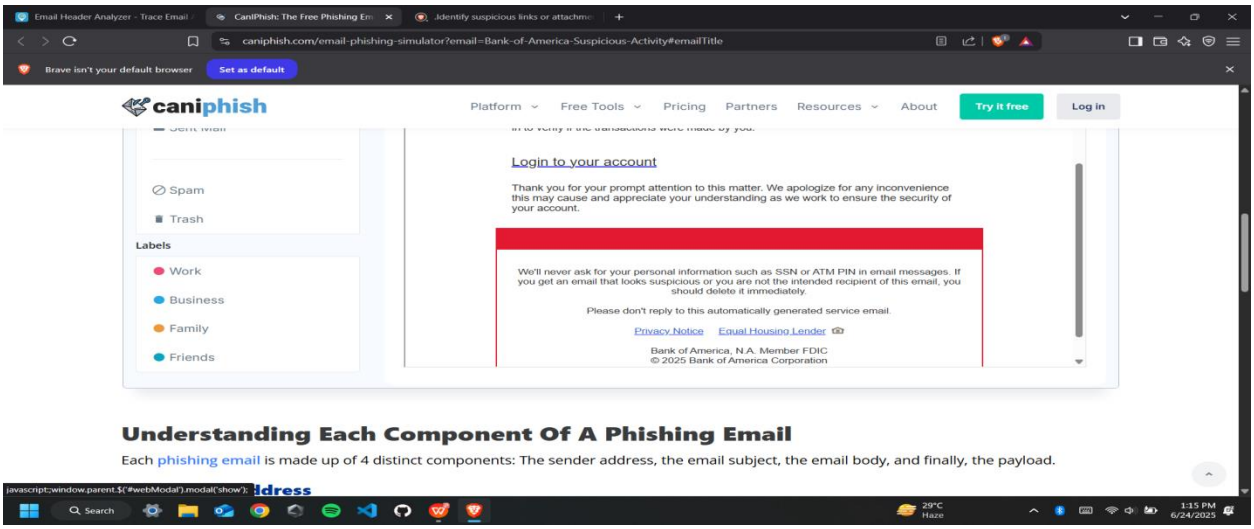
4.Identify suspicious links or attachments

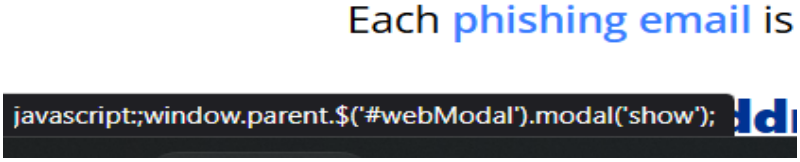


5.Look for urgent or threatening language in the email body

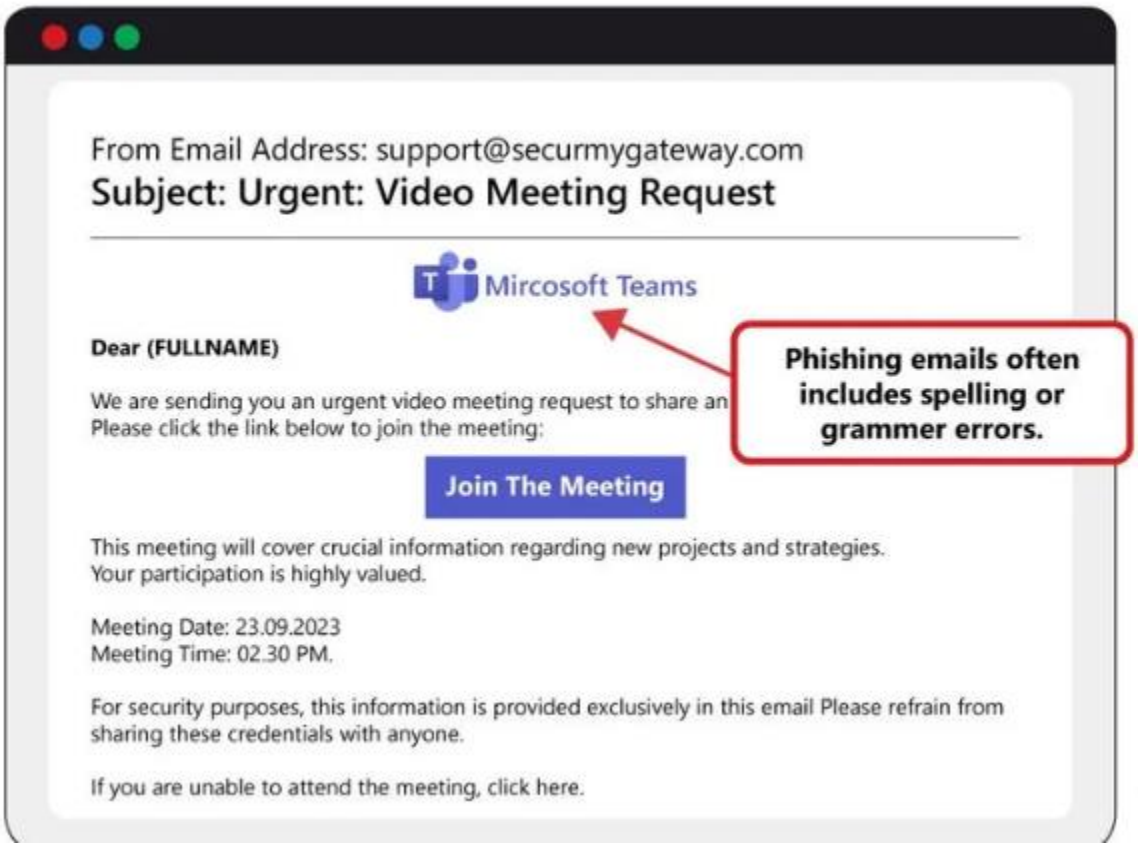
For the security of your account, we have temporarily put a hold on any further transactions. We kindly ask that you review the recent activity on your account by logging in to verify if the transactions were made by you.

6.Note any mismatched URLs (hover to see real link).





7.Verify presence of spelling or grammar errors.



8. Summarize phishing traits found in the email.

1. Suspicious Sender Email Address

Displayed name: "Bank of America"

Actual email address: `bank-of-america@cmail31[.]com`

This domain is **not** associated with Bank of America.

Legitimate institutions use official domains (e.g., `@bankofamerica.com`).

2. Urgent and Alarming Language

"We have detected unusual activity on your account"

"We have temporarily put a hold on any further transactions"

These statements create a **sense of urgency** to push the user to act quickly and emotionally, without thinking

3. Suspicious Link

Text says: **"Login to your account"**

Links like this in phishing emails often direct users to **fake login pages** that look like real banking sites, but are designed to steal credentials.

4. Generic Greeting

Addressed to **"John Doe"**

Real banks typically personalize emails using **your actual name**, not placeholders or generic names.

5. Fake Assurance Statement

"We'll never ask for your personal information…" is meant to **build false trust**, but contradicts the email's behavior asking you to click a login link.

6. Unprofessional Elements

Slight formatting inconsistencies and **overuse of red text** may indicate the email is not professionally crafted.

The email footer says it's an **automatically generated email**, but asks for sensitive actions—which is contradictory.

7. No Secure HTTPS Link Visible

There's no visible hyperlink or secure connection preview (e.g., `https://bankofamerica.com`), which legitimate emails usually show.

CONCLUSION

This email is almost certainly a **phishing attempt**. Do **not click any links**, and report it to your IT/security team or the actual Bank of America.