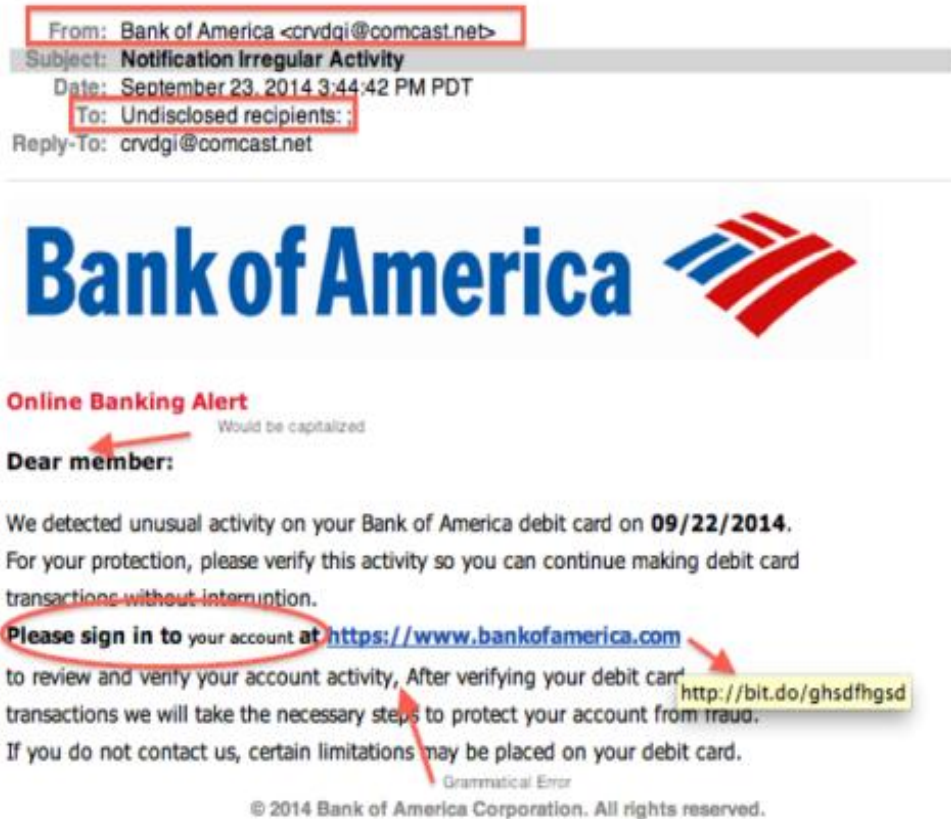


Task 2: Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Outcome: Awareness of phishing tactics and email threat analysis skills.



❑ What is this?


This is a **fake email** pretending to be from **Bank of America**. This type of email is called a **phishing email**.

Phishing is a trick used by cybercriminals to steal your personal information like your passwords, bank details, or credit card numbers.




Let's break down the email:

1. Fake Email Address

- Look at the “From” part at the top:
It says it's from "Bank of America" but the actual email is:
 crvdqi@comcast.net
- Real emails from Bank of America would use something like @bankofamerica.com.

Why it's bad: Scammers are pretending to be the bank, but they're using a personal email provider like Comcast.

2. Strange Subject and Urgency

- The subject says: **“Notification Irregular Activity”**
- In the message, it says:
 *“We detected unusual activity on your Bank of America debit card.”*

Why it's bad:



They are trying to **scare you** so you **click quickly** without thinking. Real banks **don't use fear** to make you act fast.

3. Generic Greeting

- It says: **“Dear member”**
But a real bank knows your name and would say something like **“Dear John Smith”**

Why it's bad: Scammers send this to **many people**, not just you. That's why it's not personalized.

4. Fake Links

- It shows this link:
 <https://www.bankofamerica.com>
- But when you click it, it takes you to:
 <http://bit.do/ghsdfhgsd> (a short link)

Why it's bad:

They are **hiding the real link**. That short link could lead to a **fake website** that looks like Bank of America but is designed to **steal your password**.

5. Bad Grammar and Spelling

- Examples in the email:
 - “limitations may be placed” – unclear sentence.
 - “would be capitalized” – weird comment left in the email.
 - Random bold and capital letters.

Why it's bad:

Real companies check spelling and grammar. Bad grammar is often a **sign of a scam**.

6. Unusual Behavior

- They ask you to click a link to verify your debit card.

Why it's bad:

Banks **never** ask for sensitive details like this through email. They want you to call or log in from their official website directly.





7. Misleading Branding

- While the **Bank of America logo** is used, scammers often copy brand images to make phishing emails look authentic.

Conclusion:

This email is a **phishing attempt** and should **not be trusted or acted upon**. Users should avoid clicking on any links and report the email to their bank or appropriate cybersecurity authority.

What Should You Do If You Get an Email Like This?

-  Don't click any links.
-  Don't reply.
-  Delete the email.
-  Report it to the real bank or your country's cybercrime center.

Tips to Stay Safe

- Always check the sender's email address.
- Don't trust emails that try to scare you.
- Type the website name yourself in your browser.
- Enable two-step verification (like a code to your phone) for extra security.

