Phishing Email Analysis Report

Objective:

To identify phishing characteristics in a suspicious email sample using free online tools such as Email Header Analyzer, VirusTotal, and MXToolbox.

Sample Phishing Email:

Subject: Urgent: Account Verification Required
From: info@securebank-verification.com
To: yagnasree43@gmail.com
Date: September 25, 2025
Body:
Dear Customer,
We detected unusual login attempts on your bank account. To prevent unauthorized access, please verify your account details by clicking the link below:
Verify Your Account
Failure to complete verification within 24 hours will lead to account suspension.
Thank you,
SecureBank Customer Service.

Analysis:

1. Suspicious Sender Address:

Email: info@securebank-verification.com

Issue: The domain 'securebank-verification.com' is not an official bank domain and is likely registered to impersonate a legitimate organization.

2. Urgent or Threatening Language:

The phrases "Urgent" and "Failure to complete verification within 24 hours will lead to account suspension" create panic and pressure the recipient into acting quickly.

3. Suspicious Link:

Displayed Text: Verify Your Account

Actual URL: http://secure-login-confirm.com/verify

Issue: The link leads to a fake banking domain designed to steal credentials. When checked on VirusTotal, the domain shows malicious indicators.

4. Generic Greeting:

Text: "Dear Customer"

Issue: The email does not address the recipient by name, indicating it is likely sent to multiple users at once.

5. Grammar and Tone Issues:

The tone is overly urgent and fear-inducing. While the grammar is correct, legitimate financial institutions avoid threats of account suspension via email.

6. Email Header Check:

Domain: securebank-verification.com

Issue: WHOIS lookup reveals the domain was recently registered and not linked to any official banking organization. SPF and DKIM records failed validation, indicating potential spoofing.

⍰ Tools Used:

- Email Header Analyzer (MXToolbox) – to inspect sender authentication
- VirusTotal – to scan URLs for malicious content
- WHOIS Lookup – to verify domain ownership and registration date
- Hook Security Phishing Email Examples – reference samples
- EML Analyzer – to examine raw email headers

Conclusion:

This email shows multiple phishing indicators such as a spoofed sender domain, urgent tone, fake verification link, and lack of personalization. The domain analysis and VirusTotal results confirm that the URLs are potentially malicious.

Recommendation: Do not click any links or reply to the message. Immediately report this email as phishing to your email provider or IT department.