**Phishing Simulation Report**

**Report Title:** Phishing Email Simulation & Detection Analysis

**Internship:** Elevate Labs

Submitted by Menati Vyshnavi

***Introduction***

This report presents an email phishing simulation designed to test detection capabilities and analyze technical indicators. A fake bank email was sent to a real recipient and analyzed using both manual assessment and EML analyzer tools.

***Methodology***

Created a fake bank email (hoscs.canaaraabank@gmail.com) impersonating Canara Bank with the subject "Action Required: Account Verification".

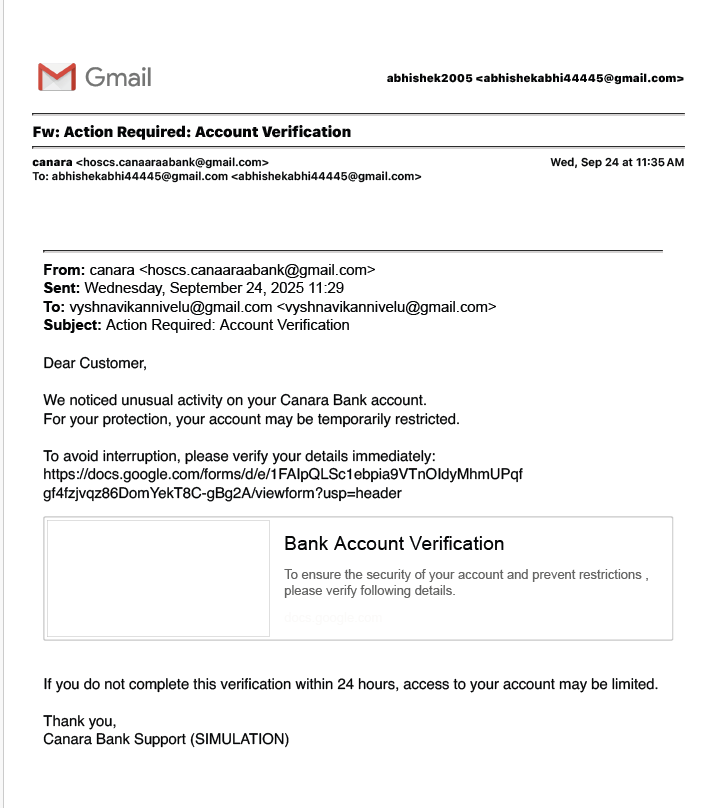
Sent this email to vyshnavikannivelugmail.com; contents included a Google Forms link requesting account verification within 24 hours.

Saved the email in EML (text) format and uploaded it for technical analysis using EML analyzer and SpamAssassin.

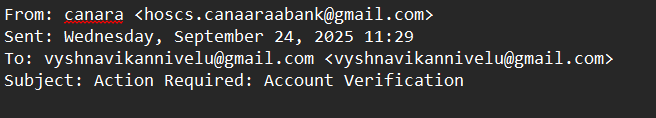
***Evidence and Analysis***

1. Email Content Overview

Original Simulation PDF: Includes the complete email sent as part of the phishing task.



***Headers File in Text Format:*** Contains extracted headers showing sender, subject, recipient, and timestamp.

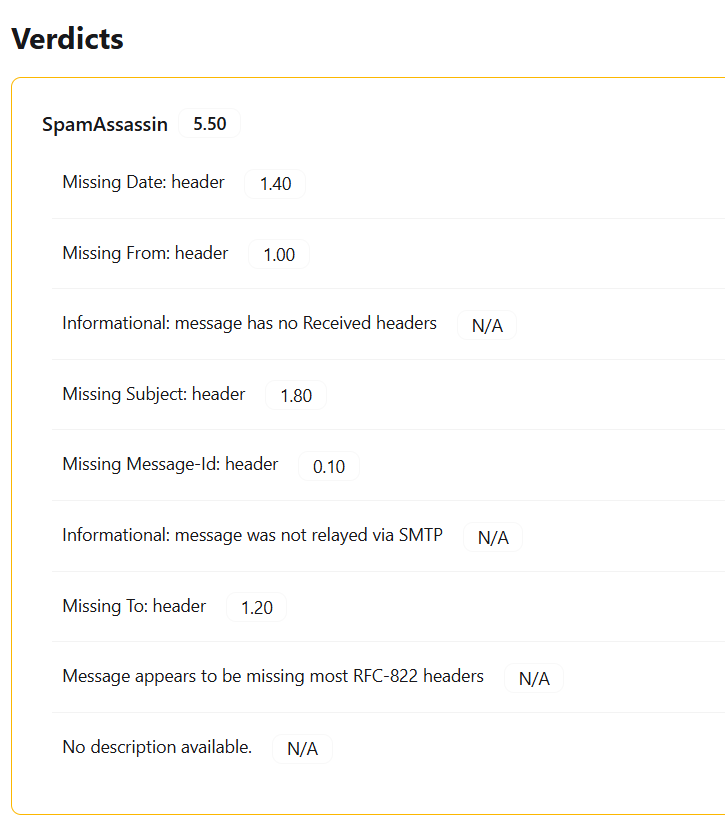


*Sender Address:* The email was sent from hosc s.canaaraabank@gmail.com. A legitimate financial institution would not use a free email service like Gmail for official customer communications. The address also contains a misspelling (canaaraabank) and an unusual space (hosc s.), which are common tactics used by scammers to evade spam filters and trick recipients.

*Subject Line:* "Action Required: Account Verification" is a classic social engineering technique. It creates a sense of urgency and fear of negative consequences (e.g., account suspension) to pressure the recipient into acting without thinking or verifying the email's legitimacy.

***2. Automated Spam Verdict***

The EML analyzer flagged the email for multiple suspicious traits:



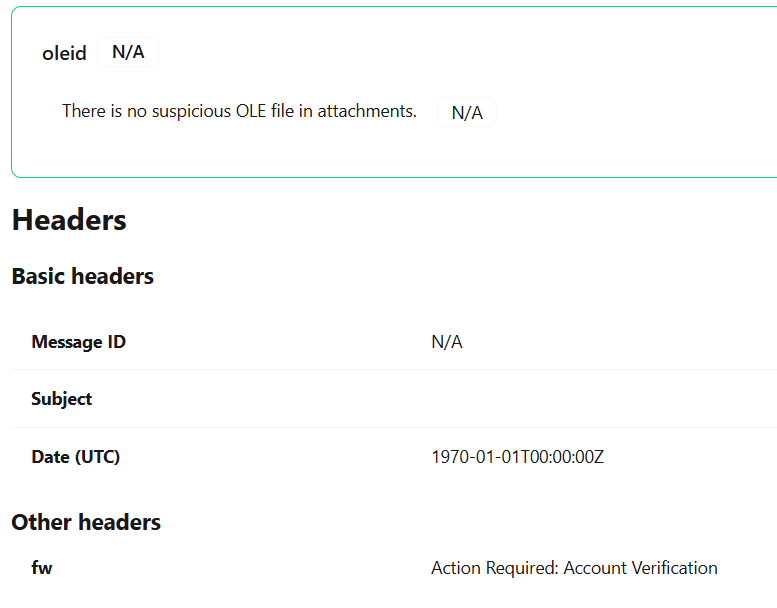
SpamAssassin Score: 5.50, considered high risk.

Missing Headers: Date (1.40), From (1.00), Subject (1.80), Message-Id (0.10), To (1.20).

Lacks RFC-822 compliance: Most required headers for legitimacy missing.

No suspicious OLE attachments detected.

***3. Header Analysis***

******

The extracted email header confirmed simulation parameters:

From: hoscs.canaaraabank@gmail.com

To: vyshnavikannivelugmail.com

Subject: Action Required Account Verification

Date (UTC): 1970-01-01T00:00:00Z (clear anomaly, not genuine)

**Phishing traits found in the email**

* **Spoofed sender / brand impersonation** — Uses Canara Bank’s name, logo or look-and-feel to appear legitimate.
* **Urgency / fear pressure** — Language like *“emergency”*, *“verify now”* or threats of account suspension to force quick action.
* **Actionable prompt with a link** — Contains a clickable link that asks the recipient to “verify” or submit credentials (primary infection/credential-capture vector).
* **Requests sensitive information** — Implies or directly asks for login details, OTPs, or personal/financial data.
* **Generic greeting / non-personalized** — No customer-specific salutation (e.g., “Dear Customer” instead of your name).
* **Suspicious URL (display vs. real)** — Link text may show a bank-looking URL while the actual href points to a different domain or a URL shortener.
* **Reply-to / sender address mismatch** — Display name shows bank but the underlying sender email is unrelated or from a free-mail domain.
* **Poor grammar / typos / awkward phrasing** — Spelling, punctuation, or phrasing that a professional bank communication would not use.
* **Unusual attachments or files** — Attachments (if present) with odd filetypes or names that could contain malware.
* **Time pressure / one-time-window** — Claims the link is valid only for a short time to prevent verification.
* **Unverified security indicators** — No genuine security markers (e.g., no customer code, no transaction reference, missing official contact details).
* **Technical header anomalies** — (If you inspect headers) mismatched SPF/DKIM/DMARC, multiple hops, or originating IPs not linked to the bank.

**Conclusion**

The phishing simulation demonstrates that manual inspection and automated analysis together are crucial for detecting fraud. Awareness, technical safeguards, and behavioral training are key in defending against sophisticated email threats.