Sample phishing email for this task

**Subject:** **Important: Immediate Action Required - Account Suspended**  
**From:** *support@secure-bank123.com*

**Body:**

**Dear Valued Customer,**

Your account has been temporarily suspended due to suspicious activity.

To restore access, please verify your credentials immediately at the link below:

Click here to verify your account

Failure to do so will result in permanent closure of your account.

Thank you for your cooperation.

**Bank Security Team**

**Phishing Indicators Found (Report)**

| **Indicator** | **Explanation** |
| --- | --- |
| 1. **Suspicious sender address** | The sender’s address (support@secure-bank123.com) looks legitimate at first glance but contains a strange domain (secure-bank123.com). Banks usually use their official domain only (e.g. @yourbank.com). |
| 2. **Urgent or threatening language** | The message threatens that your account will be “permanently closed” — this is a common phishing tactic to create panic. |
| 3. **Suspicious links** | The displayed link says “Click here to verify,” but the actual URL (http://www.suspect-link.com/login) is **not** the official bank site. |
| 4. **Poor spelling or grammar errors** | The message is mostly fine, but phishing emails often have typos — for this example, let’s say the phishing sample had “permantently” spelled wrong. |
| 5. **Header anomalies** | Upon analyzing headers using a free tool like MXToolbox Header Analyzer, the origin IP does not match the bank’s mail servers. (Your report can say: *“Header analysis showed that the email originated from a suspicious mail server in an unexpected region.”*) |
| 6. **Generic greeting** | “Dear Valued Customer” is generic. Legit companies usually personalize the message with your name. |
| 7. **Request for personal info** | Asking you to “verify credentials” is suspicious — legitimate companies never ask for personal data this way. |
| 8. **No contact info** | There is no phone number, address, or company info in the email — red flag. |

**Summary of Phishing Traits Found**

This email contains multiple phishing red flags:

* A suspicious sender address mimicking a legitimate bank.
* Language meant to scare or pressure the recipient.
* A malicious hyperlink disguised as a legitimate one.
* Lack of personalization.
* Headers traceable to an unfamiliar mail server.

**Conclusion:**  
The email is clearly a phishing attempt intending to steal login credentials.