**Phishing mail**

**From:** support@yourbank-secure.com  
**To:** anilagali11@gmail.com

Dear Valued Customer,

We have detected **unusual activity** in your bank account and have temporarily **suspended access** for your protection.

To restore access, please verify your identity by clicking the secure link below:

👉 Verify Now 👈

Failure to verify your information within 24 hours will result in **permanent suspension** of your account.

Thank you for banking with us.

Sincerely,  
**YourBank Security Team**  
[support@yourbank-secure.com](mailto:support@yourbank-secure.com)

1. Sender email looks legitimate but it is not original as “–“ in mail address is suspicious in banks original id – is not present
2. Mail header check

Return-Path: <support@yourbank-secure.com>

Received: from suspiciousmail.ru (123.45.67.89)

by mx.google.com with ESMTPS id abc123xyz

for <youremail@example.com>;

Mon, 5 Aug 2025 14:55:00 -0700 (PDT)

Authentication-Results: mx.google.com;

spf=fail (google.com: domain of support@yourbank-secure.com does not designate 123.45.67.89 as permitted sender)

From: YourBank <support@yourbank-secure.com>

To: youremail@example.com

Subject: URGENT: Your Account is Suspended

**Red Flags in a Header:**

| **Header Field** | **Red Flag Example** | **Meaning** |
| --- | --- | --- |
| **Return-Path** | support@yourbank-secure.com | Not the official domain |
| **Received** | from suspiciousmail.ru (123.45.67.89) | Sent from non-company server |
| **SPF/DKIM/DMARC** | spf=fail, dkim=fail, dmarc=fail | Fails email authentication |
| **From** | Shows official name, but the domain is off (e.g., -secure.com) | Fake display name |
| **Reply-To** | Different from From: address | Redirecting replies elsewhere |

1. Suspicious link present as verify now
2. Mail contains state of urgency as threatening of account block in 24hous
3. [support@yourbank-secure.com](mailto:support@yourbank-secure.com) - suspicious mail

[support@yourbank.secure.com](mailto:support@yourbank.secure.com) – original mail

6.grammer mistake

Legitimate companies rarely send threat message. This mail includes threat of account block

Last line – thanking for banking with us – this is not a way of bank mail closure

Mail is generic most of genuine bank mails contain name of customer

### 7. **Phishing Traits in the Sample Email**

1. **Generic Greeting**
   * Uses “Dear Valued Customer” instead of the recipient’s name.
2. **Urgent and Fear-Inducing Language**
   * Words like **“URGENT,” “Suspicious Activity,” “Account Suspended”** create panic.
3. **Unusual or Fake Sender Address**
   * Example: support@yourbank-secure.com instead of the official domain.
4. **Suspicious Links**
   * Encourages clicking on vague or disguised links like **“Verify Now.”**
5. **Threat of Consequences**
   * “Failure to verify… will result in permanent suspension” – creates urgency and fear.
6. **Poor Grammar and Awkward Phrasing**
   * Slight grammatical issues and unnatural sentence structure.
7. **No Personalization**
   * No use of the recipient's name, account number, or reference ID.
8. **Unverified or Mismatched Contact Information**
   * Uses a support email that does not match the official bank domain.
9. **Request for Immediate Action**
   * Pushes the user to act **within 24 hours** – a common phishing tactic.
10. **Too Generic and Vague**
    * Doesn’t mention which bank account or activity is in question