Title: **Phishing Email Analysis**
Author: <Pritam>
Date: 26 October 2025

Executive Summary:
The email analyzed is classified as phishing due to mismatched sender headers, failed SPF/DKIM/DMARC checks, suspicious links, and urgent threatening language.

1. Sample Email:

From: "Your Bank - Important" <support@secure-bank.com>
To: you@example.com
Subject: Urgent: Verify Your Bank Account Now
Date: Mon, 20 Oct 2025 08:12:03 +0000
<body>...</body>

2. Sender Analysis:

- Display Name: Your Bank - Important
- From: support@secure-bank.com (suspicious domain)
- Reply-To: support@secure-bank-secure.com (mismatch)

3. Header Analysis:

- SPF: fail
- DKIM: none
- DMARC: fail
- Originating IP: 203.0.113.45 (not recognized bank IP)

4. Links & Attachments:

- Visible Link: https://secure-bank.com/verify
- Actual Href: http://malicious.example/login

- Attachments: invoice.doc.exe (potentially malicious)

5. Language & Social Engineering:
   - Urgent/Threatening: "verify within 24 hours", "account suspension"
   - Spelling/grammar errors: "immediatly"

6. Risk Assessment:
   - Clicking the link could lead to credential theft.
   - Executing attachments could compromise the system.

7. Remediation:
   - Do not click links or open attachments.
   - Report to official bank channels.
   - Mark email as phishing.
   - Change passwords if credentials were entered.
   - Enable MFA.

Appendix:
   - Screenshots and artifacts included in respective folders.