Phishing Email Analysis Report

Intern Name: Hemanth Kumar
Date: 24-09-2025
Task: Analyze a Phishing Email Sample

Step 1: Obtain a Sample Phishing Email

Sample Email:

From: "Bank Security Team" security@onlinebank.example
To: hemanth@example.edu
Subject: Urgent: Verify Your Account Immediately

Email Body:

```
Dear Customer,

We have detected unusual activity on your OnlineBank account. To prevent
temporary suspension, please verify your account information immediately.

Click the link below to verify your account:
https://onlinebank.example/verify-account

Failure to verify within 24 hours will result in account suspension.

Thank you for your prompt attention.

Sincerely,
Bank Security Team
OnlineBank
```

Step 2: Examine Sender's Email Address for Spoofing

- **From:** security@onlinebank.example
- **Return-Path:** no-reply@mail-notify.example
  Analysis: Sender domain does not match the return path, indicating possible spoofing.

Step 3: Check Email Headers for Discrepancies

Header Analysis:

```
Received-SPF: fail
Authentication-Results: spf=fail; dkim=neutral; dmarc=fail
Received: from unknown (203.0.113.10)
```

Analysis: - SPF failed, DKIM neutral, DMARC failed → email not verified by domain. - Received from an unknown IP address → suspicious.

Step 4: Identify Suspicious Links or Attachments

- **Suspicious Link:** https://onlinebank.example/verify-account
- **Attachments:** None
  Analysis: Link may redirect to a malicious website if clicked.

Step 5: Look for Urgent or Threatening Language

- **Examples:**
- "Failure to verify within 24 hours will result in account suspension"
- Pressure tactic to force immediate action.

Step 6: Note Any Mismatched URLs

- Hovering over the link may reveal a different domain than the bank's official site → mismatch indicating phishing.

Step 7: Verify Presence of Spelling or Grammar Errors

- **Observation:** No major errors found.
- Note: Many phishing emails often contain spelling or grammar mistakes.

Step 8: Summarize Phishing Traits Found in the Email

- Sender spoofing / mismatched email addresses.
- Email fails SPF, DKIM, and DMARC authentication checks.
- Urgent language to scare the recipient.
- Suspicious link that could redirect to a malicious website.
- Generic greeting ("Dear Customer") instead of recipient's name.
- Possible branding inconsistencies (fake bank domain, no logo).

Conclusion: This email is a phishing attempt. Users should **not click links or provide credentials** and report it to the IT/security team.