1. Sample Phishing Email

- Subject: Urgent: Verify Your Account Now!
- From: support@secure-paypal.com
- Body: Your account has been suspended. Click the link to verify your account.
- Link: http://paypal.account-verify.com/

2. Examine Sender's Email Address

- Email address: support@secure-paypal.com
- Looks like a trusted source, but is not from the official PayPal domain.
- Spoofing technique to mislead the recipient.

3. Check Email Headers

- Header shows mismatch in 'From' and 'Return-Path' addresses.
- IP address does not belong to PayPal.
- SPF and DKIM records fail to authenticate.

4. Suspicious Links or Attachments

- Link appears to be from PayPal but leads to a phishing site.
- Attachments may contain malware (.exe, .zip, .pdf).
- Never download or click unknown attachments.

5. Urgent or Threatening Language

- Email states: 'Your account has been suspended'.
- Creates a sense of urgency to act quickly.
- Often used to bypass rational decision-making.

6. Mismatched URLs

- Visible link: https://www.paypal.com
- Real link (hover): http://paypal.account-verify.com
- Mismatch indicates phishing attempt.

7. Spelling or Grammar Errors

- Example: 'Your account has been suspnded'.
- Grammar errors: awkward sentence structure or types.
- Legitimate companies rarely send such emails with mistakes.

8. Summary of Phishing Traits

- Spoofed sender address
- Header inconsistencies
- Mismatched or suspicious links
- Urgent and threatening language
- Poor spelling/grammar
- Unusual attachments