CYBER SECURITY INTERNSHIP
Task 2

Hints/Mini Guide:
1.Obtain a sample phishing email (many free samples online).
2.Examine sender's email address for spoofing.
3.Check email headers for discrepancies (using online header analyzer).
4.Identify suspicious links or attachments.
5.Look for urgent or threatening language in the email body.
6.Note any mismatched URLs (hover to see real link).
7.Verify presence of spelling or grammar errors.
8.Summarize phishing traits found in the email.
Outcome: : Awareness of phishing tactics and email threat analysis skills.

Ans.

1. Sample Phishing Email

(Representative sample taken from PhishTank-style phishing examples):

```
Subject: Urgent: Account Verification Required

From: [email protected]

Dear User,

Due to suspicious activity, your account is temporarily suspended. Please
click the link below to verify your account immediately to avoid permanent
deactivation:

Verify Now

Best regards,
Your Service Team
```

---

2. Sender's Email Address (Spoofing)

- Displays as a known organization’s name, but the actual address (`[email protected]`) is unrelated and suspicious.
- Spoofed domains often mimic real ones with subtle typos or unfamiliar domains — a common red flag

---

3. Header Analysis

- If you paste full headers into an online header analyzer (e.g. MXToolbox), you'd likely see mismatched **Return-Path**, **Reply-To**, or **Received** lines that don't align with legitimate mail servers.
- Spoofed headers are often used to hide the true sender origin

---

4. Suspicious Links or Attachments

- Contains a "Verify Now" button or link.
- Hovering reveals the actual destination isn't the trusted company domain — it points to a suspicious, unrelated domain.
- No attachments here, but even attachments labeled `.exe`, `.docm`, or `.zip` would be red flags

---

5. Urgent / Threatening Language

- "Temporarily suspended" and "immediately … avoid permanent deactivation" create urgency.
- This is a typical social engineering tactic to prompt an emotional, hasty response.

---

6. Mismatched URLs

- Hovering over "Verify Now" shows a URL different from the displayed domain/name.
- The visible text may say "YourCompany.com", but the actual URL directs to something like `malicious-site.xyz` —

---

7. Spelling & Grammar Errors

- Generic greeting like "Dear User" instead of your name.
- Might include minor spelling mistakes or awkward phrasing ("account is temporarily suspended").
- Such mistakes are common in phishing emails

8. Summary of Phishing Traits

Indicator	Details
Spoofed Sender	Domain in sender email doesn’t match a verified one
Misleading Header	Email origin and reply paths don’t match legitimate sources
Suspicious Link	Link text mismatched with actual URL upon hovering
Urgent Tone	Threat of account suspension to prompt rash clicking
Generic Greeting	Not addressed to you personally
Language Issues	Subtle grammar/spelling mistakes and awkward phrasing
No Official Branding	Doesn’t include authentic formatting, signatures, or digital security seal artifacts

Conclusion & Awareness Skills

This phishing email exhibits multiple red flags—spoofed sender, urgent language, link mismatches, and generic tone. Recognizing these traits helps build awareness of phishing tactics and strengthens your email threat analysis skills.

Interview Questions:

1.What is phishing?
2.How to identify a phishing email?
3.What is email spoofing?
4.Why are phishing emails dangerous?
5.How can you verify the sender’s authenticity?
6.What tools can analyze email headers?
7.What actions should be taken on suspected phishing emails?
8.How do attackers use social engineering in phishing?

1. What is phishing?

Phishing is a type of cyberattack where attackers impersonate trusted entities (like banks, companies, or services) via email, SMS, or websites to trick individuals into revealing sensitive information such as login credentials, credit card numbers, or personal data.

---

2. How to identify a phishing email?

You can spot a phishing email by looking for these common signs:

- Suspicious sender address (spoofed or unknown domain)
- Urgent or threatening language ("Act now or lose access")
- Generic greetings ("Dear Customer")
- Spelling/grammar errors
- Mismatched or masked URLs (hover to reveal true link)

- Unexpected attachments or requests for personal information

---

3. What is email spoofing?
Email spoofing is when an attacker forges the "From" address in an email header to make it look like it came from a trusted source. This is often used in phishing to trick recipients into believing the email is legitimate.

---

4. Why are phishing emails dangerous?
Phishing emails are dangerous because they can:

- Steal sensitive information (logins, banking info, identity)
- Deliver malware or ransomware via attachments or links
- Trick users into financial fraud or account compromise
- Lead to large-scale data breaches in organizations

---

5. How can you verify the sender's authenticity?
To verify an email sender:

- Check the full email address, not just the display name
- Analyze email headers to trace the real sending domain
- Hover over links to inspect the URL
- Contact the sender through official channels (not by replying to the suspicious email)

---

6. What tools can analyze email headers?
Some popular tools for email header analysis include:

- Google Admin Toolbox – Messageheader
- MXToolbox Header Analyzer
- DNSstuff Email Analyzer
- Mail server logs or email security gateways

---

7. What actions should be taken on suspected phishing emails?

- Do **not** click links or download attachments
- **Report** the email to your IT/security team or email provider
- **Mark it as phishing** or spam in your email client

- **Delete** the email after reporting
- If clicked, run antivirus and change passwords immediately

---

8. How do attackers use social engineering in phishing?
Attackers manipulate emotions and behavior to trick victims into acting. Common tactics include:

- Creating urgency or fear (“Your account will be deleted!”)
- Pretending to be someone familiar or in authority (boss, bank)
- Offering rewards (fake prizes or refunds)
  These psychological tricks pressure users to respond without thinking critically.