# Task 2: Phishing Email Analysis

Objective:

Analyze a sample phishing email and identify common phishing characteristics.

Sample Phishing Email (Microsoft Outlook Scam):

From: Microsoft Outlook <noreply@mícrosoft-support.com>

To: You <youremail@example.com>

Subject: [Action Required] Incoming Emails Are On Hold

Dear User,

We noticed that your Outlook mailbox has exceeded its storage limit. As a result, you are no longer able to receive new emails.

To continue receiving emails and avoid permanent loss of data, please verify your account and increase your storage by clicking the link below:

* [Increase Mailbox Storage](http://outlook-mail-support-verify.com)

If no action is taken within 12 hours, your account will be suspended.

Thank you for your prompt attention to this matter.

Microsoft Mail Support Team

© 2025 Microsoft Corporation. All rights reserved.

## 🔎 Analysis:

### 1. Sender Spoofing:

- Email address: `noreply@mícrosoft-support.com` uses a special character `í` to mimic 'i' in `microsoft`.

### 2. Email Header Discrepancies:

- (Header analysis not available in sample, but could be tested using tools like MXToolbox or Google's Admin Toolbox)

### 3. Suspicious Links:

- The link looks legitimate but leads to `http://outlook-mail-support-verify.com`, which is \*\*not\*\* owned by Microsoft.

### 4. Urgency or Threat:

- "If no action is taken within 12 hours, your account will be suspended."

### 5. Generic Greeting:

- “Dear User” – instead of the user’s actual name.

### 6. Branding Tricks:

- Claims to be from Microsoft with a fake copyright.

## ⚠️ Summary of Phishing Traits Found:

- Spoofed sender address

- Suspicious link

- Threatening/urgent message

- Generic greeting

- Misleading branding

---

## ❓ Interview Questions (with Answers):

1. \*\*What is phishing?\*\*

A cyberattack method where attackers pose as trusted entities to trick users into revealing personal or financial information.

2. \*\*How to identify a phishing email?\*\*

By checking sender email, hovering on links, noticing poor grammar, and analyzing urgency.

3. \*\*What is email spoofing?\*\*

Faking the "From" address to appear as someone the user trusts.

4. \*\*Why are phishing emails dangerous?\*\*

They steal passwords, install malware, and lead to data or financial loss.

5. \*\*How can you verify the sender’s authenticity?\*\*

Use tools to check headers, confirm domain names, or contact the sender via official channels.

6. \*\*What tools can analyze email headers?\*\*

- MXToolbox

- Google Admin Toolbox

- MailHeader Analyzer

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

- Report to IT/security team

- Don’t click or download anything

- Mark as spam

8. \*\*How do attackers use social engineering in phishing?\*\*

They exploit emotions like fear, urgency, and trust to manipulate users into acting quickly.