Phishing Email Analysis Report – Task 2

Name: Neerudi Sharanya

Date: 05-08-2025

Email Sample Source: https://www.hooksecurity.co/phishing-email-examples

# 🎯 Objective

To identify phishing characteristics in a suspicious email that pretends to be from Amazon, using an example found on the Hook Security website.

# 🛠️ Tools Used

- Email Source: Hook Security sample phishing email

- Header Analysis Tool: MXToolbox Email Header Analyzer (used in real cases)

- Browser (for link hover checks)

- Phishing analysis knowledge

# 📨 Step-by-Step Analysis

## Step 1: Sender’s Email Address (Spoofing Check)

The email claims to be from Amazon, but the actual sender address is not visible. In phishing attempts, attackers typically use spoofed domains or public email addresses like gmail.com. This is a strong sign of spoofing.

## Step 2: Email Header Check

Not applicable in this image-based sample. However, in real scenarios, email headers reveal SPF/DKIM failures and IP mismatches.

## Step 3: Suspicious Links or Attachments

Order numbers and tracking links are usually clickable in real emails. Phishing emails link to fake domains such as 'amazon-support-verify.com'. These are meant to harvest login credentials.

## Step 4: Urgent or Threatening Language

The email uses psychological manipulation by implying that a product was ordered without your knowledge. This creates panic and prompts the recipient to click the link.

## Step 5: Mismatched URLs

Although hover-check is not possible on an image, phishing emails typically use URLs that appear legitimate but redirect to fake websites.

## Step 6: Spelling or Grammar Errors

The greeting uses 'Hello ,' with an extra space and no name. This is a clear sign of a generic phishing email.

## Step 7: Missing Security/Branding Details

The email lacks a proper footer, digital signature, and personalized account information that is typically present in legitimate Amazon emails.

# Summary of Phishing Traits Found

|  |  |  |
| --- | --- | --- |
| # | Indicator | Description |
| 1 | Spoofed Sender | Missing/unknown email address — likely fake |
| 2 | Urgent Setup | Implies a purchase you didn’t make |
| 3 | Suspicious Links | Order ID or delivery links likely redirect to phishing |
| 4 | Generic Greeting | No name personalization |
| 5 | Mismatched URLs | Hovering (in real email) likely reveals fake domains |
| 6 | Styling Issues | Slight formatting problems ("Hello ,") |
| 7 | Missing Security Info | No footer links, no digital signature, lacks Amazon authenticity |

# ✅ Conclusion

This email is a classic phishing attempt designed to mimic Amazon’s shipping confirmation format. It relies on confusion and urgency to trick recipients into clicking fake links. Users should verify all unexpected emails before taking action.