Task 2: Analyse a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

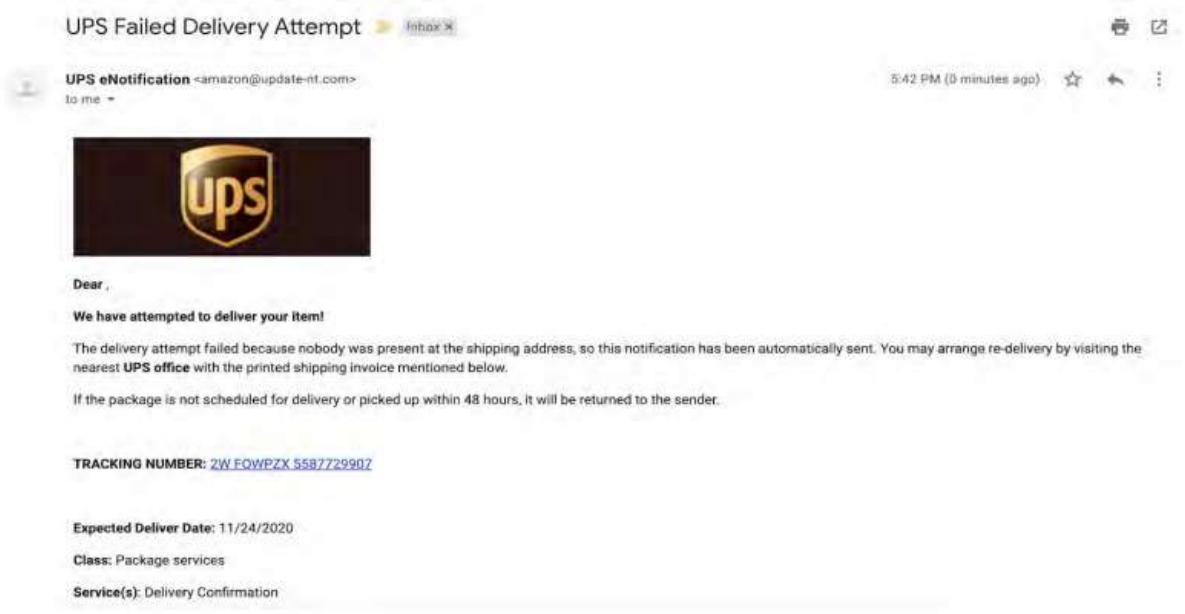
Tools: Email client or saved email file (text), free online header analyser.

Deliverables: A report listing phishing indicators found

Step-by-Step Guide: Phishing Email Analysis

Step 1: Examine the Sender's Email Address

The sender appears as 'UPS eNotification <amazon@update-nt.com>'. The domain 'update-nt.com' is unrelated to UPS. UPS official emails come from '@ups.com'. The mismatch indicates potential spoofing.



UPS Failed Delivery Attempt Inbox ×

UPS eNotification <amazon@update-nt.com>
to me

5:42 PM (0 minutes ago)

Dear ,

We have attempted to deliver your item!

The delivery attempt failed because nobody was present at the shipping address, so this notification has been automatically sent. You may arrange re-delivery by visiting the nearest **UPS office** with the printed shipping invoice mentioned below.

If the package is not scheduled for delivery or picked up within 48 hours, it will be returned to the sender.

TRACKING NUMBER: 2W FOWPZX 5587729907

Expected Deliver Date: 11/24/2020

Class: Package services

Service(s): Delivery Confirmation

Step 2: Check Email Headers

Full email headers should be retrieved from the email client (e.g., Gmail: Show Original). These can be analyzed using an Email Header Analyzer. Potential issues include SPF/DKIM/DMARC failures, IP address anomalies, and mismatches between 'From' and 'Return-Path' fields.

Step 3: Identify Suspicious Links or Attachments

The tracking number link should be hovered over to reveal the actual URL. Phishing emails often disguise malicious sites under seemingly legitimate text. No attachments are shown in this sample, but dangerous formats include '.zip', '.exe', or '.docm'.

Step 4: Look for Urgent or Threatening Language

The message states that if the package is not scheduled for delivery or picked up within 48 hours, it will be returned to the sender. This is a common urgency tactic in phishing emails.

Step 5: Check for Mismatched URLs

Any visible text links (such as 'UPS office') or tracking links should be compared to the actual hyperlink destination. If they do not match, this is a strong phishing indicator.

Step 6: Verify Spelling or Grammar Errors

Minor grammatical issues are present, such as 'Expected Deliver Date' missing the 'y'. Some awkward phrasing exists, such as 'printed shipping invoice mentioned below' when no invoice is provided.

Step 7: Summarize Phishing Traits

Key indicators include:
- Fake sender domain
- Urgent time limit
- Suspicious tracking link
- Brand mismatch (Amazon in sender, UPS in message)
- Minor grammar errors
- Missing personalization (no name after 'Dear,')

Summary Table of Phishing Traits

Trait	Evidence from Email
Fake sender domain	amazon@update-nt.com instead of official UPS domain
Urgency	Warning to act within 48 hours
Suspicious link	Tracking number hyperlink (possible malicious URL)
Brand mismatch	Mentions UPS but sender name is Amazon
Grammar errors	'Expected Deliver Date' missing 'y'
Missing personalization	No recipient name after 'Dear,'