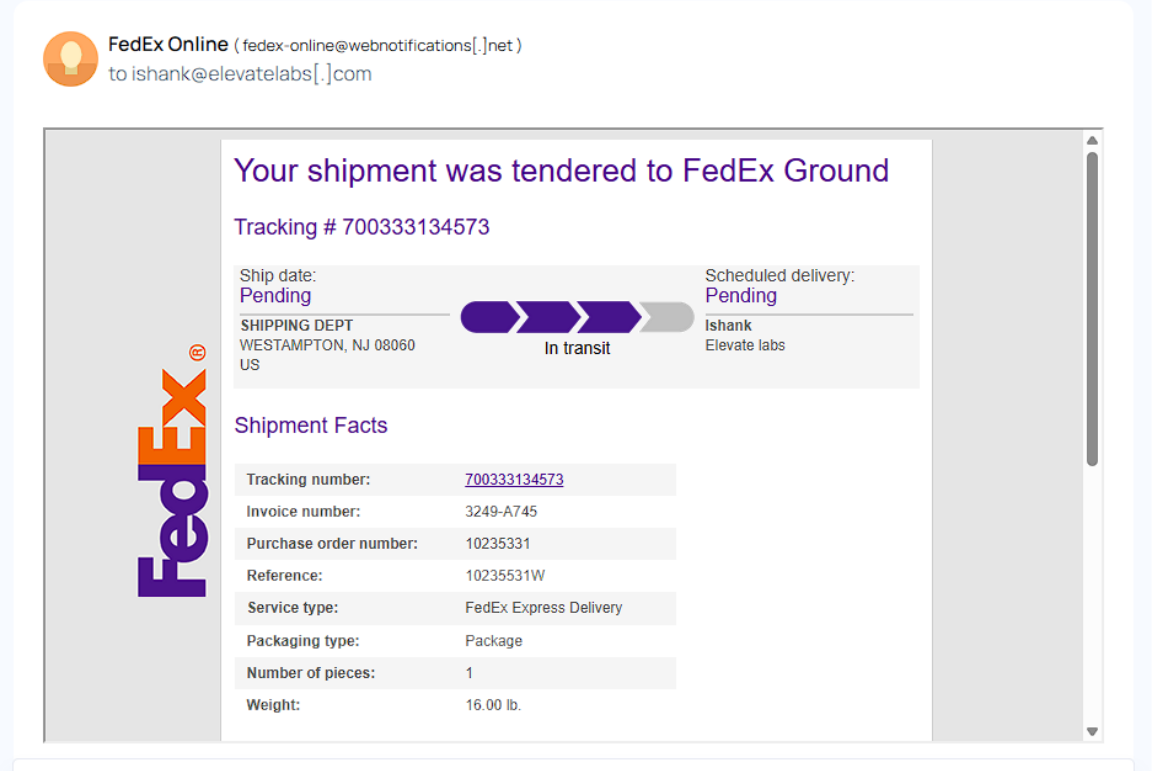
Day 2 Task2 Phishing Mail

1.Obtain a sample phishing email (many free samples online)



FedEx Online (fedex-online@webnotifications[.]net)
to ishank@elevatelabs[.]com

Your shipment was tendered to FedEx Ground

Tracking # 700333134573

Ship date:
Pending
SHIPPING DEPT
WESTAMPTON, NJ 08060
US

In transit

Scheduled delivery:
Pending
Ishank
Elevate labs

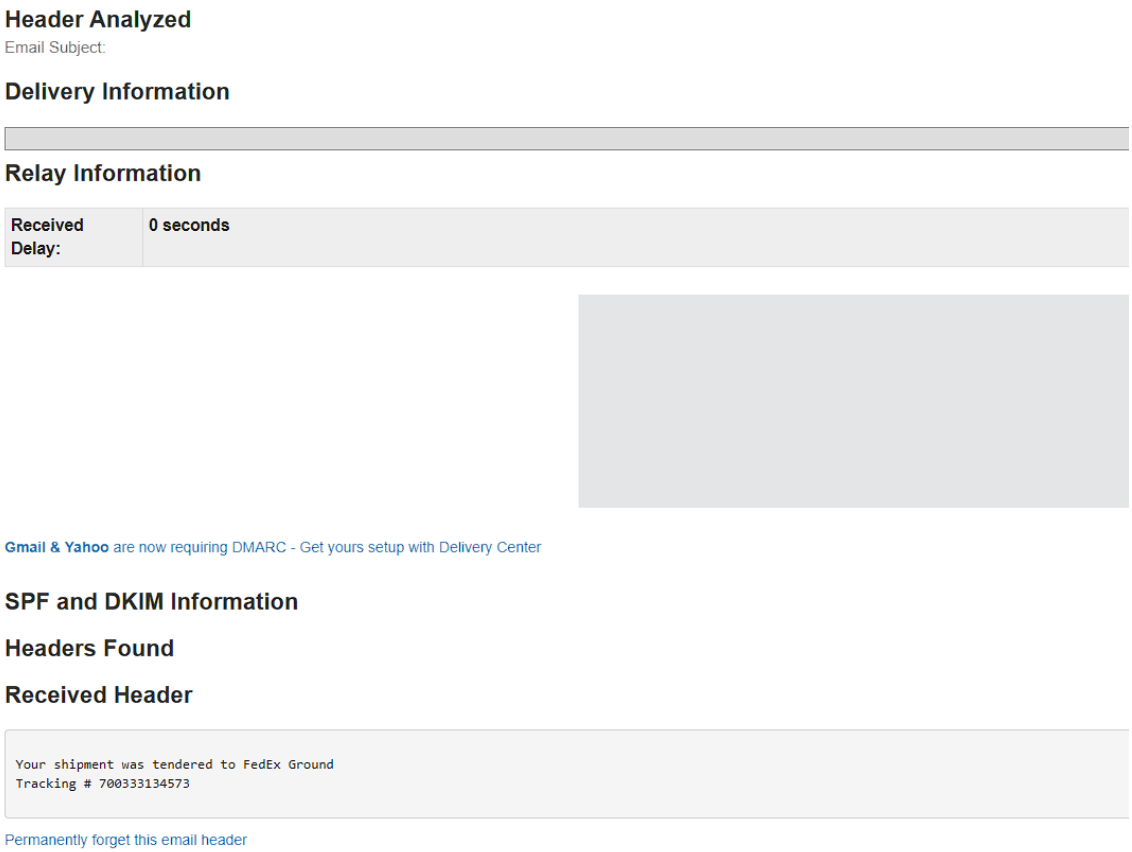
Shipment Facts

Tracking number:	700333134573
Invoice number:	3249-A745
Purchase order number:	10235331
Reference:	10235531W
Service type:	FedEx Express Delivery
Packaging type:	Package
Number of pieces:	1
Weight:	16.00 lb.

2.Examine sender's email address for spoofing.

FedEx Online (fedex-online@webnotifications[.]net)

3.Check email headers for discrepancies (using online header analyzer)



Header Analyzed

Email Subject:

Delivery Information

Relay Information

Received Delay:	**0 seconds**

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

Headers Found

Received Header

```
Your shipment was tendered to FedEx Ground
Tracking # 700333134573
```

Permanently forget this email header

4.Identify suspicious links or attachments.

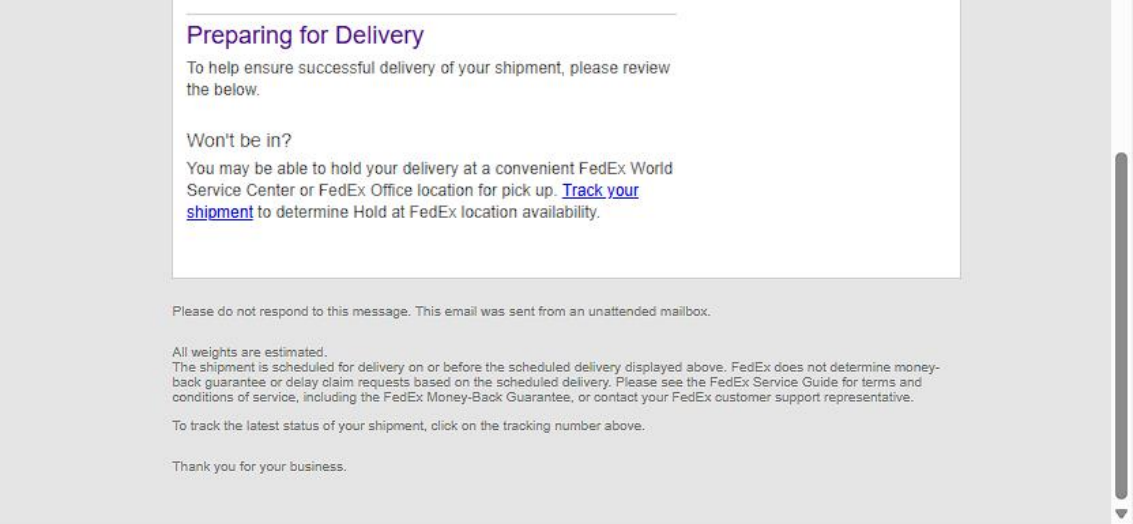
Preparing for Delivery

To help ensure successful delivery of your shipment, please review the below.

Won't be in?

You may be able to hold your delivery at a convenient FedEx World Service Center or FedEx Office location for pick up. ***Track your shipment*** to determine Hold at FedEx location availability.

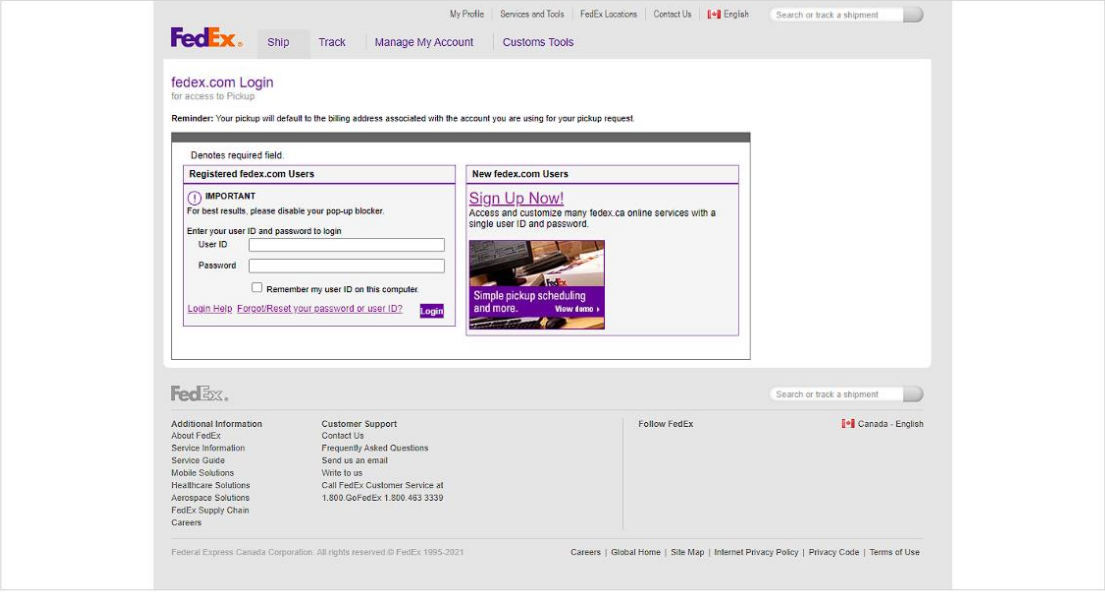
5.Look for urgent or threatening language in the email body



6.Note any mismatched URLs (hover to see real link).

Track your shipment to determine Hold at FedEx location availability.

Redirects to this page.



7.Verify presence of spelling or grammar errors.

Link of sample :
https://caniphish.com/email-phishing-simulator?email=FedEx-Shipment-Tracking#emailTitle

8.Summarize phishing traits found in the email.

Vague or Missing Crucial Details (The "Bait"): Shipment Details are "Pending" or Generic: The Ship

date, Scheduled delivery, and even the initial status ("Your shipment was tendered to FedEx Ground") are either "Pending" or sound very generic for an important notification. A real delivery notification often has a concrete expected date once it's "tendered."

Unfamiliar Sender/Recipient Information (Potentially): The recipient ("Ishank") is mentioned, but the full recipient address is not shown, and the sender is a generic "SHIPPING DEPT WESTAMPTON, NJ 08060 US" without a clear company name attached to the shipment itself (other than "Elevate labs" being associated with the recipient).

Sense of Urgency/Action Required (The "Hook"):Call to Action to "Review the Below" or Track: The line "To help ensure successful delivery of your shipment, please review the below" and the embedded links/instructions to "Track your shipment" or "click on the tracking number" are the primary mechanism for a phishing attack. The goal is to make the user click a malicious link disguised as a FedEx tracking link.

The "Won't be in?" Section: This is a common tactic to prompt a click, as users often want to manage their delivery, and the link to "Track your shipment to determine Hold at FedEx location availability" provides the opportunity for the phisher to redirect to a malicious site.

Inconsistent/Suspicious Professionalism (Potential Phishing Error):Inconsistent Tracking Information: The email starts by saying "Your shipment was tendered to FedEx Ground" but then lists the Service type as "FedEx Express Delivery." This is a major contradiction in shipping details that a legitimate, automated system should not make.

The primary goal of this email is to trick the recipient into clicking the embedded links (e.g., the tracking number, "Track your shipment" button) which, in a real phishing scenario, would lead to a fake website designed to steal personal information, login credentials, or install malware. The vague and contradictory shipping details help mask the illegitimacy of the email.