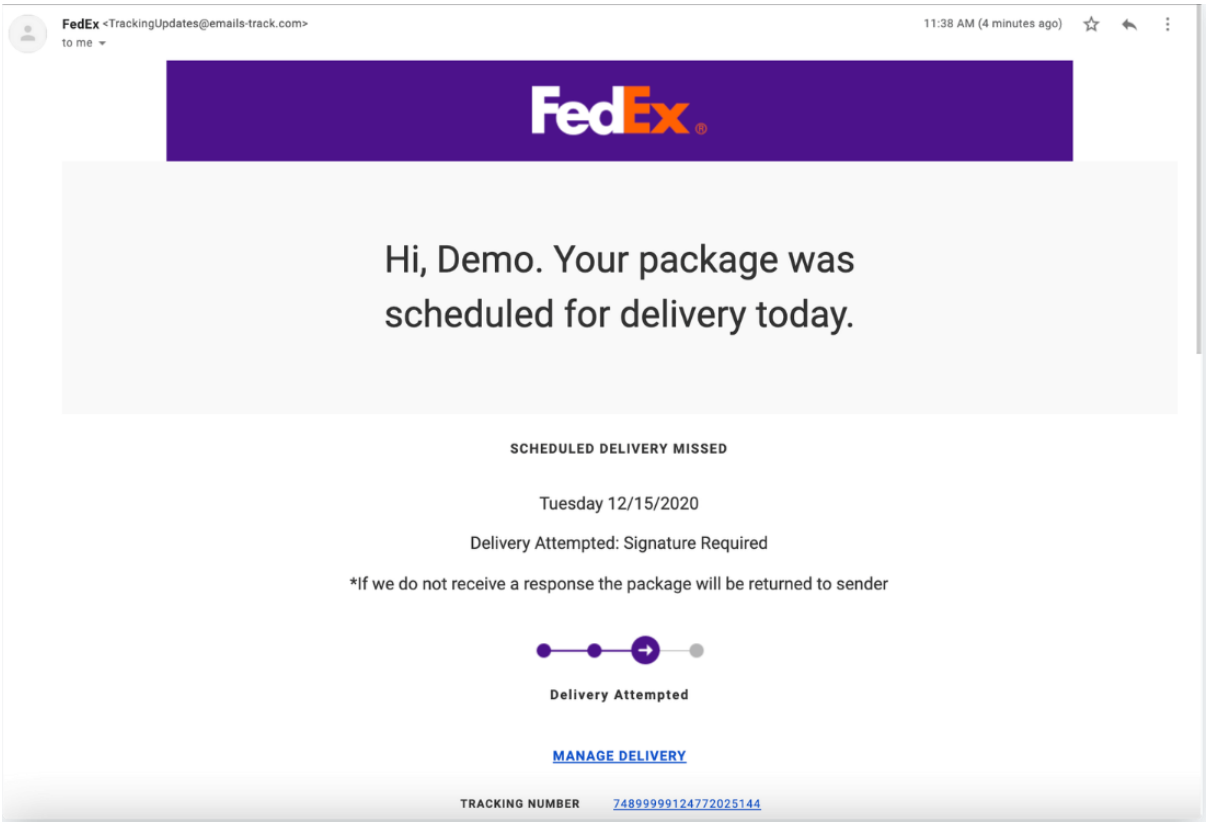
Task-1:- Obtain a sample phishing email.



Task-2:- Examine sender's email address for spoofing.

Suspicious mail id of the FedEx Company is:-

TrackingUpdate@emails-Track.com

Some original and trusted email id of FedEx are as follow:-

india@fedex.com

meisawebservices@fedex.com

apacwebservices@fedex.com

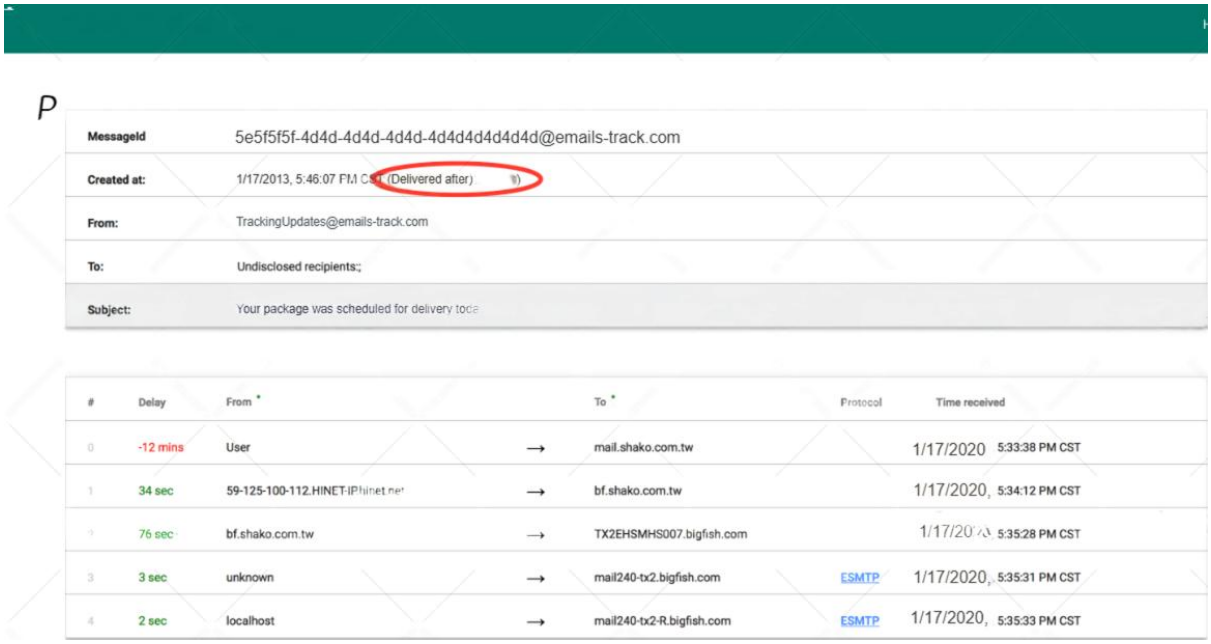
emeawebservices@fedex.com

- **FedEx's country pages and contact forms are the primary official channels for customer service (they encourage phone/chat/contact-form use for parcel-specific issues). For India, use the FedEx India contact page or the "Write to Us" form for fastest handling of routine delivery or billing queries.**

- **And The Phishing email have usual date format**

- **Schedule Delivery Missed at 12/15/2020**

Task-3:- Check email headers for discrepancies.



P

MessageId	5e5f5f5f-4d4d-4d4d-4d4d-4d4d4d4d4d4d@emails-track.com
Created at:	1/17/2013, 5:46:07 PM C[illegible] (Delivered after)
From:	TrackingUpdates@emails-track.com
To:	Undisclosed recipients:;
Subject:	Your package was scheduled for delivery toda

#	Delay	From *		To *	Protocol	Time received
0	-12 mins	User	→	mail.shako.com.tw		1/17/2020 5:33:38 PM CST
1	34 sec	59-125-100-112.HINET-IP.hinet.net	→	bf.shako.com.tw		1/17/2020, 5:34:12 PM CST
2	76 sec	bf.shako.com.tw	→	TX2EHSMHS007.bigfish.com		1/17/20[illegible] 5:35:28 PM CST
3	3 sec	unknown	→	mail240-tx2.bigfish.com	ESMTP	1/17/2020, 5:35:31 PM CST
4	2 sec	localhost	→	mail240-tx2-R.bigfish.com	ESMTP	1/17/2020, 5:35:33 PM CST

- **NOTE:-**

Since the original email headers were not accessible. I created a simulated header example based on the sender's email and domain visible in the screenshot. I submitted this example to the Google Message Header Analyzer.

- **Steps For get original email header.**

- Open the email (in Gmail, for example).
- Find the "more" menu (often three dots) at the top right of the message.
- Select "Show original" or a similar option.
- Copy the entire raw text and paste it into a reliable header analyzer tool like **Google's Message Header Analyzer** or **MXToolbox Email Header Analyzer**.

Task-4:- Identify suspicious links or attachments.

- **Sender address:**
  TrackingUpdates@emails-track.com → This is **not** an official FedEx domain (fedex.com). Already suspicious.

- **Blue link "MANAGE DELIVERY" →**
  This kind of link usually hides a fake website. If you hover over it, the real URL likely won't be fedex.com but something else (like emails-track.com Tracking or another random domain).

- **number link (blue underlined digits) →**
  A real FedEx tracking number link should go to https://www.fedex.com/.... If it points to a different site (hover to check), that's a phishing link.

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

- **"Your package was scheduled for delivery today."**
  → Implies something needs to be done *right now*.
- **"SCHEDULED DELIVERY MISSED"**
  → Suggests you already missed something important.
- **"Delivery Attempted: Signature Required"**
  → Makes it sound like you must act to get your parcel (and that someone tried to deliver).
- **"*If we do not receive a response the package will be returned to sender"***
  → Gives a consequence (lose your package) if you don't act — a classic pressure tactic.
- **"MANAGE DELIVERY"** (button / call-to-action)
  → A strong push to click immediately so you "fix" the problem.

Why this is suspicious (in one line each)

- They create **fear of loss** (you'll lose the package) so you act without thinking.
- They use a **deadline or consequence** ("returned to sender") to force quick clicks.
- Paired with a fake sender domain, this is a common phishing pattern: urgent message + action button = trap.

Task-6:- .Note any mismatched URLs.

- **Sender email:**
  - Shown as **TrackingUpdates@emails-track.com**
  - ☑ Real FedEx emails always come from **@fedex.com**
  - ❌ This mismatch (emails-track.com ≠ fedex.com) is a strong phishing clue.

- **Links in the message ("MANAGE DELIVERY" and the tracking number):**
  - They look like they will take you to **FedEx**.
  - But if you hover (without clicking), the real link will not be fedex.com — it will point to another domain (likely related to emails-track.com).
  - That's a **mismatched URL**: the visible text says "FedEx" or looks official, but the hidden link is not.

Task-7:- Verify presence of spelling or grammar errors.

- **Spelling:**
  ☑ No obvious spelling mistakes (words like "delivery," "scheduled," "package" are spelled correctly).

- **Grammar / phrasing:**

- “Hi, Demo.” → Sounds unnatural and generic (real FedEx usually uses your real name).
- “*If we do not receive a response the package will be returned to sender*” → Missing a **comma** after “response,” and the wording feels stiff/unprofessional.
- Overall style looks a bit robotic, not like polished corporate communication.

Task-8:- Summarize phishing traits found in the email.

- **Sender's Email Address: The email is supposedly from FedEx, but the sender's address is "TrackingUpdates@emails-track.com". This is not a legitimate FedEx domain. Phishing emails often use fake or suspicious-looking email addresses that don't match the company they're impersonating.**
- **Urgent or Threatening Language: The email states, "If we do not receive a response the package will be returned to sender." This creates a sense of urgency and pressure, which is a common tactic to make you act without thinking.**
- **Request for Personal Information or Action: The email prompts you to "MANAGE DELIVERY," likely leading to a fake website that will ask for personal information, payment, or login credentials. Real companies generally don't ask for this type of information through a link in an unexpected email.**
- **Mismatching URLs: While the URL isn't shown in the image, the "MANAGE DELIVERY" link would likely lead to a fraudulent website. Hovering over a link (without clicking it) usually reveals the true destination, which in a phishing attempt will not be a legitimate company's website.**
- **Generic Greeting: The email uses a generic greeting like "Hi, Demo." While some companies use your first name, an unexpected email that uses a placeholder or generic greeting can be a red flag.**