PROJECT REPORT TASK 2

ANALYZE A PHISHING EMAIL SAMPLE

Objective

The objective of this task is to analyze a suspicious email sample and identify common characteristics of phishing attempts. This includes examining the sender's email address, checking email headers, inspecting links and attachments, evaluating the language and tone used, and summarizing all indicators that suggest the email is fraudulent. The goal is to develop awareness of phishing tactics and improve the ability to detect and report such threats.

Tools Used

Tool	Website	Purpose
PhishTank	https://www.phishtank.com	To verify if a suspicious URL is reported and listed as a phishing site.
DomainTools	https://whois.domaintools.com	To perform a WHOIS lookup and gather domain registration details (e.g., owner, creation date) to assess legitimacy.
MxToolbox	https://mxtoolbox.com/EmailHeaders.aspx	To analyze email headers for authentication failures (SPF, DKIM, DMARC) and mail server paths.
VirusTotal	https://www.virustotal.com	To scan suspicious URLs and attachments for malware, phishing behavior, or known blacklists.

Sample Phishing Email

Subject: Urgent Account Verification Required!

From: PayPal Support <service@paypal-secure.com>

Dear Customer,

We detected unusual activity in your PayPal account and have temporarily limited your account access. To restore full access, please verify your identity immediately.

Failure to do so will result in permanent suspension of your PayPal account.

Click the link below to verify your information:

https://paypal.com.secure-login247.info/login

Thank you for your cooperation.

PayPal Security Team

Examine Sender's Email Address for Spoofing

Email spoofing is when attackers make the email appear as if it's coming from a legitimate source (like support@paypal.com) — but it's actually sent from a different, **unauthorized** email address.

Let's Analyze This Example:

From our sample phishing email:

From: PayPal Support <service@paypal-secure.com>

Step-by-Step Breakdown:

1. Look at the Display Name

- **"PayPal Support"** — This *looks legitimate* at first glance.
- But don't trust the display name alone. It can be **easily faked**.

2. Check the Actual Email Address

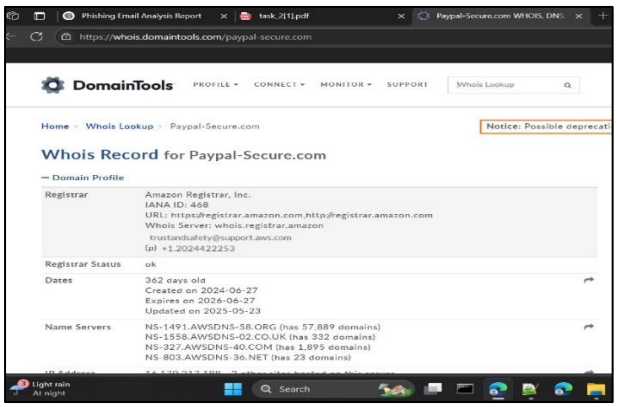
- **Actual sender email**: service@paypal-secure.com
- Real PayPal emails come from:
  - @paypal.com
  - @e.paypal.com
- This email is from a **look-alike domain**: paypal-secure.com
  - This is a **spoof** domain — not the official PayPal domain.
  - Legit companies don't use random hyphenated domains like this.

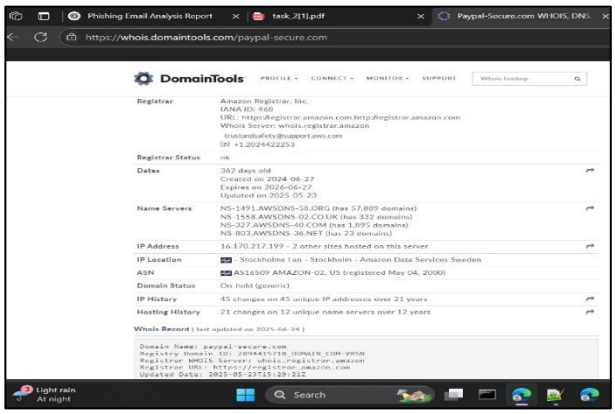
Use Online Tools to Check Domains

To investigate suspicious domains:

- Visit https://whois.domaintools.com/
- Enter paypal-secure.com
- Check:
  - Is it recently created?
  - Who owns it?

- Is it connected to the real company?





The sender's email address in the sample (service@paypal-secure.com) is a spoofed address. Although it uses the name "PayPal Support," the domain is fake and does not belong to the official PayPal company. It is a clear indicator of phishing and domain impersonation.

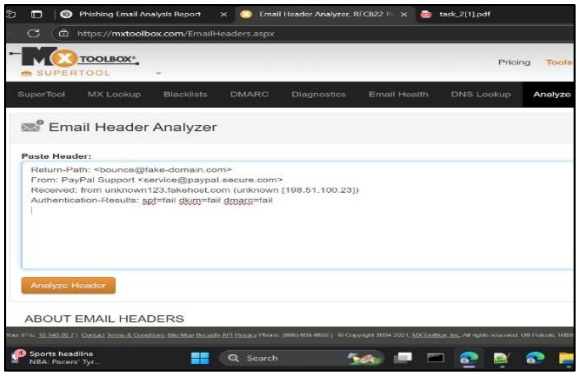
Check Email Headers for Discrepancies

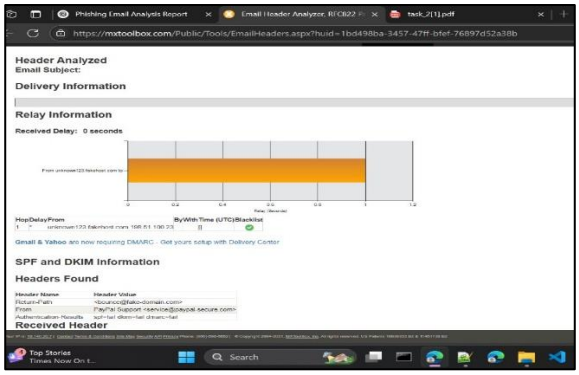
How to Analyze It Using an Online Tool

Step-by-Step Instructions:

1. **Get the Full Email Header**
   - In **Gmail**:
     - Open the email → Click the 3-dot menu → "Show original"
     - Copy the entire text under "Original Message"
   - In **Outlook**:
     - Open the email → File → Properties → Look under "Internet headers"
   - Paste it into Notepad.
2. **Go to an Online Header Analyzer Tool**
   Here are free tool:
   - https://mxtoolbox.com/EmailHeaders.aspx
3. **Paste the Header into the Tool**
   - Copy the full email header text
   - Paste it into the online tool's input box
   - Click "Analyze" or "Submit"

After analyzing, you might see this result:





The email header analysis reveals failed SPF, DKIM, and DMARC checks, indicating that the sender was **not authorized** to send emails on behalf of the domain paypal-secure.com. Additionally, the Return-Path is different from the sender, and the Received fields show suspicious mail server origins. These are clear signs of **spoofing and phishing**.

Identify Suspicious Links or Attachments

1. Look at the Displayed Link vs. Actual Link

In phishing emails, the **text you see** (displayed link) is often **different** from the actual link it opens.

From our sample phishing email:

https://paypal.com.secure-login247.info/login

Check for:

Suspicious Trait	**Example**	**Why It's Suspicious**
Fake subdomains	paypal.com.secure-login247.info	Looks like PayPal, but hosted on another domain
Misspelled URLs	paypa1.com, paypol.com	Typo tricks the user
HTTP instead of HTTPS	http://...	No secure encryption
URL shorteners	bit.ly, tinyurl.com	Hides real destination

2. Hover Over the Link (on Desktop)

- **DON'T CLICK** the link.

- Just place your mouse pointer over the link.
- Look at the bottom of your screen (browser or email client) — it will show the **real destination**.

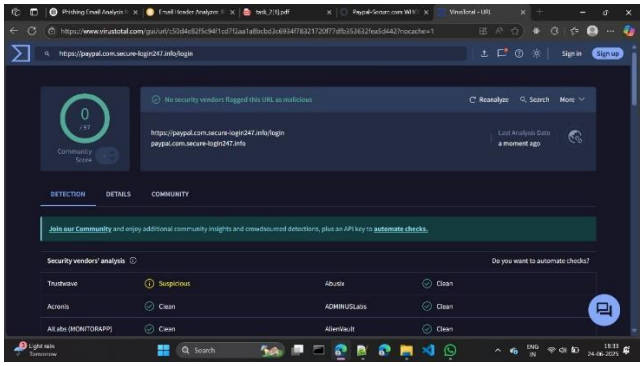
3. Use a URL Scanner Tool (Optional but Safe)

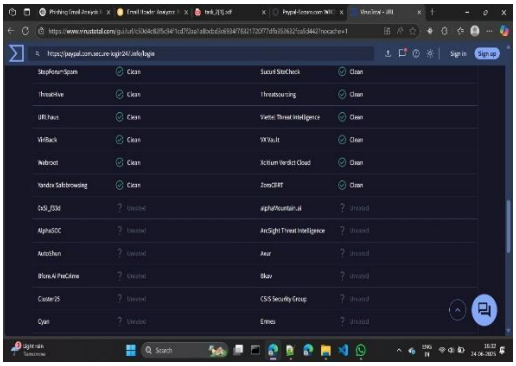
Use tool:

- https://www.virustotal.com/

Steps:

- Copy the suspicious URL
- Paste it into the tool
- Review the results — they tell you if it's linked to known phishing or malware





The email contains a suspicious link https://paypal.com.secure-login247.info/log which misleads the user by placing "paypal.com" within a fake domain.

Analyze the Language in the Sample Email

1. Subject Line:

"Urgent Account Verification Required!"

- The word **"Urgent"** creates **pressure** and **panic**.
- Aims to make the user act quickly without thinking.

Phishing Indicator: High urgency = social engineering tactic.

2. Message Body:

"We detected unusual activity in your PayPal account..."
"...have temporarily limited your account access."

- Creates **fear** that the account is compromised.
- Suggests that something serious has happened.

Phishing Indicator: Claims of account risk to gain trust and urgency.

"To restore full access, please verify your identity immediately."

- Uses **urgency** ("immediately") to pressure the user.
- Pushes the victim toward the **malicious link** without thinking.

Phishing Indicator: Urging immediate action is a red flag.

"Failure to do so will result in permanent suspension..."

- A **threat** to scare the victim.
- Most real companies don't use threatening tone like this.

Phishing Indicator: Threatens loss of service to manipulate the user.

Conclusion

The email uses **multiple manipulation tactics**:

Tactic	**Example Phrase**	**Effect**
Urgency	“Urgent”, “immediately”	Pressures fast reaction
Fear & Alarm	“unusual activity”, “limited your account”	Triggers concern
Threats	“will result in permanent suspension”	Creates panic
Authority tone	“PayPal Security Team”	Pretends to be trustworthy

The phishing email contains **urgent and threatening language** designed to pressure the recipient into immediate action. Words like **“Urgent”**, **“immediately”**, and **“permanent suspension”** are clear examples of social engineering. These phrases aim to **create fear, urgency, and panic**, which are **key indicators of a phishing attempt**.\

Check for Spelling or Grammar Errors

1. Check for Typos

- **In this case:** No obvious typos like “**acount**” or “**suspnsion**”.
- But some phishing emails deliberately avoid mistakes now, to appear professional.

Still, many real phishing emails do contain:

- Wrong spelling: ***"Your acount is at risk"***
- Keyboard mistakes: ***"immediatly", "sucure"***

2. Check for Awkward or Unnatural English

"To restore full access, please verify your identity immediately."

- Grammatically correct, but robotic — lacks personalization or brand tone.

"Failure to do so will result in permanent suspension of your PayPal account."

- The tone is harsh and threatening, which is uncommon in real customer support emails.

Phishing Sign (Language tone):
Even if spelling is perfect, phishing emails often sound:

- Overly urgent
- Robotic
- Impersonal
- Slightly "**off**" from the company's usual tone

3. Lack of Personalization

"Dear Customer,"

Real emails from PayPal usually say:

"Dear [Your Name]"

Red Flag: Phishing emails use generic greetings to target many users at once.

Summary

After analyzing the sample email, several phishing indicators were identified. These include a spoofed sender email address, a misleading login link, and urgent/threatening language that attempts to scare the user into acting quickly. The lack of personalization and unnatural tone further confirm that the email is not from the real PayPal team. The structure and content strongly suggest this is a phishing attempt designed to steal user credentials.