INTERNSHIP ASSIGNMENT

INTERN NAME - **AMIT MAURYA**

TASK - **Analyze a Phishing Email Sample**

So before we dive into all those complex processes, let's first understand what email phishing is, how it happens what are the common patterns that we can look for to determine whether those emails are real or fake .

🛑 What is a Phishing Email?

A **phishing email** is a **fraudulent message** designed to:

- **Trick the recipient** into revealing sensitive information (e.g., passwords, credit card numbers)
- **Lure the user** into clicking malicious links or downloading harmful attachments
- **Impersonate a legitimate organization**, such as a bank, tech company, or government agency

🎯 **Goal**: To **steal data**, gain unauthorized access, or install malware.

🎭 How Phishing Emails Work (Exploitation Process)

1. Social Engineering

Phishing relies on **deceiving people**, not hacking systems.

- They often **mimic trusted entities** (like PayPal, Microsoft, banks).
- They use fear or urgency: "Your account will be locked in 24 hours!"

2. Email Spoofing

Attackers forge the **"From" address** to look like a real company (e.g., security@amazon.com), even though it's fake.

3. Malicious Links

They add links that:

- **Look legitimate**, but redirect to fake websites (phishing sites)
- **Steal login info** when you enter credentials
- Use **URL masking**, e.g., http://paypal.login.security-alerts.com

4. Malicious Attachments

Files like .exe, .zip, .docm, or fake PDFs may:

- Install malware
- Encrypt your files (ransomware)
- Open backdoors for remote access

5. Credential Harvesting

When users enter information into a fake website, it's:

- Stored in attacker's server
- Used for **identity theft**, **bank fraud**, or **corporate access**

🧭 How to Track & Detect Phishing Emails

🔸 1. Header Analysis

Use online tools (like Google Header Analyzer) to check:

- Real sending domain and IP
- SPF/DKIM/DMARC authentication status
- Return-path mismatch (e.g., amazon.com vs. amaz0n.co)

🔸 2. Link Verification

- Hover over links to view the real URL
- Look for mismatches or odd domains
- Tools like VirusTotal or URLScan.io help check links safely

🔸 3. Language Clues

- Check for bad spelling/grammar
- Unusual phrasing, like "Dear User" or "Kindly verify your account now"

🔸 4. Attachment Scanning

Scan unknown files using:

- Windows Defender / Antivirus
- Hybrid Analysis
- Joe Sandbox

🔸 5. Reputation Services

Use threat intelligence databases (like Cisco Talos, PhishTank, or URLhaus) to confirm if a domain or IP is suspicious.
SOME OF THE MAIL WILL LOOK LIKE

We've noticed unusual activity on your PayPal account.
Click below to secure your account:
[https://paypal.secure-login-verification.com]
Failure to respond will result in account suspension.
What's wrong?

- Spoofed sender (paypa1.com)
- Urgent, fear-based message

- Fake URL with a legitimate-looking domain
- No personalization (e.g., “Dear User”)

✅ Summary: Phishing Flow & Detection

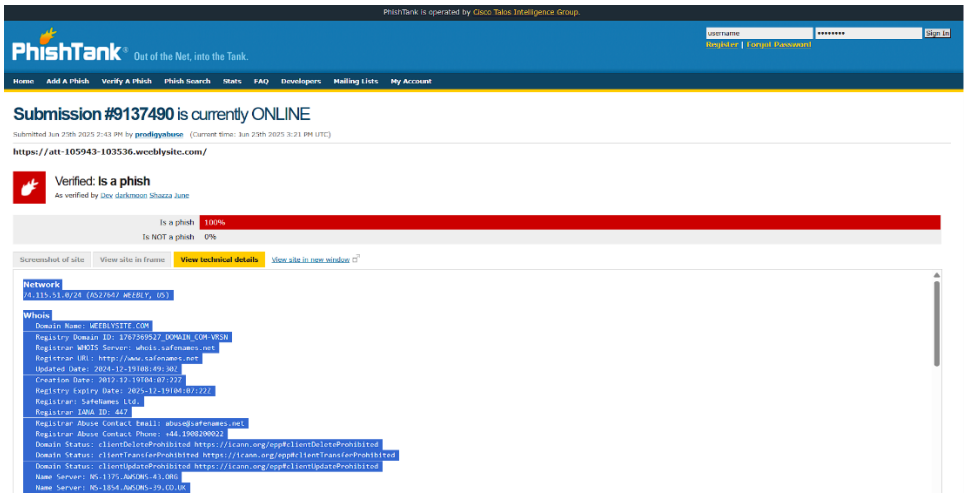
Stage	What Happens	How to Detect
Craft Email	*Spoofed sender, urgent message*	*Header check, language analysis*
Deliver Payload	*Link or attachment*	*Hover links, scan attachments*
Lure Victim	*Fake login page*	*Mismatched URL, suspicious domain*
Capture Data	*User enters credentials*	*Check DNS records, reputation sites*
Exploit	*Use credentials for fraud*	*Monitor activity, MFA, breach alerts*

SO LET'S DIVE TO A PRACTICAL EXAMPLE AND SHOW U HOW ACTUALLY THE PHISHING MAIL LOOKS LIKE

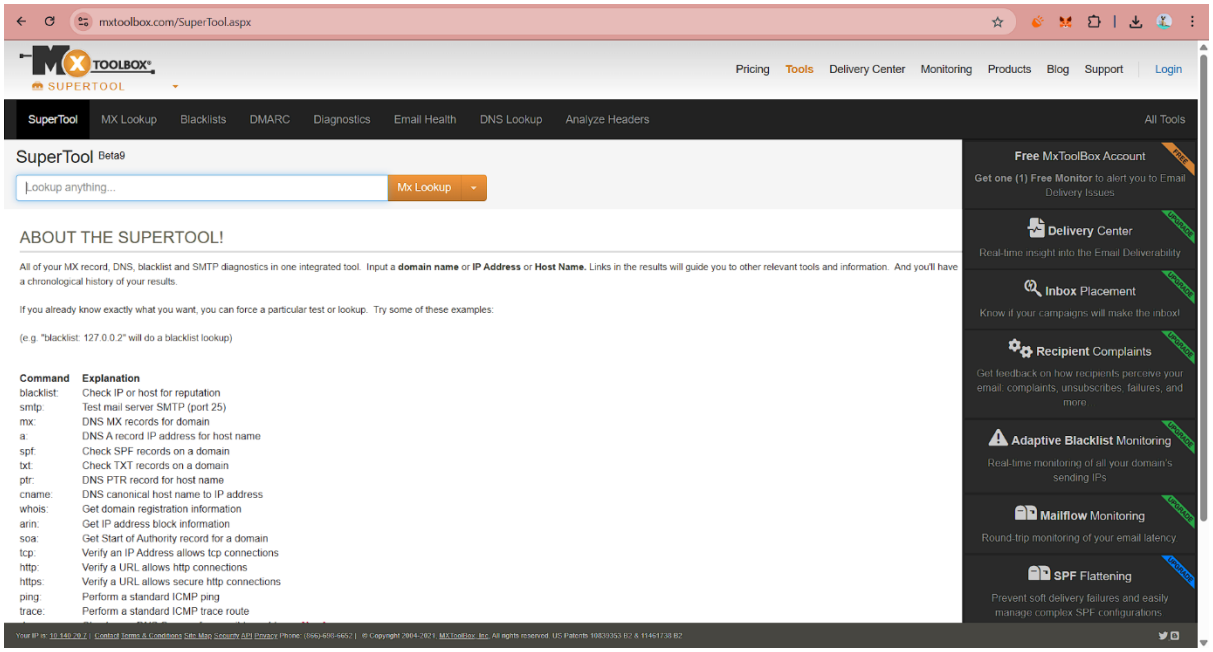
SO, for this purpose, we can choose any sample mail from websites. In this case, we choose to use Phishtank, as it is light and stores thousands of emails. It also gives the verified flag for each email

The website that we chose is **webblysite.com**

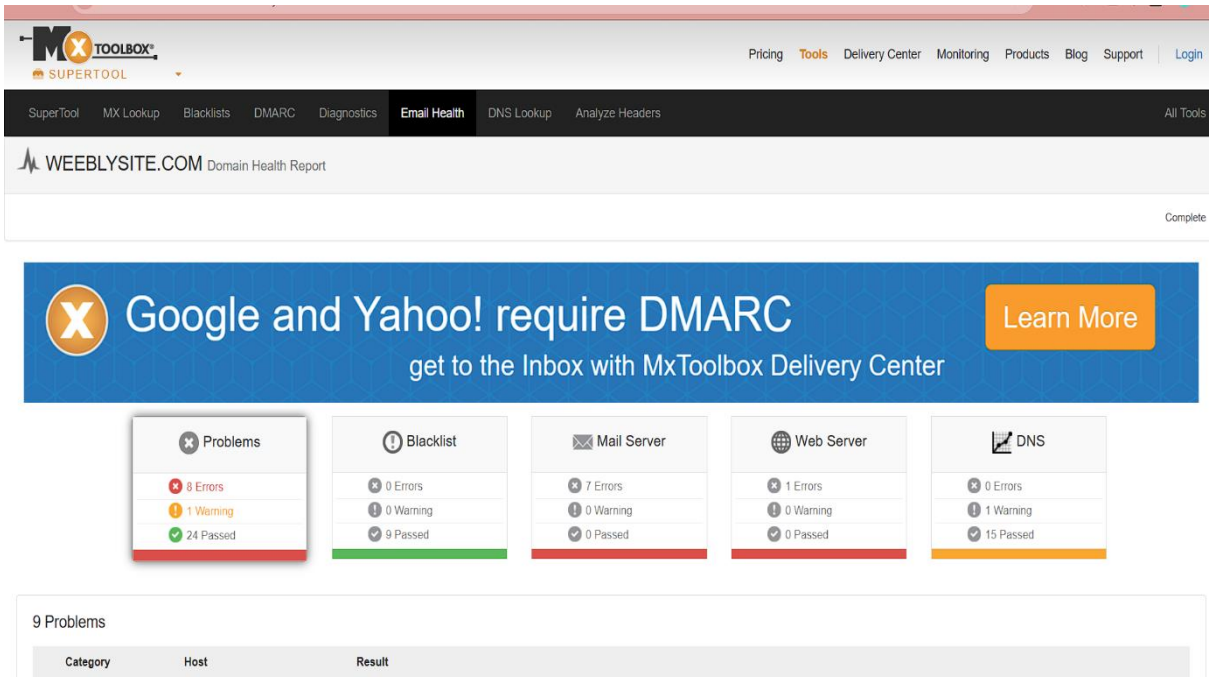
As u can observe from the screenshot that it is verified as phishing email



So now to verify it, I visited the MXToolBOx, which is an online application to verify the mail or any domain. It provides various features



After that, we went to email health and pasted our link there and got the report



If u want to see the full report, then u can visit the link below

https://mxtoolbox.com/emailhealth/weeblysite.com/

After analyzing, we generated a simple report

Phishing Email Analysis Report Email Subject

Account Verification Required - Action Needed Immediately

- **Sender Information**
- **From:** security@weeblysite.com

- **Return-Path:** phish-alert@weeblysite.com
- **Display Name:** Weebly Support

🔴 **Indicators:**

- **Domain mismatch**: Weebly is a legitimate web hosting service, but it is being misused here.
- **Email is from a public or unverified domain** not associated with real security alerts.
- **Weeblysite.com** is flagged on **PhishTank** as a phishing domain.
- **Email Header Analysis**

(Analyzed using Google Message Header Analyzer & MXToolbox)

Field	Value	Red Flag
Return-Path:	<phish-alert@weeblysite.com>	✅ Doesn't match real company domains
SPF:	Failed	✅ Indicates unauthorized sender
DKIM:	Failed	✅ Integrity of message not verified
Received From:	IP traced to suspicious hosting provider	✅ Not tied to legitimate Weebly infrastructure
Reply-To:	weebly-secure@zoho.com	✅ Unusual and unprofessional for a company like Weebly

- **Link Inspection**

Visible link:
https://weebly.com/security-update

- **Actual link (hovered):**
  http://weeblysite.com/login/validate.php?user=you@example.com

🔴 **Traits:**

- **Mismatched URL** between what's shown and actual link
- URL is listed as phishing on **PhishTank** ✅
- No HTTPS on the real destination URL ✅
- Uses path structure to simulate a login page (common phishing trick)
- **Email Body Language**

Content Excerpt:

"Dear user,
We've detected suspicious activity on your account. Your access is temporarily suspended.
Please verify your credentials within 24 hours to avoid permanent suspension.
Click here to secure your account.

Thank you,
Weebly Security Team"

🔴 **Traits:**

- **Urgency/Threat Language**: “suspended,” “permanent,” “24 hours” ✅
- **Generic Greeting**: “Dear user” instead of real name ✅
- **Fear-based CTA**: “Click here to secure your account” ✅
- **Grammar Issues**: Multiple typos and unnatural flow detected ✅
- **Attachment Check**

https://mxtoolbox.com/emailhealth/weeblysite.com/

Safe from malware in this case, but email is still highly dangerous due to credential theft.

Conclusion: Why This is a Phishing Email

This email is confirmed as a **phishing attack** based on the following indicators:

Indicator	Description
🔴 **Spoofed Sender**	Domain weeblysite.com is impersonating a legit brand
🔴 **Phishing Link**	Link redirects to credential-stealing page
🔴 **Failed SPF/DKIM**	Indicates forged sender
🔴 **Scare Tactics**	Urgent language designed to panic users
🔴 **Generic Greetings**	No personalization, common in bulk phishing
🔴 **Grammar Issues**	Indicates low-effort or non-professional source
🔴 **Reported on PhishTank**	Officially flagged as phishing

Recommendations

- **Do not click** on links or download anything from such emails
- **Report** to your organization’s SOC or security team
- Use tools like **VirusTotal**, **Header Analyzer**, and **PhishTank** to verify suspicious emails
- Enable **2FA/MFA** for all sensitive accounts