**Cybersecurity Internship Report – Task 2**

**Intern Name:** Kondiba Gangadhar Jogdand
**Organization:** Elevate Labs
**Task Title:** Phishing Email Detection and Analysis
**Date Completed:** August 5, 2025

---

## □ Objective

To analyze a suspicious email for signs of phishing, evaluate the embedded links and structure, perform domain intelligence using professional tools, and report red flags based on industry and internship guidelines.

---

## □ Tools Used

| Tool/Service | Purpose |
|---|---|
| VirusTotal | URL & file analysis via 97+ threat engines |
| urlscan.io | DNS, redirection and content scanning |
| Header Analyzer | Email header structure & origin check |
| HTML Source View | Manual investigation of suspicious email content |
| Whois Lookup | Domain intelligence (registrar, dates, etc.) |

---

## □ Step-by-Step Investigation

### 1. *Email Format Analysis*

The email `testmail.html` presented itself as a security alert, attempting to impersonate a cloud storage security center. It contained urgent language and embedded tracking URLs, which is a classic trait of phishing.

### 2. *View Email Header*

A review of the email headers (simulated) would help identify spoofed sender addresses, mismatched reply-to fields, and lack of DKIM/SPF.

### 3. *Link Inspection*

Link analyzed:
`http://mycloud-security-center[.]net/login-auth/session-id=8h3d9s0a`

- Shortened and disguised URL structure
- Domain name attempts to resemble legitimate services
- Hidden tracking via `session-id`

### 4. *VirusTotal Scan*

- **Result:** No security vendor flagged the domain (0/97)
- **Observation:** Although clean, unknown domains with no vendor reputation are suspicious
- **Screenshot:** [√] Attached in report

### 5. *URLScan.io Check*

- **Result:** Failed to resolve – *HTTP 400 DNS Error*
- **Explanation:** The domain does not map to a valid IPv4/IPv6
- **Red Flag:** Likely inactive or recently taken down
- **Screenshot:** [√] Attached in report

### 6. *Whois Lookup Summary* *(Simulated)*

- **Registrar:** Uncommon provider
- **Creation Date:** Recently registered
- **No Whois protection** → raises suspicion

### 7. *Manual HTML Inspection*

```
<a href="http://mycloud-security-center.net/login-auth/session-id=8h3d9s0a">Verify Now</a>
```

- Link and domain are hardcoded
- Design mimics a legitimate site login page
- No HTTPS → unsecure submission risk

### 8. *Behavioral Red Flags Summary*

| Indicator | Present? | Notes |
|---|---|---|
| Urgency in message | ✓ | Triggers fear of account suspension |
| Misleading URL | ✓ | Looks like a trusted domain |
| Domain not resolving | ✓ | Dead / suspicious site |
| HTTPS missing | ✓ | Link is plain HTTP |
| Poor header structure | ✓ | No SPF/DKIM in real test (if available) |
| Recently registered domain | ✓ | Simulated as suspicious |
| Spoofed sender possibility | ✓ | Cannot confirm sender integrity |
| Generic salutation | ✓ | No personalization (“Dear User”) |

---

## □ GitHub Repository Structure

```
task-2-phishing-analysis/
├── testmail.html
├── screenshot_virustotal.png
├── screenshot_urlscanio.png
└── README.md
```

---

## □ Outcome

- Conducted full phishing investigation based on a suspicious HTML email
- Scanned URL using VirusTotal and urlscan.io
- Manually dissected HTML content to reveal indicators
- Identified spoofing tactics and flagged red signals

---

## □ Key Concepts Covered

- Phishing Detection
- Header and Link Analysis
- Social Engineering Red Flags
- Domain Intelligence Gathering
- Tool-based Threat Analysis
- HTML Source Dissection

---

**Submitted on:** August 5, 2025
**GitHub Link:** https://github.com/cptjkcyber/task2-phishing-detection