# **Phishing Emails in Action**

**Lab Report — Phishing Emails in the Wild**

**Lab Platform:** TryHackMe

Inam Qadeer  
**Difficulty:** Easy – Medium  
**Category:** SOC Analyst / Threat Intelligence

**Objective**

The goal of this lab was to investigate real-world phishing emails, extract malicious indicators, and document findings as a SOC analyst. This exercise focused on email header analysis, link inspection, and attachment examination to detect phishing attempts and prevent successful attacks.

**Key Skills Practiced**

* Email header and metadata analysis
* Detection of spoofed sender domains
* URL and attachment investigation
* IOC (Indicators of Compromise) extraction and documentation
* Threat intelligence correlation using online tools

**Tools Used**

* **Mxtoolbox / Google Header Analyzer** — Email header parsing
* **VirusTotal** — File & URL scanning for malware
* **URLScan.io** — Visual and behavioral analysis of suspicious links
* **WHOIS Lookup** — Domain registration information
* **PhishTool / Manual IOC extraction** — Threat data gathering

**Investigation Summary**

1. **Email Header Analysis**
   * Identified spoofed sender domain mimicking a trusted financial institution.
   * Discrepancies found in “Received” fields pointing to an unknown IP address.
2. **URL Analysis**
   * Hyperlink in the email body redirected to an **HTML credential harvesting page**.
   * Domain registered recently with no legitimate reputation score.
3. **Attachment Analysis**
   * PDF file contained **embedded JavaScript payload**.
   * Payload attempted to connect to a malicious C2 server.
4. **Threat Intelligence Correlation**
   * IOCs (domains, IPs, hashes) matched known phishing campaigns in threat intel databases.

**Indicators of Compromise (IOCs)**

* **Domains:** [maliciousdomain.com]
* **IP Address:** [192.0.2.123]
* **File Hash (SHA256):** [Insert Hash]
* **URL:** [Insert Suspicious URL]

**Conclusion & Takeaways**

This lab reinforced the importance of deep email inspection in detecting phishing campaigns. Early identification of spoofed domains, malicious URLs, and weaponized attachments can significantly reduce the risk of successful phishing attacks. Maintaining an updated SOC watchlist with confirmed IOCs improves proactive defense measures.

