Task 2 — Phishing Email Analysis (Let's Defend Hands-on)

Author: Pratyush Raj
Date: 22-10-2025
Platform Used: Let's Defend — Phishing Email Analysis Course
Task Type: Cyber Security Internship — Practical Analysis & Documentation

---

🧭 Overview

Phishing Email Analysis involves the systematic examination of emails suspected to be fraudulent to identify and mitigate cybersecurity threats. This process includes scrutinizing the email's content, sender details, and technical markers for signs of deception or malicious intent. Analysts look for common phishing techniques such as spoofed email addresses, urgent or threatening language, and suspicious attachments or links. Advanced methods may involve analyzing metadata and deploying machine learning algorithms to detect subtle patterns indicative of phishing. The goal is to protect sensitive information by understanding the tactics used by cybercriminals, thereby enhancing an organization's email security protocols and user awareness.

📚 Table of Contents

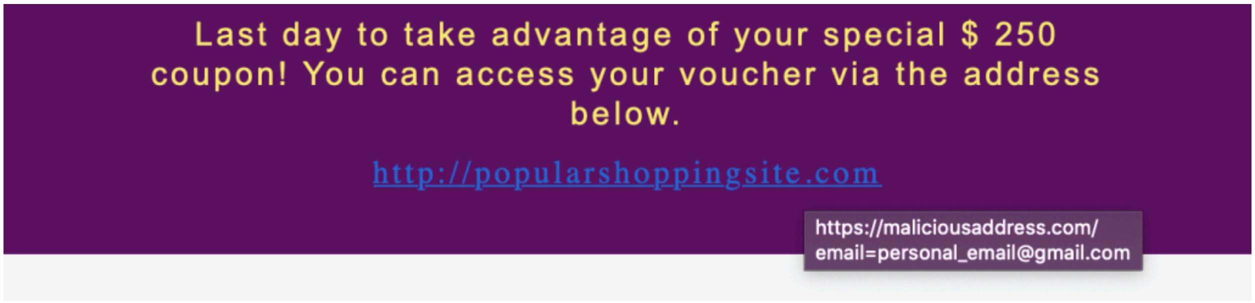
1. Introduction to Phishing
2. Information Gathering
3. What is an Email Header and How to Read Them?
4. Email Header Analysis
5. Static Analysis
6. Dynamic Analysis
7. Additional Techniques
8. Phishing Email Analysis Completion

🧩 Introduction to Phishing

A phishing attack is a type of cyberattack that aims to steal a user's personal information by tricking them into clicking on malicious links in emails or running malicious files on their computer.

Phishing attacks fall under the **Delivery phase** of the Cyber Kill Chain — the stage where attackers deliver malicious content to victims. Typical phishing messages use **social engineering phrases** such as:

- “You have won a gift!”
- “Don’t miss out on this big discount!”
- “If you don’t click this link, your account will be suspended.”

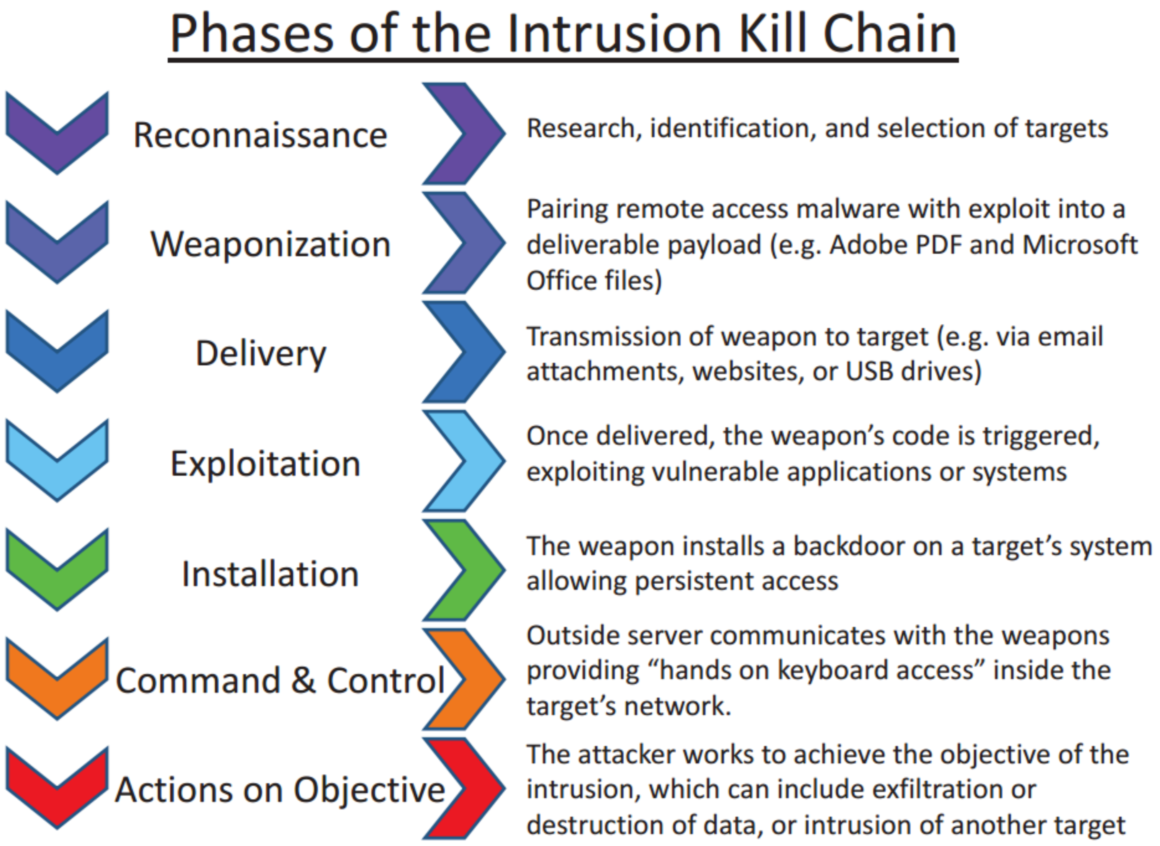


Last day to take advantage of your special $ 250 coupon! You can access your voucher via the address below.

http://popularshoppingsite.com

https://maliciousaddress.com/
email=personal_email@gmail.com

The goal is not just credential theft, but **exploiting the human factor**, often the weakest link in cybersecurity. These attacks act as an initial entry point for deeper system compromise.



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon’s code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target’s system allowing persistent access
Command & Control	Outside server communicates with the weapons providing “hands on keyboard access” inside the target’s network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

🧠 Information Gathering

1. Spoofing

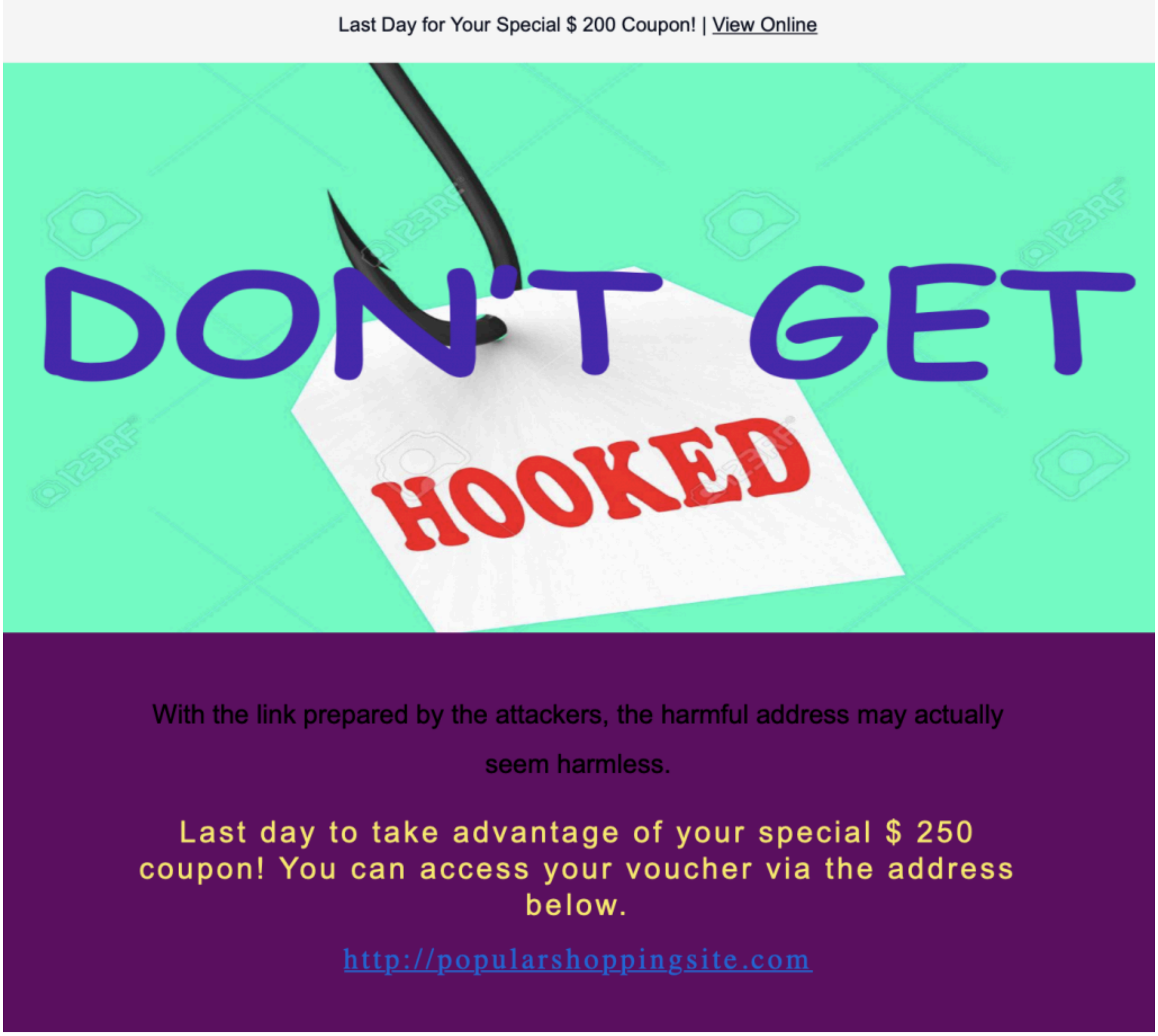
Attackers use spoofing to impersonate legitimate senders, exploiting the lack of strict authentication in email protocols. Key authentication protocols used to prevent spoofing include:

- **SPF (Sender Policy Framework)**
- **DKIM (DomainKeys Identified Mail)**
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**

Even with these, spoofing can still occur if not implemented properly.

Analysts can check domain legitimacy by using tools like **MXToolbox** or **Whois lookup** to analyze the SMTP IP and domain records.

Example: If an email claims to come from `info@company.com`, analysts can verify whether the SMTP IP truly belongs to that organization.



Last Day for Your Special $ 200 Coupon! | View Online

With the link prepared by the attackers, the harmful address may actually seem harmless.

Last day to take advantage of your special $ 250 coupon! You can access your voucher via the address below.

http://popularshoppingsite.com

2. E-mail Traffic Analysis

Analyzing sender addresses, SMTP IPs, subject patterns, and time of sending can reveal attack patterns. If emails are sent repeatedly to the same users or outside of business hours, it may indicate targeted campaigns or leaks.

Attackers often use tools like **theHarvester** (on Kali Linux) to collect target email addresses from public sources.

✉️ What is an Email Header and How to Read Them?

Definition

An **Email Header** is the metadata portion of an email containing details such as sender, recipient, timestamps, mail servers used, and routing information.

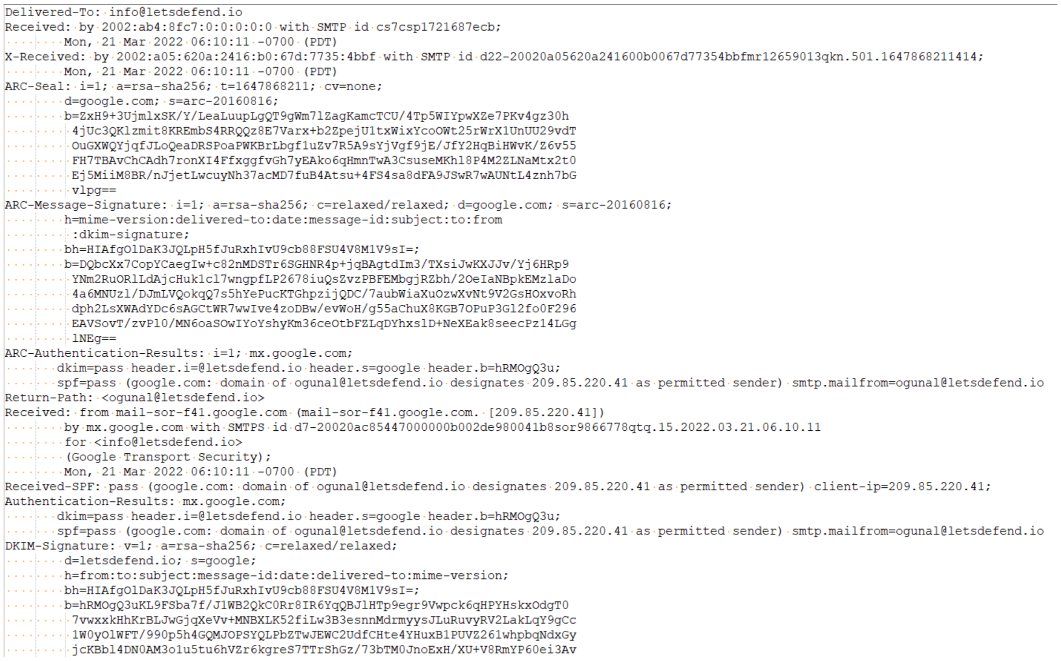
Why Analyze Headers?

- Identify spoofing and sender authenticity
- Track email delivery paths
- Detect spam or malicious routing

Important Header Fields

Field	Description
From	Shows the name and address of the sender
To / CC / BCC	Recipient information
Date	Timestamp of when the email was sent
Subject	Topic or title of the email
Return-Path	Reply-to address for responses
Message-ID	Unique identifier for each email
Received	Chain of mail servers through which the message passed
X-Spam-Status	Indicates if the message was classified as spam
MIME-Version	Describes the content encoding standard
DKIM / SPF	Authentication signatures to verify legitimacy

Accessing Email Headers



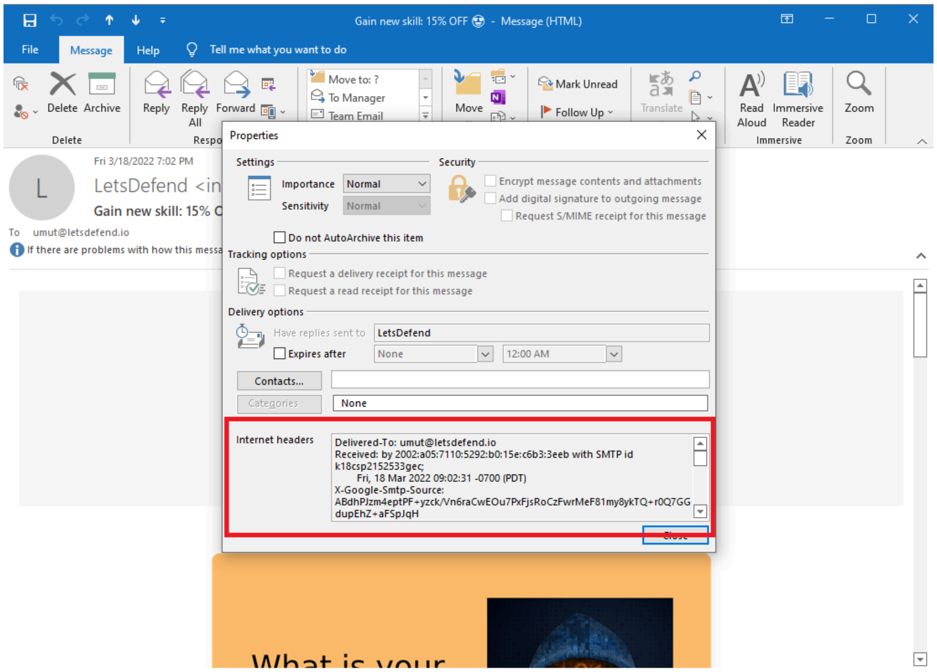
```
Delivered-To: info@letsdefend.io
Received: by 2002:ab4:8fc7:0:0:0:0:0 with SMTP id cs7csp1721687ecb;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
X-Received: by 2002:a05:620a:2416:b0:67d:7735:4bbf with SMTP id d22-20020a05620a241600b0067d77354bbfmr12659013qkn.501.1647868211414;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647868211; cv=none;
        d=google.com; s=arc-20160816;
        b=ZxH9+3UjmlxSK/Y/LeaLuupLgQT9gWm7lZagKamcTCU/4Tp5WIYpwXZe7PKv4gz30h
         4jUc3QKlzmit8KREmbS4RRQQz8E7Varx+b2ZpejU1txWixYcoOWt25rWrX1UnUU29vdT
         OuGXWQYjqfJLoQeaDRSPoaPWKBrLbgf1uZv7R5A9sYjVgf9jE/JfY2HqBiHWvK/Z6v55
         FH7TBAvChCAdh7ronXI4FfxggfvGh7yEAko6qHmnTwA3CsuseMKhl8P4M2ZLNaMtx2t0
         Ej5MiiM8BR/nJjetLwcuyNh37acMD7fuB4Atsu+4FS4sa8dFA9JSwR7wAUNtL4znh7bG
         vlpg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:delivered-to:date:message-id:subject:to:from
         :dkim-signature;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8M1V9sI=;
        b=DQbcXx7CopYCaegIw+c82nMDSTr6SGHNR4p+jqBAgtdIm3/TXsiJwKXJJv/Yj6HRp9
         YNm2RuORlLdAjcHuk1cl7wngpfLP2678iuQsZvzPBFEMbgjRZbh/2OeIaNBpkEMzlaDo
         4a6MNUzl/DJmLVQokqQ7s5hYePucKTGhpzijQDC/7aubWiaXuOzwXvNt9V2GsHOxvoRh
         dph2LsXWAdYDc6sAGCtWR7wwIve4zoDBw/evWoH/g55aChuX8KGB7OPuP3Gl2fo0F296
         EAVSovT/zvPl0/MN6oaSOwIYoYshyKm36ceOtbFZLqDYhxslD+NeXEak8seecPz14LGg
         lNEg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
Return-Path: <ogunal@letsdefend.io>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id d7-20020ac85447000000b002de980041b8sor9866778qtq.15.2022.03.21.06.10.11
        for <info@letsdefend.io>
        (Google Transport Security);
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
Received-SPF: pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=letsdefend.io; s=google;
        h=from:to:subject:message-id:date:delivered-to:mime-version;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8M1V9sI=;
        b=hRMOgQ3uKL9FSba7f/J1WB2QkC0Rr8IR6YqQBJlHTp9egr9Vwpck6qHPYHskxOdgT0
         7vwxxkHhKrBLJwGjqXeVv+MNBXLK52fiLw3B3esnnMdrmyysJLuRuvyRV2LakLqY9gCc
         1W0yOlWFT/990p5h4GQMJOPSYQLPbZTwJEWC2UdfCHte4YHuxB1PUVZ261whpbqNdxGy
         jcKBbl4DN0AM3o1u5tu6hVZr6kgreS7TTrShGz/73bTM0JnoExH/XU+V8RmYP60ei3Av
```

In Gmail:

1. Open email → click 3 dots ⋮
2. Select **"Download message"** → saves as `.eml`
3. Open the file using a text editor

In Outlook:

1. Open email → Go to **File** → **Info** → **Properties**
2. Look under **Internet headers**



Fri 3/18/2022 7:02 PM

LetsDefend <in

Gain new skill: 15% C

To umut@letsdefend.io

If there are problems with how this messa

Properties

Settings

Importance: Normal

Sensitivity: Normal

Security

☐ Encrypt message contents and attachments

☐ Add digital signature to outgoing message

☐ Request S/MIME receipt for this message

☐ Do not AutoArchive this item

Tracking options

☐ Request a delivery receipt for this message

☐ Request a read receipt for this message

Delivery options

Have replies sent to: LetsDefend

☐ Expires after: None 12:00 AM

Contacts...

Categories: None

Internet headers

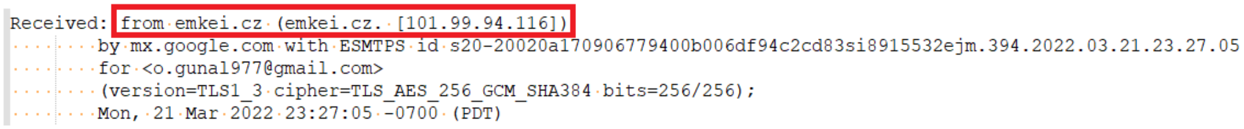
```
Delivered-To: umut@letsdefend.io
Received: by 2002:a05:7110:5292:b0:15e:c6b3:3eeb with SMTP id
k18csp2152533gec;
        Fri, 18 Mar 2022 09:02:31 -0700 (PDT)
X-Google-Smtp-Source:
ABdhPJzm4eptPF+yzck/Vn6raCwEOu7PxFjsRoCzFwrMeF81my8ykTQ+r0Q7GG
dupEhZ+aFSpJqH
```

Close

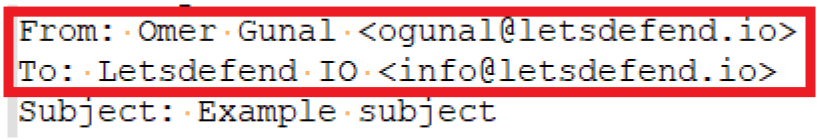
🔍 Email Header Analysis

When investigating a suspected phishing email, key checks include:

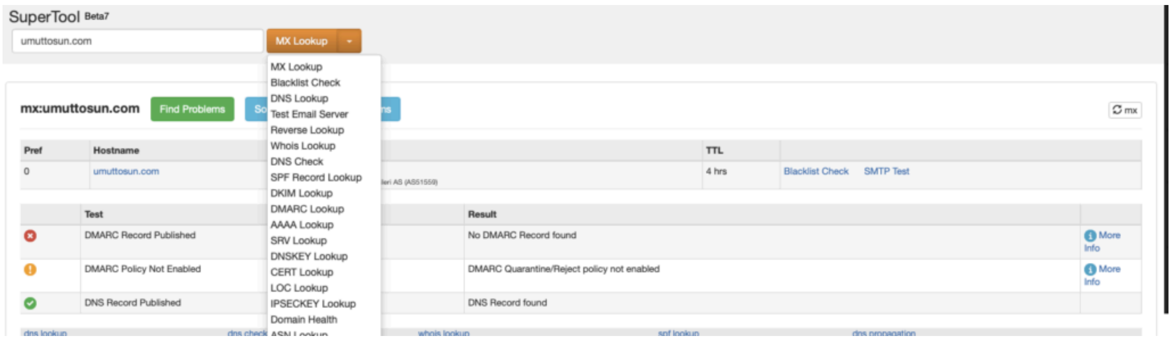
1. **Was the email sent from the correct SMTP server?**
   - ○ Compare the “Received” IP and domain with legitimate mail servers (using MXToolbox).
   - ○ Example: `letsdefend.io` should use Google’s mail servers, not `101.99.94.116` → indicates spoofing.
2. **Are the 'From' and 'Return-Path / Reply-To' fields identical?**
   - ○ Differences between them can suggest phishing, especially when combined with malicious content or attachments.



```
Received: from emkei.cz (emkei.cz. [101.99.94.116])
        by mx.google.com with ESMTPS id s20-20020a170906779400b006df94c2cd83si8915532ejm.394.2022.03.21.23.27.05
        for <o.gunal977@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 21 Mar 2022 23:27:05 -0700 (PDT)
```



```
From: Omer Gunal <ogunal@letsdefend.io>
To: Letsdefend IO <info@letsdefend.io>
Subject: Example subject
```



SuperTool Beta7

umuttosun.com

mx:umuttosun.com

Pref	Hostname		TTL	
0	umuttosun.com	eri AS (AS51559)	4 hrs	Blacklist Check SMTP Test

	Test	Result	
⊗	DMARC Record Published	No DMARC Record found	More Info
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DNS Record Published	DNS Record found	

🧮 Static Analysis

Static analysis involves examining email content and attachments without executing them.

- Attackers often use **HTML emails** with deceptive links.
- Hovering over links can reveal mismatched URLs.
- Newly registered domains often indicate phishing attempts.

Tools Used:

- **VirusTotal** — Scan links/files for known threats
- **Cisco Talos Intelligence** — Check IP reputation
- **AbuseIPDB** — Verify if IP has past malicious reports

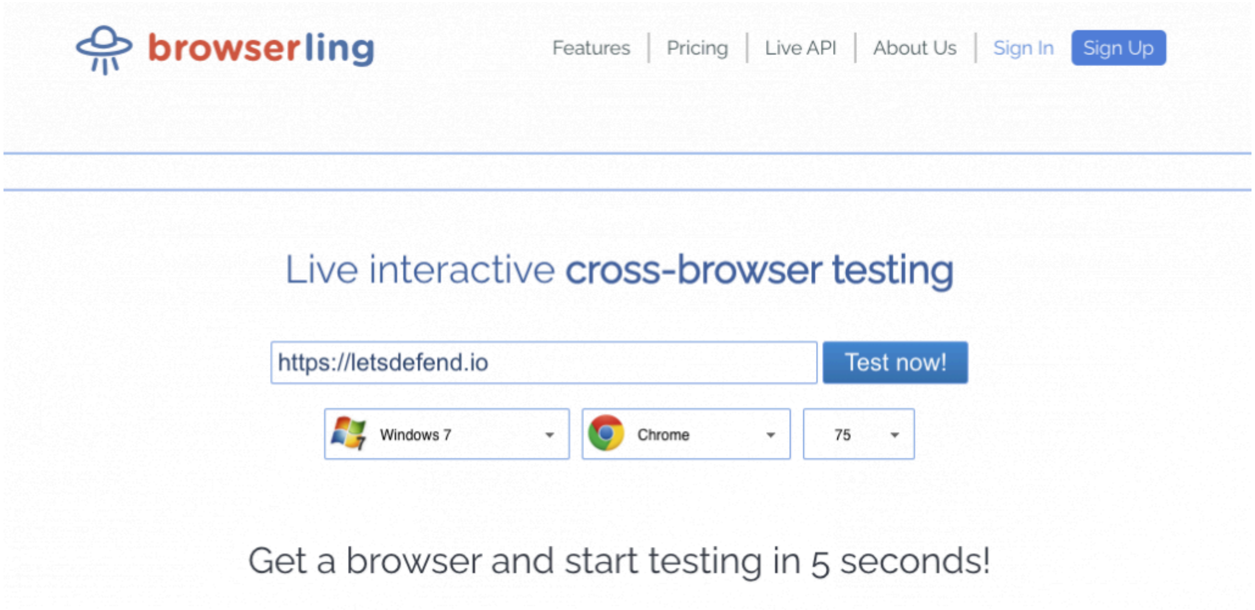
⚙️ Dynamic Analysis

Dynamic analysis executes suspicious links or files in **isolated environments** (sandboxes) to observe behavior safely.

Safe Environments to Use

- **Browserling** — Online virtual browser testing
- **Hybrid Analysis (Falcon Sandbox)**
- **AnyRun**
- **VMRay**

Analysts must inspect the **URL parameters** carefully; sometimes personal information (like email IDs) is embedded in URLs, revealing valid targets to attackers.

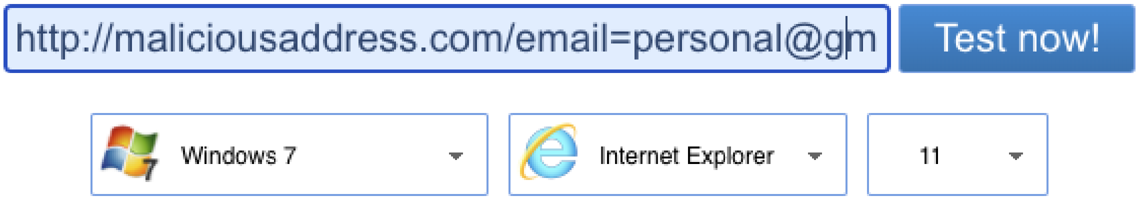

browserling
Features | Pricing | Live API | About Us | Sign In | Sign Up

Live interactive cross-browser testing

https://letsdefend.io

Windows 7 | Chrome | 75

Get a browser and start testing in 5 seconds!



http://maliciousaddress.com/email=personal@gm

Windows 7 | Internet Explorer | 11

🧰 Additional Techniques

Attackers may also leverage legitimate platforms to host phishing payloads:

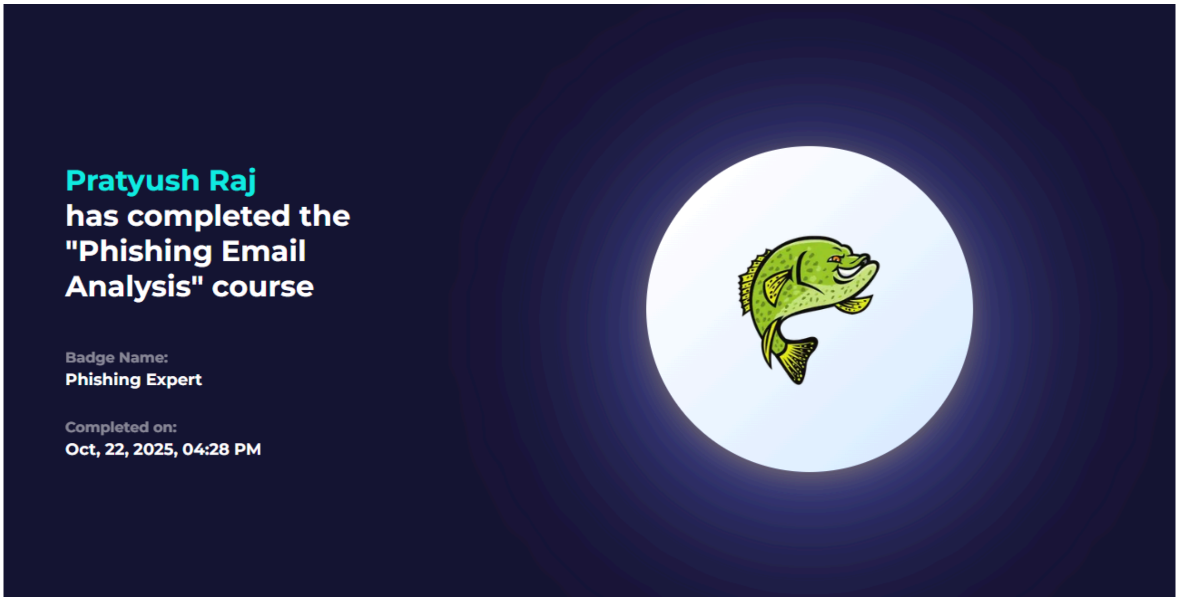
- **Cloud Storage Services** (Google Drive, OneDrive) — deliver malicious files via trusted links
- **Free Subdomain Services** (Blogspot, Wix, WordPress) — disguise phishing pages
- **Form-based Applications** (Google Forms, Typeform) — collect credentials without triggering AV tools

These techniques exploit the reputation of legitimate services to bypass filters.

🎯 Phishing Email Analysis Completion

Completed the Course successfully:

[Link: https://app.letsdefend.io/my-rewards/detail/7286ef1d-6d3f-475c-9902-1cc29ae70fd7]



Pratyush Raj
has completed the "Phishing Email Analysis" course

Badge Name:
Phishing Expert

Completed on:
Oct, 22, 2025, 04:28 PM

✅ Conclusion

This hands-on exercise in phishing analysis on LetsDefend demonstrates a real-world workflow for identifying, analyzing, and mitigating phishing threats. It reinforced understanding of:

- Email authentication (SPF/DKIM/DMARC)
- Header analysis
- Static and dynamic content examination
- Use of OSINT and sandbox tools
- Recognizing social engineering tactics

By completing this course and documenting the process, I developed practical experience in threat analysis and SOC-style investigation for phishing incidents.
