Phishing Email Analysis Guide

This document provides step-by-step guidance for analyzing suspicious or malicious emails to detect phishing attempts. It covers email headers, body content, attachments, and tool recommendations.

1.1 What Information Should an Analyst Collect?

Email Header Collect:

- Sender Email Address
- Sender IP Address
- Reverse Lookup of Sender IP
- Subject Line
- Recipient Email Address (To/CC/BCC)
- Reply-To Email Address (if different from sender)
- Date & Time

⚠️ Warning: Do not click on any links or open attachments during analysis.

Email Body Collect:

- URLs (expand shortened links using preview or URL decoding tools)
- Attachment Names
- Attachment Hash (SHA-256 preferred)

1.2 Email Header Analysis Tools

Tool	Description	Link
Google Admin Toolbox – MessageHeader	Parses and visualizes email headers	https://toolbox.googleapps.com/apps/messageheader/analyzeheader
Azure Message Header Analyzer	Web-based analyzer for Exchange and Office 365 headers	https://mha.azurewebsites.net/

Created By- Muhammad Arsalan Siddiqui

MailHeader.org	Decodes standard email headers	https://mailheader.org/
IPinfo.io	Gives location, ISP, and abuse info of IPs	https://ipinfo.io/

1.3 URL and Email Body Analysis Tools

Tool	Purpose	Link
URL Extractor (ConvertCSV)	Extracts all URLs from email text	https://www.convertcsv.com/url-extractor.htm
CyberChef	Advanced URL, encoding, and decoding operations	https://gchq.github.io/CyberChef/#recipe=Extract_URLs(false,false,false)
URLscan.io	Scans and visualizes URLs with passive/active scan	https://urlscan.io/
URL2PNG	Takes screenshots of URLs (headless browser)	https://www.url2png.com/
WannaBrowser	Simulate and interact with webpage behavior	https://www.wannabrowser.net/

Key Point:

- Always identify the root domain of URLs.
- Validate domains/URLs using reputation intelligence tools.

Attachment Analysis

Steps:
1. Safely save the attachment (e.g., via Thunderbird or email client).
2. Generate the SHA-256 hash or just attachment on the “Virustotal”.

On Linux Terminal:

```
sha256sum /path/to/your/file.ext
```

On Windows PowerShell:

```
Get-FileHash -Algorithm SHA256 -Path "C:\Path\To\File.ext"
```

On Windows CMD:

```
certutil -hashfile "C:\Path\To\File.ext" SHA256
```

Example: Replace `file.ext` with your actual file name and file path.

Analyse the File:

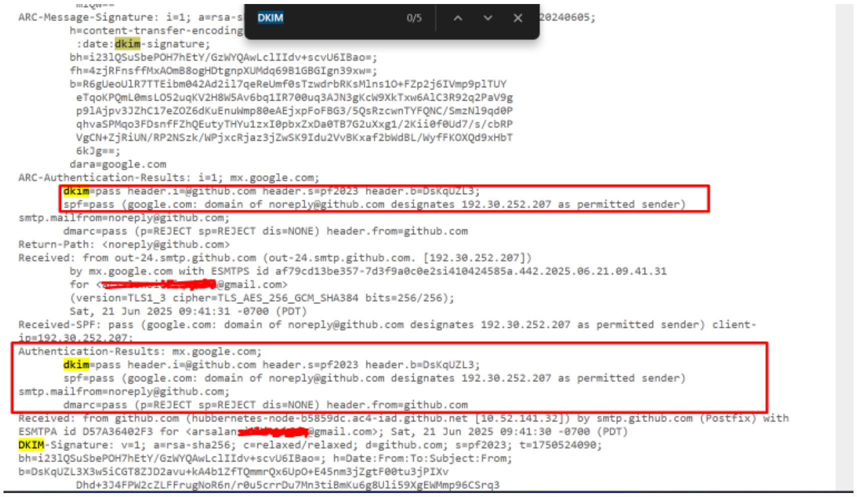
Tool	Purpose	Link
VirusTotal	Multi-engine antivirus scanner	https://www.virustotal.com/
Cisco Talos Intelligence	File reputation, domain, and IP threat intel	https://talosintelligence.com/talos_file_reputation
ANY.RUN Sandbox	Real-time interactive malware analysis	https://any.run/
Joe Sandbox	Advanced malware and phishing attachment behavior analysis	https://www.joesandbox.com/
Hybrid Analysis	Static and dynamic analysis of suspicious files	https://www.hybrid-analysis.com/

Advanced Phishing Email Analysis Techniques

For seasoned analysts or incident responders, deeper phishing analysis often involves behavioral insights, threat actor attribution, and tactical countermeasures. This section includes more complex techniques that extend beyond basic static analysis.

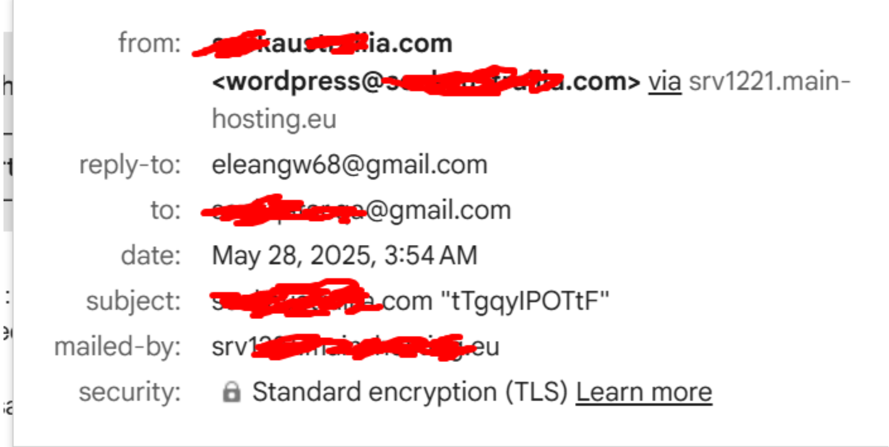
1. Advanced Email Threat Hunting Techniques

- Perform full MIME inspection to analyze multi-part email structures and embedded scripts.
- Check DKIM, SPF, and DMARC authentication results in the header.



```
ARC-Message-Signature: i=1; a=rsa-s                                    20240605;
        h=content-transfer-encoding
         :date:dkim-signature;
        bh=i231QSuSbePOH7hEtY/GzWYQAwLclIIdv+scvU6IBao=;
        fh=4zjRFnsffMxAOmB8ogHDtgnpXUMdq69B1GBGIgn39xw=;
        b=R6gUeoUlR7TTEibm042Ad2il7qeReUmf0sTzwdrbRKsMlns1O+FZp2j6IVmp9plTUY
         eTqoKPQmL0msLO52uqKV2H8W5Av6bq1IR700uq3AJN3gKcW9XkTxw6AlC3R92q2PaV9g
         p9lAjpv3JZhC17eZOZ6dKuEnuWmp80eAEjxpFoFBG3/5QsRzcwnTYFQNC/SmzNl9qd0P
         qhvaSPMqo3FDsnfFZhQEutyTHYu1zxI0pbxZxDa0TB7G2uXxg1/2Kii0f0Ud7/s/cbRP
         VgCN+ZjRiUN/RP2NSzk/WPjxcRjaz3jZwSK9Idu2VvBKxaf2bWdBL/WyfFKOXQd9xHbT
         6kJg==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@github.com header.s=pf2023 header.b=DsKqUZL3;
       spf=pass (google.com: domain of noreply@github.com designates 192.30.252.207 as permitted sender)
smtp.mailfrom=noreply@github.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
Return-Path: <noreply@github.com>
Received: from out-24.smtp.github.com (out-24.smtp.github.com. [192.30.252.207])
        by mx.google.com with ESMTPS id af79cd13be357-7d3f9a0c0e2si410424585a.442.2025.06.21.09.41.31
        for <[redacted]@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Sat, 21 Jun 2025 09:41:31 -0700 (PDT)
Received-SPF: pass (google.com: domain of noreply@github.com designates 192.30.252.207 as permitted sender) client-
ip=192.30.252.207;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@github.com header.s=pf2023 header.b=DsKqUZL3;
       spf=pass (google.com: domain of noreply@github.com designates 192.30.252.207 as permitted sender)
smtp.mailfrom=noreply@github.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=github.com
Received: from github.com (hubbernetes-node-b5859dc.ac4-iad.github.net [10.52.141.32]) by smtp.github.com (Postfix) with
ESMTPA id D57A36402F3 for <arsalan[redacted]@gmail.com>; Sat, 21 Jun 2025 09:41:30 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=github.com; s=pf2023; t=1750524090;
bh=i231QSuSbePOH7hEtY/GzWYQAwLclIIdv+scvU6IBao=; h=Date:From:To:Subject:From;
b=DsKqUZL3X3w5iCGT8ZJD2avu+kA4b1ZfTQmmrQx6UpO+E45nm3jZgtF00tu3jPIXv
         Dhd+3J4FPW2cZLFFrugNoR6n/r0u5crrDu7Mn3tiBmKu6g8Uli59XgEWMmp96CSrq3
```

- Use regex or scripts to extract and decode obfuscated content.
- Compare sender domain with display name and reply-to address.



from: [redacted]aust[redacted]ia.com <wordpress@[redacted].com> via srv1221.main-hosting.eu
reply-to: eleangw68@gmail.com
to: [redacted]@gmail.com
date: May 28, 2025, 3:54 AM
subject: s[redacted].com "tTgqyIPOTtF"
mailed-by: srv1[redacted]eu
security: Standard encryption (TLS) Learn more

- Use tools like eml-analyzer and RATdecoders for decoding phishing payloads.

Created By- Muhammad Arsalan Siddiqui

2. Advanced Tools for Complex Analysis

Tool	Purpose	Link
eml-analyzer	Python-based tool to analyze .eml files and extract IOCs	https://pypi.org/project/eml-analyzer/
RATDecoders	Decode strings used by RATs, like njRAT or Remcos	https://github.com/ytisf/theZoo
Regex101	Online regex debugger for parsing obfuscated payloads	https://regex101.com/
CheckPhish.ai	Visual AI-based phishing page detection	https://checkphish.ai/

3. Threat Intelligence Correlation

Correlate IOCs (Indicators of Compromise) with global threat intel sources to identify campaigns and actors.
• Use MISP or OpenCTI for structured threat intelligence.
• Perform passive DNS lookups with PassiveTotal or RiskIQ.
• Query commercial or open-source feeds like OTX and AbuseIPDB.
• Pivot from IOCs to discover attacker infrastructure.

Final Notes

- ➢ Always perform email analysis in a controlled environment such as a sandbox or virtual machine to avoid accidental execution of malicious payloads.
- ➢ Maintain an analysis checklist or report template including:
- ➢ Email headers and anomalies
- ➢ URLs and domain reputations
- ➢ Attachment behaviour
- ➢ Observed Indicators of Compromise (IOCs)
- ➢ Document and escalate findings to your Security Operations Center (SOC) or Incident Response Team (IRT) as per your organization’s protocol.
- ➢ Continuously update your tooling stack and threat intel feeds to stay current with phishing tactics (TTPs).
- ➢ Participate in community platforms (like OTX, AbuseIPDB, MISP) to share IOCs and improve global threat visibility.

Created By- Muhammad Arsalan Siddiqui