Phishing Email Analysis Tools –

Email Header Analysis Tools

- **Google Admin Toolbox** – Messageheader Analyzer
  - Link: https://toolbox.googleapps.com/apps/messageheader/analyzeheader
  - Purpose: Analyze SMTP headers to identify spoofing, routing issues, SPF/DKIM/DMARC validation.

- **Message Header Analyzer (Azure)**
  - Link: https://mha.azurewebsites.net/
  - Purpose: Clean visualization of email headers and relay paths.

- **MailHeader.org**
  - Link: https://mailheader.org/
  - Purpose: Independent email header parsing and hop analysis.

Sender IP & Reputation Analysis

- **IPinfo.io**
  - Link: https://ipinfo.io/
  - Purpose: IP geolocation, ISP, ASN, VPN/proxy detection.

- **Talos Reputation Center**
  - Link: https://talosintelligence.com/reputation
  - Purpose: Cisco-backed IP/domain reputation intelligence.

URL Analysis

- **URLScan.io**
  - Link: https://urlscan.io/
  - Purpose: Sandbox-based URL analysis with screenshots and network activity.

- **URL2PNG**
  - Link: https://www.url2png.com/
  - Purpose: Screenshot URLs without opening them locally.

- **WannaBrowser**
  - Link: https://www.wannabrowser.net/
  - Purpose: View websites from different browsers/locations.

URL Extraction

- **URL Extractor (ConvertCSV)**
  - Link: https://www.convertcsv.com/url-extractor.htm
  - Purpose: Automatically extract URLs from email headers or body.

- **CyberChef**
  - Link: https://gchq.github.io/CyberChef/
  - Purpose: Decode, deobfuscate, and extract indicators from malicious content.

File & Attachment Analysis

- **Talos File Reputation**
  - Link: https://talosintelligence.com/talos_file_reputation
    Purpose: Hash-based file reputation lookup.

- **VirusTotal**
  - Link: https://www.virustotal.com/gui/
  - Purpose: Multi-engine malware and URL analysis platform.

- **ReversingLabs**
  - Link: https://www.reversinglabs.com/
  - Purpose: Enterprise malware classification and reputation.

Malware Sandboxes

- **ANY.RUN**
  - Link: https://app.any.run/
  - Purpose: Interactive real-time malware analysis sandbox.

- **Hybrid Analysis**
  - Link: https://www.hybrid-analysis.com/
  - Purpose: Automated static and dynamic malware analysis.

- **Joe Sandbox**
  - Link: https://www.joesecurity.org/
  - Purpose: Advanced enterprise sandbox with MITRE mapping.

Automated Phishing Analysis

- **PhishTool**
  - Link: https://www.phishtool.com/
  - Purpose: End-to-end phishing investigation and case management.

Defanging Tool

- **Defa.ng**
  - Link: https://defa.ng/
  - Purpose: Safely defang malicious URLs and IPs for reporting.

WHOIS – Checking IP / Domain Ownership

https://www.whois.com/whois/

◇ **What is WHOIS?**

WHOIS is used to **identify who owns an IP address or domain** and **where it comes from**.

It helps answer:

- Who owns this IP/domain?
- Which organization controls it?
- Which country is it registered in?
- Is it suspicious or legitimate?

MXToolbox – Email Security & DNS Analysis

- https://mxtoolbox.com • ◇ **What is MXToolbox?**
- MXToolbox is used to analyze **email security and DNS records**.
- It helps find:
- SPF
- DKIM
- DMARC
- Blacklist status
- Mail server configuration
-