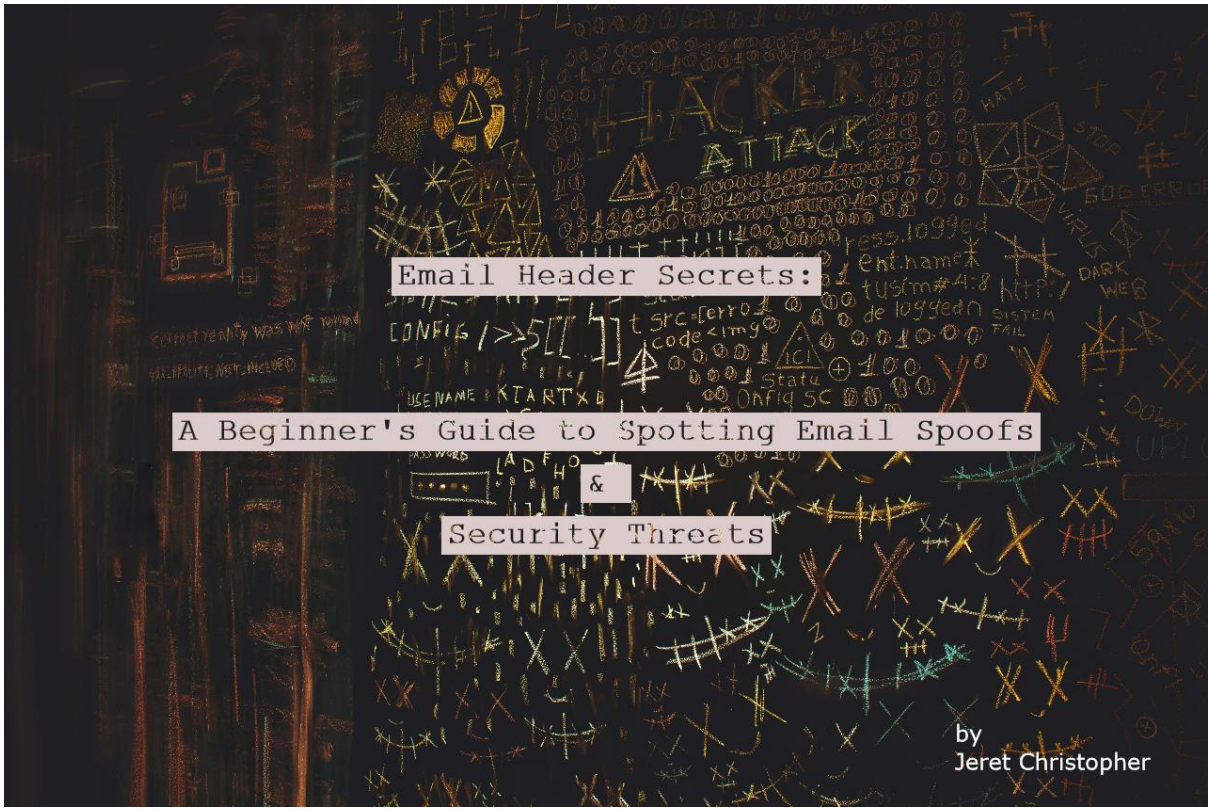

Email Header Secrets: A Beginner's Guide to Spotting Email Spoofs and Security Threats

Introduction to Email Header Analysis

Email header analysis is the process of examining the metadata embedded in email messages to gain insights into their origins, authenticity, and security status. Each email carries a header that contains vital information, including the sender’s and recipient’s addresses, the message’s route through mail servers, and authentication details that help verify its legitimacy.

Understanding how to read and analyze email headers is crucial in today’s digital landscape, where phishing attacks, spam, and email spoofing are prevalent threats. By analyzing email headers, individ uals can identify potential risks, verify the authenticity of messages, and take necessary precautions to protect themselves and their organizations from malicious activities.

In this guide, "Email Header Secrets: A Beginner’s Guide to Spotting Email Spoofs and Security Threats," we will explore the components of email headers, how to interpret them, and the tools available for effective analysis. Whether you’re an individual looking to secure your personal inbox or a professional seeking to enhance organizational email security, this guide will provide you with the essential knowledge to navigate the complexities of email header analysis.

Real-world Examples:

Case Study 1: Phishing Attack

Scenario: A large corporation received an email appearing to come from their CEO. The email requested a transfer of funds and included a convincing header.

Header Analysis:

- **Message ID**: <fakeid-1234-5678@phishingdomain.com>
- **Return-Path**: <ceo@legitcompany.com>
- **From**: ceo@legitcompany.com
- **Received**: from [192.0.2.1] (unknown [192.0.2.1]) by mailserver.legitcompany.com
- **SPF**: pass
- **DKIM**: none
- **DMARC**: fail

Analysis:

- **Message ID** was unusual and didn't match known patterns.
- **Return-Path** and **From** headers matched, but the **Received** header indicated a suspicious origin IP not associated with the company.
- **DKIM** was missing, and **DMARC** failed, indicating spoofing attempts.

Outcome: The suspicious email was identified before any funds were transferred.

Case Study 2: Spoofed Email

Scenario: A non-profit organization received an email claiming to be from a trusted partner. The email headers showed discrepancies in the return-path and from header fields, revealing a spoofed attempt.

Header Analysis:

- **Message ID**: <legitpartner-7890-1234@trusteddomain.com>
- **Return-Path**: <partner@trusteddomain.com>
- **From**: spoof@fakedomain.com
- **Received**: from [203.0.113.2] (unknown [203.0.113.2]) by nonprofit.org
- **SPF**: fail
- **DKIM**: fail
- **DMARC**: fail

Analysis:

- **Message ID** seemed legitimate but wasn't sufficient alone.
- **Return-Path** didn't match the **From** header, raising red flags.
- **Received** header indicated an IP address not associated with the trusted partner.
- **SPF**, **DKIM**, and **DMARC** all failed, confirming the email was spoofed.

Outcome: The email was flagged as fraudulent, prompting a review and enhancement of email security protocols.

How to Access and Analyze Email Headers

Accessing Email Headers

- **Gmail**: Open the email you want to analyze and click on the three vertical dots (More options) in the top right corner. Select "Show original" to view the full email header.
- **Outlook**: Open the email and click on the three dots (...) in the top right corner. Then, select "View message source" to see the email header.
- **Yahoo Mail**: Open the desired email and click on the three dots in the top right corner. From there, select "View raw message" to access the email header.
- **Mozilla Thunderbird**: Open the email, click on "More" in the top right corner, and select "View Source" to display the email header.
- **Apple Mail**: Open the email, click on "View" in the menu bar, select "Message," and then choose "All Headers" to show the full header.

Email Header Analysis

Email headers contain various components that help in determining the authenticity and path of an email. Here's a detailed look at each component:

1. **Message ID**:
    - Typically generated by the sending mail server, the Message ID allows email systems to track individual messages as they are processed, routed, and delivered. The format of the Message ID may vary according to the email service provider.
    - **Example**: <SEYPR02MB5704F95A7D4D383661821568D01BA@SEYPR02MB5704.apcprd02.prod.outlook.com> or <568ebb11-6e5c-c4c1-0e3f-e0d85200f3d7@example.com.>
2. **Mail User Agent (MUA)**:
    - The Mail User Agent is the email client used by the sender to send or receive the email.
    - **Examples**: Apple Mail, Thunderbird, Outlook.

3. **Mail Transfer Agent (MTA)**:
    - The Mail Transfer Agent is responsible for routing and delivering email from the send er to the recipient.
    - **Examples**: Sendmail, Postfix, MS-Exchange.
4. **SPF: Sender Policy Framework**:
    - SPF is used to prevent email spoofing by specifying which mail servers are allowed to send email on behalf of a domain. This information is published via DNS in a TXT record type.
    - **Example**: dig @1.1.1.1 example.com txt +short results in "v=spf1 ip4:66.96.128.0/18 include:websitewelcome.com ?all"
5. **DKIM: DomainKeys Identified Mail**:
    - DKIM provides a cryptographic method to verify that the email originated from the specified domain. It helps to ensure the integrity of the message and detect forged or spammy emails.
6. **DMARC: Domain-based Message Authentication, Reporting, and Conformance**:
    - DMARC helps domain owners instruct email receivers on how to handle unauthorize d emails claiming to come from their domain. It enhances SPF and DKIM checks by defining actions such as reject, quarantine, or none.
7. **Security Headers**:
    - Security headers provide authentication results to verify the legitimacy of the email.
    - **Example**: Authentication-
      Results: spf=fail (sender IP is 153.123.100.10) smtp.mailfrom=example.com; dkim=n one (message not signed) header.d=none; dmarc=fail action=quarantine header.from =example.com; compauth=fail reason=000

Common Pitfalls:

1. **Ignoring SPF, DKIM, and DMARC failures**: Users might overlook these critical checks. It's essential to investigate further when these fail.
2. **Trusting Visual Cues Alone**: Emails can be designed to look legitimate. Always verify the headers instead of relying solely on the appearance of the email.
3. **Not Checking Received Headers**: Skipping the analysis of received headers can result in missing out on identifying the true origin of the email.

4. **Received Headers**:
    - The Received header traces the path of the email from sender to receiver. Each hop the email makes adds a new "Received" entry.

- **Example**: Received: from PSAPR02MB4597.apcprd02.prod.outlook.com (2603:1096:301:42::13) by TY2PR02MB4463.apcprd02.prod.outlook.com with HTTPS; Tue, 5 Sep 2023 05:42:52 +0000
- **Tip**: Compare the Return-Path header with the From header. If they don't match, this could indicate a spoofed email.

5. **X-Headers (Extended Headers)**:
    - X-Headers contain additional information specific to certain email providers.
    - **Example**: X-MS-PublicTrafficType: Email X-MS-TrafficTypeDiagnostic: TYZPR02MB6431:EE_|PSAPR02MB4597:EE_|TY2PR02MB4463:EE_
6. **IPv6 Consideration**:
    - Email headers may include IPv6 addresses. For example, if you see an address starting with fe80, this is a link-local address and is used for internal routing.

Tools for Analyzing Email Headers:

- **PhishTool**: Online tool.
- **Trustifi Email Analyzer**: Online tool.
- **MXToolbox Email Header Analyzer**: Online tool.
- **Mail Header Analyzer (MHA)**: Online tool.

Email Header Analysis Checklist:

- Check the Message ID for consistency.
- Verify SPF results.
- Confirm DKIM signatures.
- Assess DMARC alignment.
- Cross-check received headers for the email route.
- Compare Return-Path and from headers.
- Review X-Headers for additional insights.
- Consider the presence of IPv6 addresses.

Acknowledgments

Creating **"Email Header Secrets: A Beginner's Guide to Spotting Email Spoofs and Security Threats"** has been a rewarding journey. I would like to acknowledge the developers of the online tools referenced in this guide for their efforts in making cybersecurity accessible to all, including resources like PhishTool, Trustifi Email Analyzer, MXToolbox Email Header Analyzer, and Mail Header Analyzer (MHA).

Jeret Christopher

Jeret Christopher is a cybersecurity enthusiast and IT professional with a passion for educating others about online security and email safety. With extensive experience in various cybersecurity practices, Jeret aims to empower individuals and organizations to recognize and mitigate digital threats.

Contact Information

For questions, feedback, or inquiries, you can reach Jeret at:

- GitHub: https://github.com/jeretc
- LinkedIn: https://my.linkedin.com/in/jeret-christopher-46b67688

Additionally, Jeret is the admin at Kali Linux Nethunter, where he shares insights and resources on cybersecurity tools and techniques.

Thank you for reading **"Email Header Secrets: A Beginner's Guide to Spotting Email Spoofs and Security Threats."** Your commitment to understanding email security is the first step toward a safer online experience.

Bonus Resources for "Email Header Secrets: A Beginner’s Guide to Spotting Email Spoofs and Security Threats"

1. Email Security Checklist

10 Steps to Improve Email Security Today!

Description: This checklist gives you 10 essential steps to protect your email accounts from security threats. Follow these guidelines to ensure your emails are secure and your communications remain private.

---

10 Steps to Improve Email Security:

1. Enable Two-Factor Authentication (2FA): Add an extra layer of protection by requiring both a password and a verification code for account access.
2. Use Strong and Unique Passwords: Avoid simple passwords and never reuse passwords across different platforms. Use a combination of letters, numbers, and symbols.
3. Verify Sender Email Addresses: Always double-check email addresses, especially for unsolicited attachments or links. Watch for typos or slight changes in domain names.
4. Be Cautious with Attachments and Links: Don’t open attachments or click on links from unknown senders. Scan attachments for malware before downloading.
5. Avoid Public Wi-Fi for Accessing Emails: Public Wi-Fi networks are often unencrypted, making it easier for attackers to intercept data. Use a VPN if you must access emails on public networks.
6. Review Email Headers for Anomalies: If an email looks suspicious, check the email headers to verify the origin and see if authentication protocols (SPF/DKIM/DMARC) passed.
7. Update Email Clients and Software Regularly: Security vulnerabilities are often fixed in updates. Ensure your email client, browser, and antivirus software are always up to date.
8. Monitor Your Inbox for Unusual Activity: If you receive unexpected emails, especially with links or attachments, verify their legitimacy before responding.
9. Backup Important Emails: In case of a cyber-attack, have regular backups of important emails to avoid loss of crucial information.
10. Educate Yourself and Team Members: Learn about email security best practices, and ensure that everyone in your organization understands the risks of email-based attacks.

---

2. Common Email Scams to Avoid

Watch Out! Common Email Scams and How to Avoid Them

Description: Learn about the most common email scams and how you can protect yourself and your business from falling victim to them. This guide helps you spot the telltale signs of fraudulent emails.

Common Email Scams to Avoid:

1. Phishing Scams: Scammers impersonate reputable institutions, like banks, to steal your personal or financial information. Look for suspicious sender addresses or urgent language pressuring you to act quickly.
2. Spear Phishing: Unlike generic phishing attempts, spear phishing is highly targeted and personalized using information about you or your business. Be wary of unexpected requests from people you know.
3. Business Email Compromise (BEC): Attackers impersonate executives or suppliers and request wire transfers or sensitive information. Verify any unusual requests through another communication channel before proceeding.
4. Fake Invoices: Fraudsters send invoices pretending to be a legitimate vendor or service provider. Always verify invoice details by contacting the vendor directly before making payments.
5. Tech Support Scams: Emails claim to be from legitimate tech support services and request you to click on a link to resolve an issue. Legitimate companies won’t ask you to click on random links or share sensitive information over email.
6. Lottery or Prize Scams: Emails claiming you’ve won a lottery or prize that you didn’t enter are usually scams designed to steal your personal or financial information.

Tips to Avoid Scams:

- Always hover over links to see the actual URL before clicking.
- Don’t share sensitive information via email, especially if requested unexpectedly.
- Use email filtering tools to block common scam emails.

---

3. Email Header Cheat Sheet

Quick Email Header Cheat Sheet

Description: A handy one-page guide to help you quickly understand and analyze email headers, making it easy to spot suspicious or spoofed emails.

Email Header Breakdown:

- From:
  The sender’s email address. Check for mismatches between the sender's address and the domain.
- Return-Path:
  Indicates the actual origin of the email. Compare this with the "From" field to catch possible spoofing attempts.
- Received:
  Shows the path the email took across mail servers before reaching your inbox. Look for unfamiliar or suspicious sources.
- SPF (Sender Policy Framework):
  This field tells you if the email came from an authorized server. A "pass" means the email’s server is authorized by the domain.
- DKIM (DomainKeys Identified Mail):
  Indicates whether the email was signed by the domain owner. A "pass" indicates that the email hasn’t been tampered with in transit.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance):
  A "pass" here means the domain owner has verified that the email passed both SPF and DKIM checks.

Quick Tips:

- Always check for the SPF, DKIM, and DMARC results.
- Watch for mismatches between the "From" and "Return-Path" fields.
- Pay attention to the "Received" field to track the email’s journey.

---

4. Access to Recommended Tools or Resources

Top Free Tools for Email Header Analysis

Description: This resource list contains the best free tools available online for analyzing email headers. These tools help you verify the legitimacy of emails and protect your inbox from fraud.

Free Tools for Email Header Analysis:

1. Phishtool Email Analyzer: An online tool that helps you decode email headers and check for potential threats, spoofing, or phishing attacks.
2. MXToolbox Email Headers Analyzer: A powerful email header analysis tool that decodes the headers and gives you valuable information about the origin and routing of the email.
3. Trustifi Email Analyzer: Another online service for analyzing email headers to help detect suspicious or potentially fraudulent messages.
4. Mail Header Analyzer (MHA): This tool decodes email headers and provides a detailed breakdown of the sender's information, SPF/DKIM results, and the email's journey.

How to Use These Tools:

- Simply paste your email header into the tool's interface, and the system will decode it for you, showing you the detailed path, the email took and whether it passed authentication checks.