

# **A Research Report on E-mail Analysis**

Prepared by  
Siva Krishna Siripurapu

# Report on E-Mail Analysis

Author: Sivakrishna Siripurapu

Date: 08-12-2024

## 1. Objective:

### Purpose:

- E-Mail Analysis involves studying the content of E-Mails to ascertain the techniques the attacker used.

### Goals:

- Learn how to read and find details of E-mail Headers.
- Spot signs of phishing and potential threats.

## 2. Scope:

**Target Audience:** Security teams, students, or anyone studying phishing.

### Focus Areas:

- How E-mails are sent and received (headers).
- Finding fake senders and dangerous attachments or links to get access to our systems.

## 3. Tools and Resources Used:

### Software/Tools:

- Outlook or email apps to see email details.
- Websites like MX Toolbox to check email data.
- Virus scanners like Virus Total for files or links.

### Hardware Requirements:

Standard computer with internet access.

### References:

- Microsoft documentation for email header properties.
- Phish Tank Website is a collaborative clearing house for data and information about phishing on the Internet.

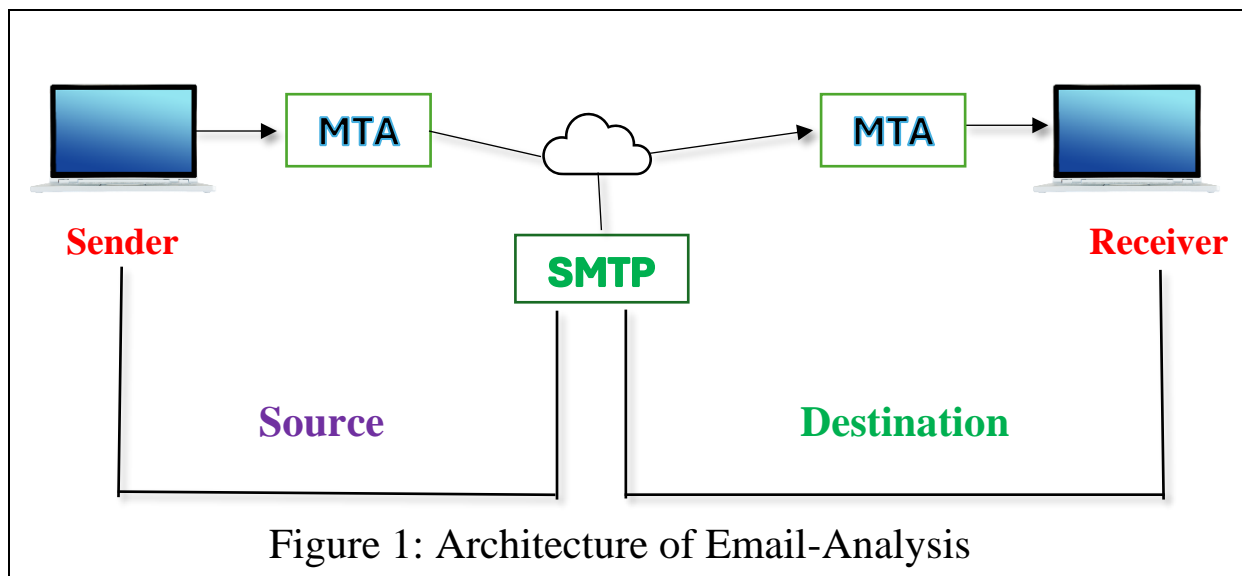
## 4. Components and Concepts:

- Email metadata (headers, routing paths, timestamps).

### Key Concepts:

- Spoofing SPF (Sender-policy Framework).
- DKIM (DomainKeys Identified Mail).

- DMARC (Domain-based Message Authentication, Reporting and Conformance), and Phishing.
- MUA (Mail-User Agent).
- MTA (Mail-Transfer Agent).
- SMTP (Simple-Mail Transfer Protocol).



## 5. Procedure/Implementation Steps:

### 1. Preparation:

- Collecting Phishing E-mails in a Safe Environment.
- Install required tools and ensure a secure analysis environment.

### 2. Execution:

- Open the E-mail (as per your Outlook or G-mail version).
- View Message Options > Click File > **Properties**.
- Open email headers & copy and paste the E-mail Headers in Online Analyzer Tools.
- Note anomalies like mismatched "From" and "Reply-To" addresses.
- Scan attachments/links in a malware sandbox.

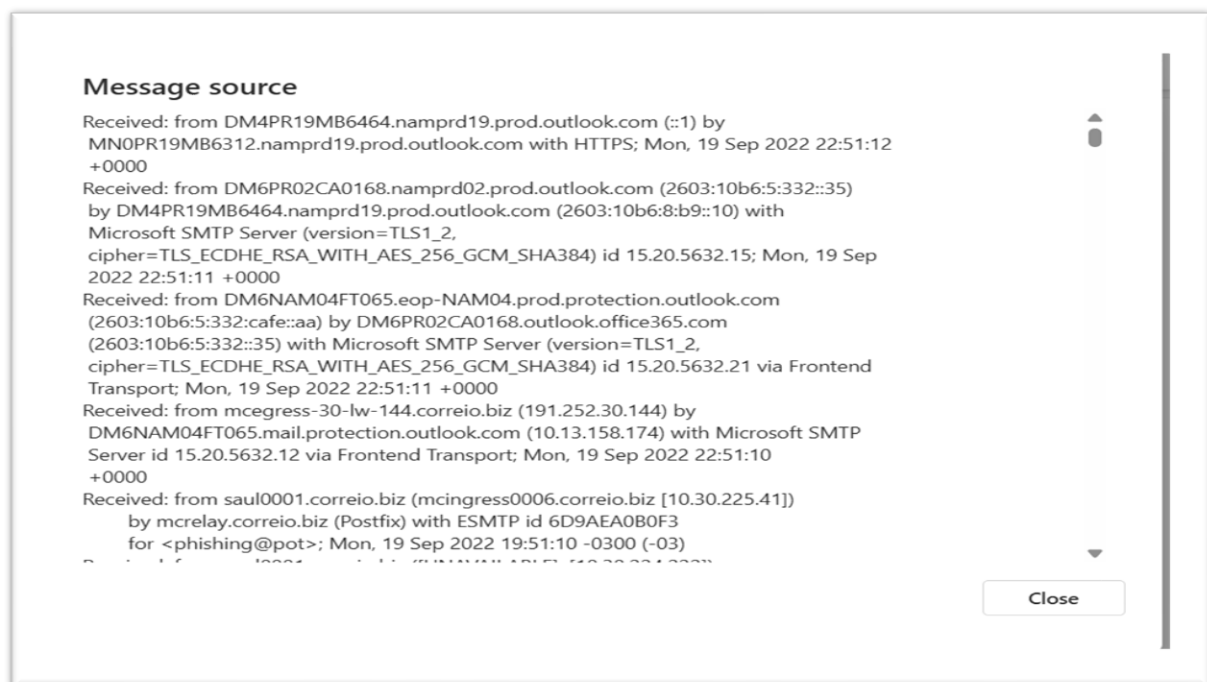


Figure 2: Email Header of sample mail from outlook

### 3. Validation:

- Confirm findings with trusted sources or cross-check with analysis tools.

### 4. Challenges and Errors:

- Managing obfuscated or encoded malicious content.

## 6. Results and Analysis:

### 1.Findings:

Header Analysis

Received Headers

- Outlook Servers:
- MN0PR19MB6312.namprd19.prod.outlook.com
- MW4PR04CA0228.outlook.office365.com
- Mail Server:
- mail229-223.static.kajabimail.net
- Sender's IP: 143.55.229.223 resolves to domain kajabimail.net.

Authentication Results

- DMARC: Pass.
- Note: Proper configuration doesn't guarantee legitimacy.
- SPF: Pass (Authorized sending IP).
- DKIM: Pass (Signature verification successful).

Suspicious Indicators

- Subject: "Your wallet may get suspended!" suggests urgency.
- Sender: Encoded name likely obfuscates true identity.
- Reply-To: rafiakhan314@gmail.com mismatches the sending domain.

### Security Measures and Recommendations

C

Verify the Source

□

Avoid interacting with links or replying.

■

Cross-check the sender's domain (kajabimail.net).

C

Use Advanced Security Tools

□

Analyze with anti-phishing tools.

□

Perform DNS lookup for IP.

C

Enable Multi-Factor Authentication

□

Protect associated accounts.

C

Report the Incident

□

Forward to IT/security team.

■

Submit to anti-phishing services (e.g., phishing-report@us-cert.gov).

### Introduction

This report outlines the analysis of a suspicious email received by the user on October 4, 2022, titled "Your wallet may get suspended!". The email appears to be a phishing attempt, and the following report examines its headers, source, and potential indicators of compromise.

### Payload Analysis

- Multipart/alternative message with HTML and plain text.
- Red flags:
  - Urgent Action Request: Provokes response.
  - Links: Verify embedded URLs.
  - Attachments: None detected but potentially malicious.

### Conclusion

The email exhibits characteristics of a phishing attempt:

- Mismatch between sending domain and reply-to address.
- Urgency in subject and body.
- Obfuscated sender details.

Immediate precautionary measures are recommended.

Figure 3: Sample E-mail Analysis Full Report

## 2. Insights:

Immediate measures, such as reporting the email and avoiding interaction, are crucial to prevent compromise. Always remain cautious of emails demanding urgent actions

## 7. Discussion:

- **Strengths:** Effective Detection of Phishing elements.
- **Limitations:** Use Online Tools for Header Decoding.
- **Improvements:** Automating analysis using scripts and tools.

## 8. Conclusion:

E-mail analysis is a critical aspect of cybersecurity, as it helps detect and mitigate threats such as phishing, spoofing, and other malicious activities. Through the systematic examination of email headers, metadata, and attachments, we gain insights into the sender's authenticity and identify potential risks. This research highlights the importance of understanding email structures, leveraging analytical tools, and adopting best practices for secure communication. By implementing the knowledge gained from this analysis, individuals and organizations can enhance their defenses against email-based attacks, ensuring a safer digital environment.

## 9. Recommendation:

- Teach people how to spot phishing.
- Use email security tools like filters.
- Follow email security practices.

## 10. Reference:

Microsoft Documentation - "Understanding Email Header Properties"

<https://learn.microsoft.com/en-us/>

MX Toolbox - "Email Header Analyzer Tool"

<https://mxtoolbox.com/>

Virus Total - "Analyze Suspicious Files and URLs"

<https://www.virustotal.com/>

Phish Tank - "Data on Phishing on the Internet"

<https://www.phishtank.com/>

RFC 5321 - "Simple Mail Transfer Protocol (SMTP)"

<https://datatracker.ietf.org/doc/html/rfc5321>

RFC 7208 - "Sender Policy Framework (SPF)"

<https://datatracker.ietf.org/doc/html/rfc7208>

Google Workspace Documentation - "Viewing and Analyzing Email Headers in Gmail"

<https://support.google.com/>

OWASP - "Phishing Guidance and Prevention Measures"

<https://owasp.org/>

## 11. Appendices:

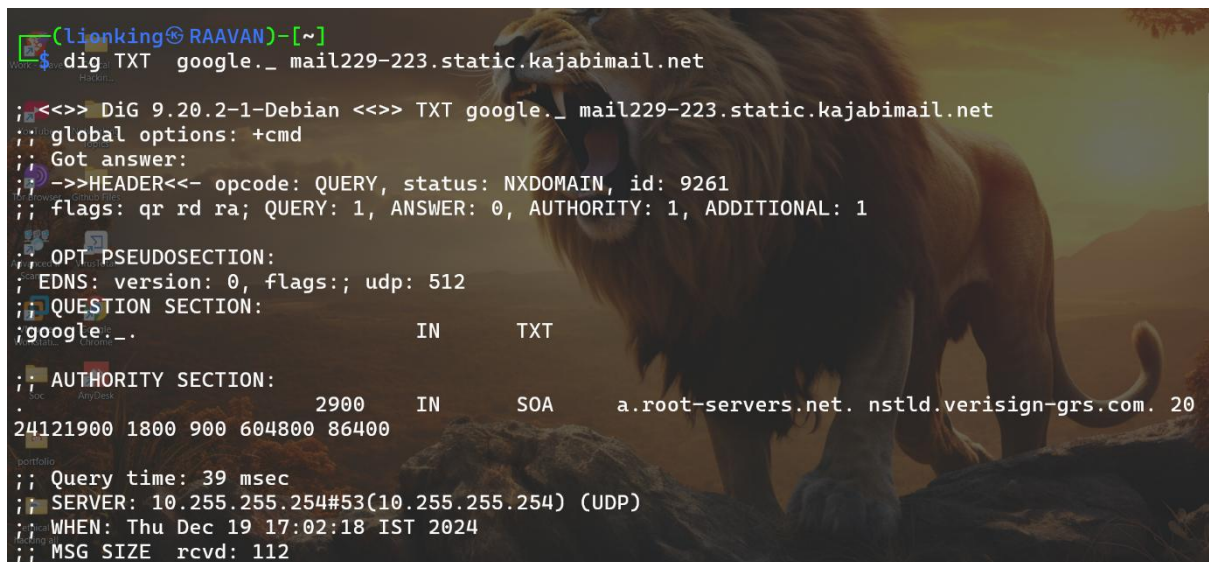


```
(lionking@RAAVAN)~$ nslookup -type=TXT kajabimail.net
Server:      10.255.255.254
Address:     10.255.255.254#53

Non-authoritative answer:
kjabimail.net text = "google-site-verification=MXy5Pm30dNEgPZINK90-tyuVR0fN17RTuH8VEF13NTk"

Authoritative answers can be found from:
```

Figure 4: SPF Not found domain.



```
(lionking@RAAVAN)~$ dig TXT google._mail229-223.static.kjabimail.net

;<<>> DiG 9.20.2-1-Debian <<>> TXT google._mail229-223.static.kjabimail.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 9261
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;google._.                IN      TXT

;; AUTHORITY SECTION:
.                2900    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20
24121900 1800 900 604800 86400

;; Query time: 39 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Thu Dec 19 17:02:18 IST 2024
;; MSG SIZE rcvd: 112
```

Figure 5: DKIM Lookup

## 2. E-Mail Investigation

E-mail investigation is a process in digital forensics used to find evidence from emails. It helps investigators analyze, protect, and understand email data to solve cases.

### Main Goals:

- Find the person responsible.
- Gather important evidence.
- Share the findings clearly.
- Build a convincing case.

### Challenges Faced:

- Detecting fake emails.
- Identifying spoofed (fake) senders.
- Tracking emails sent through anonymous services.

### Techniques Used:

- **Email Header Analysis:** Checking email headers for details like sender and path.
- **Server Investigation:** Looking at mail server records.
- **Network Investigation:** Analyzing data from network devices like routers.
- **Sender Mail Analysis:** Identifying the tools used to send the email.
- **Embedded Data Check:** Finding hidden information within the email.

### DMARC

- **Full Form:** Domain-based Message Authentication, Reporting, and Conformance.
- **Purpose:** An additional security protocol for email protection.
- **Function:** Works on top of DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework).
- **Role:** Acts as a decision-making layer to verify if both DKIM and SPF conditions are met.
- **Action:** Based on condition results, appropriate actions (allow, reject, or quarantine) are performed.



## SCL

- **Full Form:** Spam Confidence Level.
- **Purpose:** Microsoft technology for spam filtering.
- **Process:**
  - Emails received by Microsoft are scanned using Exchange Online Protection (EOP).
  - The service analyzes the email and adds anti-spam information to the message headers.
- **Output:** Each email is assigned a Spam Confidence Level score, indicating its likelihood of being spam.

### Spam Confidence Level (SCL) Scoring Breakdown

SCL is a score assigned to emails by Microsoft's spam filtering systems, indicating how likely the email is to be spam.

#### SCL Values and Their Actions:

##### 1. SCL -1 or 0:

- **Meaning:** Safe email, not spam.
- **Action:** Delivered to the inbox.

##### 2. SCL 1 to 4:

- **Meaning:** Low chance of being spam.
- **Action:** Delivered to the inbox but monitored.

##### 3. SCL 5 or 6:

- **Meaning:** Spam.
- **Action:** Delivered to the Junk Email folder.

##### 4. SCL 7 to 8:

- **Meaning:** High chance of being spam.
- **Action:** Delivered to the Junk Email folder.

##### 5. SCL 9:

- **Meaning:** Confirmed as high-confidence spam.
- **Action:** Rejected or quarantined (based on organization settings).

#### Key Notes:

- Higher SCL scores mean greater confidence that the email is spam.
- Actions (e.g., delivery to inbox, junk, or rejection) depend on organizational email policies.

## PCL

- **Full Form:** Phishing Confidence Level.
- **Purpose:** Microsoft technology to detect and classify phishing emails.
- **Process:**
  - Microsoft's Exchange Online Protection (EOP) scans emails.
  - The service analyzes email content, sender information, and embedded links to identify phishing attempts.
  - Anti-phishing details are added to the email headers.
- **Output:** Each email is assigned a Phishing Confidence Level score, indicating its likelihood of being a phishing attempt.

### Phishing Confidence Level (PCL) Breakdown

**Phishing Confidence Level (PCL)** is a Microsoft rating system that evaluates how likely an email is a phishing attempt. It helps identify phishing emails based on certain patterns and characteristics.

### PCL Scores and Their Meaning:

#### 1. PCL 0:

- **Meaning:** Safe email, no phishing detected.
- **Action:** Delivered to the inbox.

#### 2. PCL 1 to 3:

- **Meaning:** Minimal risk of phishing.
- **Action:** Delivered to the inbox but flagged for monitoring.

#### 3. PCL 4 to 7:

- **Meaning:** Suspicious email, phishing detected.
- **Action:** Delivered to Junk Email or quarantined based on settings.

#### 4. PCL 8 to 9:

- **Meaning:** High-confidence phishing email.
- **Action:** Quarantined, rejected, or blocked (depending on policy).

### Key Points:

- **Higher PCL scores** indicate a greater likelihood of phishing content.
- Microsoft uses advanced filters and machine learning to assign PCL scores.
- PCL works alongside SCL to improve overall email security.

## BCL (Bulk Confidence Level)

- **Full Form:** Bulk Confidence Level
- **Purpose:** Microsoft technology used for classifying bulk or promotional emails.
- **Process:**
  - Emails received by Microsoft are analyzed through email filtering systems like Exchange Online Protection (EOP).
  - The service evaluates the message content, sender behavior, and metadata to determine whether it is part of a bulk email campaign.
  - Bulk email campaigns, such as newsletters, advertisements, or marketing content, are categorized based on their characteristics.
  - The analysis assigns a Bulk Confidence Level score to each email, indicating how likely it is to be categorized as bulk or promotional.
- **Output:**
  - Each email is assigned a Bulk Confidence Level score from 0 to 10.
  - The score reflects the likelihood of the email being classified as bulk email and determines whether the email is delivered to the inbox or redirected to folders like "Promotions," "Updates," or "Junk."

This process helps in separating bulk messages from personal emails, making inbox management more efficient for users.

## BCL (Bulk Confidence Level) Breakdown:

The **Bulk Confidence Level (BCL)** is a Microsoft rating system that assesses how likely an email is to be classified as bulk or promotional email. It helps identify non-personal, high-volume emails that might be deemed as marketing or unwanted communication.

### BCL Breakdown:

#### 1. BCL 0 (Not Bulk):

- The email is considered personal or highly relevant.
- It is sent by a trusted sender and contains genuine content, making it suitable for the inbox.

#### 2. BCL 1-3 (Low Bulk):

- These emails might be promotional or from known sources like businesses or newsletters.

- They are usually not flagged as spam, but they may be categorized as non-personal or marketing emails.
  - The content is not typically harmful but can be filtered into separate folders like "Promotions" or "Updates."
3. **BCL 4-6 (Moderate Bulk):**
- These emails have a higher likelihood of being from bulk senders or campaigns.
  - They may contain offers, advertisements, or other mass marketing content.
  - Email services may categorize them as "Junk" or place them under less important tabs.
4. **BCL 7-9 (High Bulk):**
- These emails are certainly mass-marketing emails or from suspicious sources.
  - They may contain aggressive marketing tactics and are often flagged as unwanted or promotional.
  - Likely to be automatically filtered as junk or placed in a promotions folder.
5. **BCL 10 (Blocked):**
- The email is recognized as bulk or spam with high certainty.
  - It is typically blocked or rejected by the email service due to content that matches known bulk email patterns.
  - This includes newsletters or promotional content that is flagged as non-personal or irrelevant.

### **Purpose:**

The BCL system helps email services classify non-personal or marketing emails while keeping personal, relevant communication separate. It assists in managing email overload, ensuring important messages are not lost in spam or promotional folders.

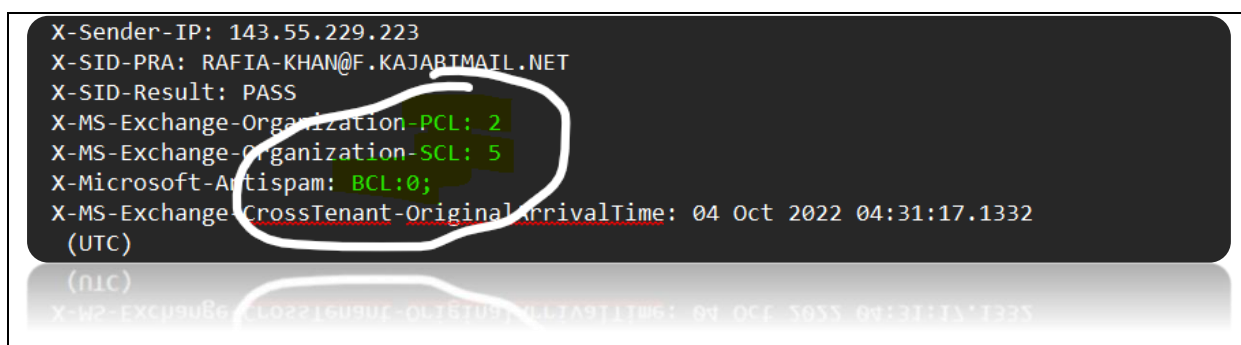


Figure 6: PCL, SCL, BCL Score Report

## Sender Reputation

Sender reputation is a key factor in determining whether an email is delivered to the inbox or marked as spam. It reflects the trustworthiness of the sender based on various metrics. A good sender reputation improves deliverability, while a poor reputation may lead to emails being sent to the junk folder. The main factors affecting sender reputation include:

### 1. **Authenticated Framework:**

- Use of authentication protocols like SPF, DKIM, and DMARC helps verify the legitimacy of the sender.

### 2. **Send Volumes:**

- Sending emails at high volumes without proper targeting or engagement can negatively affect the sender's reputation.

### 3. **Complaints Rate:**

- High numbers of recipients marking emails as spam or unsubscribing negatively impacts the reputation.

### 4. **Blocking and Spam Trap Hits:**

- Being listed on block lists or hitting spam traps can severely damage a sender's reputation, affecting email deliverability.

## IP Reputation

IP reputation is a metric used by Internet Service Providers (ISPs) to evaluate whether an email sender's IP address is associated with legitimate email behavior. It helps ISPs determine if emails should be delivered to the inbox or redirected to spam/junk folders. Several factors influence IP reputation:

### 1. **Open and Click Rates:**

- High open and click rates indicate that recipients find the emails valuable and engaging, positively influencing IP reputation.

### 2. **Spam Complaint Rates:**

- A high rate of spam complaints signals to ISPs that the email may be unwanted, damaging the sender's reputation.

### 3. **Bounce Rates:**

- High bounce rates, especially from invalid email addresses, can indicate poor list management and impact IP reputation negatively.

#### 4. Shared vs Dedicated IP Reputation:

- **Shared IP:**

- Multiple senders use a shared IP. The actions of one sender (e.g., sending spam) can impact the reputation of all senders using the same IP.
- Example: If one sender sends spam emails, ISPs may flag the entire shared IP, affecting other senders using the same address.

- **Dedicated IP:**

- A dedicated IP is used by a single sender or organization, providing full control over email reputation. It is essential to warm up a new dedicated IP by gradually increasing the sending volume to build a positive reputation.
- Example: A dedicated IP allows you to control your reputation based on your email practices, but improper use (e.g., sending too many emails at once) can harm your reputation.

Both **sender reputation** and **IP reputation** are crucial for email deliverability. Proper email authentication, monitoring complaint rates, and careful management of sending volumes and bounce rates help ensure good email reputation, which leads to better inbox placement.

#### **SFV (Spam Filtering Validation) Extensions**

SFV is a spam filtering technique used to classify emails based on predefined policies and actions. It involves sending a report in the form of an extension that reflects the results of the spam filtering process. The **X-Forefront-Antispam-Report** is a common example, where SFV values define the actions taken on the email based on its analysis.

Here are the different SFV extensions and their meanings:

##### 1. **SFV:BLK**

- **Action:** Block the sender.
- **Description:** The sender is blocked, and emails from this source will be rejected or discarded.

##### 2. **SFV:NSPM**

- **Action:** Marked as non-spam.
- **Description:** The email is classified as legitimate and not flagged as spam. It will be delivered to the inbox.

##### 3. **SFV:SFE**

- **Action:** Sender's safe list.

- **Description:** The sender is on a trusted list, meaning the message is considered safe and will be delivered without further filtering.

#### 4. **SFV:SKA**

- **Action:** The message is skipped to anti-spam filtering.
- **Description:** The message is bypassed or skipped for further spam analysis, likely because of internal policies or exceptions.

#### 5. **SFV:SKB**

- **Action:** The message is marked as spam due to anti-spam policy match.
- **Description:** The email matches known spam characteristics or patterns, and thus is flagged as spam.

#### 6. **SFV:SKI**

- **Action:** The message is skipped for spam filtering because it is an intra-zone mail.
- **Description:** The email comes from within the same organization or zone, and spam filtering is skipped due to internal mail rules.

#### 7. **SFV:SKQ**

- **Action:** The message is released to quarantine.
- **Description:** The email is placed in quarantine for further review or analysis due to suspicion of being spam or malicious.

#### 8. **SFV:SKS**

- **Action:** The message is marked as spam prior to 5 to 9.
- **Description:** This indicates the email was flagged as spam during an earlier stage of the filtering process (preliminary analysis).

#### 9. **SFV:SPM**

- **Action:** The message was marked as spam by spam filtering.
- **Description:** The email was detected as spam by the filtering system and will be treated accordingly (e.g., moved to the junk folder).

#### **Example SFV Header:**

X-Forefront-Antispam-Report: CTRY;; LANG:hr; SCL:1; SRV;; IPV:NLI; SFV:NSPM; PTR;; CAT:NONE; SFTY;;...

In the example above:

- **SFV:NSPM** indicates the message is marked as non-spam.
- **SCL:1** suggests the spam confidence level score.

These SFV extensions help in the spam filtering process by providing clear instructions about the classification and handling of emails, ensuring better management of incoming messages.

### **Email Security Solutions Software:**

#### **1. Microsoft Defender for Office 365**

- Phishing, Malware, BEC, Threat Protection, Spam Filtering, Microsoft 365.

#### **2. Barracuda Email Security Gateway**

- Spam, Virus, Malware, DLP, Encryption, Cloud, On-premises.

#### **3. Proofpoint Email Protection**

- Spear-Phishing, Malware, BEC, Threat Detection, URL Protection, Reporting.

#### **4. Mimecast Email Security**

- Multi-layered Protection, Spam, Malware, Phishing, Archiving, Continuity, Encryption.

#### **5. Symantec Email Security (Broadcom)**

- Phishing, BEC, Ransomware, Attachment Scanning, Reputation Filtering, DLP, Encryption.

#### **6. Cisco Email Security**

- Spam, Phishing, Malware, Filtering, Encryption, DLP, Threat Analysis, Management.

#### **7. Trend Micro Email Security**

- Spam, Phishing, Ransomware, URL Filtering, Sandboxing, DLP, Reporting.

#### **8. Fortinet Forti Mail**

- Spam, Malware, Phishing, Encryption, Threat Protection, Hardware, Virtual, Cloud.