Chapter 1: Investigating Email Threats

Email threat types

• Spearphishing attachments :

A spearphishing attachment involves adversaries sending phishing emails to target victims with malicious attachments, either to gain initial access to their systems or harvest their credentials

Note : Phishing emails are mass email attacks that are sent to a randomly large number of people. In contrast, spearphishing emails are much more targeted and personalized. They are specifically crafted to target a particular individual or group of individuals, such as employees of a particular company or members of a specific organization

Phishing attachment types:

- Malicious Microsoft Office documents
- Malicious PDF files
- Compressed files (.rar, .7z, zip, etc.)
- ISO images
- HTML file

• Spearphishing links

A spearphishing link involves adversaries sending spearphishing emails to target victims with a malicious link, to either harvest their credentials or trick them into downloading malware and executing it on their machine, thus gaining initial access to their systems.

Phishing link types:

- A phishing link to harvest credentials
- A phishing link to download malware

• Blackmail emails

A blackmail email, also known as a **“sextortion”** email, is a term used to describe an email scam where an attacker claims to have compromised the victim’s machine and exfiltrated sensitive data, including sexual content and pictures to the attacker’s server

• Business Email Compromise

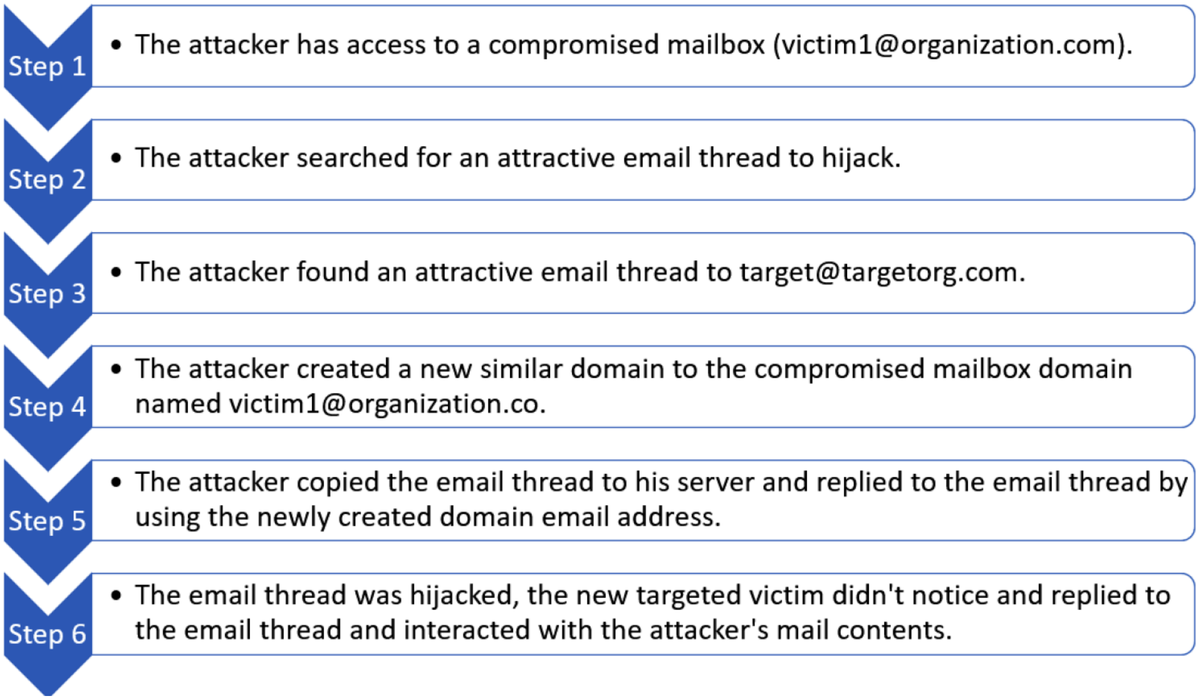
is a type of email scam where the attacker targets a specific individual within a company who has access to financial information, such as an executive or a finance employee, and tricks them into making a fraudulent financial transaction or wire transfer

Attacker techniques to evade email security detection

1. Using newly created domains to send a malicious email
2. Using non-blacklisted SMTP servers:
3. Sandbox analysis evasion
    - Malware sleep:
    - Encrypted file:
    - Sandbox discovery:
    - Responding to specific requests:
4. Trusted domains hosting phishing pages

Social engineering techniques to trick the victim

- Email spoofing
- Email thread hijacking’



Step 1
- The attacker has access to a compromised mailbox (victim1@organization.com).

Step 2
- The attacker searched for an attractive email thread to hijack.

Step 3
- The attacker found an attractive email thread to target@targetorg.com.

Step 4
- The attacker created a new similar domain to the compromised mailbox domain named victim1@organization.co.

Step 5
- The attacker copied the email thread to his server and replied to the email thread by using the newly created domain email address.

Step 6
- The email thread was hijacked, the new targeted victim didn't notice and replied to the email thread and interacted with the attacker's mail contents.

- Hosting phishing pages on trusted websites that issue an SSL certificate

Chapter2: Email Flow and Header Analysis

• Email flow

1. Mail User Agent (MUA)
2. Mail Submission Agent(MSA)
3. Mail Transfer Agent (MTS)
4. Mail Exchange (MX)
5. Mail Delivery Agent(MDA)

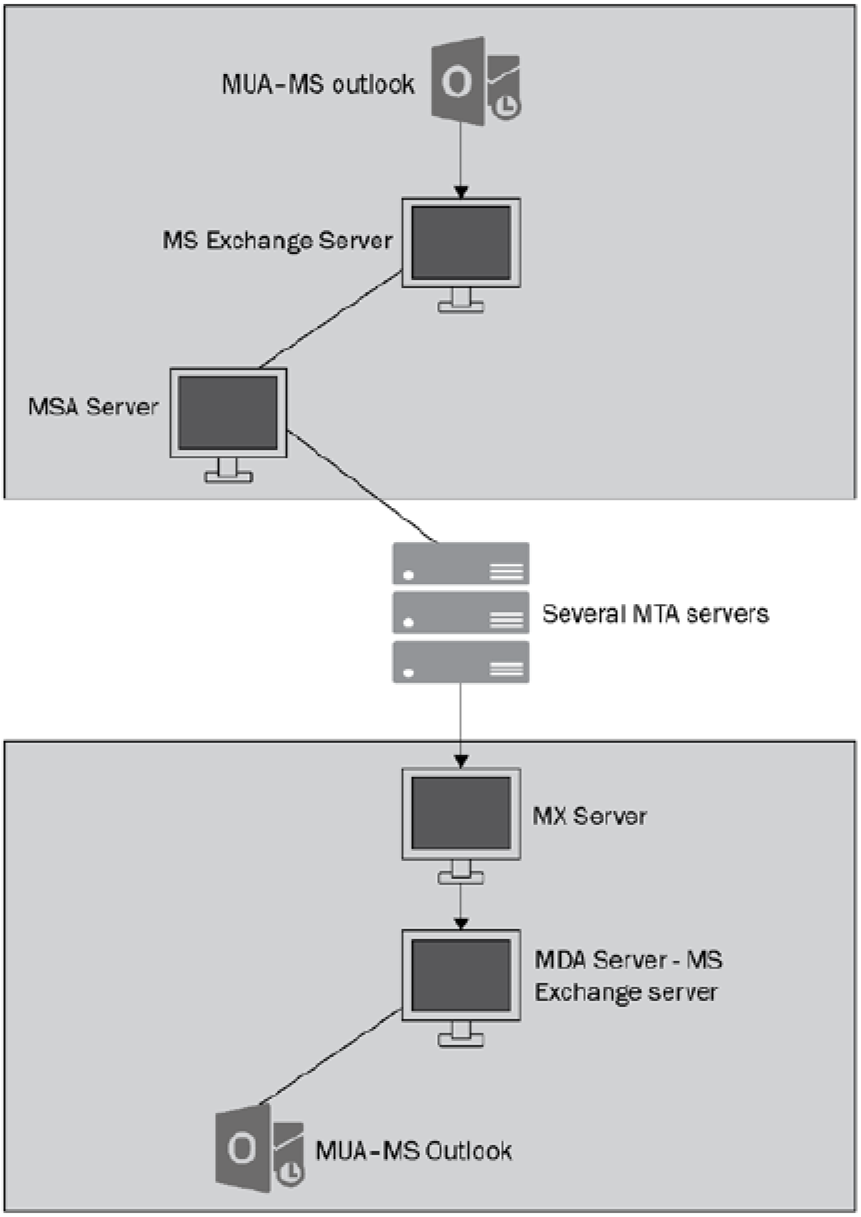
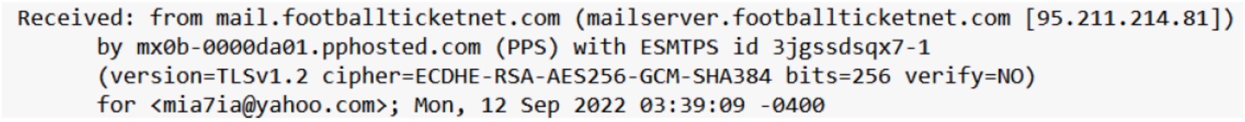


Figure 2.1 – Email flow

The purpose of understanding the email flow and the hops that the email passes is to be aware that every hop adds a header to the email message header that contains at least the email server’s hostname, server IP, and date and time of email processing.



```
Received: from mail.footballticketnet.com (mailserver.footballticketnet.com [95.211.214.81])
        by mx0b-0000da01.pphosted.com (PPS) with ESMTPS id 3jgssdsqx7-1
        (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO)
        for <mia7ia@yahoo.com>; Mon, 12 Sep 2022 03:39:09 -0400
```

• Email header analysis

To break down the email header, we will divide this section into four subsections:

1. Email message content and metadata

- Date
- From
- To
- Subject
- MIME-Version: Multipurpose Internet Mail Extensions (MIME)
- Content-Type
- Content-Transfer-Encoding
- References
- Content-Length

2. Email X-headers

Email X-headers are custom headers that are added to the email header by the mailbox providers in addition to the standard headers, such as To, From, Subject, and MIME-Version, all of which are defined by the RFC standards. Custom X-headers are added to the email header according to the needs of the mailbox provider.

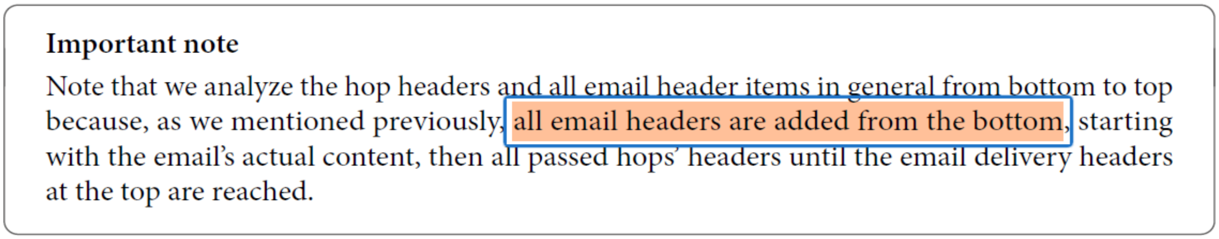
- X-Mailer
- X-YMail-OSG
- X-Sonic-MF
- X-SONIC-DKIM-SIGN

Important note

There is a common X-header called the **X-Originating-IP** header. This is an email header that contains the IP address of the device that is the origin of the email. It helps identify the origin IP of the message and can be used for spam filtering and tracking purposes.

3. The header that was added by the hop servers

As we discussed previously, email headers are added by every server that an email passes through, including the MX, MSA, MTA, and MDA servers. These headers contain critical information such as the server's hostname, IP address, and timestamp for email processing.



Important note

Note that we analyze the hop headers and all email header items in general from bottom to top because, as we mentioned previously, all email headers are added from the bottom, starting with the email's actual content, then all passed hops' headers until the email delivery headers at the top are reached.

- **Email authentication**
- How does email authentication work?

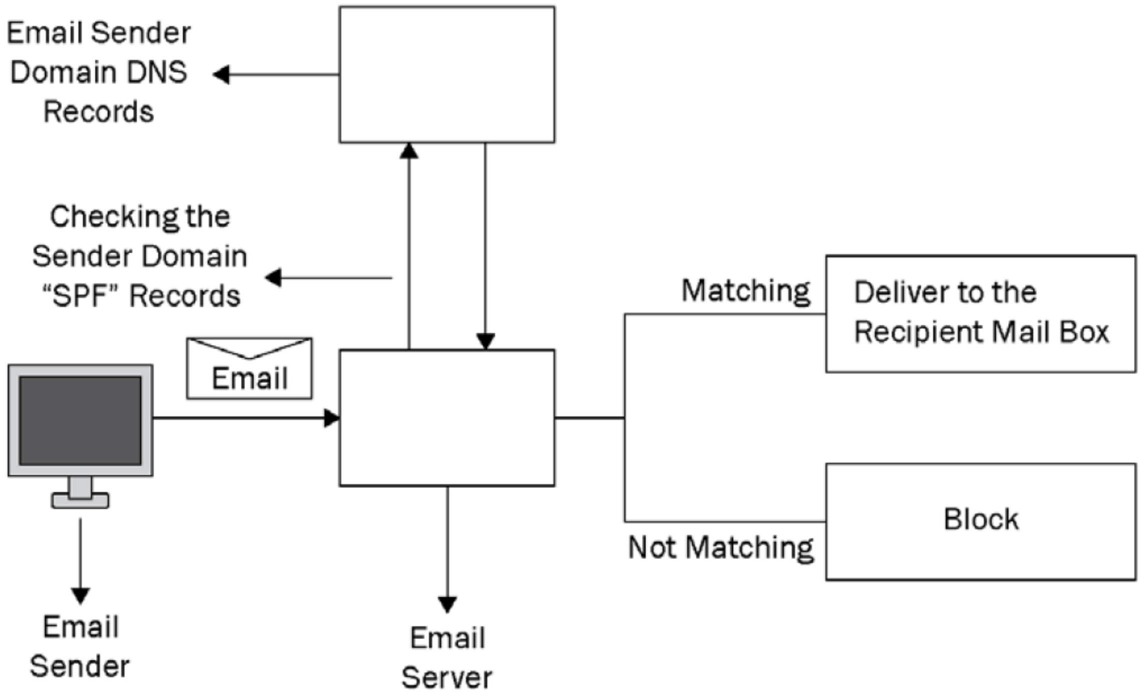
1. The email sender domain owner, which for this example is Microsoft.com, establishes and defines rules for authenticating emails that are sent from or on behalf of its domain and publishes these records and rules in the domain's DNS records.
2. When the email servers receive emails from the Microsoft.com domain, they attempt to authenticate the email messages using the published records and rules.
3. Finally, the receiving email server determines the legitimacy of the email and follows the published rules to decide whether to deliver the email message to the recipient's mailbox or drop it.

- Email authentication protocols

The three protocols that are used in the email authentication process are called **SPF, DKIM, and DMARC.**

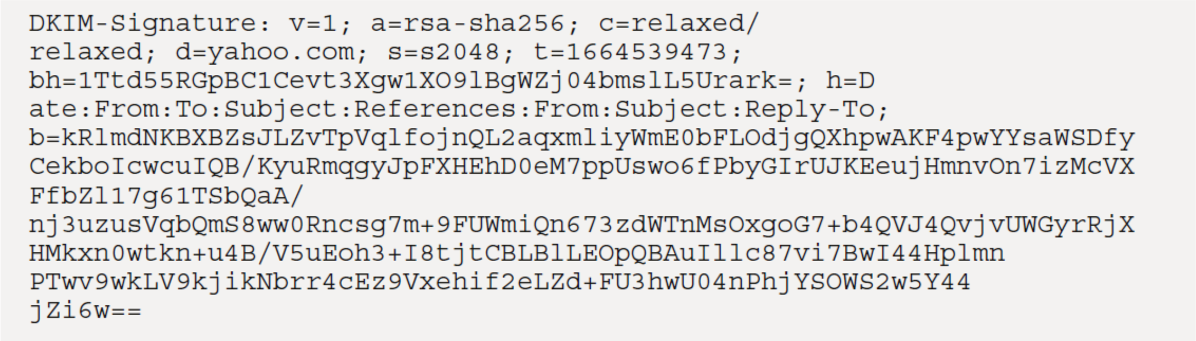
- **Sender Policy Framework (SPF)**

Sender Policy Framework (SPF) is an email authentication protocol that provides a DNS TXT record in the domain's DNS records that specifies which IP addresses or hostnames are authorized to send emails for and on behalf of this domain.


Email Sender Domain DNS Records
Checking the Sender Domain "SPF" Records
Email
Matching
Deliver to the Recipient Mail Box
Not Matching
Block
Email Sender
Email Server

- **DomainKeys Identified Mail (DKIM)**

Is an encryption methodology or digital signature that's added to email headers as an email authentication mechanism to prevent email spoofing attempts.



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/
relaxed; d=yahoo.com; s=s2048; t=1664539473;
bh=1Ttd55RGpBC1Cevt3Xgw1XO9lBgWZj04bmslL5Urark=; h=D
ate:From:To:Subject:References:From:Subject:Reply-To;
b=kRlmdNKBXBZsJLZvTpVqlfojnQL2aqxmliyWmE0bFLOdjgQXhpwAKF4pwYYsaWSDfy
CekboIcwcuIQB/KyuRmqgyJpFXHEhD0eM7ppUswo6fPbyGIrUJKEeujHmnvOn7izMcVX
FfbZl17g61TSbQaA/
nj3uzusVqbQmS8ww0Rncsg7m+9FUWmiQn673zdWTnMsOxgoG7+b4QVJ4QvjvUWGyrRjX
HMkxn0wtkn+u4B/V5uEoh3+I8tjtCBLBlLEOpQBAuIllc87vi7BwI44Hplmn
PTwv9wkLV9kjikNbrr4cEz9Vxehif2eLZd+FU3hwU04nPhjYSOWS2w5Y44
jZi6w==
```

v: This field’s value refers to the version of the DKIM.

a: This field’s value refers to the algorithm that’s used for both encryption and hashing to generate the digital signature. In this case, it uses RSA and SHA256.

C: This field’s value refers to the canonicalization algorithm that determines how the body and the header are prepared for the hashing algorithm.

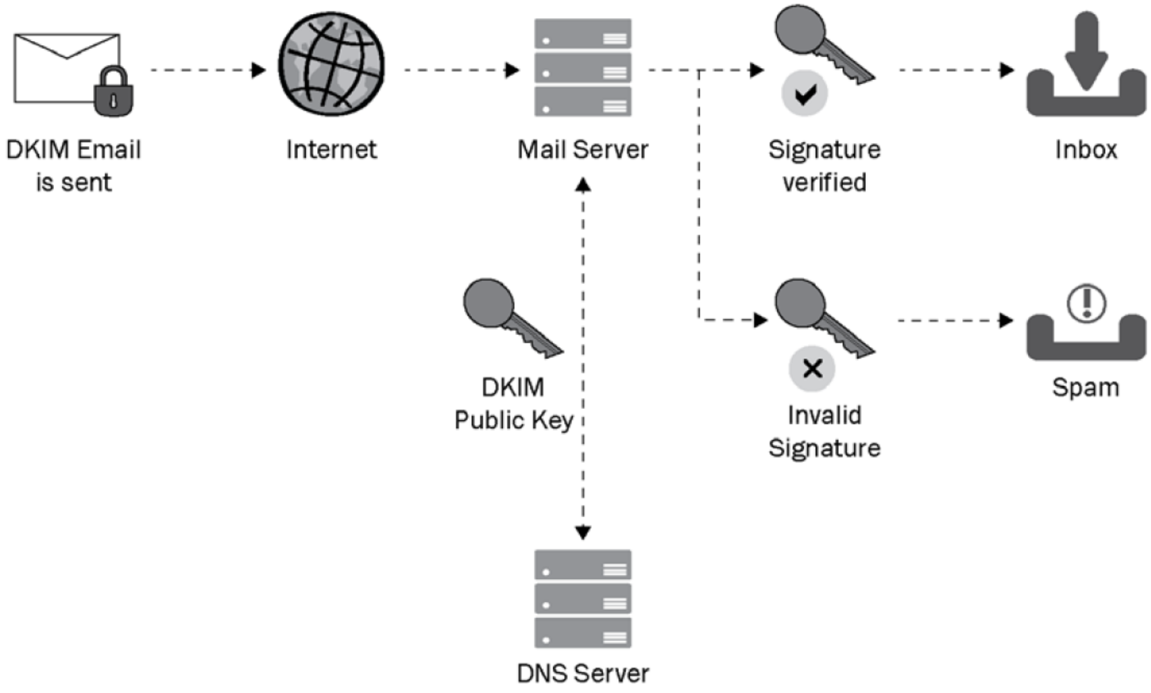
d: This field’s value refers to the domain that is claiming to be authorized to send the email.

s: This field’s value refers to the selector value used to define the value used in the DNS lookup to get the public key.

t: This field’s value refers to the epoch timestamp,

bh: This field’s value refers to the base64-encoded strings of the email message body after it was canonicalized via the method in c and then hashed via the hashing function in a.

b: This field’s value refers to the DKIM signature itself and is calculated using all the previous values.



Extra resources:
https://postmarkapp.com/blog/what-is-arc-or-authenticated-received-chain
How DKIM SPF & DMARC Work to Prevent Email Spoofing

Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

```
"v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@test.com"
```

- v: This field’s value refers to the version of DMARC that the domain uses.
- p: This field’s value tells the recipient server what policy should be applied if the email fails the authentication process.
- pct: This field’s value refers to the percentage of email messages subjected to the policy; the range is from 1 to 100
- rua: This specifies the URI of the mailbox that will receive DMARC aggregate reports.

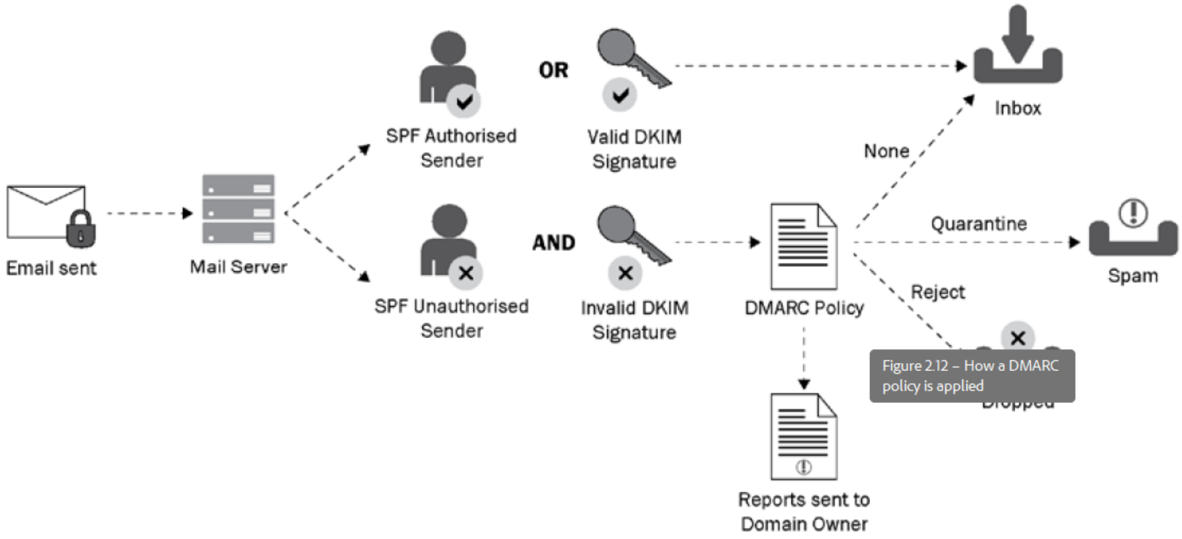
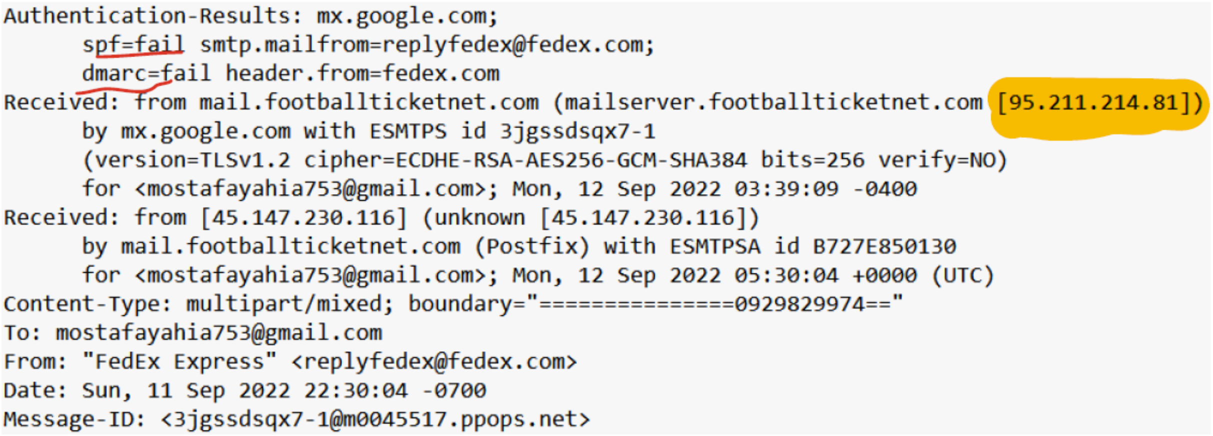


Figure 2.12 – How a DMARC policy is applied

• Investigating the email header of a spoofed message



```
Authentication-Results: mx.google.com;
      spf=fail smtp.mailfrom=replyfedex@fedex.com;
      dmarc=fail header.from=fedex.com
Received: from mail.footballticketnet.com (mailserver.footballticketnet.com [95.211.214.81])
      by mx.google.com with ESMTPS id 3jgssdsqx7-1
      (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO)
      for <mostafayahia753@gmail.com>; Mon, 12 Sep 2022 03:39:09 -0400
Received: from [45.147.230.116] (unknown [45.147.230.116])
      by mail.footballticketnet.com (Postfix) with ESMTPSA id B727E850130
      for <mostafayahia753@gmail.com>; Mon, 12 Sep 2022 05:30:04 +0000 (UTC)
Content-Type: multipart/mixed; boundary="===============0929829974=="
To: mostafayahia753@gmail.com
From: "FedEx Express" <replyfedex@fedex.com>
Date: Sun, 11 Sep 2022 22:30:04 -0700
Message-ID: <3jgssdsqx7-1@m0045517.ppops.net>
```