MITRE ATTACK FRAMEWORK

WHAT IS THE MITRE ATTACK FRAMEWORK

It is a **framework** that contains adversary tactics and techniques based on real-world observations.

In 2013, MITRE began to address the need to record and document common TTPs (**Tactics, Techniques, and Procedures**)
that APT (**Advanced Persistent Threat**) groups used against enterprise Windows networks.

https://attack.mitre.org/

FASLE POSITIVE

A "false positive" refers to an error in a process that mistakenly identifies something as true or present when it's not.

You get an alert even though nothing happened.

FASLE NEGATIVE

A "false negative" is an error that occurs when a system or analysis wrongly indicates the absence of a condition, event, or attribute that is actually present.

Something happened but you did not get an alert.

TRUE POSITIVE

A "true positive" refers to a correct and accurate result in an analysis.

It occurs when the test correctly identifies or detects the presence of a specific condition when it is genuinely present.

You get an alert when something happens.

TRUE NEGATIVE

A "true negative" occurs when the test correctly identifies the absence of a specific condition or event when it is genuinely not present.

You did not get an alert because nothing happened.

EMAIL HEADER ANALYSIS

Email Header Analysis

Mail User Agent (MUA)

Client application running on your computer that is used to send and receive mail. Examples include Apple Mail, Microsoft Outlook, and Mozilla Thunderbird.

Mail Transfer Agent (MTA)

Accepts messages from a sender and routes them along to their destinations. Examples include Sendmail, Postfix, and Microsoft Exchange.

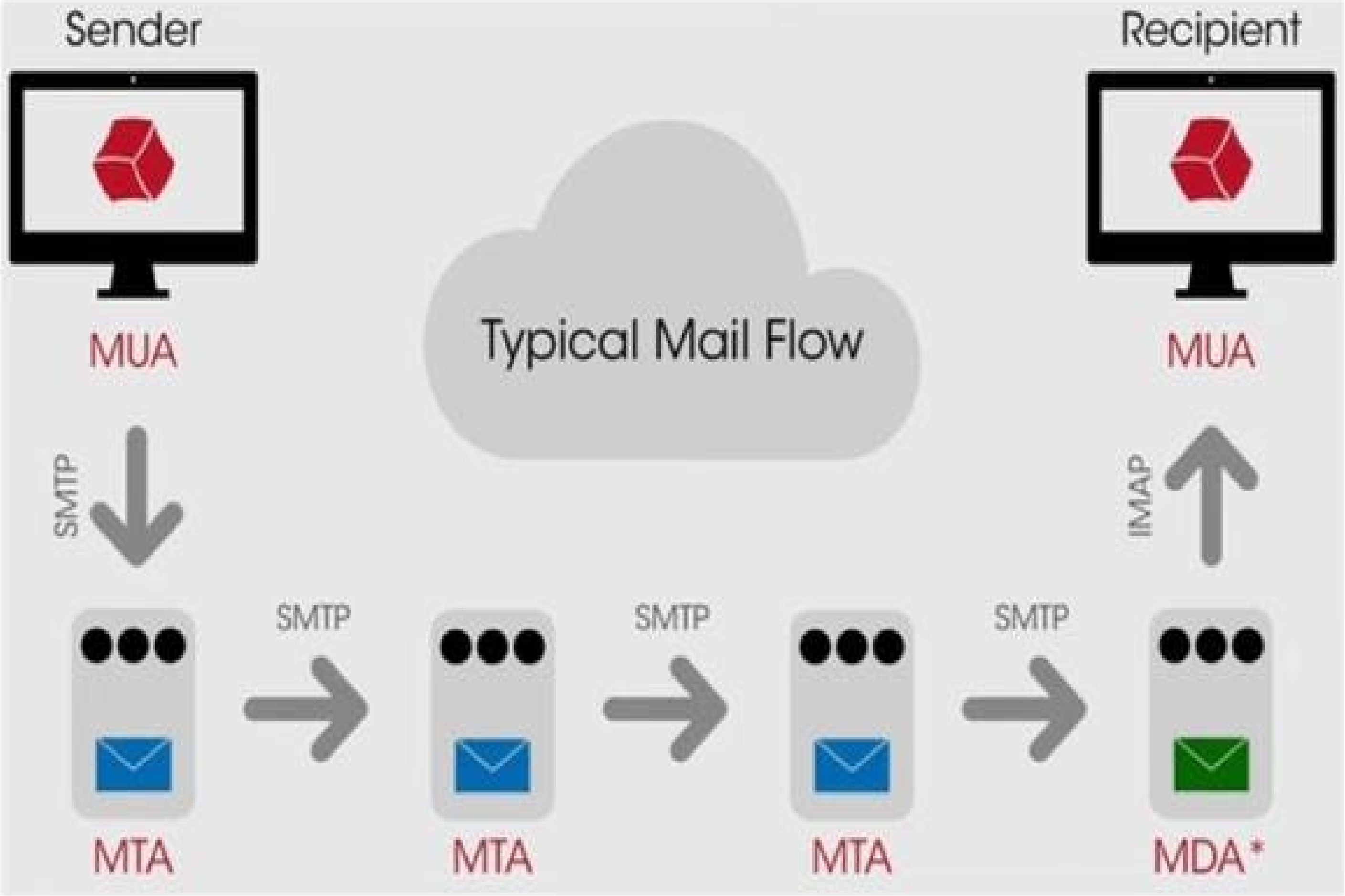
Sender Policy Framework (SPF)

Defines a mechanism by which an organization can specify server(s) that are allowed to send email on behalf of that domain. If an email fails an SPF check, it can be an easy mechanism we can use to detect spam.

DomainKeys Identified Mail (DKIM)

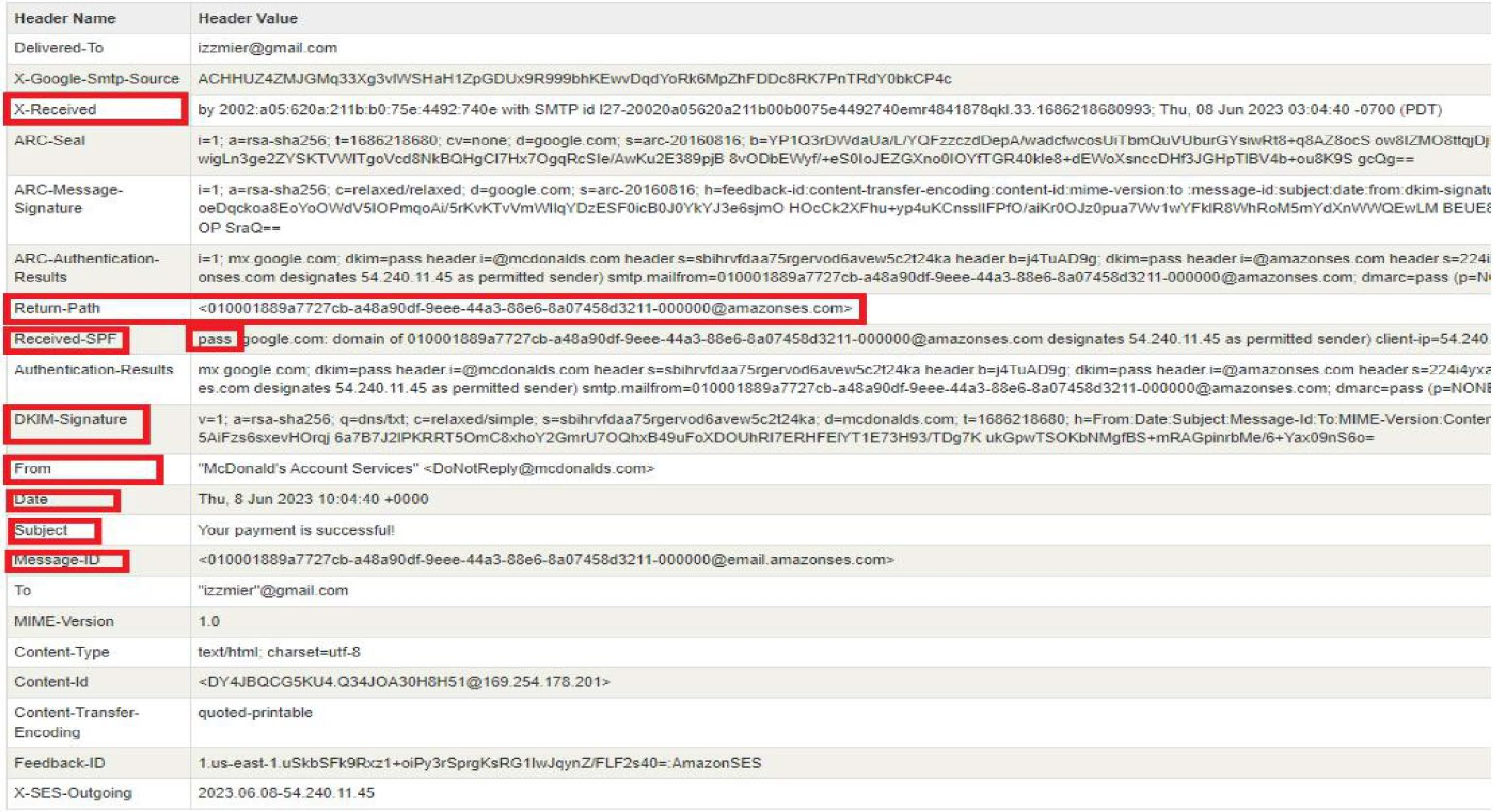
Provides a cryptographic method of verifying a received email actually originated from the sending domain. We can use this to detect forged senders and spam.

*Mail Delivery Agent responsible for final delivery of the mail to the recipient's inbox.



WHAT IS AN EMAIL HEADER?

Email headers contain tracking information for an individual email, detailing the path a message took as it went through various mail servers. The headers contain **time-stamps**, **IP addresses** and **sender/recipient** information etc.…



Header Name	Header Value
Delivered-To	izzmier@gmail.com
X-Google-Smtp-Source	ACHHUZ4ZMJGMq33Xg3vlWSHaH1ZpGDUx9R999bhKEwvDqdYoRk6MpZhFDDc8RK7PnTRdY0bkCP4c
X-Received	by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id l27-20020a05620a211b00b0075e4492740emr4841878qkl.33.1686218680993; Thu, 08 Jun 2023 03:04:40 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1686218680; cv=none; d=google.com; s=arc-20160816; b=YP1Q3rDWdaUa/L/YQFzzczdDepA/wadcfwcosUiTbmQuVUburGYsiwRt8+q8AZ8ocS ow8IZMO8ttqjDj wigLn3ge2ZYSKTVWITgoVcd8NkBQHgCI7Hx7OgqRcSle/AwKu2E389pjB 8vODbEWyf/+eS0IoJEZGXno0IOYfTGR40kle8+dEWoXsnccDHf3JGHpTIBV4b+ou8K9S gcQg==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=feedback-id:content-transfer-encoding:content-id:mime-version:to :message-id:subject:date:from:dkim-signatu oeDqckoa8EoYoOWdV5IOPmqoAi/5rKvKTvVmWIlqYDzESF0icB0J0YkYJ3e6sjmO HOcCk2XFhu+yp4uKCnssIIFPfO/aiKr0OJz0pua7Wv1wYFkIR8WhRoM5mYdXnWWQEwLM BEUE OP SraQ==
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@mcdonalds.com header.s=sbihrvfdaa75rgervod6avew5c2t24ka header.b=j4TuAD9g; dkim=pass header.i=@amazonses.com header.s=224i onses.com designates 54.240.11.45 as permitted sender) smtp.mailfrom=010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com; dmarc=pass (p=N
Return-Path	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com>
Received-SPF	pass google.com: domain of 010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com designates 54.240.11.45 as permitted sender) client-ip=54.240
Authentication-Results	mx.google.com; dkim=pass header.i=@mcdonalds.com header.s=sbihrvfdaa75rgervod6avew5c2t24ka header.b=j4TuAD9g; dkim=pass header.i=@amazonses.com header.s=224i4yxa es.com designates 54.240.11.45 as permitted sender) smtp.mailfrom=010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com; dmarc=pass (p=NON
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=sbihrvfdaa75rgervod6avew5c2t24ka; d=mcdonalds.com; t=1686218680; h=From:Date:Subject:Message-Id:To:MIME-Version:Conten 5AiFzs6sxevHOrqj 6a7B7J2IPKRRT5OmC8xhoY2GmrU7OQhxB49uFoXDOUhRI7ERHFEIYT1E73H93/TDg7K ukGpwTSOKbNMgfBS+mRAGpinrbMe/6+Yax09nS6o=
From	"McDonald's Account Services" <DoNotReply@mcdonalds.com>
Date	Thu, 8 Jun 2023 10:04:40 +0000
Subject	Your payment is successful!
Message-ID	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@email.amazonses.com>
To	"izzmier"@gmail.com
MIME-Version	1.0
Content-Type	text/html; charset=utf-8
Content-Id	<DY4JBQCG5KU4.Q34JOA30H8H51@169.254.178.201>
Content-Transfer-Encoding	quoted-printable
Feedback-ID	1.us-east-1.uSkbSFk9Rxz1+oiPy3rSprgKsRG1lwJqynZ/FLF2s40=:AmazonSES
X-SES-Outgoing	2023.06.08-54.240.11.45

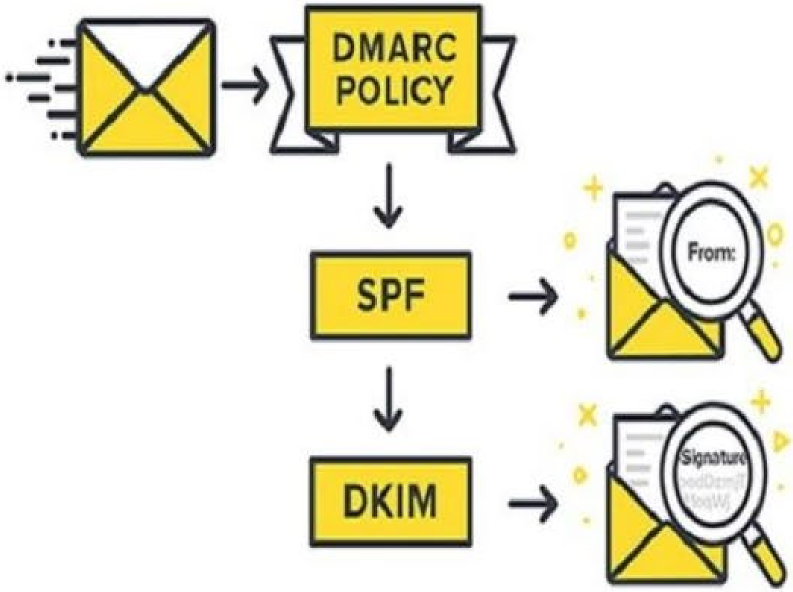
KEY ACRONYMS

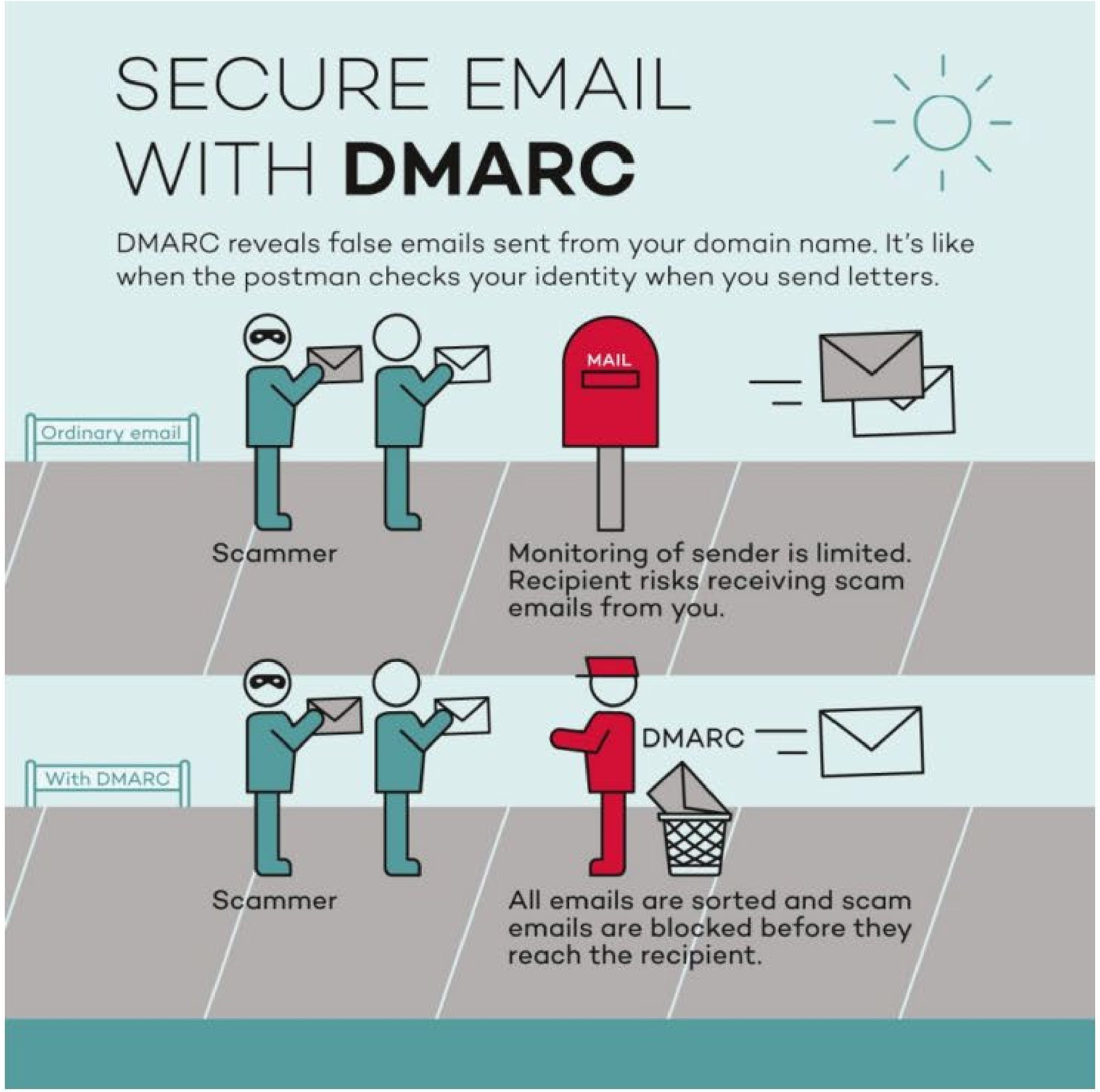
Domain-based Message Authentication, Reporting and Conformance(DMARC) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing

Sender Policy Framework (SPF) allows the receiving mail server to check during mail delivery that a mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators.

Domain Keys Identified Mail (DKIM) is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature.

ROLE OF DMARC





SECURE EMAIL WITH **DMARC**

DMARC reveals false emails sent from your domain name. It's like when the postman checks your identity when you send letters.

Monitoring of sender is limited. Recipient risks receiving scam emails from you.

All emails are sorted and scam emails are blocked before they reach the recipient.

EMAIL HEADER ANALYSIS

- Check **SPF**,**DKIM** and **DMARC**
- Find domain of sender, Ips and return path in
  - www.mxtoolbox.com
  - https://mha.azurewebsites.net

- If you see 550 **SPF** check **failed** (it means 80% this email is spoofed)

- Use **ctl+f** (windows) to find Remote (if any remote IP exist)

- Check if **Return-Path** is similar to **From:**

HOW TO VIEW HEADERS IN GMAIL

Gmail

- Log into Gmail.
- Open the message.
- Click the 3 dots next to **Reply**
- Select **Show original**.
- The full headers will appear in a new window.

HOW TO VIEW HEADERS IN YAHOO

Yahoo

- Log into Yahoo webmail.
- Open the message.
- Click on the 3 dots next to **spam** towards the top of the page.
- click on **view raw message**
- The full headers will appear on a new tab.

WHAT TO LOOK FOR WHEN ANALYZING

EMAIL HEADERS

STEPS TO ANALYZE EMAILS

1. Check the "From" Field:

Look for inconsistencies between the sender's displayed name and the actual email address.

2. Examine the "Return-Path" and "Reply-To" Fields:

Verify that the Return-Path and Reply-To fields align with the sender's information. Spoofed emails might display different addresses in these fields.

3. Inspect Email Authentication Methods:

Check for authentication methods such as SPF, DKIM, and DMARC. Absence or failure of these authentications could indicate a potential spoofing attempt.

SPF AUTHENTICATION

If SPF authentication is FAIL, it means the sender IP address is **NOT authorized** to send email on behalf of the legit domain.

IMPORTANCE OF EMAIL HEADER ANALYSIS

Spam Detection: Reveals suspicious sources or paths.

Security: Helps identify phishing or spoofed emails.

Troubleshooting: Assists in diagnosing email delivery issues.

The **Return-Path** and **From** field should be the same

EXERCISE

- challenge1.eml
- challenge2.eml
- challenge3.eml

ANSWER THE FOLLOWING QUESTIONS

What is the email subject?

Who sent the email?

Who was the email sent to?

When was the email sent?

Is DKIM, SPF, DMARC Pass or Fail?

Is the **Return-Path** similar to **From** field?

What is the email all about?

Is this email legitimate or a spam email?

ASSIGNMENT

Create an account on **TryHackMe**

https://tryhackme.com/

PHISHING EXERCISE

https://tryhackme.com/module/phishing

Task 2 → Email dates back to what time frame?

Task 3 → What port is classified as Secure Transport for SMTP?

What port is classified as Secure Transport for IMAP?

What port is classified as Secure Transport for POP3?

Task 4 → What email header is the same as "Reply-to"?

Once you find the email sender's IP address, where can you retrieve more information about the IP?

Task 5 → In the above screenshots, what is the URI of the blocked image?

In the above screenshots, what is the name of the PDF attachment?

In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data.

What is the text within the PDF?

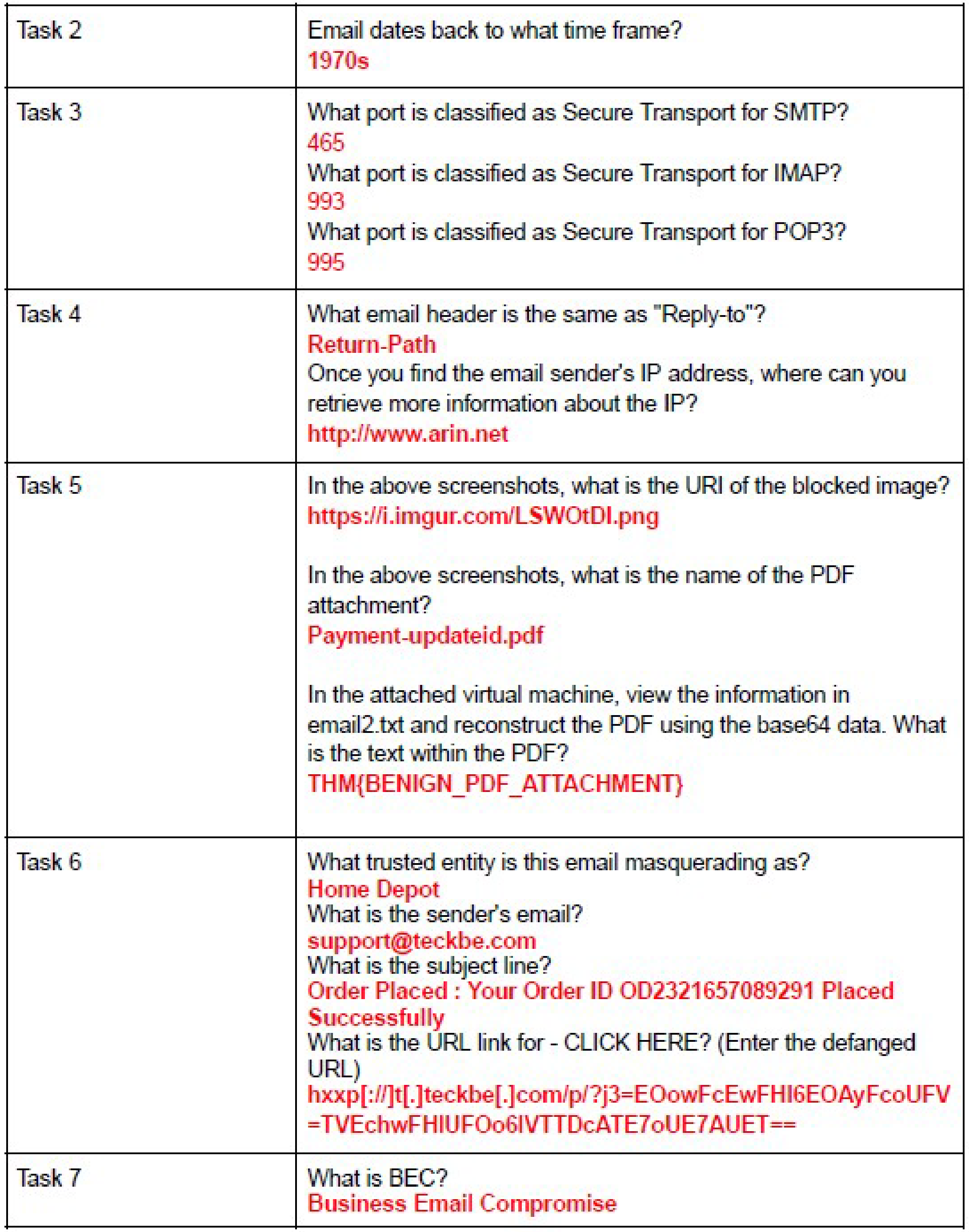
Task 6 → What trusted entity is this email masquerading as?

What is the sender's email?

What is the subject line?

What is the URL link for - CLICK HERE? (Enter the defanged URL)

Task 7 → What is BEC?



Task 2	Email dates back to what time frame? 1970s
Task 3	What port is classified as Secure Transport for SMTP? 465 What port is classified as Secure Transport for IMAP? 993 What port is classified as Secure Transport for POP3? 995
Task 4	What email header is the same as "Reply-to"? Return-Path Once you find the email sender's IP address, where can you retrieve more information about the IP? http://www.arin.net
Task 5	In the above screenshots, what is the URI of the blocked image? https://i.imgur.com/LSWOtDI.png In the above screenshots, what is the name of the PDF attachment? Payment-updateid.pdf In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data. What is the text within the PDF? THM{BENIGN_PDF_ATTACHMENT}
Task 6	What trusted entity is this email masquerading as? Home Depot What is the sender's email? support@teckbe.com What is the subject line? Order Placed : Your Order ID OD2321657089291 Placed Successfully What is the URL link for - CLICK HERE? (Enter the defanged URL) hxxp[://]t[.]teckbe[.]com/p/?j3=EOowFcEwFHI6EOAyFcoUFV=TVEchwFHIUFOo6IVTTDcATE7oUE7AUET==
Task 7	What is BEC? Business Email Compromise