

You will need:
File task1.txt on Canvas
Lab Computer

COS30015 IT Security

Lab 9 week 9

In this lab, you will engage in email forensics as your primary task. You will explore fundamental concepts such as agents, protocols, and authentication, and analyse an email formatted in MIME. This foundational knowledge will enhance your understanding of email forensics analysis. Afterward, you will be required to answer some related questions to reinforce your understanding.

Task 1 Understanding the Process of Sending and Receiving Emails

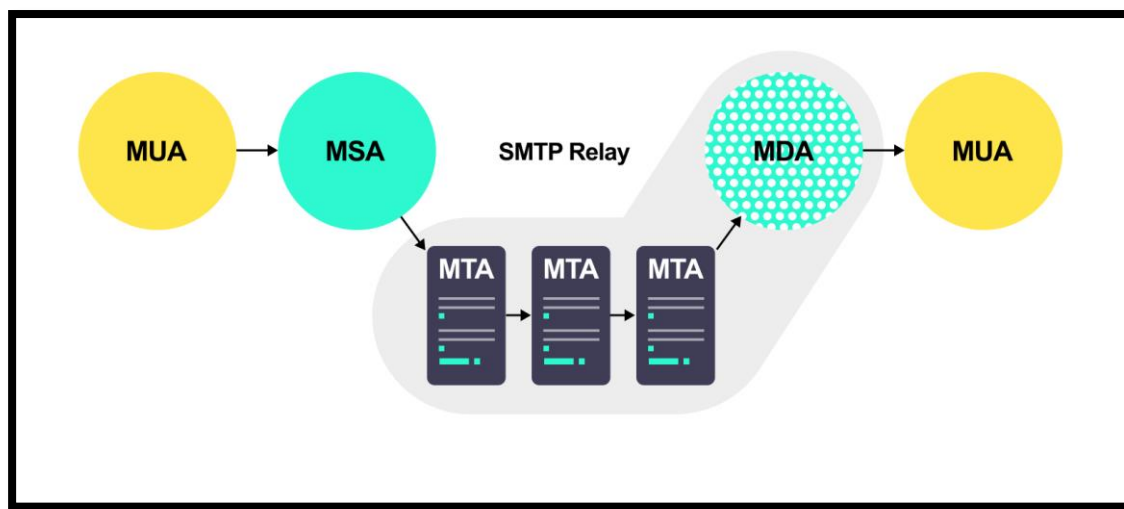


Figure 1 Process of Sending and Receiving Emails

1.1 Agent

In email transmission, an agent refers to specific software components responsible for handling and managing emails during the processes of sending, transferring, and receiving. This includes MUA, MSA, MTA, and MDA.

1. MUA

- **Concept:** MUA stands for Mail User Agent, which is a software application that enables users to send, receive, and organize email messages. Essentially, it acts as the client-side component in the email architecture, interfacing directly with end-users.
- **Key Functions:** Composing Email; Sending Email; Receiving Email; Email Organization; Address Book Management:

2. MSA

- **Concept:** MSA stands for Mail Submission Agent, which is a software application responsible for receiving outgoing email messages from the Mail User Agent (MUA) and ensuring their proper submission to the

Mail Transfer Agent (MTA) for further delivery. It acts as the intermediary between the MUA and MTA in the email architecture.

- **Key Functions:** Receiving Emails; Authentication and Authorization; Email Formatting and Compliance; Error Handling; Communication with MTA;

3. MTA

- **Concept:** MTA stands for Mail Transfer Agent, which is a software application that transfers email messages from one computer to another using the Simple Mail Transfer Protocol (SMTP). The MTA acts as the middleman between Mail User Agents (MUAs) and Mail Delivery Agents (MDAs) within the email delivery process.
- **Key Functions** Routing; Relaying; Queue Management; Policy Enforcement; Reporting;

4. MDA

- **Concept:** MDA stands for Mail Delivery Agent, a software application responsible for receiving email messages from the Mail Transfer Agent (MTA) and delivering them to the recipient's mailbox. It acts as the final step in the email delivery process, ensuring that emails reach their intended destination on the server or the user's local machine.

1.2 Protocol

In the process of email transmission, discussing key communication protocols is crucial because these protocols ensure the secure, accurate, and efficient delivery of emails from sender to recipient. Understanding how these protocols collaborate can help us design and maintain stable email systems and address common issues during transmission. Please consider the following protocols: their functions, application scenarios, and Ports:

1. **SMTP (Simple Mail Transfer Protocol)**
2. **POP3 (Post Office Protocol, Version 3)**
3. **IMAP (Internet Message Access Protocol)**
4. **ESMTP (Extended Simple Mail Transfer Protocol)**

1.3 Digital Signature

Digital Signature is an electronic signature based on cryptographic techniques used to verify the identity of the sender of a message or file and ensure that its content has not been tampered with during transmission. It is generated using the sender's private key, and the recipient uses the public key to verify the authenticity of the signature and the integrity of the data.



Think about what a PGP (Pretty Good Privacy) is and how it works

1.4 MIME (Multipurpose Internet Mail Extensions)

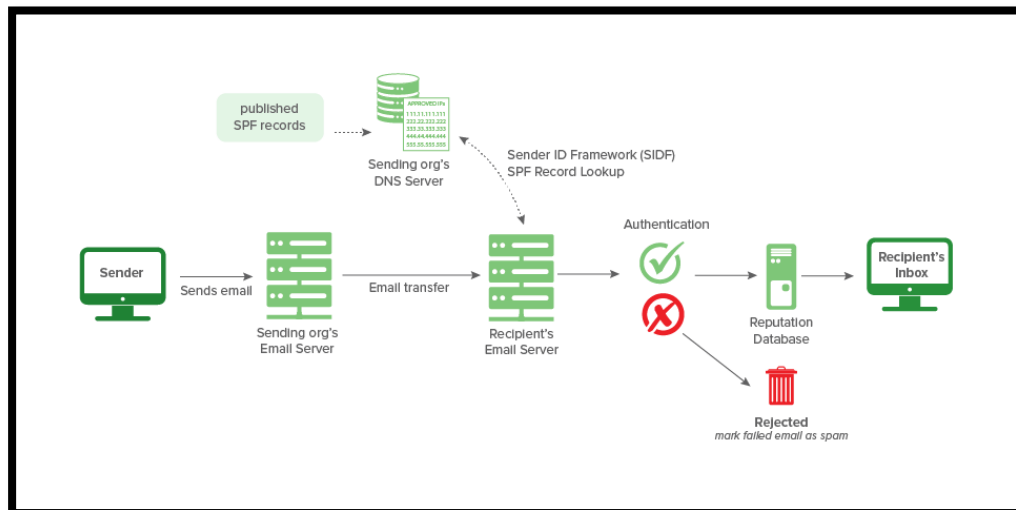
MIME (Multipurpose Internet Mail Extensions) is an internet standard that extends the functionality of email, enabling it to transmit multimedia content beyond plain text, such as images, audio, video, file attachments, and text in different character encodings. MIME adds formatting rules to email, allowing complex files and content to be transmitted via email.

1.5 Email Authentication Standards

1.5.1 SPF (Sender Policy Framework)

SPF is an email authentication mechanism used to prevent sender address forgery. It allows domain owners to specify which servers are authorized to send emails on behalf of their domain.

How SPF Works



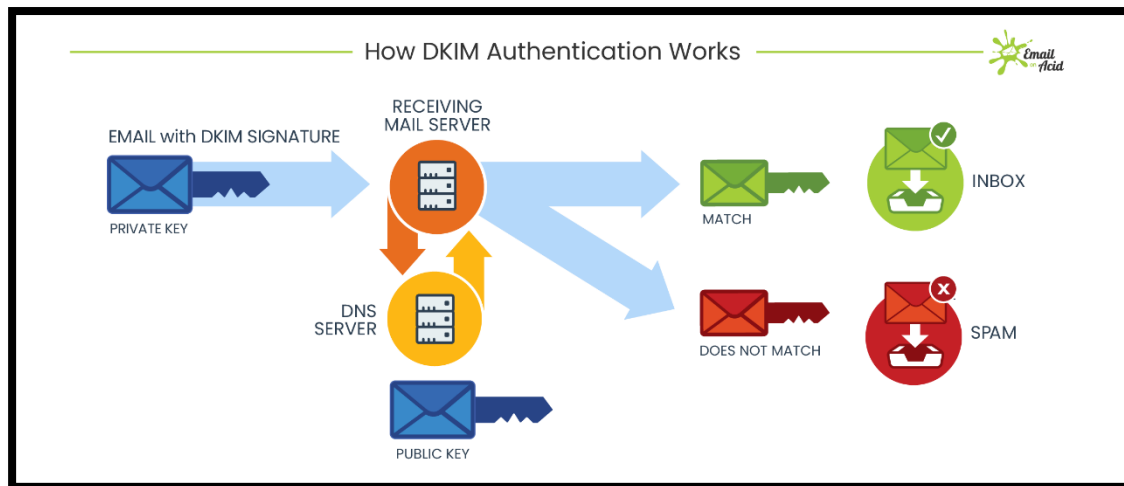
1.5.2 DKIM (DomainKeys Identified Mail)

DKIM (DomainKeys Identified Mail) is an email authentication protocol that generates a digital signature to verify the identity of an email sender. Mail providers check the DKIM signature in the email header against records published in the sender's domain name system (DNS). This process uses an encrypted key to help detect forged sender addresses. Major email providers, such as Google, Apple Mail, and Outlook, rely on DKIM signatures when authenticating emails.

? Question ?

- Consider how the hash function is used in this scenario.
- What is its role?

How DKIM Works



Task 2: Understand the basic structure of an email header.

The current task is to understand the main components of an email header to prepare for identifying potential attacks. The following exercises will focus on analysing email headers.

Open the file task1.txt from Canvas.

task1.txt is one of the logs from SpamAssassin, which includes the complete details of a processed email. Let's extract some key components to analyse their purposes.

2.1 Basic email transmission information

```
From exmh-workers-admin@redhat.com Thu Aug 22 15:15:12 2002
Return-Path: <exmh-workers-admin@example.com>
Delivered-To: zzzz@localhost.netnoteinc.com
```

Figure 2 Basic email transmission information

1. What is the purpose of the From field?

- displays the email sender's address, which is one of the most basic email header fields.
- From: exmh-workers-admin@redhat.com indicates that the email was sent by the address exmh-workers-admin@redhat.com. This field is typically used to show the recipient who the email is from.

2. What is the purpose of the Return-Path field?

- The Return-Path field, also known as the bounce path, specifies the address to which undeliverable mail should be returned. This field is typically set by the final receiving mail server after the mail transfer is complete, indicating where non-delivery reports (such as bounce messages) should be sent.
- Return-Path: `exmh-workers-admin@example.com` indicates that any delivery issues related to this email will be sent to `exmh-workers-admin@example.com`.

3. What is the purpose of the Delivered-To field?

- The Delivered-To field indicates the final delivery address of the email, specifying which mailbox the email ultimately reached. This field helps track the last-hop delivery information, especially when the email has been processed through forwarding or mailing list servers.
- Delivered-To: `zzzz@localhost.netnoteinc.com` shows that the email was delivered to the address `zzzz@localhost.netnoteinc.com`. header, Return-Path: `exmh-workers-admin@example.com` indicates that any delivery issues related to this email will be sent to `exmh-workers-admin@example.com`.

2.2 Received Field

```
Received: from localhost (localhost [127.0.0.1])
  by phobos.labs.netnoteinc.com (Postfix) with ESMTP id 1AD7B43F99
  for <zzzz@localhost>; Thu, 22 Aug 2002 10:15:11 -0400 (EDT)
Received: from phobos [127.0.0.1]
  by localhost with IMAP (fetchmail-5.9.0)
  for zzzz@localhost (single-drop); Thu, 22 Aug 2002 15:15:12 +0100 (IST)
Received: from listman.example.com (listman.example.com [66.187.233.211]) by
  dogma.slashnull.org (8.11.6/8.11.6) with ESMTP id g7MECrZ09674 for
  <zzzz-exmh@example.com>; Thu, 22 Aug 2002 15:12:54 +0100
Received: from listman.example.com (localhost.localdomain [127.0.0.1]) by
  listman.redhat.com (Postfix) with ESMTP id C57DA3ECC9; Thu, 22 Aug 2002
  10:13:02 -0400 (EDT)
Delivered-To: exmh-workers@listman.example.com
Received: from int-mx1.corp.example.com (int-mx1.corp.example.com
  [172.16.52.254]) by listman.redhat.com (Postfix) with ESMTP id 6854840C75
  for <exmh-workers@listman.redhat.com>; Thu, 22 Aug 2002 10:12:27 -0400
  (EDT)
Received: (from mail@localhost) by int-mx1.corp.example.com (8.11.6/8.11.6)
  id g7MECOK08343 for exmh-workers@listman.redhat.com; Thu, 22 Aug 2002
  10:12:24 -0400
Received: from mx1.example.com (mx1.example.com [172.16.48.31]) by
  int-mx1.corp.redhat.com (8.11.6/8.11.6) with SMTP id g7MECOY08339 for
  <exmh-workers@redhat.com>; Thu, 22 Aug 2002 10:12:24 -0400
```

Figure 3 Basic email transmission information

1. What is the purpose of the Received field?

Received Headers: This section records the path of the servers the email has passed through. The email has gone through multiple servers in succession, such as localhost.netnoteinc.com, listman.example.com, and mx1.example.com, each with a timestamp showing the various stages of the email's transmission.

Breakdown explanation

```
Received: from listman.example.com (listman.example.com [66.187.233.211])  
by dogma.slashnull.org (8.11.6/8.11.6) with ESMTP id g7MECrZ09674 for  
<zzzz-exmh@example.com>; Thu, 22 Aug 2002 15:12:54 +0100
```

Figure 4 Basic email transmission information

1. What does the part "from listman.example.com (listman.example.com [66.187.233.211])" indicate about the origin of the email?

Answer: It indicates that the email was sent from the server named listman.example.com, which has an IP address of 66.187.233.211. Typically, the hostname and corresponding IP address are displayed in parentheses after DNS resolution.

2. Receiving Server: What does "by dogma.slashnull.org (8.11.6/8.11.6)" tell us about the server that received the email and the software it is running?

Answer: It shows that the email was received by the server named dogma.slashnull.org, and the version numbers 8.11.6/8.11.6 indicate the version of the Mail Transfer Agent (MTA) software (likely Sendmail) running on that server.

3. Transmission Protocol: What does "with ESMTP" signify regarding the protocol used for receiving the email?

Answer: It signifies that the email was received using the Extended Simple Mail Transfer Protocol (ESMTP), which is an extension of SMTP that supports more commands and features.

4. **Transaction ID:** How is the "id g7MECrZ09674" utilized in tracking the email?

Answer: The ID "g7MECrZ09674" is a unique identifier generated during the email's processing on the dogma.slashnull.org server, useful for tracking the status of the email and debugging transmission issues.

5. **Receiving Recipient:** What is the significance of "for zzzz-exmh@example.com" in the email header?

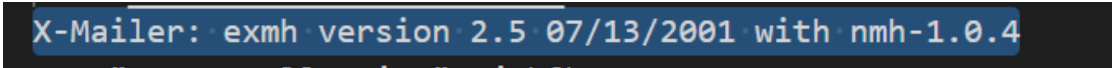
Answer: It specifies the final or intermediate mailbox address to which the email was sent

6. **Receiving Time:** What information does "Thu, 22 Aug 2002 15:12:54 +0100" provide about the timing of the email's receipt?

Answer: It indicates the specific date and time when the email was received by the server, based on the GMT/UTC+1 time zone.

? Question: what PGP is, what the web of trust is and what its purpose is? ?

2.3 X-Mailer

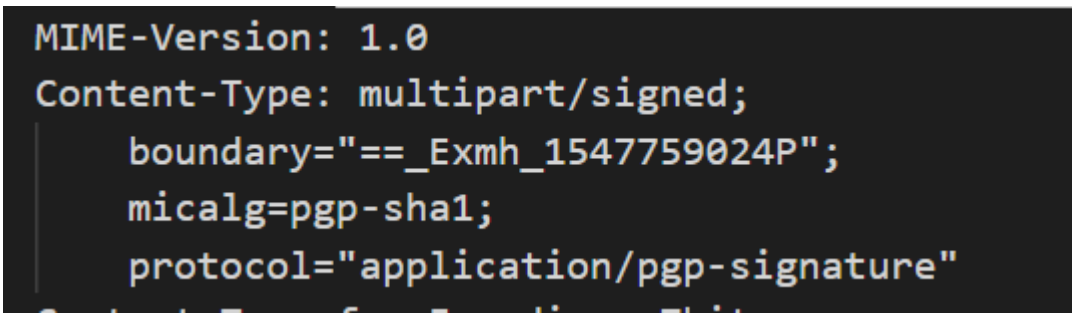


```
X-Mailer: exmh version 2.5 07/13/2001 with nmh-1.0.4
```

Figure 5 X-Mailer

Answer: This indicates that the email was created and sent using exmh version 2.5 and nmh-1.0.4.

2.4 Email Content Type & Encoding



```
MIME-Version: 1.0
Content-Type: multipart/signed;
    boundary=="_Exmh_1547759024P";
    micalg=pgp-sha1;
    protocol="application/pgp-signature"
```

Figure 6 Email Content Type & Encoding

1. What does "MIME-Version: 1.0" indicate about the email?

It indicates that the email follows the MIME 1.0 standard, allowing it to include non-text content, such as attachments.

2. What does "Content-Type: multipart/signed" signify regarding the email's content?

Answer: It signifies that the email content consists of multiple parts and includes a digital signature to verify the email's integrity.

3. What is the purpose of the digital signature protocol "application/pgp-signature"?

Answer: The application/pgp-signature protocol is used for PGP encryption signatures, ensuring the authenticity and security of the email content.

? Question: what PGP is, what the web of trust is and what its purpose is? ?

2.5 Email Body

To efficiently locate the body section in a MIME message, one can examine the **Content-Type header**, where the charset parameter may have various values, such as us-ascii or 'UTF-8,' as illustrated in Figure 7. Alternatively, **the original message can be highlighted**, as demonstrated in Figure 8.

```
--=_Exmh_1547759024P
Content-Type: text/plain; charset=us-ascii

> From: "J. W. Ballantine" <jwb@homer.att.com>
> Date: Wed, 21 Aug 2002 09:51:31 -0400
>
> I CVS'ed the unseen/Sequences changes and installed them, and have only one
> real issue.
>
> I use the unseen window rather than the exmh icon, and with the new code
> I can't seem to be able to. How many unseen when I have the main window open
> is not really necessary.

hmmm, I stole the code from unseenwin, but I never tested it since I don't use
that functionality. Consider it on my list of things to check.

Chris
```

Figure 7 Email Body


```
> -----Original Message-----
> From: Kiall Mac Innes [mailto:kiall@redpie.com]
> Sent: 22 August 2002 17:23
> To: ILUG
> Subject: [ILUG] Sun Solaris..
>
>
> Can someone explain what type of operating system Solaris
> is... as ive never seen or used it i dont know wheather to
> get a server from Sun or from DELL i would prefer a linux
> based server and Sun seems to be the one for that but im not
> sure if Solaris is a distro of linux or a completely
> different operating system? can someone explain...
>
> Kiall Mac Innes
>
>
> --
> Irish Linux Users' Group: ilug@linux.ie
> http://www.linux.ie/mailman/listinfo/ilug for
> (un)subscription information. List maintainer: listmaster@linux.ie
>
```

Figure 8 Email Body (come from record 0022.7241da4491c49b50c0470a3638ee35c4)

2.6 Digital Signature

At the end of the email, there is a PGP signature included, which is used to verify the sender's identity and ensure that the email content has not been altered during transmission.

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: Exmh version 2.2_20000822 06/23/2000

iD8DBQE9ZPFAK9b4h5R0IUIRAKjyAJ4jjjhAVRx5FiwuCMa+QBWsbbE2jQCaAj4x
NhIgYqnx9/1wvdSgesQhMIU=
=vA3k
-----END PGP SIGNATURE-----
```

Figure 9 Digital Signature

Name: _____ Student ID: _____

Practice1: Map out the journey of the email from sender to recipient

After reviewing the details of the email header in the MIME format, please answer the following three questions based on Figure 10.

```
Received: from mail.example.com (example.com. [192.0.2.1])
    by mx.google.com with ESMTPS id d1234567890abcde.2023.01.01.08.00.00
    for <example@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
    Sun, 01 Jan 2023 08:15:00 -0800 (PST)
Received: from [10.0.0.1] (unknown [203.0.113.1])
    by mail.example.com (Postfix) with ESMTP id 123456789AB
    for <example@example.com>; Sun, 01 Jan 2023 08:00:00 -0800 (PST)
From: sender@example.com
To: example@gmail.com
Subject: Important Update
Date: Sun, 01 Jan 2023 08:00:00 -0800 (PST)
```

Figure 10 Practice for mapping

Q1: What is the IP address of the original sender?

The original sender's IP address is 203.0.113.1.

Q2: Which servers (IP addresses) did the email pass through?

The email passed through the following servers:

- 203.0.113.1 (sender's computer or local server)
- 192.0.2.1 (mail.example.com, the intermediate relay server)
- mx.google.com (final recipient server)

Q3: What can you deduce about the timing of the email's journey?

The email was sent from the sender at 08:00:00 and was received by the final server at 08:15:00. The total time for email transmission was 15 minutes, indicating a typical delay in email processing and delivery.

Practice2: Map out the journey of the email from sender to recipient

After reviewing the details of the email header in the MIME format, please answer the following three questions based on Figure 11.

```
From: sender@example.com
To: recipient@example.com
Subject: Sample Email
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="XYZ123"

--XYZ123
Content-Type: text/plain; charset="UTF-8"

Hello,
This is a sample email in plain text format.
Thank you!

--XYZ123
Content-Type: text/html; charset="UTF-8"

<html>
<body>
<p>Hello,</p>
<p>This is a sample <strong>email</strong> in HTML format.</p>
<p>Thank you!</p>
</body>
</html>

--XYZ123--
```

Figure 11 Example of Email Data

Analysis Steps:

- Look for the Content-Type header and find the boundary identifier boundary="XYZ123".
- Use this boundary identifier to search within the email content and locate the first instance—XYZ123.
- Examine the Content-Type declaration of each part to determine the content type, such as text/plain or text/html.

Q1: What is the content of the plain text version of the email?

*Hello,
This is a sample email in plain text format.
Thank you!*

Q2: How does the email client decide which part of the email to display?

Answer: Email clients that support HTML will typically display the HTML part of a "multipart/alternative" email because it is listed last and considered the most fully featured version. Clients that do not support HTML or are configured to prefer plain text will display the plain text part. The order of the parts in a "multipart/alternative" MIME structure can influence which version is shown by default in clients that support both formats

Note: Including a plain text version alongside an HTML version offers several benefits

- Accessibility: Some users might have email clients that can only display plain text, or they may use screen readers that handle plain text better than HTML.
- Deliverability: Emails that include a plain text version alongside HTML are less likely to be flagged as spam by email servers, improving deliverability.
- Preference: Some users prefer the simplicity of plain text emails, either for ease of reading or due to bandwidth concerns.

Practice3: Authentication Verification Task

Verifying the authentication mechanisms used in the email, such as SPF, DKIM, and DMARC records in the header. Have them evaluate whether the email could be considered authentic or spoofed based on these records. Answer the following five questions based on Figure 12.

```
From: user@example.com
To: recipient@example.net
Subject: Test Email
Date: Mon, 26 Oct 2020 14:22:15 +0200
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8

Received: from mail.example.com (mail.example.com. [192.0.2.1])
  by mx.google.com with ESMTPS id 123456789abcdef.2020.10.26.05.22.15
  for <recipient@example.net>
  (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
  Mon, 26 Oct 2020 05:22:15 -0700 (PDT)
Received-SPF: pass (google.com: domain of user@example.com designates 192.0.2.1 as permitted sender) client-ip=192.0.2.1;
Authentication-Results: mx.google.com;
  dkim=pass header.i@example.com;
  spf=pass (google.com: domain of user@example.com designates 192.0.2.1 as permitted sender) smtp.mailfrom=user@example.com;
  dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=example.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=example.com; s=selector; h=from:to:date:subject;
  bh=fRC7YPZ6fgt3oL8kpI+Jqpt1P6lSaeghpqlq4Uld1QM=;
  b=XYZABC123456789/QWERTYUIOPASDFGHJKLZXCVBNM=

Hello,

This is a test email to demonstrate SPF, DKIM, and DMARC verification.
```

Figure 12 Example of Email Data

Q1: What does the email's SPF record indicate?

Answer: Received-SPF: pass indicates that the sending server (IP address 192.0.2.1) is authorized by the email's sending domain (example.com) to send emails. This suggests that the email sender is verified.

Name: _____ Student ID: _____

Q2: What is the result of the DKIM verification?

dkim=pass signifies that the DKIM signature validation was successful, indicating that the content of the email has not been altered since it was signed, maintaining the integrity of the email header.

Q3: What does the DMARC record verification indicate?

dmarc=pass shows that the email complies with the sending domain's DMARC policy, increasing the likelihood that the email is not forged.

Q4: How can discrepancies in SPF and DKIM records affect email deliverability?

Discrepancies in SPF and DKIM records can lead to emails being flagged as spam or rejected by receiving email servers. Consistency and correct configuration are crucial for ensuring email deliverability and trust.

Q5: Why might an organization choose a DMARC policy of p=NONE?

Answer: An organization might choose a DMARC policy of p=NONE for monitoring and data collection purposes without enforcing action on emails that fail DMARC checks. This allows them to understand how their emails

Task 2: Body Content Analysis Task

The current task is to analyse the body of the email to identify potential phishing attack tactics. This involves examining the language used, looking for suspicious links or requests, and assessing any unusual formatting or content that could indicate a phishing attempt. By understanding these tactics, we can better protect ourselves against malicious emails.

Question

Q1: What phishing emails are?

Phishing emails are crafted to appear as though they come from legitimate sources, such as a well-known company, a bank, or a trusted individual. Their goal is to trick recipients into providing sensitive data such as usernames, passwords, credit card information, or other personal details. Phishing attacks might direct the recipient to a fake website that looks nearly identical to a legitimate one, where they are prompted to enter their information.

Q2: What the common tactics used in phishing email attacks

Red Flags to Watch Out For

1. Inconsistencies in Email Addresses, Links, and Domain Names:

2. Unsolicited Requests for Sensitive Information:

3. Mismatched URLs:

4. Poorly Written Email Content

Look out for poor grammar and spelling as these are professional businesses' emails and are usually well-composed. Many phishing emails originate overseas and are composed by non-native speakers.

5. Unusual Sender

If an email comes from someone in your contact list but has an unusual tone or does not seem like something they would typically send, be cautious. Verify through other means that they sent the email.

6. Attachments with Strange File Types

Name: _____ Student ID: _____

Practice4: Phishing Email Red Flags Identify

Please answer the questions based on the following fake phishing email:

Subject: **Urgent: Unauthorized Access Detected!**

From: **Security Team** supp0rt@apple.com

Date: **October 5, 2024**

Dear Customer,

We detected unusual activity in your Apple account from an unrecognized device on October 4, 2024. For your protection, your account has been temporarily locked. You must verify your identity within 24 hours to avoid permanent suspension.

Please visit the link below to verify your account: [Verify My Account](#)

Thank you for taking immediate action.

Best Regards,

Apple Security Team

Q1: What are the issues with the sender's email address in this email? [Analyze the Sender's Email Address]

Character Substitution: The email address uses a common phishing tactic known as character substitution or homoglyph attacks. In this case, the number '0' (zero) is used to replace the letter 'o' in the word "support." The use of similar-looking characters makes the email address visually resemble a trusted source (in this case, an email that might come from Apple's actual support team). However, this slight alteration creates a completely different email address that is controlled by the attacker.

Q2: How does the language used in the email influence the recipient's actions? [Evaluate the Urgency and Language Used]

Answer: The email uses urgent language encouraging immediate action, which is a common tactic in phishing to pressure the recipient into acting without thinking critically about the legitimacy of the email.

- *We detected unusual activity in your Apple account from an unrecognized device.*
- *By adding, "your account has been temporarily locked," the email introduces a problem that requires swift resolution*
- *"You must verify your identity within 24 hours to avoid permanent suspension," sets a specific time limit*
- *Please visit the link below to verify your account," directly calls for immediate action*

Q3: What can you find out about the link included in the email? [Inspect the Link]

Hovering over the link (without clicking) should reveal that it directs to "http://apple-verify-login.com," which is not a secure (https) or official Apple domain, indicating that it's likely a phishing site.

Q4: What can be said about the way the email addresses the recipient? [Look for Generic Greetings]

Answer: The email uses a generic greeting ("Dear Customer"), which is not personalized. Legitimate communications from companies with whom you have an account typically use your first name or full name.

Q4: Does this email request any personal information directly? [Request for Personal Information]

Answer: While the email itself does not directly ask for personal information, it indirectly does by luring the recipient to a fake website through the link, where personal information is likely requested.