Email Networks and Security

Cybersecurity

Networking 2, Day 2

9.2: Network 2 - Email Networks & Security

Class Preparation

1. Check into BCS
2. Update your git repository with `` `git pull` ``
3. Launch and login to your Ubuntu VM
   - You do not need to update VirtualBox if prompted

Homeworks Due

- Unit 7 (Windows): due last night
- Unit 8 (Networking): due Sunday November 22
- Unit 9 (Networking 2): due Sunday November 29
- Homework Make Up: due Sunday November 29

Upcoming Units

- Week 10: Network Security (11/23 - 12/02)
- Week 11: Cloud Sec. & Virtualization (12/05 - 12/12)
- Week 12: Project Week (12/14 - 12/19)

Schedule Notes

Thanksgiving Break - No Class

- Off: Wed 11/25 & Sat 11/28
- Return on Monday 11/30

Project 1 (Individual; Required)

- Mon 12/14 - Sat 12/19

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

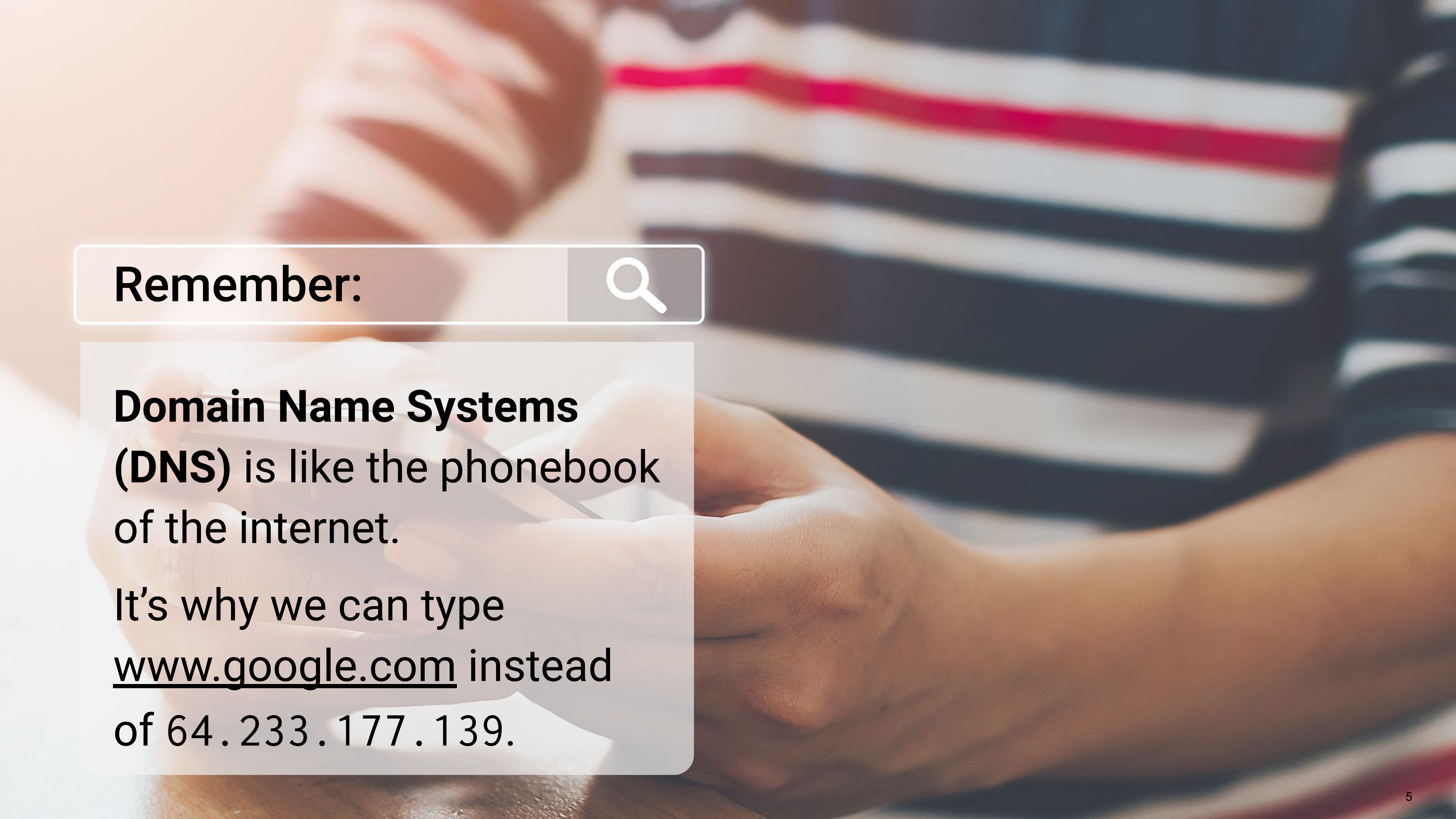
- Crypto delayed until after Winter Break

Class Objectives

By the end of today's class, you will be able to:

- Validate DNS records using `nslookup`.
- Describe the processes, protocols, and headers associated with email communication.
- Analyze email headers to identify suspicious content.

DNS Record Types



Remember:

Domain Name Systems (DNS) is like the phonebook of the internet.

It’s why we can type www.google.com instead of `64.233.177.139`.

Domain-to-IP-address is just one type of DNS translation.

DNS Record Types

DNS provides many details about a domain.

For example:

- When you send an email to **IT@acmecorp.com**, your server must find the mail server name (**mailhost.acmecorp.com**) for the domain receiving the email.
- The server checks that the mail record for **acmecorp.com** is **mailhost.acmecorp.com**.

DNS Zone File

All the records for a particular domain are stored in a file called the DNS zone file.

01

A DNS zone file lives in a DNS server.

02

DNS zone files contain a Time to Live (TTL), indicating how long a DNS cache will remember information in the file before having to request an updated copy.

03

DNS zone files also contain the DNS records with information about the domain.

DNS Record Types

Some common DNS record types include:

A Record: Translates a domain to an IP address. (widgets.com → `23.43.54.234`)

PTR Record: Translates an IP address to a domain. (`23.43.54.234` → widgets.com)

CNAME (canonical name) Record: An alias record used to point one domain to another domain. (widgets2.com → widgets.com)

SOA (state of authority) Record: Contains administrative details about a domain, such as the email of the administrator, TTL value, and time of last update.

NS (name server) Record: Indicates which server contains actual DNS records for a domain.

There are also DNS record types that assist with email communication.

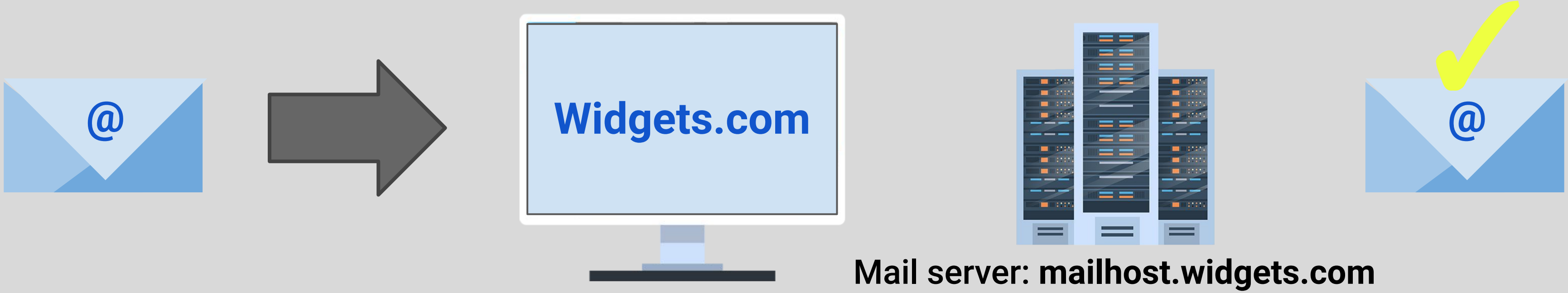
MX (Mail Exchange) Record

MX records directs emails to a specific mail server for a domain.

widgets.com has a mail server called **mailhost.widgets.com**.

If an email is sent to bob@widgets.com, the sender validates that the MX record for widgets.com is **mailhost.widgets.com**.

The sender directs the email to the mail server **mailhost.widget.com**.



Mail server: mailhost.widgets.com

MX Record

Just like NS Records, domains can have multiple MX records in case one goes down or can't handle all the traffic.

- Preference numbers set the primary and secondary mail servers.
- For example: gadgets.com has the following MX records:
    - `10 mailhost_Atlanta.gadgets.com`
    - `5 mailhost_NewYork.gadgets.com`
    - `20 mailhost_LA.gadgets.com`

Emails sent to gadgets.com are first received by New York (5). If NY is down, Atlanta (10) will be tried next. If Atlanta is down, LA (20).

TXT (Text) Record

TXT Records are used to include notes related to the DNS.

- Some notes are human-readable, such as the associated company name.
- Other notes are read by the computer, such as the SPF (Sender Policy Framework), which determines if an email is from a trusted server.

SPF Record

Organizations might send emails from mail servers outside their domain.

- Mail servers may exist in another domain, and outside companies often send marketing emails on behalf of an organization.
- An SPF record indicates mail servers that can send emails on behalf of a domain to prevent spam, phishing, and email spoofing, by detecting emails that may have a forged sender email.

Example of an SPF record: `v=spf1 ip4:192.41.100.193`

- `v=` is the version of SPF used.
- `ip4`: indicates a IPv4 host is allowed to send emails.
- `192.41.100.193` is the IP allowed to send emails on behalf of the domain.

How SPF Works

widgets.com’s DNS SPF record indicates that `23.43.54.235` and `23.43.54.236` are the IP addresses of mail servers allowed to send emails on its behalf.

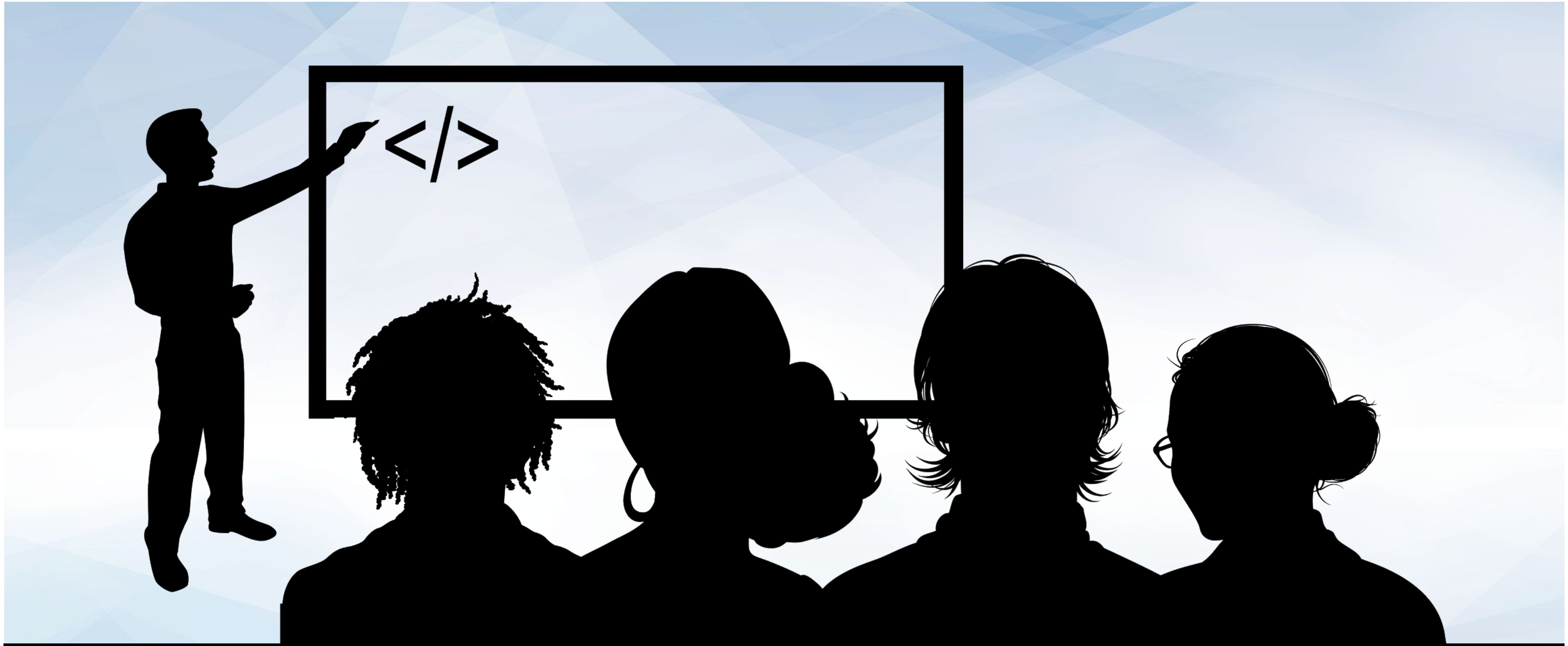
- gadgets.com receives a suspicious email from a widgets.com email.
- When the receiving email server at gadgets.com receives the email, it:
  a. Checks the sending mail server's IP address, which is `12.54.54.23`.
  b. Validates the DNS record of widget.com’s SPF record to confirm the sending mail server's IP address is either `23.43.54.235` or `23.43.54.236`.

The sender’s IP is `12.54.54.23`, not `23.43.54.235` or `23.43.54.236`. gadgets.com’s mail server can identify the email as spam and reject or send it to the spam folder.

nslookup

If emails are not reaching their final destination, we need to check that the MX DNS record for that particular domain is accurate.

- **`nslookup`** (name server lookup) is a command-line tool that allows us to easily look up the DNS records of any domain.



Instructor Demonstration

nslookup

Activity: DNS Record Types

In this activity, you will continue to play the role of a security analyst for Acme Corp.

Acme Corp recently updated several domain DNS records. Your task is to use `nslookup` to validate the updates of the DNS records for each of the domains provided.

Suggested Time:
10 minutes

Introduction to Email Networking

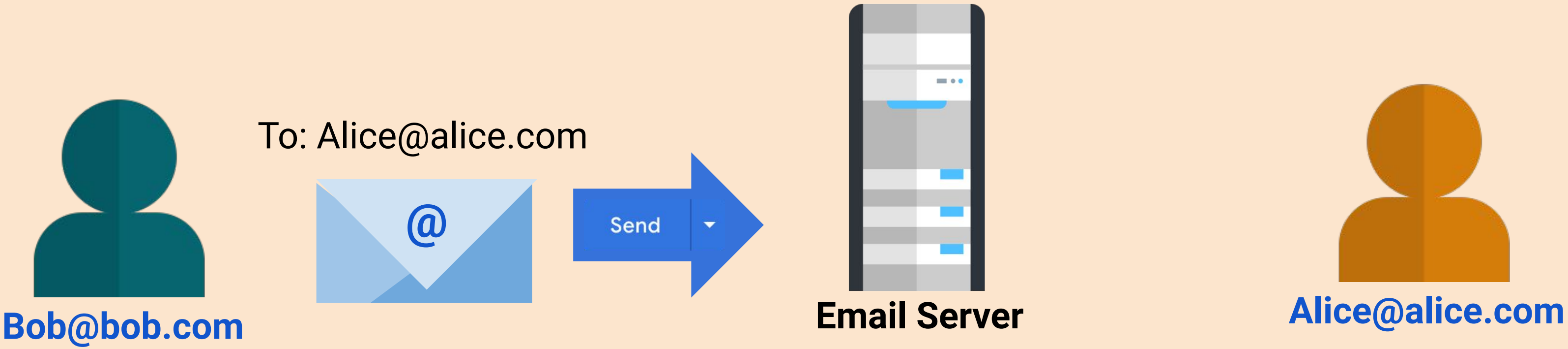
An understanding of the processes and technologies involved in sending emails is key for security professionals, who have to manage email issues or attacks.

How Emails are Sent

How Emails Work

Step 1: Bob uses Microsoft Outlook to type and send an email to Alice.

- Bob**, bob@bob.com**, composes an email to Alice, at **alice@alice.com**.
- Once Bob clicks **Send**, the email is forwarded to Bob’s company’s email server.
- The email server is also referred to as the MTA (mail transfer agent).



To: Alice@alice.com

Bob@bob.com

Email Server

Alice@alice.com

How Emails Work

Step 2: Bob’s mail server finds Alice’s mail server.

- Bob's mail server does a DNS lookup against **alice.com** to determine its mail server.
- Bob's mail server gets this information from **alice.com**'s MX record.

Bob@bob.com

Email Server

Looking for alice.com

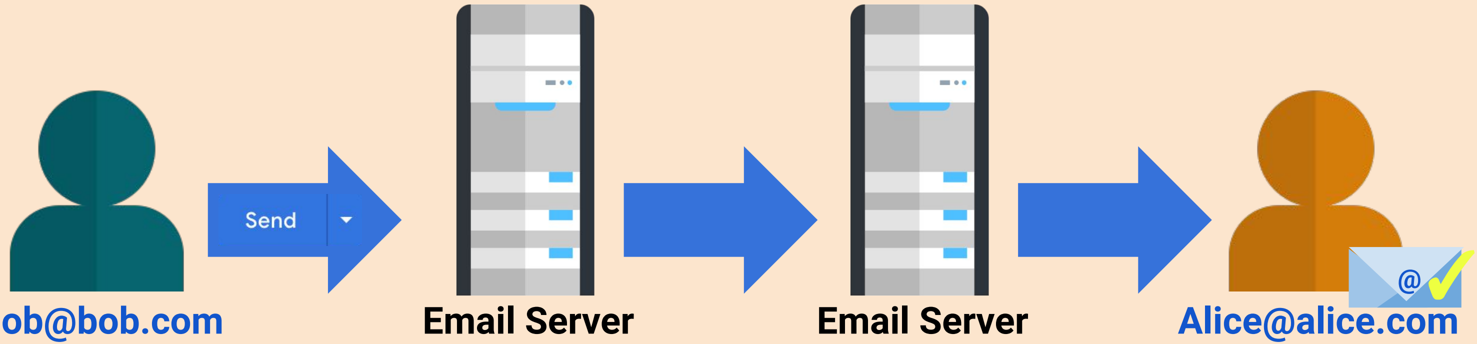
Alice@alice.com

How Emails Work

Step 3: Bob's mail server forwards the email to Alice’s mail server.

- Using SMTP (Simple Mail Transfer), Bob’s mail server sends the email to Alice’s mail server.

- SMTP uses port 25 and is part of Layer 7: Application of the OSI model.
  Secure SMTP (SMTP with TLS) uses port 465 (or sometimes 587)



How Emails Work

Two Layer 7 protocols can be used to access the email to Alice's local computer.

Step 4: Alice pulls Bob's email onto her local computer to read it.

POP3 (Post Office Protocol)

- When Alice logs in and checks her email from Bob, the POP3 mailbox doesn't keep a copy of the email.
- Alice would not be able to log into another computer to view Bob's email, as it already has been downloaded from the mail server.
- POP3 has a security benefit, as the email will not exist on a server the recipient doesn't control.
- Port 110 (Secure = 995)

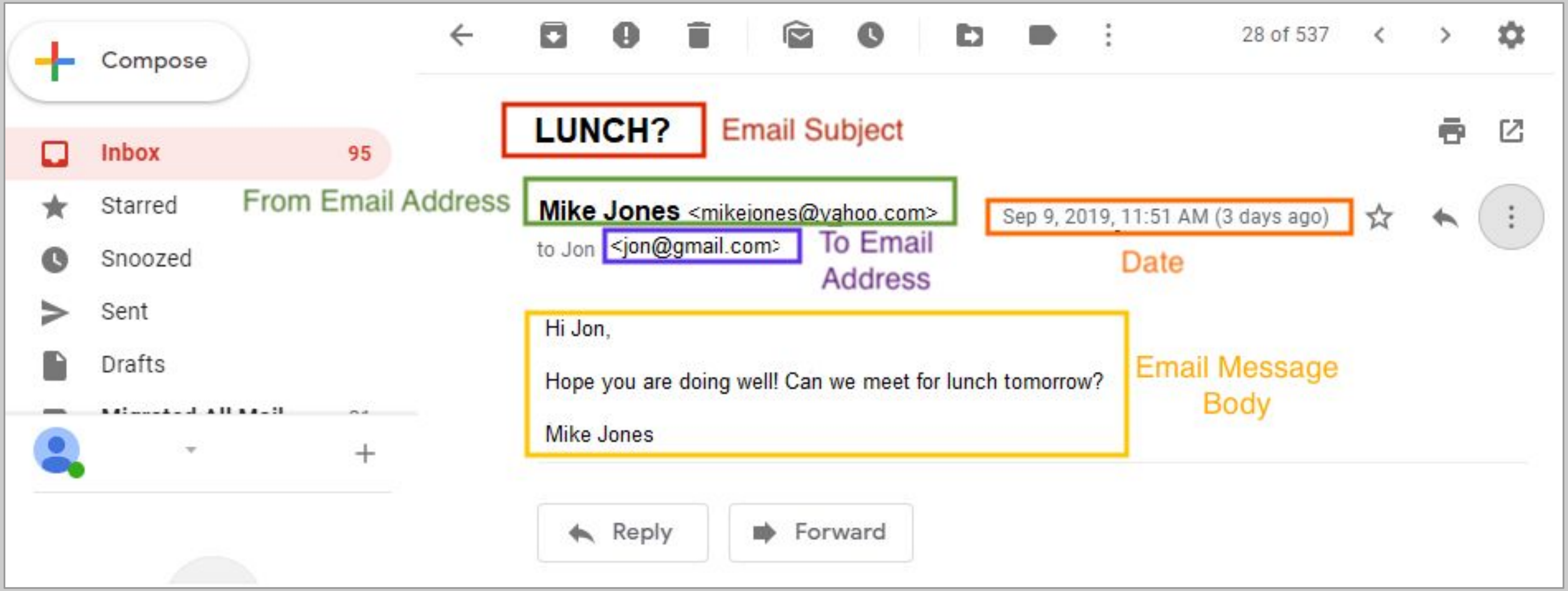
IMAP (Internet Message Access Protocol)

- A copy of the email is kept on the server.
- Even after Alice logs in and check her email from Bob, she can check it again from another computer.
- IMAP has the benefit of preventing data from being lost, as it backs up emails on a server.
- Port 143 (Secure = 993)

To complete the previous steps, emails use headers made up of specific fields.

Familiar Fields

If you've ever sent an email, you're probably familiar with the following fields:



LUNCH?

Email Subject

Mike Jones <mikejones@yahoo.com>

From Email Address

to Jon <jon@gmail.com>

To Email Address

Sep 9, 2019, 11:51 AM (3 days ago)

Date

Hi Jon,

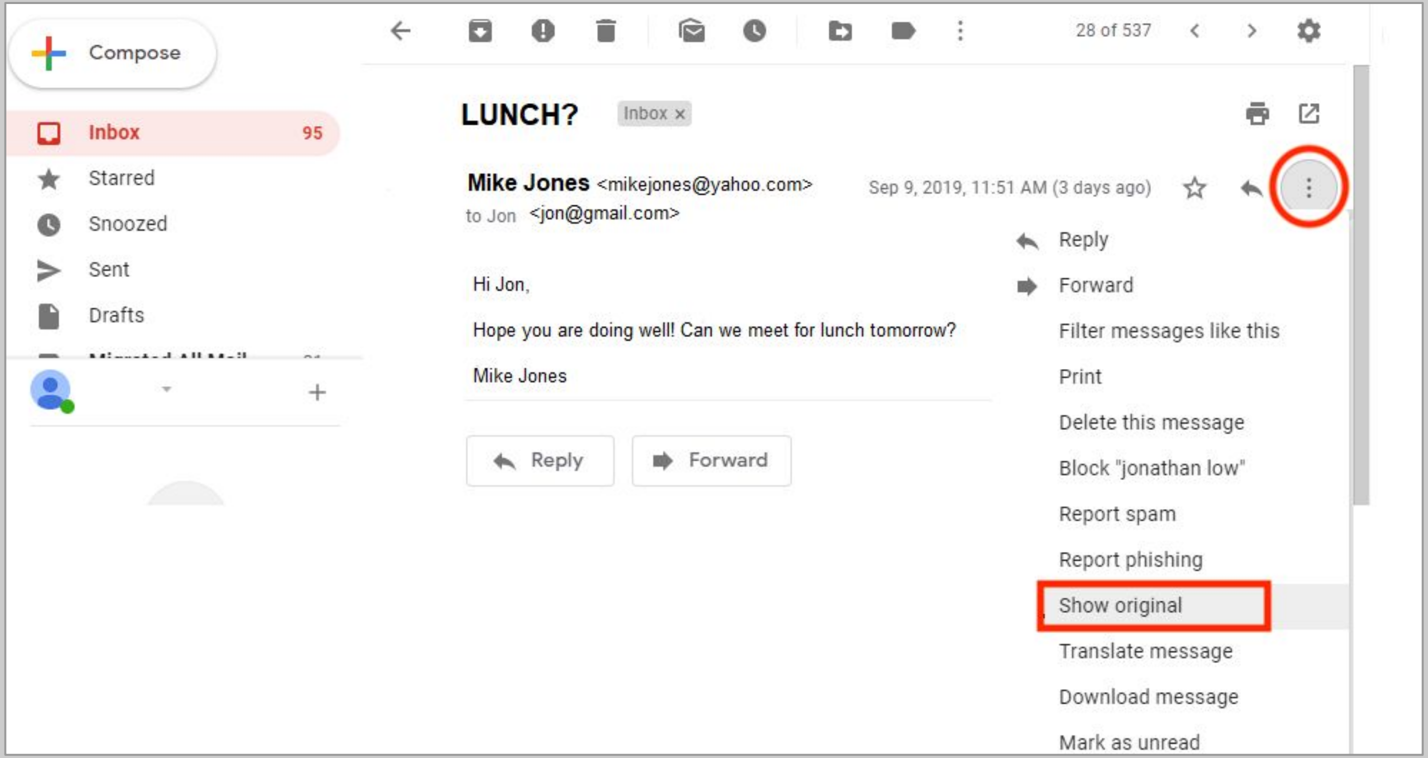
Hope you are doing well! Can we meet for lunch tomorrow?

Mike Jones

Email Message Body

Unfamiliar Fields

More fields are revealed by viewing the complete raw email:



LUNCH?

Mike Jones <mikejones@yahoo.com>
to Jon <jon@gmail.com>

Sep 9, 2019, 11:51 AM (3 days ago)

Hi Jon,

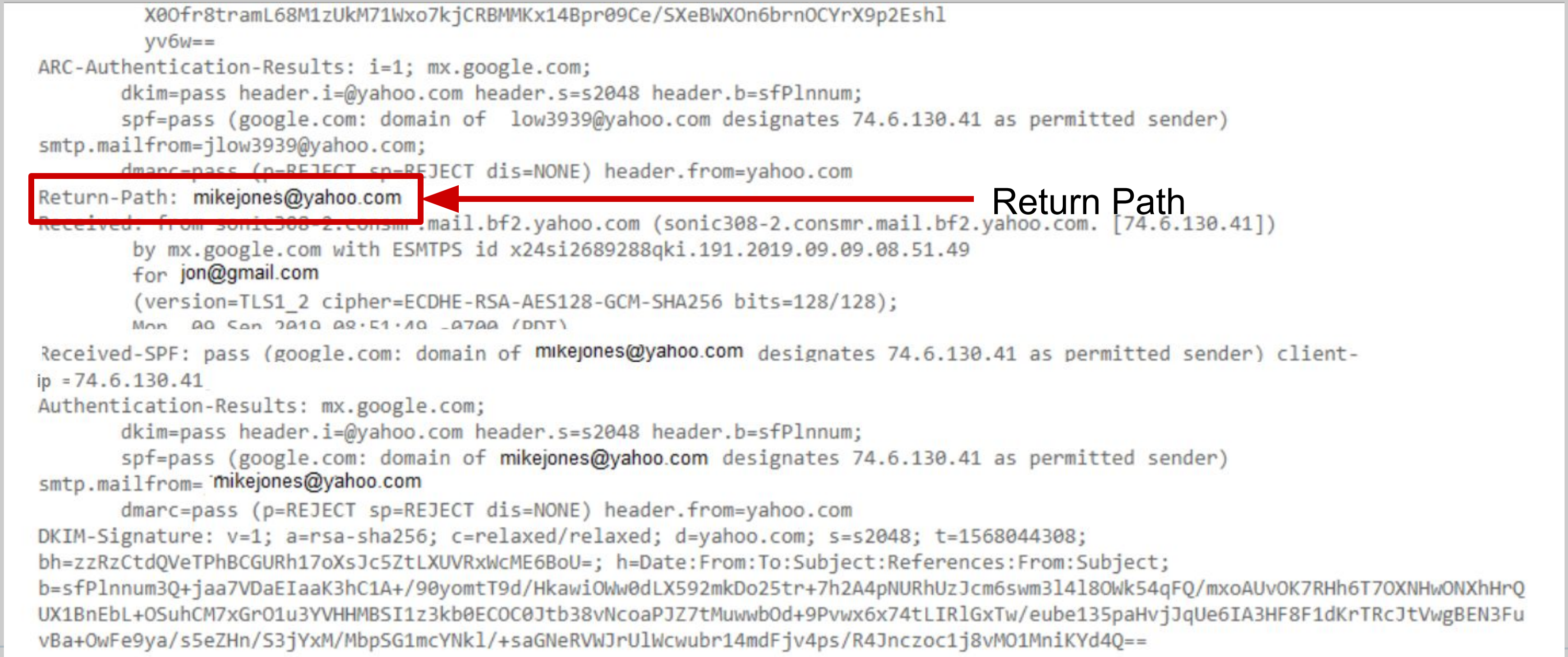
Hope you are doing well! Can we meet for lunch tomorrow?

Mike Jones

Unfamiliar Fields

The raw email will reveal other fields:

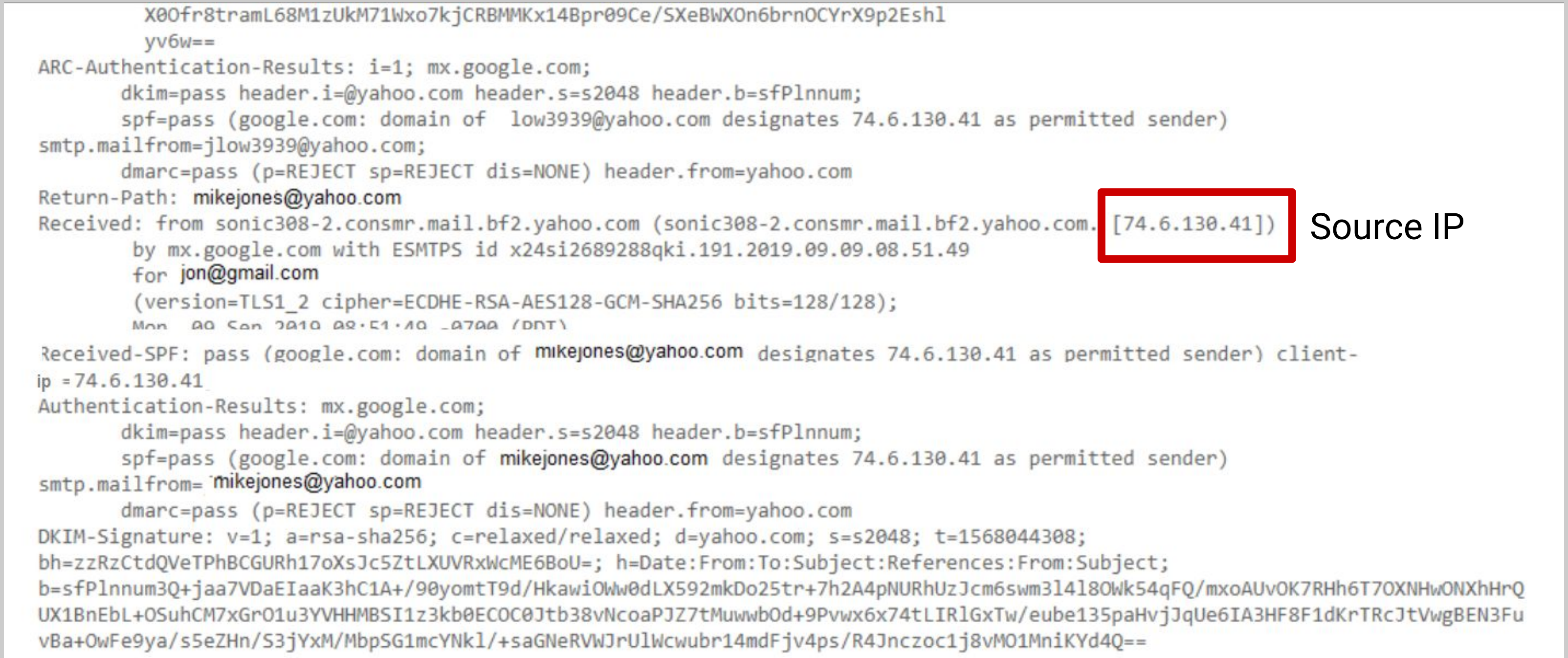
Return-Path: Specifies the sender's return email.



```
         X0Ofr8tramL68M1zUkM71Wxo7kjCRBMMKx14Bpr09Ce/SXeBWXOn6brnOCYrX9p2Eshl
         yv6w==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of  low3939@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom=jlow3939@yahoo.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path:  mikejones@yahoo.com
Received: from sonic308-2.consmr.mail.bf2.yahoo.com (sonic308-2.consmr.mail.bf2.yahoo.com. [74.6.130.41])
        by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
        for  jon@gmail.com
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender) client-
ip =74.6.130.41
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom= mikejones@yahoo.com
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1568044308;
bh=zzRzCtdQVeTPhBCGURh17oXsJc5ZtLXUVRxWcME6BoU=; h=Date:From:To:Subject:References:From:Subject;
b=sfPlnnum3Q+jaa7VDaEIaaK3hC1A+/90yomtT9d/HkawiOWw0dLX592mkDo25tr+7h2A4pNURhUzJcm6swm314l8OWk54qFQ/mxoAUvOK7RHh6T7OXNHwONXhHrQ
UX1BnEbL+OSuhCM7xGrO1u3YVHHMBSI1z3kb0ECOC0Jtb38vNcoaPJZ7tMuwwbOd+9Pvwx6x74tLIRlGxTw/eube135paHvjJqUe6IA3HF8F1dKrTRcJtVwgBEN3Fu
vBa+OwFe9ya/s5eZHn/S3jYxM/MbpSG1mcYNkl/+saGNeRVWJrUlWcwubr14mdFjv4ps/R4Jnczoc1j8vMO1MniKYd4Q==
```

Un-Familiar Fields

Received: Shows a list of the mail servers, illustrating the path of the email from source to destination.



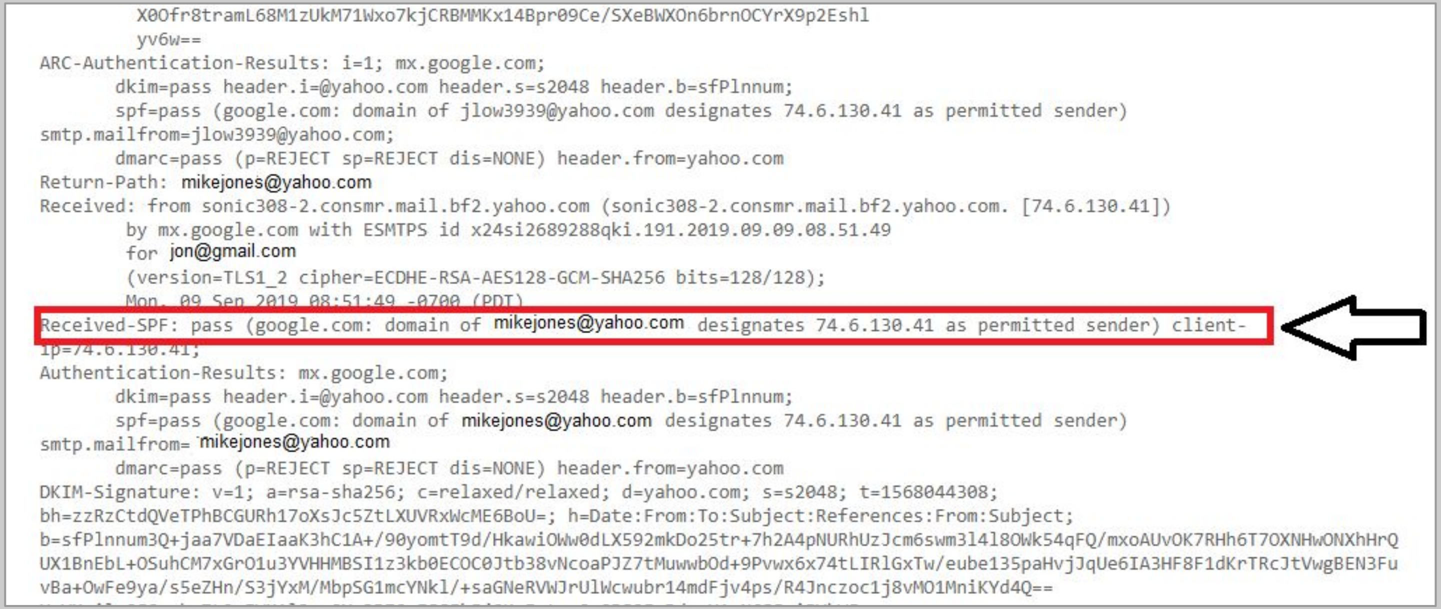
```
         X0Ofr8tramL68M1zUkM71Wxo7kjCRBMMKx14Bpr09Ce/SXeBWXOn6brnOCYrX9p2Eshl
         yv6w==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of  low3939@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom=jlow3939@yahoo.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: mikejones@yahoo.com
Received: from sonic308-2.consmr.mail.bf2.yahoo.com (sonic308-2.consmr.mail.bf2.yahoo.com. [74.6.130.41])
        by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
        for jon@gmail.com
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender) client-
ip =74.6.130.41
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom= mikejones@yahoo.com
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1568044308;
bh=zzRzCtdQVeTPhBCGURh17oXsJc5ZtLXUVRxWcME6BoU=; h=Date:From:To:Subject:References:From:Subject;
b=sfPlnnum3Q+jaa7VDaEIaaK3hC1A+/90yomtT9d/HkawiOWw0dLX592mkDo25tr+7h2A4pNURhUzJcm6swm314180Wk54qFQ/mxoAUvOK7RHh6T7OXNHwONXhHrQ
UX1BnEbL+OSuhCM7xGrO1u3YVHHMBSI1z3kb0ECOC0Jtb38vNcoaPJZ7tMuwwbOd+9Pvwx6x74tLIRlGxTw/eube135paHvjJqUe6IA3HF8F1dKrTRcJtVwgBEN3Fu
vBa+OwFe9ya/s5eZHn/S3jYxM/MbpSG1mcYNkl/+saGNeRVWJrUlWcwubr14mdFjv4ps/R4Jnczoc1j8vMO1MniKYd4Q==
```

Source IP

Unfamiliar Fields

Message-ID: Unique string created by the sending mail server as an identifier of the email.

Received SPF: The SPF verification field.



```
         X0Ofr8tramL68M1zUkM71Wxo7kjCRBMMKx14Bpr09Ce/SXeBWXOn6brnOCYrX9p2Eshl
         yv6w==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of jlow3939@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom=jlow3939@yahoo.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: mikejones@yahoo.com
Received: from sonic308-2.consmr.mail.bf2.yahoo.com (sonic308-2.consmr.mail.bf2.yahoo.com. [74.6.130.41])
        by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
        for jon@gmail.com
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender) client-
ip=74.6.130.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom= mikejones@yahoo.com
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1568044308;
bh=zzRzCtdQVeTPhBCGURh17oXsJc5ZtLXUVRxWcME6BoU=; h=Date:From:To:Subject:References:From:Subject;
b=sfPlnnum3Q+jaa7VDaEIaaK3hC1A+/90yomtT9d/HkawiOWw0dLX592mkDo25tr+7h2A4pNURhUzJcm6swm314l8OWk54qFQ/mxoAUvOK7RHh6T7OXNHwONXhHrQ
UX1BnEbL+OSuhCM7xGrO1u3YVHHMBSI1z3kb0ECOC0Jtb38vNcoaPJZ7tMuwwbOd+9Pvwx6x74tLIRlGxTw/eube135paHvjJqUe6IA3HF8F1dKrTRcJtVwgBEN3Fu
vBa+OwFe9ya/s5eZHn/S3jYxM/MbpSG1mcYNkl/+saGNeRVWJrUlWcwubr14mdFjv4ps/R4Jnczoc1j8vMO1MniKYd4Q==
```

Activity: Email Networking

In this activity, you will continue to play the role of a security analyst for Acme Corp.

Your task is to analyze the header records of suspicious emails and document several data points.

Suggested Time:
15 minutes

Email Security Issue

Spam

Spam is the sending of unsolicited emails.

- Spam is not inherently a security threat.
- But reports state over 60% of all emails are spam. A large number of emails can be very inconvenient for organizations.
- Many email systems have developed advanced methods for detecting and stopping spam emails.
- These involve using SPF records, matching lists of known spam senders, and keyword identification.

Confidential Emails on Unencrypted Channels

Since emails are sometimes transmitted unencrypted, there are risks of interception and unwanted viewing as they are routed across servers.

Several technologies can be used to encrypt confidential emails, such as PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions).

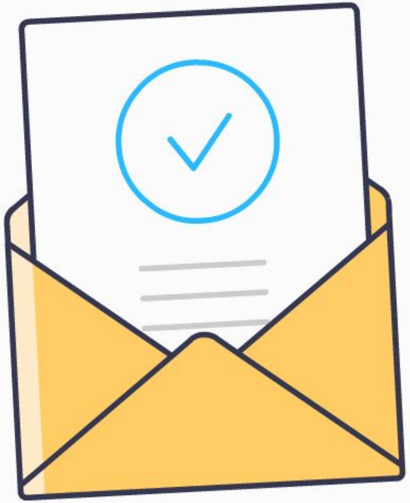
Email Spoofing

Email spoofing is designing emails to trick the receiver into believing they’re coming from a trusted source.

Phishing—the attempt to gain sensitive information from an email recipient—is often accomplished through email spoofing. For example:

- A scammer sends you an email pretending to be from your bank, asking you to update your username and password.
- The email looks legitimate, but may contain a phishing URL leading to a fake bank login page that will capture your banking login info.

According to a recent report from Microsoft, phishing attacks are by far the most common cybersecurity threat— increasing a massive 250% since the previous report was published.



Source: *CPO Magazine*

Email spoofing can be detected with several methods that analyze raw email headers in sent emails.

Method 1: the *From* Email Header

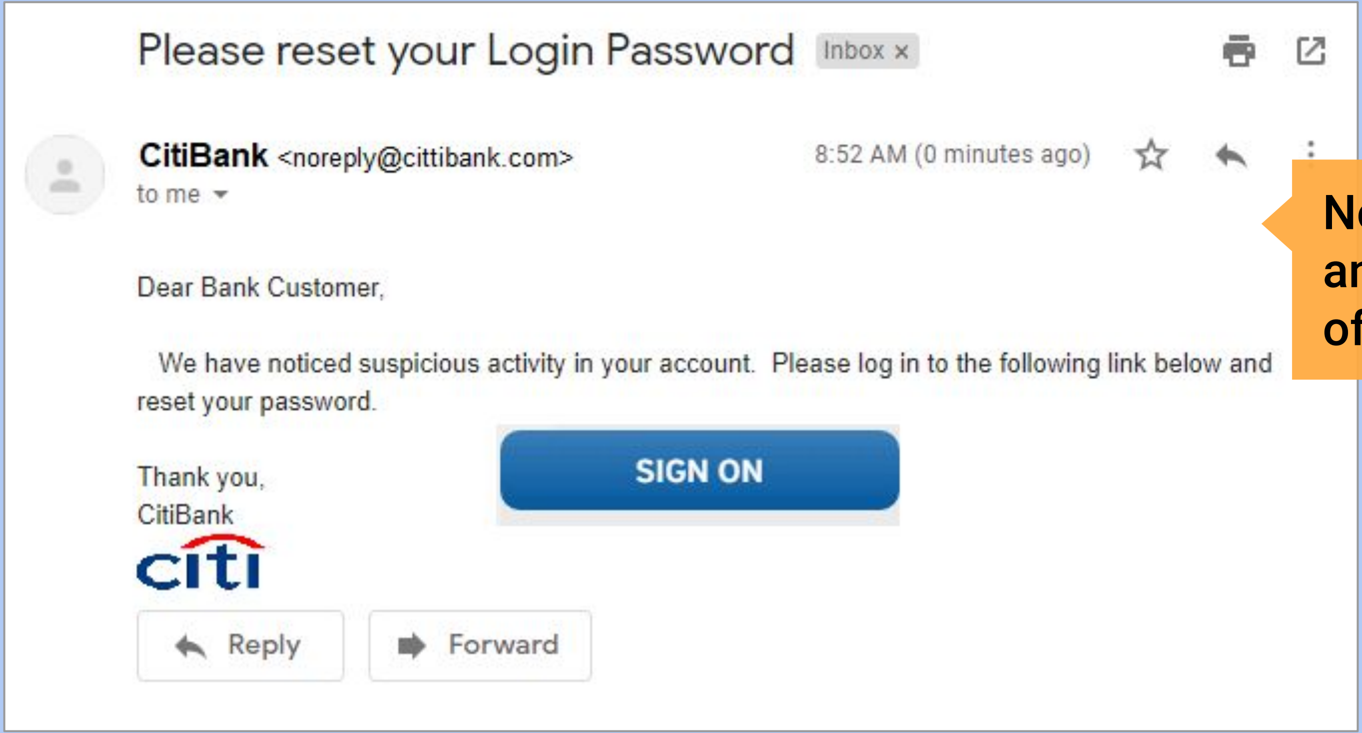
Spammers and phishers often disguise their true source email, changing the displayed email source to a name the recipient will trust or recognize.

In an email claiming to be from Citibank, you can view the raw email header and check the **From** or **Return-Path** field to display the true email address of the sender.

If the email address is **sdfs2344dsf@yahoo.com**, and doesn't have an @citibank domain, this may indicate a malicious email.

Method 1: the *From* Email Header

Spammers may also make slight changes to the sending domain name.



Please reset your Login Password

CitiBank <noreply@cittibank.com>

to me

8:52 AM (0 minutes ago)

Dear Bank Customer,

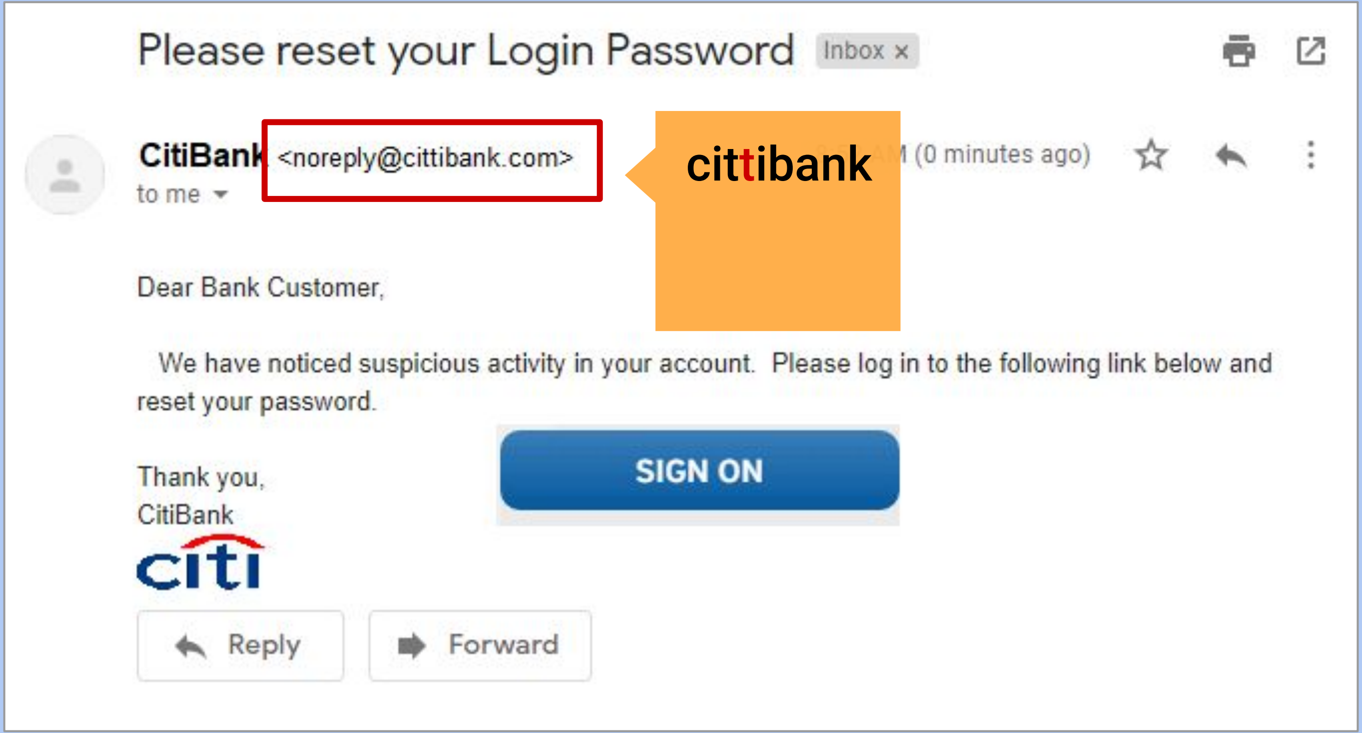
We have noticed suspicious activity in your account. Please log in to the following link below and reset your password.

Thank you,
CitiBank

Notice anything off?

Method 1: the *From* Email Header

Spammers may also make slight changes to the sending domain name.



Please reset your Login Password

CitiBank <noreply@cittibank.com>

to me

cittibank

Dear Bank Customer,

We have noticed suspicious activity in your account. Please log in to the following link below and reset your password.

Thank you,
CitiBank

Method 2: the *Received-SPF* Email Header

Remember: the SPF record is used to identify which mail servers are authorized to send emails on behalf of a domain.

Received-SPF is an email header that displays the results of validating the SPF record.

Received-SPF uses the IP address from the **Received** field and determines if it's an IP of an authorized sender.

If the IP **is** accepted it will display as a "pass."

```
Received-SPF: pass (google.com: domain of michael@acme.com
designates 76.87.4.15 as permitted sender
```

If the IP **is not** accepted it will display as a "fail."

```
Received-SPF: fail (google.com: domain of michael@acmers.com
does not designate 174.81.74.11 as permitted sender)
```

Method 3: the *Received* Email Header

The **Received** header includes the source IP of the sending mail server.

For example: You receive an email from a US-based government organization, such as the IRS.

The IP address from the Received header record is `41.32.23.52`.

When looking up this IP on a web tool like ARIN, the location of the IP is shown to be in Egypt.

This indicates that the email is probably not legitimate. It's unlikely a US government organization would have a mail server in Africa.

Activity: Email Security

In this activity, you will continue to play the role of a security analyst for Acme Corp.

You must further analyze the emails to determine which are spoofed and which are legitimate.

Suggested Time:
10 minutes

The remaining class time will be dedicated to reviewing networking and network security concepts covered in the past two units.

Activity: Networking Review (13_Networking_Review)

In this activity, you will use Wireshark to review the most important topics of the past few classes: HTTP, ARP, DHCP, TCP and UDP.

Suggested Time:
25 minutes

Activity: Networking Review 2 (14_Networking_Review2)

In this activity, you will review the most important topics of the past few classes: topologies, and routing, and network addressing.

Suggested Time:
15 minutes

Activity: Networking Attacks Review

In this activity, you will review ARP attacks, DHCP attacks, TCP attacks, wireless attacks, and email attacks.

Suggested Time:
15 Minutes