EMAIL SECURITY

INTRODUCTION

While the Email section of the Data Loss Prevention (DLP) training focused on sensitive data flowing **out** of an organization, this plan is designed to equip you with the skills and knowledge needed to effectively identify, analyze, and mitigate **inbound** email-related threats (Phishing emails, SPAM, Spoofing). Throughout this training, you will learn to recognize various types of email-based attacks, understand the lifecycle of emails, and utilize advanced techniques for thorough analysis.

EMAIL BASICS

EMAIL PROTOCOLS

It is pivotal to understand Email Protocols before email triaging to understand the protocols emails go through and how they communicate with the network. In addition, email security protocols are important to understand during the email triaging process so that analysts know what to look out for especially in common scenarios such as Spoofing, Phishing emails.

Email protocols is a set of rules defined to ensure emails exchanged between several servers and email clients are in a standard manner, ensuring that email is universal and works for all. For example, an employee using Outlook email client with an email server can send an email to another user using a Google mail server on an Apple email client. This is possible because the servers and email clients follow the rules and standards defined by the email protocol.

Consider the difference between sending a message via WhatsApp and sending an email. When we send a WhatsApp message, the recipient will also use WhatsApp to read the message. The server which processes the message is also the WhatsApp server. The same platform is used in the server and client, allowing entire flow of data to be handled by the severing platform in a custom manner. In this case, WhatsApp. In the case of an email, sender, recipient and servers involved are most often different but then they need to receive data, send data, decipher content, render it the same way a sender has sent it. Hence email protocols are utilize to standardize the way email messages has to be encoded, sent, received, rendered, ensuring that email is standard, reliable and universal mode of communication.

POP PROTOCOL

Post Office Protocol is a support protocol that allows email clients in the server to download emails. This is primarily a one-way protocol and does not sync back the emails to the server

IMAP PROTOCOL

Internet Message Access Protocol is a protocol that is used to sync emails in the server with email clients. It allows two-way sync of emails between server and email client, while the emails are stored on the server.

SMTP PROTOCOL

Simple Mail Transfer Protocol is the principal email protocol that is responsible for transfer of emails between email clients and email servers.

SMTPS is Secure SMTP which works like HTTPS for SMTP. It uses TLS to encrypt messages between clients and servers. Encrypted TLS traffic is decrypted at its destination, however, cleartext messages can be accessible on email servers as messages are routed unless another encryption protocol is used.

EMAIL SECURITY PROTOCOLS

With Email Protocols, it is also important emails have security protocols. Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) are a set of email authentication methods to prove to ISPs and mail services that senders are truly authorized to send email from a particular domain and, are a way of verifying your email sending server is sending emails through your domain. This is to prevent spoofing of domains.

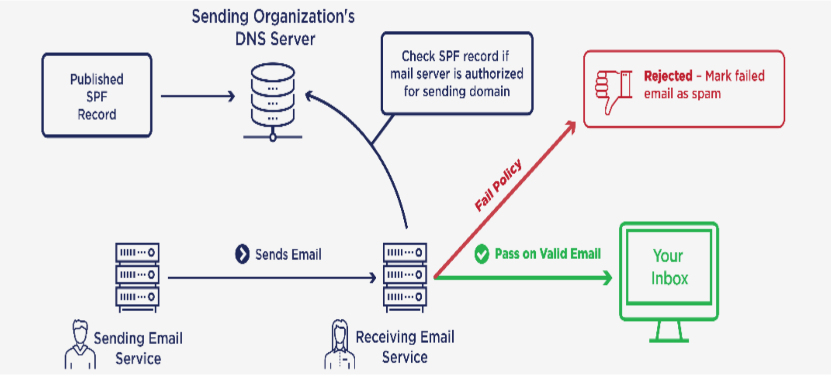
SENDER POLICY FRAMEWORK (SPF)

SPF (Sender Policy Framework) is an authentication tool which works by strictly specifying the number of allowed domains IPs that can send emails from your domain. An SPF record is a DNS entry containing IP addresses of an organization's official email servers and domains that can send emails on behalf of the organization. SPF discourages domain spoofing and spam. A simple analogy would be it works like a publicly available employee directory that helps someone confirm if an employee works in the organization.

HOW DOES IT WORK

SPF records list all the IP addresses of all the servers that are allowed to send emails from the domain, just as an employee directory lists the names of all employees for an organization. When sending an email, the recipient's email server checks for a published SPF record. When it detects an SPF record, it searches through the list of authorized addresses for the record. If a valid record exists, the validations are marked as **PASS.** Otherwise, the email would be rejected and routed to the spam server.

ADVANTAGES


Sending Organization's DNS Server
Published SPF Record
Check SPF record if mail server is authorized for sending domain
Rejected - Mark failed email as spam
Fail Policy
Sends Email
Pass on Valid Email
Your Inbox
Sending Email Service
Receiving Email Service

- SPF authenticates your email, allowing malicious sources to be identified and flagged ASAP
- Provides assurance that the email is secure and trustworthy
- SPF improves email's reputation

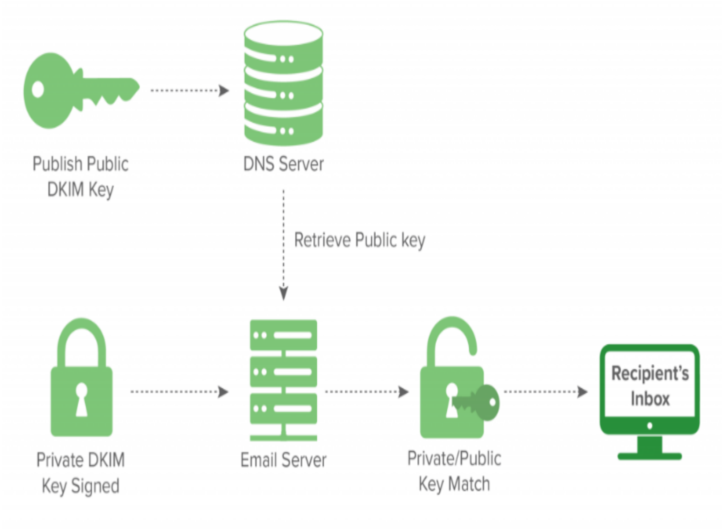
DISADVANTAGES

- If someone else forwards the email sent from your domain, your up address will not be included on your SPF record consequently, it can be mistaken as spam
- Domain owners frequently require authorized third-party vendors to send email from their domains, as such this means that SPF records would have to be constantly updated. Maintenance could be tedious
- SPF does not allow domain owners to instruct email servers how to treat a

message if authentication checks cannot be validated.

DomainKeys Identified Mail (DKIM)

DKIM is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. It utilizes public key cryptography to verify that an email was sent from an authorized mail server, preventing potential phishing/spoofing and spam mail.



HOW DOES IT WORK

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses public key cryptography to mathematically verify that the email came from the domain.

Specifically, DKIM uses public key cryptography:

- A DKIM record stores the domain's *public key*, and mail servers receiving emails from the sender can check this record to obtain the public key. The public key hash is stored in a DNS TXT record.
- The *private key* is kept secret by the sender, who signs the email's header with this key
- The recipient email server then validates the email signature by decoding and comparing the public and private key. If values are the same, it won't be considered spam.
- Mail servers receiving the email can verify that the sender's private key was used by applying the public key

ADVANTAGES

- Strong authentication due to presence of public-key cryptography
- DKIM works better than SPF when forwarding since digital signature is kept with the email message as part of the email header.
- DKIM is an email tagging system that does not filter or identify spam on its own. However, it can prevent spammers from changing message source addresses.

DISADVANTAGES

- There can be issues when the relay or filtering program changes the messages
- DKIM does not allow domain owners to instruct email servers how to treat a message if authentication checks cannot be validated

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

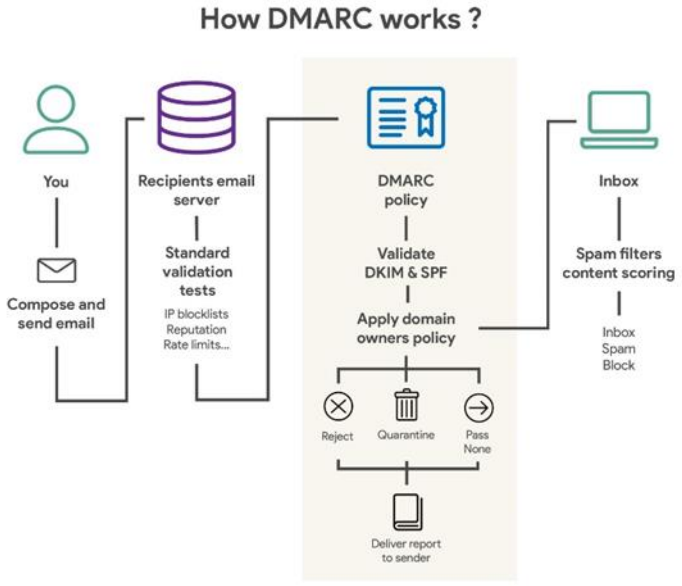
DMARC is used to authenticate an email through further validation of an email SPF and DKIM records. DMARC works as an email validation system that detects and prevents email spoofing. It helps combat certain techniques used in phishing and email spam by instructing receiving severs on what to do with outgoing messages from our organization that does not pass SPF or DKIM.

HOW DOES IT WORK

DMARCH allows domain owner to specify how email servers handle unauthenticated messages.

- Policy =(p=none): no action taken; email sent as per normal
- Policy =(p=quarantine): sends the message to the spam/junk/quarantine folder
- Policy =(p=reject): sends the message back

DMARC works upon results of SPF and DKIM. A DMARC record is first published to DNS with a text entry that tell others the email domain policy after checking SPF and DKIM status. DMARC authenticates if either SPF, DKIM or both passes. The DMARC record also tells email servers to send XML reports back to the reporting email address listed in the DMARC record. These reports provide insight on how your email is moving through the ecosystem and allows you to identify everything that is using your email domain.



ADVANTAGES

- DMARC allows organization and domain owners to receive reports on email messages they sent over the internet
- Makes email easily identifiable across the network of DMARC - capable receiver.
- DMARC allows mail severs to easily identify legitimate emails instead of having the domain administrator attempt to filter out malicious emails.

DISADVANTAGES

- Legitimate emails can potentially be blocked or marked as spam.

COMPARISON BETWEEN SPF, DKIM AND DMARC

	SPF	DKIM	DMARC
Authentication	Allows email senders to define which IP addresses can send email	Uses an encryption key and digital signature to verify an email	Validates sender of email using either SPF or DKIM
Encryption	No encryption algorithm used	Uses public-key cryptography to create a pair of electronic keys	
Compatibility	SPF does not require DKIM and DMARC but depending on SPF alone for email security is insufficient due to SPF's various flaws.	DKIM does not require SPF and DMARC	DMARC authentication result is highly dependent on SPF and DKIM authentication results. When any of the following conditions are met, an email passes DMARC authentication • When SPF with SPF identifier alignment is passed. • When DKIM with DKIM identifier alignment is passed.
Storage	Stored as a SPF record in the DNS.	Stored as a DKIM record in the DNS.	Stored as a DMARC record in the DNS.
Mediation	Does not suggest what to do with not-legitimate email, only tries to verify whether mail is legitimate or not	Does not suggest what to do with not-legitimate email, only tries to verify whether mail is legitimate or not	DMARC helps specify a reporting mechanism to assist receiving mail systems in determine what to do with messages sent from your domain should SPF or DKIM fail

Now that you have an idea of how email works, let’s talk about analysis.

EMAIL ANALYSIS

This section covers some fundamental techniques for analyzing emails to identify potential threats. By understanding the key indicators of malicious, spam, and spoofed emails, you will be able to detect and respond to suspicious activities more effectively.

INDICATORS OF MALICIOUS EMAILS

Most diligent users will report emails that they were not expecting to receive. Here are a few indicators to investigate and determine whether these emails may be malicious. The general term for these is “Phishing Emails.” A phishing email is a fraudulent attempt by malicious actors to deceive individuals into divulging sensitive information such as passwords, credit card numbers, or personal data. These emails often appear to be from legitimate sources like banks, government agencies, or well-known companies. They typically urge recipients to click on links, download attachments, or provide information through forms designed to steal personal or financial information.

SENDER INDICATORS

Misspellings and Variations:

- Check for slight misspellings or variations in the sender’s email address that mimic legitimate ones (e.g., john.smith@company.com vs. john.smiith@company.com).

Impersonation Attacks:

- Be wary of emails that appear to come from high-ranking officials or colleagues but have subtle discrepancies in the sender’s address or display name.
- Verify such emails through another communication channel if they request sensitive information or urgent actions.

Public Domain Email Addresses:

- Emails from public domains (e.g., @gmail.com, @yahoo.com) instead of the official company domain.
- Official business communication should typically come from corporate domains.

Generic Email Addresses:

- Addresses that use generic terms like info@company.com, support@company.com, or admin@company.com.
- Verify if these addresses are commonly used by your organization or if they might be spoofed.

Inconsistent Sender Name and Email Address:

- Mismatch between the display name and the actual email address (e.g., John Smith noreply@randomdomain.com).

Unusual Sending Patterns:

- Emails sent at unusual times or from locations not consistent with the sender’s typical behavior.
- Multiple emails sent in a short period, indicating possible bulk phishing attacks.
- No history record of communication between sender and users.

Lack of Proper Authentication:

- Absence of SPF, DKIM, and DMARC authentication results.
- Emails failing these authentication checks are more likely to be spoofed.

High-Risk Countries:

- Emails originating from high-risk countries known for cyber-attacks or lacking robust cybersecurity regulations.

Known Threat Actors:

- Emails from addresses associated with known threat actors or blacklisted domains.

Message Indicators

Urgency and Pressure Tactics:

- **Urgent Language:** Phrases like "Act Now," "Urgent Action Required," or "Immediate Response Needed" create a sense of urgency.
- **Threats or Consequences:** Messages that threaten consequences if immediate action is not taken (e.g., account suspension, financial loss).

Spelling and Grammar Mistakes:

- **Poor Grammar:** Unusual grammar or sentence structure that is inconsistent with the sender’s usual communication style.
- **Spelling Errors:** Frequent spelling mistakes that may indicate the email is not from a legitimate source.

Calls to Action:

- **Request for Sensitive Information:** Asking for personal or confidential information such as passwords, credit card numbers, or social security numbers.
- **Unusual Requests:** Requests that are out of the ordinary, such as urgent fund transfers or unexpected invoice payments.

Links and URLs:

- **Hidden Links:** URLs that appear legitimate but redirect to malicious websites when clicked.
- **Mismatched URLs:** The visible link text does not match the actual URL (hover over the link to check the destination).
- **Shortened URLs:** Use of URL shortening services (e.g., bit.ly) to obscure the final destination.

Attachments:

- **Unexpected Attachments:** Unanticipated attachments, especially from unknown senders or those claiming to be urgent documents.
- **Suspicious File Types:** Attachments with potentially dangerous file extensions like .exe, .scr, .zip, .js, .docm, .xlsm.
- **Macros in Documents:** Documents that prompt you to enable macros, which can execute malicious code.

Unusual Formatting:

- **Inconsistent Branding:** Emails that lack proper branding or use logos and styles that do not match the legitimate sender’s typical format.
- **Random Capitalization and Punctuation:** Excessive use of capital letters, exclamation points, or special characters.

Generic Greetings:

- **Non-personalized Salutations:** Greetings like "Dear Customer" or "Hello Friend" instead of your actual name.

Spoofed Logos and Graphics:

- **Low-Quality Images:** Logos or graphics that appear blurry or low resolution, which can indicate a fake email.
- **Incorrect Branding:** Use of outdated or incorrect branding elements that legitimate companies wouldn't use.

INDICATORS OF SPAM

Spam emails are unsolicited and typically unwanted messages sent in bulk to a large number of recipients, often for commercial purposes. They can include advertisements, promotional offers, or content unrelated to the recipient's interests. Spam emails are sent indiscriminately and can clutter inboxes, potentially containing malicious links or attachments. Email filters and anti-spam measures are commonly used to mitigate the impact of spam but sometimes these can slip through the cracks and will require our analysis when a user reports it. The objectives for Spam emails can differ greatly from phishing emails, so while they share some common indicators, there are still a few that you should look out for.

Generic Greetings:

- **Non-personalized Salutations:** Greetings such as "Dear Customer," "Hello Friend," or "To Whom It May Concern," instead of addressing you by name.

Unsolicited Offers:

- **Unexpected Promotions:** Emails offering deals, promotions, or prizes that you did not sign up for or express interest in.
- **Aggressive Marketing:** Messages pushing products or services in an overly aggressive manner.

Excessive Use of Capitalization and Punctuation:

- **Attention-Grabbing Tactics:** Subject lines or body text with excessive use of capital letters, exclamation points, or special characters to attract attention (e.g., "FREE!!! CLICK NOW!!!").

Too Good to Be True:

- **Outlandish Claims:** Offers or claims that seem too good to be true, such as winning a lottery you didn't enter, receiving an inheritance from an unknown relative, or promises of quick financial gains.

Suspicious Attachments and Links:

- **Unexpected Attachments:** Attachments that you did not expect to receive, especially from unknown senders.
- **Obscure or Suspicious Links:** Links that appear shortened or obscure, often using URL shortening services to hide the actual destination.

Unrecognized Senders:

- **Unknown Sources:** Emails from senders you do not recognize or have no prior interaction with.
- **Public Domain Addresses:** Emails from free public domains that do not seem to align with the supposed sender's identity.

Irrelevant Content:

- **Off-Topic Messages:** Content that is irrelevant to your interests or does not align with your usual communications.

Opt-Out Requests:

- **Lack of Unsubscribe Options:** Absence of a clear and functional way to opt-out or unsubscribe from future emails.
- **Untrusted Opt-Out Links:** Suspicious opt-out links that may lead to phishing websites or are not associated with the legitimate sender.

Excessive Images or Multimedia:

- **Heavy Use of Graphics:** Emails with a large number of images, videos, or other multimedia content aimed at drawing attention, often without meaningful text content.

High Volume:

- **Frequent Emails:** Receiving an unusually high volume of emails from the same sender in a short period, which may indicate bulk mailing practices.

HEADER ANALYSIS

Email headers contain vital metadata about the email's origin, path, and handling. By analyzing headers, you can uncover information that helps determine if an email is legitimate or malicious. Here's a breakdown of key components to examine in an email header:

From Header:

Purpose: Indicates the sender of the email.

Analysis: Verify the sender's email address and check for discrepancies or suspicious variations.

Reply-To Header:

Purpose: Specifies the address to which replies should be sent.

Analysis: Ensure the reply-to address matches the sender's domain and is not redirecting to a different or suspicious domain.

Return-Path Header:

Purpose: Indicates the address that bounces should be sent to.

Analysis: Check if the return-path domain is consistent with the sender's domain to verify authenticity.

Received Headers:

Purpose: Tracks the path the email took from the sender to the recipient.

Analysis: Examine the chain of received headers to identify the originating IP address and any unusual or unexpected servers through which the email passed.

Message-ID Header:

Purpose: Provides a unique identifier for the email.

Analysis: Check if the message ID is consistent with the sender's domain and follows a standard format.

Authentication Results:

Purpose: Displays the results of email authentication checks.

Analysis: Review the results of SPF, DKIM, and DMARC checks to verify the email's authenticity.

SPF (Sender Policy Framework):

Analysis: Confirm the SPF check result is "pass" to ensure the email is sent from an authorized IP address.

DKIM (DomainKeys Identified Mail):

Analysis: Verify that the DKIM signature matches the sender's domain and the check result is "pass."

DMARC (Domain-based Message Authentication, Reporting & Conformance):

Analysis: Ensure the email aligns with the sender's DMARC policy and passes the check.

EMAIL TRIAGE

Not all malicious emails can be handled the same way, but here is a brief guide, that will give you an idea of what steps you need to take to successfully mitigate an email threat.

1. CHECKING THE SENDER/DOMAIN

Verify the authenticity of the sender and the domain from which the email was sent looking out for indicators mentioned in the previous section.

- **Check Domain Reputation:**
  - Use tools to check the reputation of the sender's domain, there are open-source tools like phishtank or VirusTotal in addition to tools unique to each organization.
  - Look for domains known to be associated with spam or malicious activity.
- **SPF, DKIM, and DMARC:**
  - Ensure the email passes SPF, DKIM, and DMARC authentication checks.
  - Verify whether the sender is internal, trusted 3rd party, a supplier, client etc.
  - Leverage Email archiving tools (for ex. Global Relay) to review historical communications from the sender.

2. INVESTIGATING THE MESSAGE

Analyze the content of the email for signs of phishing or other malicious intent.

- **Content Analysis:**
  - Look for language that creates a sense of urgency or uses pressure tactics.
  - Identify spelling and grammar mistakes that are uncharacteristic of legitimate senders.
- **Request for Sensitive Information:**
  - Be cautious of emails requesting personal, financial, or login information.
- **Attachments and Links:**
  - Analyze any attachments or links for potential threats (detailed in subsequent sections).

3. INVESTIGATING URLS AND LINKS

Determine the safety and legitimacy of URLs and links included in the email.

- **Hover Over Links:**
  - Hover over any links to see the actual URL and ensure it matches the context of the email.
- **URL Reputation:**

  - Use tools to check the reputation of URLs (VirusTotal, urlscan.io).
  - Look for known malicious domains or newly registered domains.
  - Use sandbox environments to analyze the behavior of URLs without risking your main system (browserling.com is a free online option).

4. INVESTIGATING ATTACHMENTS

Safely analyze email attachments for malicious content.

- **Attachment Handling:**
  - Use secure methods to handle attachments, such as opening them in a sandbox environment.
- **Static and Dynamic Analysis:**
  - Perform static analysis to inspect the attachment without executing it.
  - Use dynamic analysis in a controlled environment to observe the behavior of the attachment.
- **Check for Macros:**
  - Be cautious of attachments prompting you to enable macros, which can execute malicious code.

5. CATEGORIZING EMAIL

Correctly categorize the email to determine the appropriate response.

- **Phish:**
  - Emails that attempt to steal sensitive information or deliver malware through deceptive tactics.
- **Spam:**
  - Unsolicited emails that are typically promotional or irrelevant but may not be directly harmful.
- **False Positive:**
  - Legitimate emails that were mistakenly flagged as suspicious.

6. CONTAINING THE THREAT

Objective: Take appropriate actions to mitigate the impact of malicious emails.

- **Exposure Check**
  - Determine whether the phish was an isolated incident or a campaign against multiple users. Determine who else may have received the email but hasn’t reported it to identify the scope of your mitigation actions.
- **Quarantine the Email:**
  - Isolate suspicious emails to prevent further spread.
- **Contain threats**
  - For URL links, your organization should have firewalls or domain filtering tools available. A means of controlling destinations a user can visit online. (OpenDNS for example is a Domain Filtering tool by Cisco that allows you to block dns destinations for

identities and control policy for various entitities)

    - Attachments that are malicious should be “blacklisted” using antivirus tools, this means that the hash of the file should be blocked with another security control across the network. If other users received the same email, they wouldn’t be able to execute the malware once it’s been blocked.
- **Block Sender/Domain:**
    - Block the sender or domain to prevent future emails from the same source.
- **Alert Relevant Parties:**
    - Notify the relevant teams or individuals about the threat to take further action.
- **Document and Report:**
    - Record your findings and actions taken in your incident management system for future reference and analysis.

EMAIL ANALYSIS FLOW

We’ll close out with a diagram to summarize the above steps. Note that every case can be different, but this should give you a good foundation to investigate emails with confidence.

Review the diagram here