W-3, D-2

1. What are the actions towards an email when it is marked as spam? How can an end user find the quarantined emails back?

Actions towards an email when it is marked as spam	Move message to the junk email folder - ✓ Add X-header ✓ Prepend subject line with text ✓ Redirect message to the email address ✓ Delete message ✓ Quarantine message

Quarantine Email Retrieve by End-user
✓ Please go to – https://protection.office.com
✓ Please navigate to – **Threat management > Review**
✓ Here, you will find a list of Quarantine message from where you can retrieve the message.

2. How to get message header from Outlook & OWA?

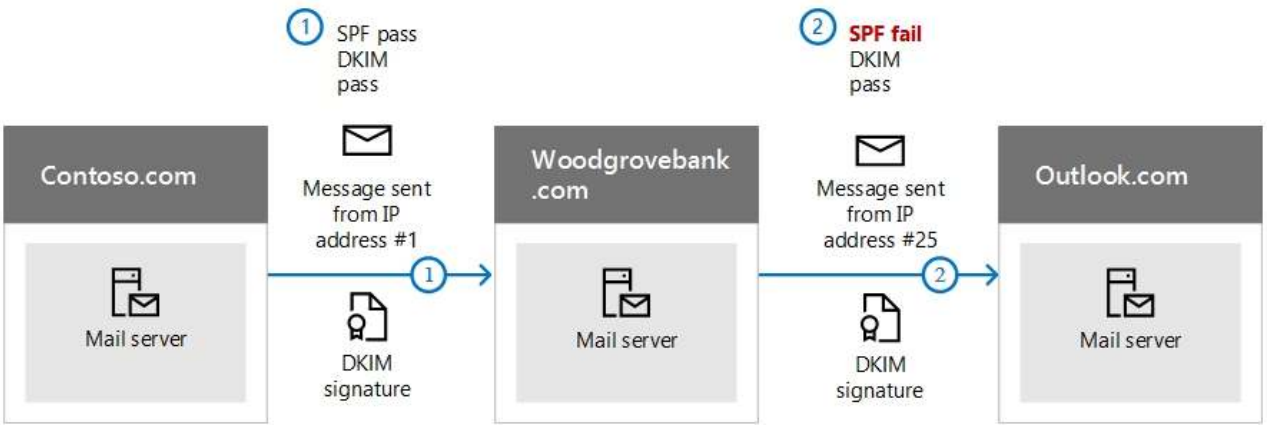
Message Header from Outlook Client
✓ Please open Outlook Client and select the inbox message, which you would like to check the message header.
✓ Double click on that message
✓ Please click **Properties**
✓ There you will find one box named – **Internet headers** ✓ This is the message header of that particular message. You can copy from here.
Message Header from OWA
✓ Please go to – https://outlook.office365.com ✓ Select and right click on the inbox message, which you would like to check the message header. ✓ Please click **View message details**
✓ This is the message header of that particular message. You can copy from here.

W-3, D-2

3. What will happen to the message header if the email was marked as spam by advanced spam filter options?

Message Header for ASF	Enabling one or more of the ASF settings is an aggressive approach to spam filtering. You can't report messages that are filtered by ASF as false positives. ASF add extra field of X-CustomSpam if the message was detected by ASF. ✓ **The specific X-CustomSpam:** X-header fields that are added to messages as described in this topic.

4. What are DKIM and DMARC?

DKIM
✓ Domain Keys Identified Mail (DKIM) ✓ Ensure that destination email systems trust messages sent outbound from the custom domain. ✓ You should use DKIM in addition to SPF and DMARC to help prevent spoofers from sending messages that look like they are coming from your domain. ✓ DKIM lets you add a digital signature to outbound email messages in the message header. ✓ A private key is used to encrypt the header in your domain's outgoing email and then publish a public key to the domain's DNS records that receiving servers can then use to decode the signature. They use the public key to verify that the messages are really coming from you and not coming from someone spoofing your domain. ✓ Microsoft 365 automatically sets up DKIM for its initial onmicrosoft.com domain.
✓ At first case, DKIM and SPF both have passes as the email comes from authorized mail server. ✓ At second case, DKIM have passed because it relies on public key cryptography to authenticate and not just IP addresses,   

W-3, D-2

DMARC

- ✓ Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- ✓ Works with SPF and DKIM to authenticate mail senders and ensure that destination email systems trust messages sent from your domain.
- ✓ Implementing DMARC with SPF and DKIM provides additional protection against spoofing and phishing email.
- ✓ DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF or DKIM checks.

How DMARC works for Outbound Message

- ✓ **Mail From" address:** Identifies the sender and specifies where to send return notices if any problems occur with the delivery of the message, such as non-delivery notices. This appears in the envelope portion of an email message and is not usually displayed by your email application. This is sometimes called the **5321.MailFrom address** or the **reverse-path address**.

- ✓ **"From" address:** The address displayed as the From address by your mail application. This address identifies the author of the email. That is, the mailbox of the person or system responsible for writing the message. This is sometimes called the **5322.From address**.

- ✓ SPF uses a DNS TXT record to provide a list of authorized sending IP addresses for a given domain. Normally, SPF checks are only performed against the 5321.MailFrom address. This means that the 5322.From address is not authenticated when you use SPF by itself. This allows for a scenario where a user can receive a message which passes an SPF check but has a spoofed 5322.From sender address. Here DMARC check fail and detected the message as spam but spf fail to detect as SPF only checks 5321.Mail From Address.

```text
S: Helo woodgrovebank.com
S: Mail from: phish@phishing.contoso.com
S: Rcpt to: astobes@tailspintoys.com
S: data
S: To: "Andrew Stobes" <astobes@tailspintoys.com>
S: From: "Woodgrove Bank Security" <security@woodgrovebank.com>
S: Subject: Woodgrove Bank - Action required
S:
S: Greetings User,
S:
S: We need to verify your banking details.
S: Please click the following link to verify that we have the right information for your account.
S:
S: https://short.url/woodgrovebank/updateaccount/12-121.aspx
S:
S: Thank you,
S: Woodgrove Bank
S: .
```

W-3, D-2

How DMARC works for Inbound Message
✓ If you configured SPF, then the receiving server performs a check against the Mail from address phish@phishing.contoso.com. If the message came from a valid source for the domain phishing.contoso.com then the SPF check passes. Since the email client only displays the From address, the user sees that this message came from security@woodgrovebank.com. With SPF alone, the validity of woodgrovebank.com was never authenticated. ✓ When you use DMARC, the receiving server also performs a check against the From address. In the example above, if there is a DMARC TXT record in place for woodgrovebank.com, then the check against the From address fails.

5. Set up DKIM with your tenant.

1. **Publish** CNAME records in the Custom Domain in **DNS Management** [**N.B.** to get the domainGUID you need to find MX records and get the mail server]	✓ **Host name:** selector1._domainkey **Value:** selector1-<domainGUID>._domainkey.<initialDomain> **TTL:** 3600 ✓ **Host name:** selector2._domainkey **Points to address or value:** selector2-<domainGUID>._domainkey.<initialDomain> **TTL:** 3600
2. **Enable** DKIM	✓ Please go to – https://outlook.office365.com/ecp ✓ Please navigate to – ① **protection** > ② **dkim** > ③ select the custom domain > ④ **Enable** ✓ Now, DKIM is enabled.

6. How to enable DMARC.

1. **Identify** valid sources of mail for your domain	✓ If you have already set up SPF then you have already gone through this exercise. However, for DMARC, there are additional considerations. When identifying sources of mail for your domain there are two questions you need to answer: o What IP addresses send messages from my domain? o For mail sent from third parties on my behalf, will the 5321.MailFrom and 5322.From domains match?
2. Set up **SPF** for your domain	✓ Update the SPF records according to the IP address.

3. Set up **DKIM** for your custom domain	✓ Publish given DKIM CNAME records in the DNS Management of the DNS hosting provider. ✓ Enable DKIM from EAC protection.
4. Update **DMARC** TXT record in the DNS management	✓ **_dmarc.<domain> TTL IN TXT "v=DMARC1; p=policy; pct=100"** ✓ domain is the domain you want to protect. By default, the record protects mail from the domain and all subdomains. For example, if you specify _dmarc.contoso.com, then DMARC protects mail from the domain and all subdomains, such as housewares.contoso.com or plumbing.contoso.com. ✓ TTL should always be the equivalent of one hour. The unit used for TTL, either hours (1 hour), minutes (60 minutes), or seconds (3600 seconds), will vary depending on the registrar for your domain. ✓ pct=100 indicates that this rule should be used for 100% of email. ✓ policy specifies what policy you want the receiving server to follow if DMARC fails. You can set the policy to **none**, **quarantine**, or **reject**.

7. How would EOP check and deal with DKIM authentication result?

Dealing with DKIM by EOP for Inbound message
✓ Exchange Online Protection (EOP) and Exchange Online support inbound validation of DKIM messages. ✓ DKIM is a method for validating that a message was sent from the domain it says it originated from and that it was not spoofed by someone else. It ties an email message to the organization responsible for sending it. DKIM verification is automatically used for all messages sent over IPv6 communications. ✓ Microsoft 365 also now supports DKIM when mail is sent over IPv4. ✓ DKIM validates a digitally signed message that appears in the DKIM-Signature header in the message headers. The result of a DKIM-Signature validation is stamped in the Authentication-Results header which conforms with **RFC 7001** (Message Header Field for Indicating Message Authentication Status). ✓ Authentication-Results: **<domain>; dkim=pass (signature was verified) header.d=example.com**

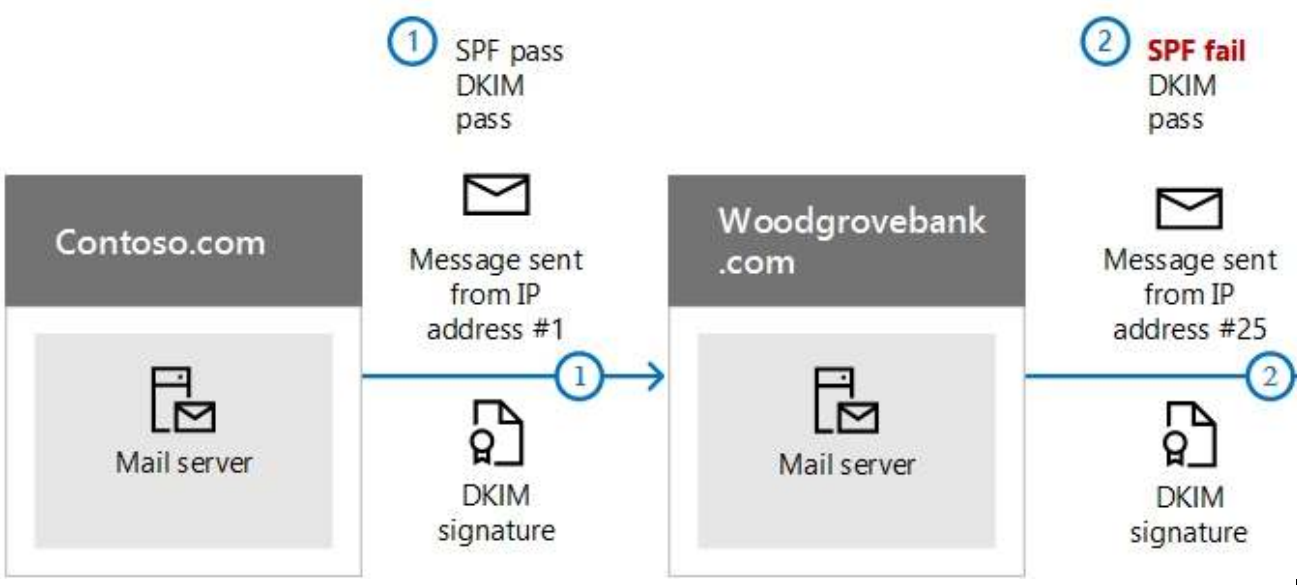
W-3, D-2

Dealing with DKIM by EOP for Outbound message

- ✓ DKIM lets you add a digital signature to outbound email messages in the message header.
- ✓ SPF adds information to a message envelope but DKIM actually encrypts a signature within the message header. When you forward a message, portions of that message's envelope can be stripped away by the forwarding server. Since the digital signature stays with the email message because it's part of the email header.

Example of DKIM and SPF work together:

- ✓ In this example, if you had only published an SPF TXT record for your domain, the recipient's mail server could have marked your email as spam and generated a false positive result. The addition of DKIM in this scenario reduces false positive spam reporting. Because DKIM relies on **public key cryptography** to authenticate and not just IP addresses, DKIM is considered a much stronger form of authentication than SPF. We recommend using both SPF and DKIM, as well as DMARC in your deployment.
- ✓ DKIM uses a **private key** to insert an encrypted signature into the message headers. The signing domain, or outbound domain, is inserted as the value of the **d= field in the header**. The verifying domain, or recipient's domain, then use the d= field to look up the public key from DNS and authenticate the message. If the message is verified, the DKIM check passes.



8. What is SPF? Why do we need SPF?

- ✓ SPF is an email authentication system, which indicates that users are sending from an authorized mail server.
- ✓ An SPF TXT record is a DNS record that helps prevent spoofing and phishing by verifying the domain name from which email messages are sent.
- ✓ SPF validates the origin of email messages by verifying the IP address of the sender against the alleged owner of the sending domain.

W-3, D-2

9. What is email authentication/email validation system?

- ✓ Email authentication is a group of standards that tries to stop spoofing (email messages from forged senders).
- ✓ In Microsoft 365 organizations with mailboxes in Exchange Online, and standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, EOP uses these standards to verify inbound email:
  - SPF (Sender Policy Framework)
  - DKIM (Domain Keys Identified Mail)
  - DMARC (Domain based Message Authorization, Reporting & Conformance)

10. What is SPF enforcement rule for the last segment?

- ✓ **-all**
  - Indicates hard fail.
  - If you know all of the authorized IP addresses for your domain, list them in the SPF TXT record and use the -all (hard fail) qualifier.
  - Also, if you are only using SPF, that is, you are not using DMARC or DKIM, you should use the -all qualifier.
  - Recommended to use always this qualifier.

- ✓ **~all**
  - Indicates soft fail.
  - If you're not sure that you have the complete list of IP addresses, then you should use the ~all (soft fail) qualifier.
  - Also, if you are using DMARC with p=quarantine or p=reject, then you can use ~all. Otherwise, use -all.

- ✓ **?all**
  - Indicates neutral.
  - This is used when testing SPF.
  - Not recommended to use this qualifier in your live deployment.

11. Explain the SPF record with Example.

- ✓ **v=spf1 ip4:192.168.0.1 ip4:192.168.0.2 include:spf.protection.outlook.com -all**
  - **v=spf1** is required.
  - **ip4** indicates that you are using IP version 4 addresses. Ip6 indicates that you are using IP version 6 addresses. If you are using **Ipv6** IP addresses, replace ip4 with ip6 in the examples in this article. You can also specify IP address ranges using CIDR notation, for example ip4:192.168.0.1/26.
  - IP address is the IP address that you want to add to the SPF TXT record. Usually, this is the IP address of the outbound mail server for your organization. You can list multiple outbound mail servers.
  - domain name is the domain you want to add as a legitimate sender.

- If you are fully using EXO then the SPF record will be – **v=spf1 include:spf.protection.outlook.com -all**

12. What is initial domain? Do we need to set up SPF, DKIM, DMARC for initial domain?

- ✓ The domain I got when I register in the tenant is known as initial domain. (onmicrosoft.com)
- ✓ For initial domain, you don't need to set up these email authentication systems. SPF, DKIM, DMARC are required for custom domain after adding the domain in the tenant.

13. Which type of records are SPF, DKIM, DMARC?

Email Authentication	DNS Record Type	When to Add in DNS Management	Process
SPF	TXT	During adding Domain Process (in step-2)	✓ Publish SPF record in DNS Management of Domain provider
DKIM	CNAME	During DKIM Enable	✓ **Publish** two CNAME records in DNS Management of Domain provider ✓ **Enable** from **Protection > dkim**
DMARC	TXT	After SPF & DKIM Set Up	✓ Check all **IP** from my email server ✓ Update **SPF** record ✓ **DKIM** set up ✓ Publish **DMARC** records in DNS Management of Domain provider

14. How to get Domain GUID?

- ✓ Domain GUID is the same as the MX record for your custom domain that appears before mail.protection.outlook.com. For example, MX record for the domain contoso.com is **contoso-com.mail.protection.outlook.com**, the domainGUID is then **contoso-com**.