Anti-spam protection in Office 365

- 03/23/2020

  Please access the link below to view the contributors to this article

  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection?view=o365-worldwide

In this article

Note

This topic is intended for Office 365 admins. For end-user topics, see Overview of the Junk Email Filter and Learn about junk email and phishing.

If you're an Office 365 customer with mailboxes in Exchange Online or a standalone Exchange Online Protection (EOP) customer without Exchange Online mailboxes, your email messages are automatically protected against spam (junk email) by EOP.

Microsoft's email safety roadmap involves an unmatched cross-product approach. EOP anti-spam and anti-phishing technology is applied across our email platforms to provide users with the latest anti-spam and anti-phishing tools and innovations throughout the network. The goal for EOP is to offer a comprehensive and usable email service that helps detect and protect users from junk email, fraudulent email threats (phishing), and malware.

As email use has grown, so has email abuse. Unmonitored junk email can clog inboxes and networks, impact user satisfaction, and hamper the effectiveness of legitimate email communications. That's why Microsoft continues to invest in anti-spam technologies. Simply put, it starts by containing and filtering junk email.

Anti-spam technologies in EOP

To help reduce junk email, EOP includes junk email protection that uses proprietary spam filtering technologies to identify and separate junk email from legitimate email. EOP spam filtering learns from known spam and phishing threats and user feedback from our consumer platform, Outlook.com. Ongoing feedback from EOP users in the junk email classification program helps ensure that the EOP technologies are continually trained and improved.

The anti-spam settings in EOP are made of the following technologies:

- **Connection filtering**: Identifies good and bad email source servers early in the inbound email connection via the IP Allow List, IP Block List, and the *safe list* (a dynamic but non-editable list of trusted senders maintained by Microsoft). You configure these settings in the connection filter policy. Learn more at Configure connection filtering in Office 365.

  Note

  Spoof intelligence uses connection filtering to create allow and block lists of senders who are spoofing your email domain. For more information, see Learn more about spoof intelligence in Office 365.

- **Spam filtering (content filtering)**: EOP uses the spam filtering verdicts **Spam**, **High confidence spam**, **Bulk email**, **Phishing email** and **High confidence phishing email** to classify messages. You can configure the actions to take based on these verdicts, and you can configure the end-user notification options for messages that were quarantined instead of delivered. For more information, see Configure anti-spam policies in Office 365.

  Note

  By default, spam filtering is configured to send messages that were marked as spam to the recipient's Junk Email folder. However, in hybrid environments where EOP protects on-premises Exchange mailboxes, you need to configure two mail flow rules (also known as transport rules) in your on-premises Exchange organization to recognize the EOP spam headers that are added to messages. For details, see Configure standalone EOP to deliver spam to the Junk Email folder in hybrid environments.

- **Outbound spam filtering**: EOP also checks to make sure that your users don't send spam, either in outbound message content or by exceeding outbound message limits. For more information, see Configure outbound spam filtering in Office 365.
- **Spoof intelligence**: For more information, see Learn more about spoof intelligence in Office 365.

Manage errors in spam filtering

It's possible that good messages can be identified as spam (also known as false positives), or that spam can be delivered to the Inbox. You can use the suggestions in the following sections to find out what happened and help prevent it from happening in the future.

Here are some best practices that apply to either scenario:

- Always submit misclassified messages to Microsoft. Admins can use Submissions Explorer, or users can report messages by using the Use the Report Message add-in.

- **Examine the anti-spam message headers**: These values will tell you why a message was marked as spam, or why it skipped spam filtering. For more information, see Anti-spam message headers.
- **Point your MX record to Office 365**: In order for EOP to provide the best protection, we always recommend that you have email delivered to Office 365 first. For instructions, see Create DNS records at any DNS hosting provider for Office 365.

  If the MX record points to some other location (for example, a third-party anti-spam solution or appliance), it's difficult for EOP to provide accurate spam filtering. In this scenario, you need to configure Enhanced Filtering for connectors (also known as *skip listing*). For instructions, see Enhanced Filtering for Connectors in Exchange Online.

- **Use email authentication**: If you own an email domain, you can use DNS to help insure that messages from senders in that domain are legitimate. To help prevent spam and unwanted spoofing in EOP, use all of the following email authentication methods:
  - **SPF**: Sender Policy Framework verifies the source IP address of the message against the owner of the sending domain. For a quick introduction to SPF and to get it configured quickly, see Set up SPF in Office 365 to help prevent spoofing. For a more in-depth understanding of how Office 365 uses SPF, or for troubleshooting or non-standard deployments such as hybrid deployments, start with How Office 365 uses Sender Policy Framework (SPF) to prevent spoofing.
  - **DKIM**: DomainKeys Identified Mail adds a digital signature to the message header of messages sent from your domain. For information, see Use DKIM to validate outbound email sent from your custom domain in Office 365.
  - **DMARC**: Domain-based Message Authentication, Reporting, and Conformance helps destination email systems determine what to do with messages that fail SPF or DKIM checks and provides another level of trust for your email partners. For more information, see Use DMARC to validate email in Office 365.
- **Verify your bulk email settings**: The bulk compliant level (BCL) threshold that you configure in anti-spam policies determines whether bulk email (also known as *gray mail*) is marked as spam. The PowerShell-only setting *MarkAsSpamBulkMail* that's on by default also contributes to the results. For more information, see Configure anti-spam policies in Office 365.

Prevent the delivery of spam to the Inbox

- **Verify your organization settings**: Watch out for settings that allow messages to skip spam filtering (for example, if you add your own domain to the allowed domains list in anti-spam policies). For our recommended settings, see Recommended settings for EOP and Office 365 ATP security and Create safe sender lists in Office 365.
- **Verify the junk email rule is enabled in the user's mailbox**: It's enabled by default, but if it's isn't messages marked as junk can't be moved into the Junk Email folder. For more information, see Configure junk email settings on Exchange Online mailboxes in Office 365.
- **Use the available blocked sender lists**: For information, see Create blocked sender lists in Office 365.

- **Unsubscribe from bulk email** If the message was something that the user signed up for (newsletters, product announcements, etc.) and contains an unsubscribe link from a reputable source, consider asking them to simply unsubscribe.
- **Standalone EOP: create mail flow rules in on-premises Exchange for EOP spam filtering verdicts**: In standalone EOP environments where EOP protects on-premises Exchange mailboxes, you need to configure mail flow rules (also known as transport rules) in on-premises Exchange to translate the EOP spam filtering verdict so the junk email rule can move the message to the Junk Email folder. For details, see Configure standalone EOP to deliver spam to the Junk Email folder in hybrid environments.

Prevent good email from being identified as spam

Here are some steps that you can take to help prevent false positives:

- **Verify the user's Outlook Junk Email Filter settings**:
  - **Verify the Outlook Junk Email Filter is disabled**: When the Outlook Junk Email Filter is set to the default value **No automatic filtering**, Outlook doesn't attempt to classify massages as spam. When it's set to **Low** or **High**, the Outlook Junk Email Filter uses its own SmartScreen filter technology to identify and move spam to the Junk Email folder, so you could get false positives. Note that Microsoft stopped producing spam definition updates for the SmartScreen filters in Exchange and Outlook in November, 2016. The existing SmartScreen spam definitions were left in place, but their effectiveness will likely degrade over time.
  - **Verify the Outlook 'Safe Lists Only' setting is disabled**: When this setting is enabled, only messages from senders in the user's Safe Senders list or Safe Recipients list are delivered to the Inbox; email from everyone else is automatically moved to the Junk Email folder.

  For more information about these settings, see Configure junk email settings on Exchange Online mailboxes in Office 365.

- **Use the available safe sender lists**: For information, see Create safe sender lists in Office 365.
- **Verify users are within the sending and receiving limits** as described in Receiving and sending limits in the Exchange Online service description.
- **Standalone EOP: use directory synchronization**: If you use standalone EOP to help protect your on-premises Exchange organization, you should sync user settings with the service by using directory synchronization. Doing this ensures that your users' Safe Senders lists are respected by EOP. For more information, see Use directory synchronization to manage mail users.

Anti-spam legislation

At Microsoft, we believe that the development of new technologies and self-regulation requires the support of effective government policy and legal frameworks. The worldwide spam proliferation has spurred numerous legislative bodies to regulate commercial email. Many

countries now have spam-fighting laws in place. The United States has both federal and state laws governing spam, and this complementary approach is helping to curtail spam while enabling legitimate e-commerce to prosper. The CAN-SPAM Act expands the tools available for curbing fraudulent and deceptive email messages.