

Overview of the Spam and Junk Email Filter for Exchange

Increase productivity with our integrated Spam Filter that allows you to review messages flagged as Spam by our three-layer scanning technology, directly from within Outlook or the web based Outlook Web App (OWA), in your Junk Email folder.

Please note that there are two ways to manage Spam when using Microsoft Exchange as part of your TriValley Internet email hosting package:

1. The preferred method is using our three-layer integrated Spam filter at the mail server level as this protects your computer from unwanted spam and viruses.
2. As an additional layer of protection, you can add email addresses to Outlook and the web based Outlook Web App (OWA) as part of those applications Junk Email functions.

The Email Server Spam and Virus Filter:

Layer 1: The Gateway Scan

As soon as an email arrives, our gateway servers try to match the sending IP address to an aggregated blacklist compiled from multiple spammer tracking systems. The servers analyze the email message in comparison to other arriving mail. If a large number of emails arrive simultaneously from a single IP, or are addressed to users that do not exist in our system, it could signify a spam attack, and the servers block the offending email.

Layer 2: Cloudmark® Scan

We scan all email with Cloudmark's industry-leading spam detection software. Cloudmark uses Advanced Message Fingerprinting™ to detect viruses, spam, and phishing. Advanced Message Fingerprinting uses algorithms that detect spam across all languages and character formats. These algorithms update every 60 seconds based on worldwide feedback loops and the latest spam tactics.

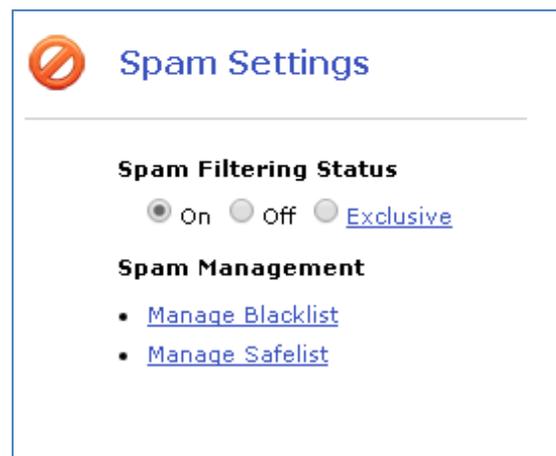
Layer 3: The Message Sniffer Scan

We scan email with Message Sniffer from ARM Research Labs. Message Sniffer relies on pattern recognition and machine learning technology to detect spam and malware. It searches the entire message for spam and malware features.

To manage your allowed senders (called “Safelists”) and your blocked senders (called “blacklists”), you need to login to your Exchange User Control Panel with your email address and password - <https://admin.emailsrvr.com/usercp/>

Scroll to the bottom of the page and look for the “Spam Settings” section. You can choose to turn off the spam filter, or set as exclusive so you only receive email from those on your Safelist, although neither of these settings are recommended.

Click on either Manage Blacklist or Safelist to add, edit or remove email addresses from those lists.



Outlook and the web based Outlook Web App (OWA) Junk Email Filter List

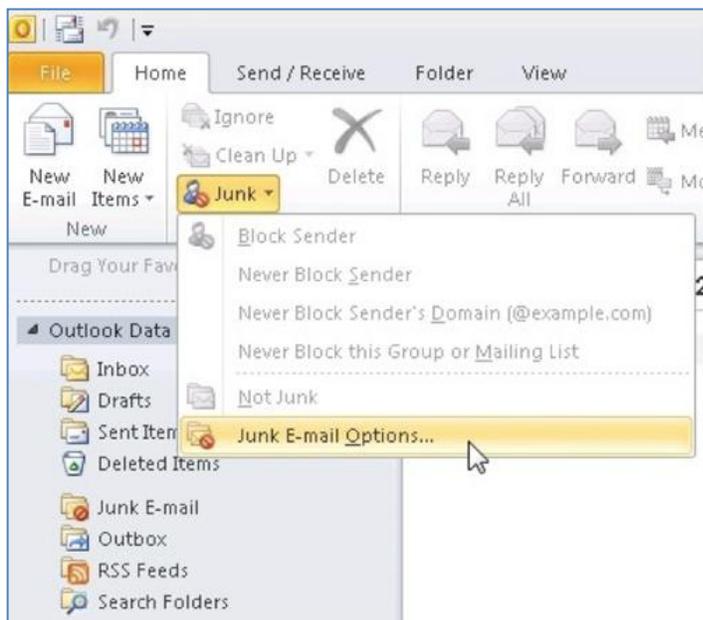
We recommend you regularly review messages in the Junk Email folder to check for legitimate messages that were incorrectly classified as junk. If you find a message that isn't junk, drag it back to the Inbox or any folder. You can also mark the item as not junk by doing the following:

Click Home > Junk > Not Junk.

By default, the Junk Email Filter is turned on and the protection level is set to No Automatic Filtering. You can make the filter more aggressive by changing the level of protection that it provides. The Junk Email Filter evaluates each incoming message based on several factors. These can include the time when the message was sent and the content of the message.

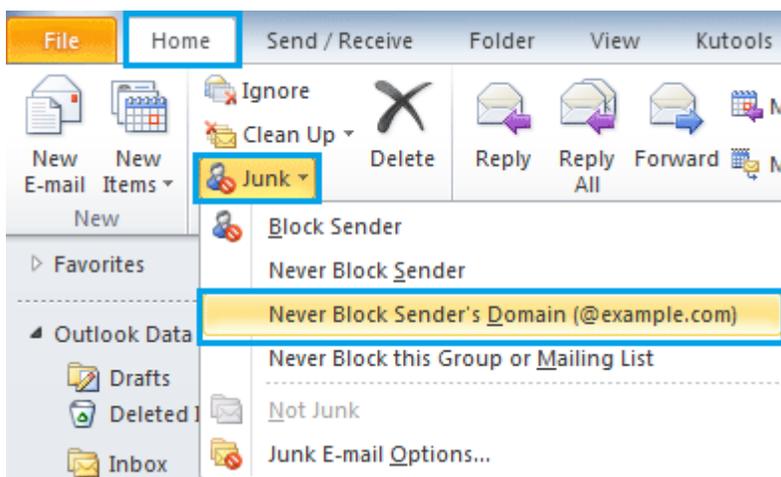
To change the options for the Junk Email Filter, do the following:

Click Home > Junk > Junk Email Options.



Junk Email Filter Lists

While the Junk Email Filter checks your incoming messages automatically, Junk Email Filter Lists let you control what is considered spam. You can add names, email addresses and domains to these lists so the filter doesn't check messages from sources you trust, or blocks messages that arrive from specific email addresses and domains you don't know or trust.



Safe Senders List Email addresses and domain names in the Safe Senders List are never treated as junk email, regardless of the content of the message. You can add your Contacts and other correspondents to this list. If you use a Microsoft Exchange Server account, all names and addresses in the global address list (GAL) are automatically considered safe.

Safe Recipients List If you belong to a mailing list or a distribution list, you can add the list sender to the Safe Recipients List. Messages sent to these email addresses or domain names are never treated as junk, regardless of the content of the message.

Blocked Senders List You can easily block messages from particular senders by adding their email addresses or domain names to the Blocked Senders List. When you add a name or email address to this list, Outlook moves any incoming message from that source to the Junk Email folder. Messages from people or domain names that appear in this list are always classified as junk, regardless of the content of the message.

Blocked Top-Level Domains List To block unwanted email messages from another country/region, you can add country/region codes to the Blocked Top-Level Domains List. For example, checking the CA [Canada], US [United States], and MX [Mexico] boxes in the list blocks messages from email addresses that end in .ca, .us, and .mx.

Blocked Encodings List To block unwanted email messages that appear in another character set or alphabet, you can add encodings to the Blocked Encodings List.

If you work online The Junk Email Filter Lists are saved on the server. They are available from any computer, but only if you have the Junk Email feature enabled in Outlook Web App.

The screenshot shows the 'block or allow' settings page in the Outlook Web App. On the left is a navigation menu with options: account, organize email, settings, phone, block or allow (highlighted), and apps. The main content area is titled 'block or allow' and contains two sections. The first section has two radio buttons: 'Don't move email to my Junk Email folder' (unselected) and 'Automatically filter junk email' (selected). The second section is titled 'safe senders and recipients' and includes the instruction 'Don't move email from these senders or domains to my Junk Email folder.' Below this is a list of entries, each with a pencil icon and a minus sign. The first entry has a text input field containing 'enter a sender or domain here'.