Overview of the Junk E-mail Filter in Outlook

(Much of this text is extracted from the Outlook Help files.)

Microsoft Outlook 2010 contains a Junk E-mail Filter designed to reduce unwanted e-mail messages in your inbox. Junk e-mail, also known as spam, is routed by the filter away from the Inbox instead to a Junk E-mail folder, where it can be more effectively managed.

How the Junk E-mail Filter works

The Junk E-mail Filter evaluates each incoming message to assess whether it may be spam, based on several factors. These can include the time when the message was sent and the content of the message. By default, the Junk E-mail Filter is turned on and the protection level is set to Low. This level catches only the most obvious spam. You can make the filter more aggressive by changing the level of protection that it provides.

NOTE The Outlook Junk E-mail Filter does not stop junk e-mail from being delivered, but rather diverts suspected spam to your Junk E-mail folder instead of your inbox.

You can control many of your Junk E-mail Filter settings with the Junk E-mail Options dialog box. From your Inbox, on the Home tab, in the Delete group, click the down arrow next to Junk and then click Junk E-mail Options.

Junk E-mail folder

Any message that is caught by the Junk E-mail Filter is moved to a special Junk E-mail folder. It is a good idea to periodically review the messages in the Junk E-mail folder to check for legitimate messages that were incorrectly treated as junk. If you do find legitimate messages, you can drag them back to the Inbox or to any folder.

You can delete the rejected messages by emptying the Deleted Items folder at any time.

Junk E-mail Filter Lists

While the Junk E-mail Filter checks your incoming messages automatically, the Junk E-mail Filter Lists give you more control over what is considered spam. You can add names, e-mail addresses and domains to these
lists so the Filter allows messages from sources that you trust, or blocks messages that arrive from specific e-mail addresses and domains that you don't know or trust.

**Safe Senders List**  E-mail addresses and domain names in the Safe Senders List are never treated as junk e-mail, regardless of the content of the message. You can add your Contacts and other correspondents to this list. If you use an Exchange 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 e-mail 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 e-mail addresses or domain names to the Blocked Senders List. When you add a name or e-mail address to this list, Outlook moves any incoming message from that source to the Junk E-mail folder. Messages from people or domain names that appear in this list are always treated as junk, regardless of the content of the message.

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

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

### Changing the level of junk e-mail protection

1. In Mail, on the **Home** tab, in the **Delete** group, click **Junk** and then click **Junk E-mail Options**.
2. On the **Options** tab, select the level of protection that you want:

- **No Automatic Filtering**  Although this turns off the automatic Junk E-mail Filter, Outlook continues to evaluate messages by using the domain names and e-mail addresses in your Blocked Senders List.

**NOTE**  If you want to completely stop junk e-mail filtering by Outlook, you must also **remove** names from the Junk E-mail Filter lists.

- **Low**  If you don’t receive many junk e-mail messages, or want to filter out only the messages that are most obviously junk, select this option.

- **High**  If you receive lots of junk e-mail messages, but do not want to restrict the messages that you see to those from senders on your safe lists, select this option. However, you should periodically **review messages moved to the Junk E-mail folder**, because some legitimate messages might also end up there.

- **Safe Lists Only**  If you receive lots of e-mail messages, you can select this option. Any e-mail message that is sent neither from someone on your Safe Senders List nor to a mailing list on your Safe Recipients List, will be treated as junk.

**Mark a message as not junk**
Depending on the Junk E-mail Filter protection level that you set, some legitimate e-mail messages might be moved to the Junk E-mail folder. For this reason, it is recommended that you periodically review messages moved to the Junk E-mail folder to ensure that you are not missing any messages that you want to see.

To mark a message as not junk, do the following:

1. In Mail, click the Junk E-mail folder in the Navigation Pane.

![Mail Folder](image)

**TIP** If you don't want to risk seeing objectionable content in the Junk E-mail folder, you can turn off the Reading Pane.

2. In the message list, click any message that you want to mark as not junk.


**Keyboard shortcut** To quickly mark a message as not junk, select the message and then press CTRL+ALT+J.

**NOTES**

- A message that is marked as not junk is moved back to its original folder, usually the Inbox. If you have more than one e-mail account, the message will be moved to the Inbox (or appropriate other folder) in the active e-mail account.

- When you mark a message as not junk, you are given the option of adding the sender or the mailing list name to your Safe Senders List or Safe Recipients List.

- By default, the Junk E-mail Filter is arranged by conversation. You can click on the conversation header and mark the entire conversation as not junk if the conversation is not expanded. You can mark individual messages in an expanded conversation.

- Any message that is sent to the Junk E-mail folder is kept there in plain text format, and any links that it contains are disabled. When you move the message out of the Junk E-mail folder, its original
message format is restored, and any links are enabled. Links remain disabled if the message is also categorized as suspicious.

**Junk E-mail Filter Lists**

Even though the Junk E-mail Filter filters your incoming messages automatically, you can control what is and is not considered spam by using the Junk E-mail Filter Lists. These lists enable you to allow or block messages that arrive from specific e-mail addresses and domains.

**Add trusted names to the Safe Senders or Safe Recipients Lists**

By adding e-mail addresses and domain names that you trust to the Safe Senders List, you instruct Outlook that messages from those sources are never to be treated as junk. If you belong to mailing lists or distribution lists, you can add these names to your Safe Recipients List.

To add a person to the Safe Senders List, click a message from the sender. On the Home tab, in the Delete group, click Junk and then click Never Block Sender.

To add a specific address or domain to the Safe Recipients List, click a message from the sender. On the Home tab, in the Delete group, click Junk and then click Never Block the Group or Mailing List.

To manually add names or domains to these lists, do the following:

1. On the Home tab, in the Delete group, click Junk and then click Junk E-mail Options.
2. Do one of the following:

- To add safe senders, on the Safe Senders tab, click Add.
- To add safe recipients, on the Safe Recipients tab, click Add.

3. In the Enter an e-mail address or Internet domain name to be added to the list box, enter the name or address that you want to add. For example, you can add:

- a specific e-mail address, such as someone@example.com
- an Internet domain, such as @example.com, or example.com.

4. Click OK and repeat for each entry you want to add.

- If you want all of your Contacts to be considered safe senders, select the Also trust e-mail from my Contacts check box in the Safe Senders tab.
Some people whom you correspond with might not be listed in your Contacts. If you want all such people to be considered as safe senders, select the **Automatically add people I e-mail to the Safe Senders List** check box.

If you have existing lists of safe names and addresses, you can move that information into Outlook. Click **Import from File** and browse for the list file that you want. To create a file with your current list, click **Export to File** and specify where you want the new file saved.

To change a name on either list, click the name that you want to change and then click **Edit**. To remove a name, click the name that you want and then click **Remove**.

If you are using a Microsoft Exchange account, all of the names and e-mail addresses that are in your organization’s address book — also known as the Global Address List — are automatically considered safe.

### Add unwanted names to the Blocked Senders List

Messages from addresses or domain names in the Blocked Senders List are always treated as junk. Outlook moves any detected incoming message from senders in the Blocked Senders List to the **Junk E-mail** folder, regardless of the content of the message.

**NOTE** The Outlook Junk E-mail Filter does not stop junk e-mail from being delivered, but instead diverts suspected spam to the Junk E-mail folder instead of your inbox. You can make the Junk E-mail Filter more strict by changing its level of protection.

To add a specific sender to the Blocked Senders List, click a message from the sender. On the **Home** tab, in the **Delete** group, click **Junk** and then click **Block Sender**.

To add names to the Blocked Senders List:

1. On the **Home** tab, in the **Delete** group, click **Junk** and then click **Junk E-mail Options**.
2. On the **Blocked Senders** tab, click **Add**.
3. In the **Enter an e-mail address or Internet domain name to be added to the list** box, enter the name or address that you want to add. For example, you can add:

- a specific e-mail address, such as someone@example.com
- an Internet domain, such as @example.com, or example.com.

4. Click **OK** and repeat for each entry you want to add.

**NOTES**

- If you have existing lists of safe names and addresses, you can move that information into Outlook. Click **Import from File** and browse for the list file that you want. To create a file with your current list, click **Export to File** and specify where you want the new file saved.

- To change a name on the list, click the name that you want to change and then click **Edit**. To remove a name, click the name that you want and then click **Remove**.

- If you are using a Microsoft Exchange account, all of the names and e-mail addresses that are in your organization’s address book — also known as the Global Address List — are automatically considered safe and cannot be added to the blocked list.

**Block messages from particular country/region codes**

You may find unwanted e-mail messages come from particular countries/regions. Outlook lets you block messages from those areas - the Blocked Top-Level Domains List lets you block messages from e-mail addresses that end in a particular top-level domain or country/region code. For example, selecting the **CA [Canada]**, **US [United States]**, and **MX [Mexico]** check boxes in the list blocks messages that come from e-mail addresses that end in ca, us or mx. Additional country/region codes appear in the list.
1. On the **Home** tab, in the **Delete** group, click **Junk** and then click **Junk E-mail Options**.

2. On the **International** tab, click **Blocked Top-Level Domain List**.

3. In the list, select the check box for the country/region code that you want to block, or click **Select All**.

4. Click **OK** twice.

### Block messages in unfamiliar alphabets

You can block all e-mail addresses in language encodings — also known as character sets, or alphabets — that you specify. Today, most junk e-mail is sent in the US-ASCII encoding. The remainder is sent in various international encodings. With the Blocked Encodings List, you can filter out unwanted e-mail messages that are displayed in languages that you don't understand.

1. On the **Home** tab, in the **Delete** group, click the arrow next to **Junk** and then click **Junk E-mail Options**.

2. On the **International** tab, click **Blocked Top-Level Domain List**.

3. In the list, click the language encoding that you want to block, or click **Select All**.

4. Click **OK** twice.
NOTES

Unicode encodings are not included in the Blocked Encodings List.

Messages that have unknown or unspecified encodings will be subject to filtering by the regular Junk E-mail

Filtering for phishing messages

The Junk E-mail Filter also automatically evaluates each incoming message to discover whether it might be suspicious, potentially fraudulent, or part of a phishing attack. For more information see, http://www.microsoft.com/protect/yourself/phishing/identify.mspx
10 tips on how to help reduce spam

Follow these guidelines to help lower your risk of receiving junk e-mail.

1. **Take advantage of the Junk E-mail Filter in Microsoft Office Outlook 2007** Office Outlook 2007 helps to mitigate the problem of spam by providing the Junk E-mail Filter, which automatically evaluates incoming messages and sends those identified as spam to the Junk E-mail folder.

2. **Block pictures in HTML messages that spammers use as Web beacons** Office Outlook 2007 has an additional anti-spam feature. By default, this feature blocks automatic picture downloads and other external content in messages if the content is linked to a server. If you open a message that has external content when this feature is turned off, the external content downloads automatically, inadvertently verifying to the server that your e-mail address is a valid one. Your e-mail address can then be sold to a spammer. You can unblock external content for messages that come from sources that you trust.

3. **Turn off read and delivery receipts and automatic processing of meeting requests** Spammers sometimes resort to sending meeting requests and messages that include requests for read and delivery receipts. Responding to such meeting requests and read receipts might help spammers to verify your e-mail address. You can turn off this functionality. However, read and delivery receipts and automatic processing of meeting requests are useful features that you should not be afraid to use within a secure corporate network.

   **NOTE** Delivery receipts can be turned off only by your e-mail server administrator.

   **Turn off read receipts**

   1. On the **Tools** menu, click **Options**.
   2. Click **E-mail Options**.
   3. Click **Tracking Options**.
   4. Under **Use this option to decide how to respond to requests for read receipts. Only applies to Internet Mail accounts**, click **Never send a response**.
**Turn off automatically acceptance of meeting requests**

5. In Outlook, on the **Tools** menu, click **Options**, and then click **Calendar Options**.

6. Under **Advanced options**, click **Resource Scheduling**.

7. Clear the **Automatically accept meeting requests and process cancellations** check box.

4. **Limit the places where you post your e-mail address** Be cautious about posting your e-mail address on public Web sites, such as newsgroups, chat rooms, bulletin boards, and so forth. When visiting public sites, you might want to use an e-mail address that is different from your main e-mail address. Remove your e-mail address from your personal Web site. Whenever you list or link to your e-mail address, you increase your chances of being spammed.

5. **Review the privacy policies of Web sites** When you sign up for online banking, shopping, or newsletters, review the privacy policy of the site carefully before you reveal your e-mail address or other personal information. Look for a link or section (usually at the bottom of the Web site’s home page) called "Privacy Statement," "Privacy Policy," "Terms and Conditions," or "Terms of Use." If the Web site does not explain how your personal information will be used, consider not using the services at that site.

6. **Watch out for check boxes that are already selected** When you shop online, companies sometimes add a check box that is already selected, which indicates that it is fine with you if the company sells or gives your e-mail address to other businesses (or "third parties"). Clear this check box so that your e-mail address is not shared.

7. **Don’t reply to spam** Never reply to an e-mail message — not even to unsubscribe from a mailing list — unless you know and trust the sender, such as when the e-mail message comes from a service, an online store, or newsletter that you have signed up with. Answering spam just confirms to the spammer that your e-mail address is an active one.

8. **If a company uses e-mail messages to ask for personal information, don’t respond by sending a message** Most legitimate companies will not ask for personal information to be sent in e-mail. Be suspicious if they do. Such a request could be a spoofed e-mail message disguised to look like a legitimate one. This tactic is known as **phishing**. If the possible spam appears to be sent by a company that you do business with — for example, your credit card company — then call the company to verify that they sent it, but don’t use any phone number that is provided in the e-mail. Instead, use a number that you find by using other means, such as directory assistance, a statement, or a bill. If the request is a legitimate one, the
company’s customer service representative should be able to assist you. The Junk E-mail Filter also includes *phishing protection* to help identify and disable suspicious messages.

9. **Don’t contribute to a charity in response to a request sent in e-mail**  Unfortunately, some spammers prey on your goodwill. If you receive an e-mail appeal from a charity, treat it as spam. If the charity is one that you want to support, locate their telephone number or Web site to find out how you can make a contribution.

10. **Don’t forward chain e-mail messages**  Besides increasing overall e-mail volume, by forwarding a chain e-mail message you might be furthering a hoax — and meanwhile, you lose control over who sees your e-mail address.