

How do I turn on the junk email feature?

Source: <http://www.tech-archive.net/Archive/Outlook/microsoft.public.outlook.general/2004-11/0958.html>

From: Chuck Davis (*anonymous_at_discussions.microsoft.com*)

Date: 11/03/04

Date: Tue, 2 Nov 2004 18:42:53 -0800

>-----Original Message-----

>I have microsoft xp and I want to filter out some of the junk email but

>outlook tells me that the junk email feature needs to be turned on, how do i

>do that?

>.

>

The following is from Outlook Help!

The new Junk E-mail Filter replaces the rules used in previous versions of Microsoft Outlook to filter e-mail messages. The Junk E-mail Filter is on by default, and the protection level is set to Low, which is designed to catch the most obvious junk e-mail messages. Any message that is caught by the Junk E-mail Filter is moved to a special Junk E-mail folder, where you can retrieve or review it at a later time. You can make the filter more aggressive, which may mistakenly catch legitimate messages, or you can even set Microsoft Office Outlook 2003 to permanently delete junk e-mail messages.

There are two parts to the Junk E-mail Filter: the Junk E-mail Filter Lists and the state-of-the-art technology developed by Microsoft Research that evaluates whether an unread message should be treated as a junk e-mail message based on several factors, such as the time it was sent and the content of the message. The filter does not single out any particular sender or type of e-mail message. The filter is based on the content of the message in general and uses advanced analysis of the message structure to determine the probability that it is a junk e-mail message.

Note Text marked with an orange asterisk (*) indicates a feature that is introduced with Microsoft Office 2003 Service Pack 1. To get Service Pack 1, go to Downloads on Office Online. Under Office Update, click Check for Updates.

Junk E-mail Filter Updates

Updates to the Junk E-mail Filter are available at Downloads on Office Online. Under Office Update, click Check for Updates.

Junk E-mail Filter Lists

There are five Junk E-mail Filter Lists: Safe Senders List (Safe Senders List: A list of domain names and e-mail addresses that you want to receive messages from. E-mail addresses in Contacts and in the Global Address Book are included in this list by default.), Safe Recipients List (Safe Recipients List: A list of mailing lists or other subscription domain names and e-mail addresses that you belong to and want to receive messages from. Messages sent to these addresses will not be treated as junk e-mail.), Blocked Senders List (Blocked Senders List: A list of domain names and e-mail addresses that you want to be blocked. E-mail addresses and domain names on this list are always treated as junk e-mail or spam.), and two International lists: Blocked Encodings List (Blocked Encodings List: A list that allows you to block a language encoding or character set in order to filter out unwanted international e-mail messages that display in a language you don't understand.) and Blocked Top-Level Domains List (Blocked Top-Level Domains List: A list that allows you to block top-level domain names. Blocking country/region top-level domains allows you to filter unwanted e-mail messages you receive from specific countries or regions.). If a name or e-mail address is on both the Blocked Senders List and the Safe Senders List, the Safe Senders List takes precedence over the Blocked Senders List; this reduces the possibility that messages that you want will be mistakenly marked as junk e-mail messages.

Safe Senders List If the filter mistakenly marks an e-mail message as a junk e-mail message, you can add the sender of that message to the Safe Senders List. E-mail addresses and domain names on the Safe Senders List are never treated as junk e-mail, regardless of the content of the message.

E-mail addresses in Contacts are included in this list by default. Therefore, messages from people in your Contacts folder will never be treated as junk e-mail messages. E-mail addresses of people who are not necessarily in your Contacts but are people whom you correspond with regularly are included in this list by default through the Automatically add people I e-mail to the Safe Senders List check box.

Notes

The recipient's e-mail address is saved by default only when you create and send the message the usual way in Outlook, as opposed to a message generated automatically by a program.

Personal distributions lists will not be added by using this check box.

If you accidentally reply to a spammer's e-mail message—for example, to unsubscribe—and this check box is selected, that spammer's address will be added to the Safe Senders List. If you notice the spammer's subsequent messages in your Inbox, you must add them to the Blocked Senders List and remove the corresponding entry from the Safe Senders List.

If the same address is in both the Blocked Senders List and the Safe Senders List, the Safe Senders List takes precedence and the address will not be considered junk.

If you are using a Microsoft Exchange Server e-mail account, names and e-mail addresses in the Global Address List (Global Address List: The address book that contains all user, group, and distribution list e-mail addresses in your organization. The administrator creates and maintains this address book. It may also contain public folder e-mail addresses.) are automatically considered safe.

You can also configure Outlook to accept messages only from people on your Safe Senders List, giving you total control over which messages are delivered to your Inbox.

Safe Recipients List If you belong to mailing lists or distribution lists, you can add these names to your Safe Recipients List so that any messages sent to these e-mail addresses or domain names will never be treated as junk, regardless of the content of the message.

Blocked Senders List You can easily block messages from a certain e-mail address or domain name by adding the sender to this list. Messages from people or domain names on this list are always treated as junk, regardless of the content of the message. When you add a sender's name or e-mail address to the Blocked Senders List, Outlook moves the message to the Junk E-mail folder.

If Automatic Picture Download is turned off, messages from or to e-mail addresses or domain names on the Safe Senders List and Safe Recipients List will be treated as exceptions and the blocked content will be downloaded.

If you have existing lists of safe or blocked names and addresses, you can import this information into Outlook 2003 by saving the list as a text (.txt) file with one entry per line, and then importing the list. If you want to

microsoft.public.outlook.general: How do I turn on the junk email feature?

share your Junk E-mail Filter Lists, create a copy for backup purposes, or print a list, you can export the e-mail addresses on the list to a text (.txt) file.

E-mail addresses are matched exactly, and specific address entries take precedence over domain name entries. To block an entire domain but still see specific safe addresses, add the specific entries to the Safe Senders List. For example, add `someonespecial@example.com` to the Safe Senders List and `@example.com` to your Blocked Senders List. This blocks any e-mail message you receive with `@example.com` in the e-mail address except `someonespecial@example.com`.

International List To block unwanted e-mail messages that come from another country or region or appear in another language, there are two lists.

Blocked Top-Level Domains List This list enables you to block e-mail addresses that end in a specific top-level domain (top-level domain: The broadest name category at the end of e-mail addresses. Generic top-level domains include `.com`, `.edu`, `.gov`, `.net`, and `.org`. Country code top-level domains use two letters, for example, `someone@example.us` and `someone@example.ca`). For example, selecting the CA [Canada], US [United States], and MX [Mexico] check boxes in the list would block messages with e-mail addresses like these: `someone@example.ca`, `someone@example.us`, and `someone@example.mx`. Additional country codes appear in the list. This helps you to eliminate unwanted e-mail messages that you receive from specific countries or regions.

Blocked Encodings List This list enables you to block all e-mail addresses in a specific language encoding (encoding: A method for representing characters in HTML or plain-text e-mail messages, examples include US-ASCII, Unicode (UTF-8), and Western European (ISO). Outlook automatically selects an optimal encoding for outgoing e-mail messages.), also known as a character set. Today, the vast majority of junk e-mail is sent in the US-ASCII encoding. The remaining junk e-mail is sent in various other international encodings, so this list gives you the ability to filter out unwanted international e-mail that is displayed in a language that you don't understand.

Notes

Unicode (Unicode: A character encoding standard developed by the Unicode Consortium. By using more than one byte to represent each character, Unicode enables almost all of the written languages in the world to be represented by using a single character set.) encodings are not included in the Blocked Encodings List.

Messages with unknown or unspecified encodings will be subject to filtering by the regular Junk E-mail Filter.

E-mail account types and the Junk E-mail Filter

The Junk E-mail Filter can be used with the following types of e-mail accounts:

A Microsoft Exchange Server e-mail account in Cached Exchange Mode

An Exchange Server account that delivers to a Personal Folders file (.pst) (Personal Folders file (.pst): Data file that stores your messages and other items on your computer. You can assign a .pst file to be the default delivery location for e-mail messages. You can use a .pst to organize and back up items for safekeeping.)

HTTP (HTTP (Hypertext Transfer Protocol): Protocol that is used when you access Web pages from the Internet. Outlook uses HTTP as an e-mail protocol.) (MSN Hotmail)

POP3 (POP3: A common protocol that is used to retrieve e-mail messages from an Internet e-mail server.)

IMAP (IMAP (Internet Message Access Protocol): Unlike Internet e-mail protocols such as POP3, IMAP creates folders on a server to store/organize messages for retrieval by other computers. You can read message headers only and select which messages to download.)

Microsoft Office Outlook Connector for IBM Lotus Domino
Outlook Connector for MSN

All e-mail accounts in the same Outlook user profile (Outlook user profile: A group of e-mail accounts and address books. Typically, a user needs only one but can create any number, each with a set of e-mail accounts and address books. Multiple profiles are useful if more than one person uses the computer.) share the same Junk E-mail settings and lists. If you have both an Exchange Server e-mail account and a Hotmail account, each e-mail account has a Junk E-mail folder. However, if you have both an Exchange Server e-mail account and a POP3 account, both e-mail accounts use the same Junk E-mail folder.

If you change your profile, you should export a copy of your Junk E-mail Lists before making the changes, and then import the information into Outlook 2003 to avoid having to re-create your Junk E-mail Filter Lists.

Different versions of Microsoft Exchange Server and the Junk E-mail Filter

Versions earlier than Microsoft Exchange Server 2003

If you use Cached Exchange Mode or download to a Personal Folders file (.pst) You can create and use the Junk E-mail Filter Lists, which are stored on the server and

microsoft.public.outlook.general: How do I turn on the junk email feature?

available from any computer that you use. Note that if you use both Cached Exchange Mode and download to a Personal Folders file (.pst) as your default delivery location, the Junk E-mail Filter Lists will be available only on the computer used to add the names and addresses.

If you work online The Junk E-mail Filter is not available.
Exchange Server 2003

If you use Cached Exchange Mode or download to a Personal Folders file (.pst) The Junk E-mail Filter Lists are stored on the server and are available from any computer. They are also used by the server to evaluate messages. This means that if a sender is on your Blocked Senders List, messages will be moved to the Junk E-mail folder on the server and not evaluated by Outlook 2003.

If you work online The Junk E-mail Filter Lists are stored on the server and are available from any computer. They are also used by the server to evaluate messages. This means that if a sender is on your Blocked Senders List, messages will be moved to the Junk E-mail folder on the server and not evaluated by Outlook 2003.

Note If you work online or use Cached Exchange Mode and download to a Personal Folders file (.pst) as your default delivery location, the Junk E-mail Filter Lists will be available only on the computer used to add the names and addresses.

Rules and the Junk E-mail Filter

Rules are now designed so that they do not act on messages that have been moved to the Junk E-mail folder. This keeps e-mail considered to be junk in the correct place rather than moving it to another folder according to the rule.

Best practices for managing junk e-mail

Increase your protection level as you need to To obtain the maximum protection possible from using the Junk E-mail Filter and other enhanced privacy features, set the protection level of the Junk E-mail Filter to High or to Safe Lists Only.

Keep your Junk E-mail Filter updated Updates are available at Downloads on Office Online. Under Office Update, click Check for Updates.

Block images in HTML messages that spammers use as Web beacons A Web beacon can be a graphic image, linked to an external Web server, that is placed in an HTML-formatted message and can be used to verify that your e-mail address is valid when the message is opened and images downloaded.

By default, Outlook is set to block automatic picture downloads. To verify what your automatic download settings are, on the Tools menu, click Options. Click the Security

tab, and then click Change Automatic Download Settings.

Verify that the Don't download pictures or other content automatically in HTML e-mail check box is selected.

Turn off automatic processing of meeting requests and read and delivery receipts Spammers sometimes resort to sending meeting requests and messages with delivery receipts requested. Responding to meeting requests and read and delivery receipts automatically makes you vulnerable to Web beacons.

Limit where you post your e-mail address Be cautious about posting your e-mail address on public Web sites, and remove your e-mail address from your personal Web site. If you list or link to your e-mail address, you can expect to be spammed.

Disguise (or "munge") your e-mail address when you post it to a newsgroup, chat room, bulletin board, or other public places For example, you can give your e-mail address as "s0me0ne@example.c0m" by using the number zero instead of the letter "o." This way, a person can interpret your address, but the automated programs that spammers use cannot.

Use multiple e-mail addresses for different purposes You might set up one for personal use to correspond with friends, family, or colleagues, and use another for more public activities, such as requesting information, shopping, or for subscribing to newsletters, discussion lists, and newsgroups.

Review the privacy policies of Web sites When you sign up for online banking, shopping, and newsletters, review the privacy policy closely before you reveal your e-mail address and other personal information. Look at the Web site for a link (usually at the bottom of the home page) or section called "Privacy Statement," "Privacy Policy," "Terms and Conditions," or "Terms of Use." If the Web site does not explain how it will use your personal information, think twice about using that service.

Watch out for check boxes that are already selected When you buy things online, companies sometimes add a check box (already selected!) to indicate that it is fine to sell or give your e-mail address to other businesses (third parties). Clear the check box so that your e-mail address won't be shared.

Don't reply to spam Don't reply even to unsubscribe unless you know and trust the sender. Answering spam just confirms that your e-mail address is live.

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 in e-mail. Be suspicious if they do. It could be a spoofed e-mail message meant to look like a legitimate one. This tactic is known as "phishing" because, as the name implies, the spam is used as a means to "fish" for your credentials,

such as your account number and passwords that are necessary to access and manipulate your financial accounts. If the spam is from a company that you do business with – for example, your credit card company – call the company, but don't use a phone number provided on the e-mail. Use a number that you find yourself, either through directory assistance, a bank statement, a bill, or other source. If it is a legitimate request, the telephone operator should be able to help you.

Don't contribute to a charity based on a request in e-mail

Unfortunately, some spammers prey on your good will. If you receive an appeal from a charity, treat it as spam. If it is a charity that you want to support, find their number elsewhere and call them to find out how you can make a contribution.

Don't forward chain e-mail messages Besides causing more traffic over the line, forwarding a chain e-mail message might be furthering a hoax, and you lose control over who sees your e-mail address.