

Configuring Spam Filter

To configure the spam filter for a mailbox:

1. On your Home page, click **Mail** in the **Services** group.
2. Click the e-mail address you need.
3. Click **Spam Filter** in the **Tools** group. Configure the following settings as desired:
 - **Use server wide settings.** Select this option if your provider or server administrator has prepared black and/or white lists of e-mail addresses that you would like to use together with your own restrictions. Black list, shown under **Black list** group, includes e-mail addresses of spammers, and White list, shown under **White list** group, includes e-mail addresses of trustworthy correspondents or entities. If the **Use server wide settings** check box is grayed out, i.e. not selectable, this means that there are no preconfigured spam filter settings on the server.
 - **Hits required for spam.** This setting adjusts spam filter sensitivity. SpamAssassin performs a number of different tests on contents and subject line of each message. As a result, each message scores a number of points. The higher the number, the more likely a message is spam. For example, a message containing the text string "BUY VIAGRA AT LOW PRICE!!!" in Subject line and message body scores 8.3 points. By default, the filter sensitivity is set so that all messages that score 7 or more points are classified as spam.
 - If you receive lots of spam messages with the current setting, to make filter more sensitive, try setting a lesser value in the **Hits required for spam** box; for example, 6.
 - If you are missing your e-mails because your spam filter thinks they are junk, try reducing filter sensitivity by setting a higher value in the **Hits required for spam** box.

Note: To further improve spam filter accuracy, you may want to train your spam filter on e-mail messages you receive (see the instructions on improving accuracy of spam detection below).

 - **What to do with spam mail.** If you are sure that your spam filter is accurate, you may want to set the filter to automatically delete all incoming messages recognized as spam. To do this, select the **Delete** option. If you wish to filter mail with the software on your local computer, select the **Mark as spam and store in mailbox** option, and then specify how spam filter should mark the messages recognized as spam. "X-Spam-Flag: YES" and "X-Spam-Status: Yes" headers are added to the message source by default, and if you want, the spam filter will also include a specific text string to the beginning of Subject line.
4. To save your changes, click **OK**.

5. If you do not want to receive e-mail from specific senders, add their e-mail addresses to the spam filter's black list.
 - To add an entry to the black list, under **Black list** group, type an e-mail address into the **E-mail pattern** box. For example:
address@spammers.net, *@spammers.net. An asterisk (*) means any combination of symbols. Click **Add**.
 - To remove an entry from the black list, select it and click **Remove**.
6. If you want to be sure that you will not miss e-mail from specific senders, add their e-mail addresses to the spam filter's white list.
 - To add an entry to the white list, under **White list** group, type an e-mail address into the **E-mail pattern** box. For example:
address@mycompany.com, *@mycompany.com. An asterisk (*) means any combination of symbols. Click **Add**.
 - To remove an entry from the black list, select it and click **Remove**.
7. If you want spam filter to consider some networks to be trusted:
 - Select the **Trusted Networks** tab.
 - To add an entry to the list, enter a network address into the fields next to **Network/Mask** and click **Add**.

A network is specified by its starting IP address in the first four fields of the **Network/Mask** field group. The fifth field is for specifying network mask. It should be a number ranging from 1 to 32, which shows how many higher bits set to '1' the mask contains. For example, for the mask 255.255.255.0 you should specify 24 as the fifth parameter.




- To remove an entry from the list, select a network and click **Remove**.

The relay hosts on trusted networks are considered not to be potentially operated by spammers, open relays, or open proxies. A trusted host could conceivably relay spam, but will not originate it, and will not forge header data. DNS blacklist checks will never query for hosts on these networks.

Improving Accuracy of Spam Detection

To improve the accuracy of spam detection:

1. On your Home page, click **Mail** in the **Services** group.
2. Click the e-mail address you need.
3. Click the **Spam Filter** icon in the **Tools** group.
4. Click the **Training** icon in the Tools group.

All e-mail messages you have in your mailbox are presented on the screen. Each message is accompanied by an icon in the left column, which tells if a message is recognized as spam - , non-spam - , or not recognized at all - . If you

have already trained your spam filter on a message and the results were recorded in the spam filter's database, an icon is shown in the right column.

5. Train the spam filter.

In most cases, you can tell if a message is spam by looking at its subject line and sender's name. If they do not give you any clue, try looking inside the message using your e-mail program or Webmail interface.

- To mark a message as spam, select the corresponding check box and click **'It's Spam!'**.
- To mark a message as not spam, select the corresponding check box and click **'It's Not Spam!'**.
- To remove any information on a given message from the spam filter database, select the corresponding check box and click **'Forget It!'**.

Once finished with training, you can remove spam e-mails from your mailbox using your e-mail program or Webmail interface.