What to do when I receive spam?

Question:

What can I do when I receive spam?

Answer:

First check whether the e-mail is filtered by SpamExperts. If so, you will find a line in the e-mail headers that starts with *X-SpamExperts-Class*. Is this line not present? The the spam filter was not used. Possible causes can be:

You configured SpamExperts less than 48 hours ago; the DNS system uses caching mechanisms that store some data locally to prevent overload of the nameservers. This might result in temporarily outdated data.

- Check whether *only* the SpamExperts MX records have been added in your DNS zone, and no other MX records. Check this by going to the Openprovider reseller control panel, menu **DNS management>DNS checks**.
- Some spammers remember old mail servers for a long time. That can cause old mail servers to be used long after you changed them to SpamExperts.
- Sometimes spammers just try to be lucky by using an ordinary hostname like *mail.yourdomain.com* to send spam, so that the official MX records are bypassed.

If *X-SpamExperts-Class* is included in the headers, but the value is *whitelisted*, then you or the e-mail user whitelisted the sender. Other values for this field are *ham* or *unsure*; in those cases, SpamExperts was not sure enough to categorize the e-mail as spam.

Note that an expired (non-renewed) bundle will automatically whitelist 'all' senders! See for more information our article about expiration of a spam filter bundle.

When a spam message has been delivered despite of the filtering, you can train the spam filter by the button *Report spam* in the SpamExperts control panel. Here, you can upload the original e-mail

in .txt or .eml format. The Microsoft Outlook .msg format cannot be used!

Revision #2
Created 2026-08-07 14:59:41 UTC by Sarath
Updated 2026-08-07 16:05:53 UTC by Sarath