We use two popular spam filters in conjunction for spam detection at the transport stage of mail processing:

1. Spamassassin for **SPAM filtering**, which uses a variety of deterministic rules in conjunction with statistical decision making to classify mails as
SPAM
or
Ham
.

2. DSPAM , which is entirely based on user specific statistical spam learning (Bayesian spam filtering
)

The statistical SPAM filters do make occasional mistakes and users are advised to check their ~/**mail**/**SPAM**
folder regularly. The spam detection rules are updated on a daily basis.

Statistical training of the DSPAM filters is enabled for every user. Initially, when the statistical filters of DSPAM are not trained, it will not detect any spams. For the statistical filters to be effective it is essential for DSPAM to be trained with a large number of examples and the detection accuracy is supposed get better with time. It is reported that the DSAPM filters become very effective with about one months training for most users. The statistical training can be done with the following method:

One may move the undetected SPAMs to a folder called ~/**mail**/**missed-spam** and *copy* the mails incorrectly detected as SPAMs to a folder called
~/**mail**/**not-spam**
, and individualistic Bayesian training will be turned on by default. There must be at least a 100 false negatives in the cumulative training set before Bayesian learning can come in to effect. The learnt messages will be purged automatically.

We use **Amavis** **and** **Clamav** **based virus scanning** for both inbound and outbound mails. The virus definitions are automatically updated on a daily basis. All mails which are detected to contain a virus are purged outright and not delivered.