Coping with Spam Using Filters

by Carl Fitch
cfit@sluug.org

I Get Spam!

I am an officer of an established computer club that has five other clubs that we support as members. I receive mail from more than eight positions in all of those groups
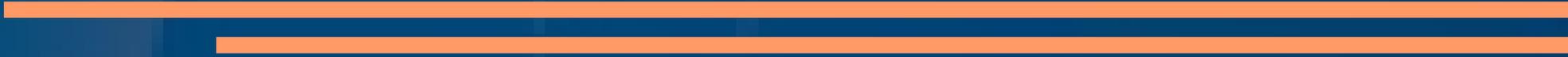
SMTP Filters

We have instituted several spam filters, greylisting etc

I STILL GET SPAM!

The following is what I do to lessen the effects. It may not stop the spam but it makes it easier to deal with
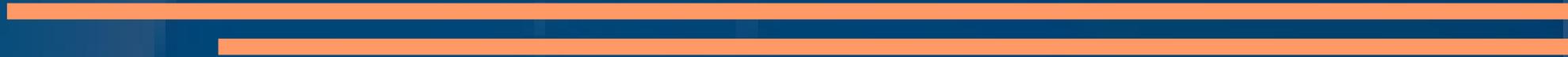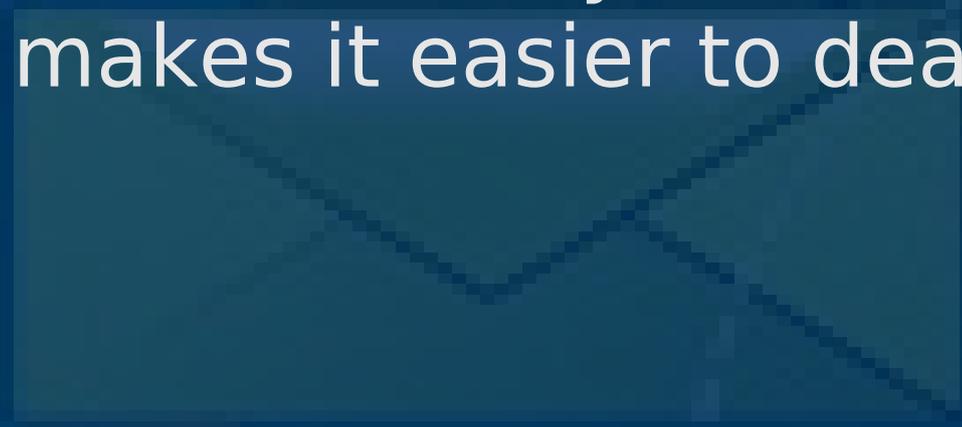
Location of Filters

Thunderbird

Tools

Message Filters

Outlook

Tools

Message Rules

Mail
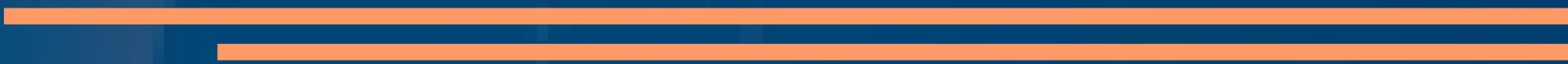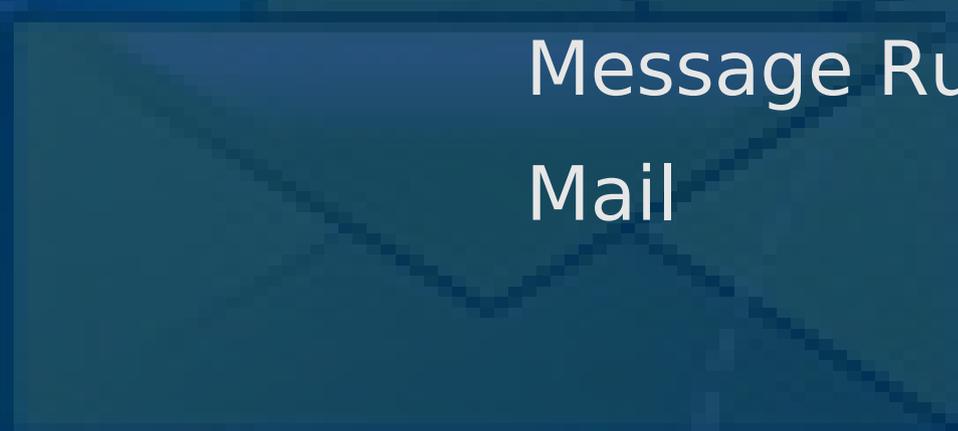
Turn off HTML

Thunderbird

View

Message Body As

Plain Text

Outlook

Tools

Options

Read

"Read all messages in plain text"

Use the Filters, Luke

Set filters to sort mail according to conditions:

- By key word

- By group

- By sender

The last filter routes remaining messages into the folder "Unknown"
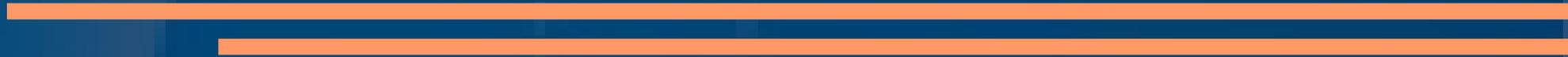
The Unknown Filter
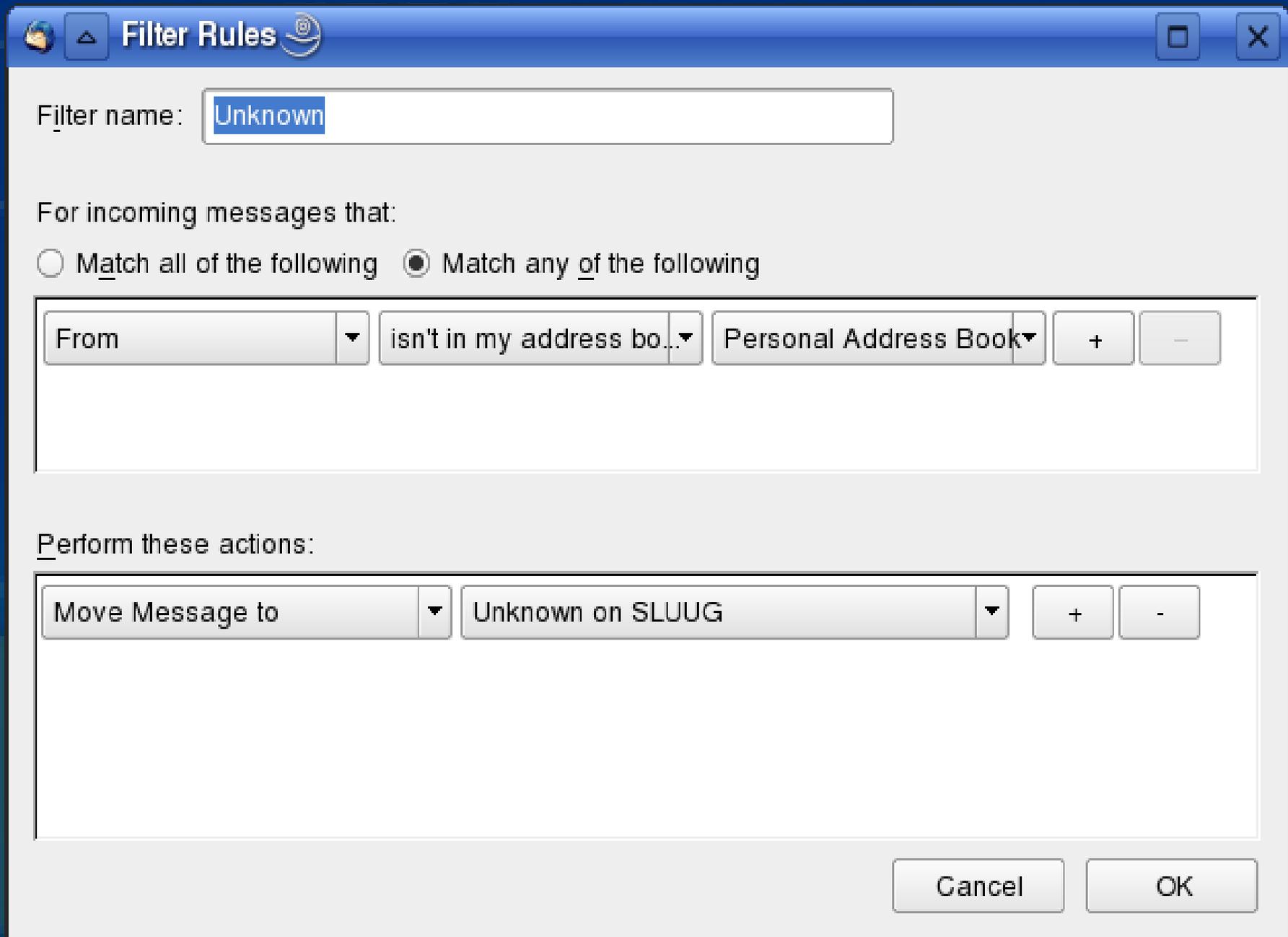
Filter Rules

Filter name: Unknown

For incoming messages that:

○ Match all of the following   ● Match any of the following

| From ▼ | isn't in my address bo... ▼ | Personal Address Book▼ | + | − |

Perform these actions:

| Move Message to ▼ | Unknown on SLUUG ▼ | + | - |

Cancel   OK

Don't Waste Bandwidth on the Body

Thunderbird

Edit

Account Settings

Server Settings

Fetch headers only.

Outlook

Need example

If you use POP 3

In folders you want to see the mail from:
In Thunderbird
    Tools
        Message Filters
        (Select the filter) Edit.
    In "Perform these actions" box add "Move Message to" if
      you don't have that already.
    Now click the "+" box to add another rule
    In that rule select "Fetch from POP server"
    Now those messages will be downloaded
    They won't be for Inbox and Unknown

View Unread Only

Junk folder - select "View Unread Only"

Scan the headers and senders

Move any false positives and add those to your address book

Look at the Senders Address

If you think an Unknown might be legitimate:
Don't download the message yet, look at the senders address
Thunderbird, right click on "From:{email address}"
Typically you won't see your bank having a return address ending with .ru
If it is from someone you want to receive email from select "Add to Address Book" so they won't end up in Unknown again

Create a filter from "Add to Address"

At the same time you can create a filter from this message from the right click menu
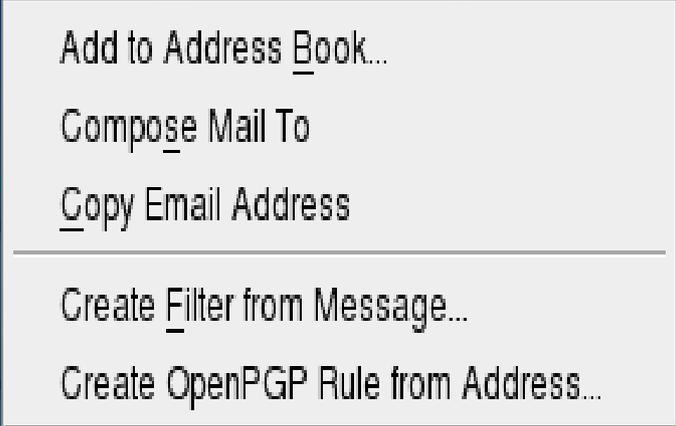
Add to Address Book...

Compose Mail To

Copy Email Address

Create Filter from Message...

Create OpenPGP Rule from Address...

Be careful to not create too many filters

Occasionally you should review your filters to see if some should be consolidated or repositioned

Rule Position

The position of a rule will determine application

The first filter to match takes precedence
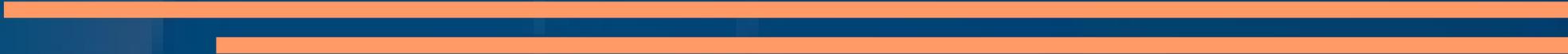
Relax

Once you have your filters set up properly, it will be easy to distinguish the email from your mother-in-law with the subject "You Must Read This" from one with the same title from Korea or Russia

Junk Mail Log

When junk mail controls are first turned on I suggest that the Junk mail log be turned on
This allows a review of what has been determined as junk and what folders it has used
It is important to review the log often and clear it after review when first starting junk mail controls
Once it is working as expected turn the log off
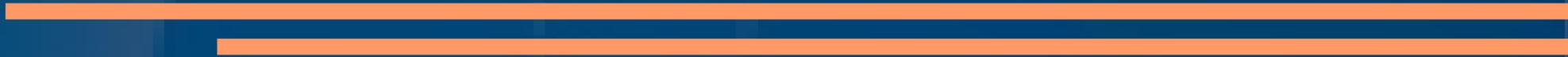
Mark Read

To mark all messages as read - right click on page and select

Mark

All Read (faster press shift-c)
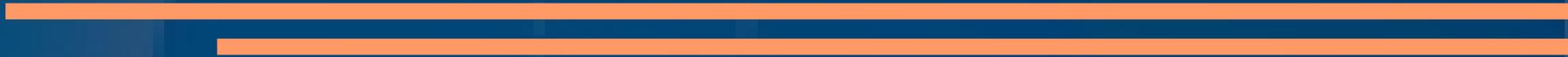
Mark Junk

To mark all messages as junk select

Edit

Select (or press and release Alt-a then j)
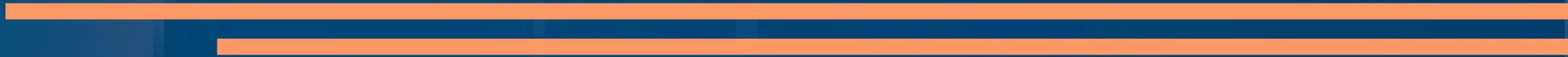
Running on Empty Headers

This way you only have "Junk mail controls" running on headers only

This really helps me because I get so many with similar headers

Once I select the first one the rest are gone before I see them

For those that the Junk mail filter does not catch in Unknown, I select all (Alt-a) mark as junk (j) and viola they are gone

These rules won't stop spam!

It just makes it less troublesome.