



# Canning the spam

Nigel Whitfield has tips on **taking spam off the menu**, and the plans to rid the world of it altogether.

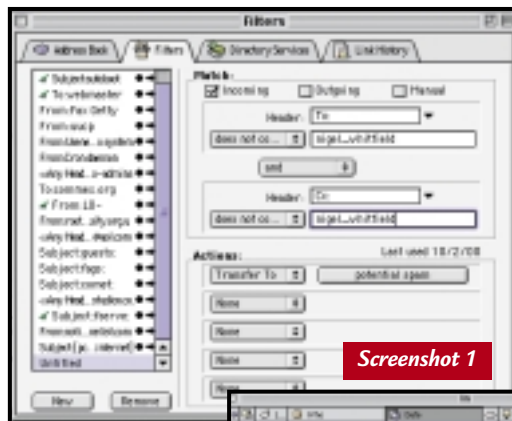
**S**pam – or unsolicited email – is one of the most irritating aspects of using the Internet. If you have an email address, the chances are that you'll have received plenty of junk mail already, some of it commercial, some not – but curiously, the bulk of it advertising programs to help send more of the stuff!

Regardless of what it's about, it's annoying. Fortunately, while you can't completely avoid it, there are ways of making sure that you see as little of it as possible, since most modern email packages have tools that will let you filter your email as it arrives.

The same tools, in fact, can be applied to the rest of your email, dropping messages from certain users into a particular folder, or just deleting them unread.

After you've signed on to your ISP and discovered 60 messages, more than half of which are junk mail, you might decide that you just want to send lots of junk back – and people have been known to send their whole Windows swap file to a persistent junk emailer.

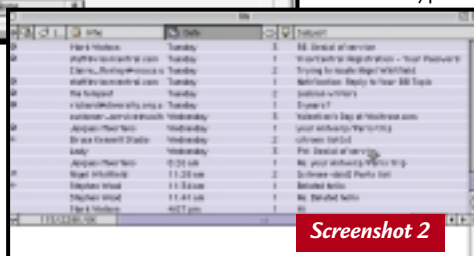
Don't! It's rarely worth responding to



Screenshot 1

the sender of a junk email message.

More often than not, you'll find that the address doesn't work, either because it was invalid to start with, or because it has been cancelled by the ISP once it started to receive complaints. And when an address does work, you'll often simply be confirming that yours is a valid email address; far from removing it from a list, it's likely to end up on more.



Screenshot 2

The best solution, if you want to do something, is to try and complain to the relevant people, in the hopes that the sender of the junk email will lose their account. And, if it's a genuine company that is trying to interest you in business, point out to them that they should consider that you're paying for their junk, and don't do business with them. This isn't the type of news that the

direct marketing guys like to hear, but then we're the people who are paying for their trash.

In some cases, you may even have legal redress against people who send you junk email; the box below explains the different ways you can obtain some protection. And on the following page you can see how a look at the headers of a message may give you some ideas

## Barriers to spam

**D**irect Marketing – the sending of promotional literature directly to buyers – is nothing new. With email, however, the recipient bears the largest proportion of the cost.

Some states in the US, such as Washington, have already made it illegal to send junk mail. The EU, however, has followed the lead of the marketing people, and proposed an opt-out method. In other words, if you don't want to pay to receive junk mail, it's up to you to say so.

Unsurprisingly, this approach is not popular with many Internet users. The Direct Marketing Association provides an email preference service. This lets you sign up on a website ([www.e-mps.org](http://www.e-mps.org)) to say that you don't want to receive junk email for a period of a year. DMA members are supposed to use the service to purge their address lists of people who have opted out. It's not compulsory and any company ignorant enough to send junk email is not likely to be a member.

One solution is more laws such as those in Washington State, which protect email recipients who live there, and make those who send them spam liable for fines of up to \$25,000 – assuming it's possible to track down the culprit.

From 1 March this year, there may be some redress, through the 1998 Data Protection Act, which lays down rules for the processing of personal information. Companies that send junk email could fall foul of the Act, but initially they'll simply

receive an enforcement notice. Only if they fail to comply will they risk prosecution and a fine of £5,000 in a Magistrates Court, or unlimited fines in the Crown Court.

For more information on campaigns for legislations, check out the Coalitions Against Unsolicited Commercial email ([www.cauce.org](http://www.cauce.org)) and Suespammers, at [www.sue-spammers.org](http://www.sue-spammers.org), which is a group helping people with prosecutions, and the Data Protection Registrar at [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)

## Reading between the lines

When you receive a piece of junk mail, your first instinct may be to look at the sender's address and fire off a furious response to their ISP – but it's seldom as simple as that.

The addresses given on most pieces of junk email are false – sometimes just to stop complaints, or sometimes to deliberately direct irate mail back to an unfortunate victim.

You can't always find out who really did send junk email, but looking at the headers of a message may give you some clues. Here are the headers of a recent message:

**Return-Path:**

<oywb@oywbxi.net>

**Received: from**

punt-1.mail.demon.net  
by mailstore

id 949771223:10:02466:3;

Sat, 05 Feb 2000

17:20:23 GMT

**Received: from**

ohc.oto.bcm.tmc.edu

([128.249.51.43]) by

punt-1.mail.demon.net

id aa1002346;

5 Feb 2000 17:20 GMT

**Received: from**

ppp226-as5.lsanca.ni.net

by ohc.oto.bcm.tmc.edu

(AIX 3.2/UCB 5.64/4.03)

id AA22333; Sat, 5 Feb 2000

11:04:00 -0600

**Date: Sat, 5 Feb 2000**

11:04:00 -0600

**From: oywb@oywbxi.net**

**Message-Id:**

<10002051704.AA22333

@ohc.oto.bcm.tmc.edu>

The From address here isn't even a valid domain – although you'll often see spammers using domains such as aol.com or

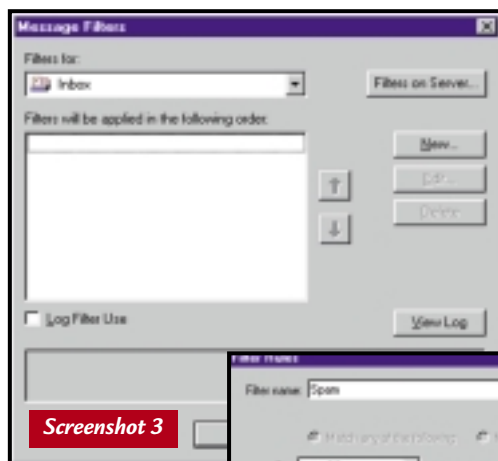
hotmail.com. Each system that the message passes through adds a Received: line at the top of the message, so the lowest one is – usually – where the email originated. In this case, it appears to be a dialup connection – ppp226-as5.lsanca.ni.net. So, abuse@ni.net would be a good place to start complaining because, if the ISP doesn't know a spammer is using one of its accounts, it can't do anything about the abuse.

Some people, however, are clever – they'll put a fake Received: line in their message before it's sent. That can make it harder to track things down but, once again, there are clues. For example, if there's no Message-ID supplied, the first real computer to see the message

will add one – in this case it was done by ohc.oto.bcm.tmc.edu, which would be able to find out from its system logs where the mail originated.

And if there's a discrepancy in the Received lines, between the name and the numeric address of a system, then that's usually also commented – but it's not necessarily proof of anything more than a badly configured email system.

If you don't want to wade through the message headers yourself and track down who to complain to, take a look at SpamCop ([www.spamcop.net](http://www.spamcop.net)) which will try to find out the addresses and send complaints for you automatically.



Screenshot 3

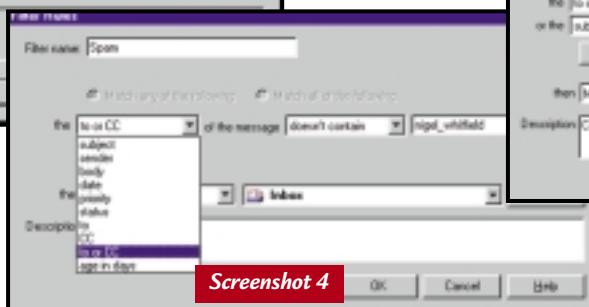
about which address was really used to mail you, and where a message actually came from – vital information if you want to complain to the sender's ISP.

All that information might help you get even, but in the real world, you're still going to receive spam. So, how do you set up your email program to see as little of it as possible?

There are various things you can do,

as long as your email program has filtering, but sadly none of it is foolproof. Most spam, however, has one feature that can make it easy to shift – it doesn't include your email address in the To or Cc fields of the message. So, if your address doesn't appear there, there's a

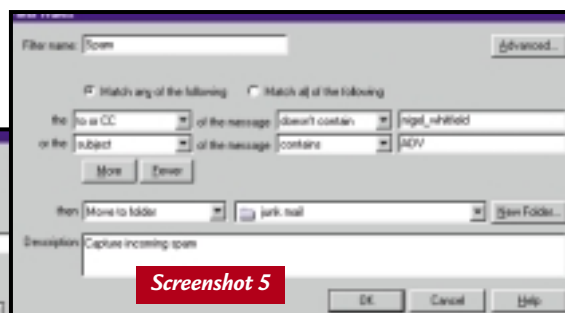
your email program. Mailing lists, for example, may put the name of the list in the subject line, so you can filter them into a folder easily. And you could set up a folder for each person you email regularly, to put their messages to one side with a simple rule.



Screenshot 4

good chance you might not be receiving personal email – but it could still be a mailing list, for example, or a newsletter-type mail from a friend who has sent it to lots of people in one go.

It's as well to think of things like this, and plan before you use lots of filters in



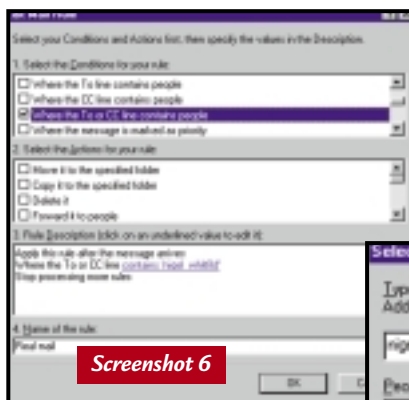
Screenshot 5

Only when you've sorted the real messages is it time to start the risky stuff – such as deleting, or moving to a 'spam' folder, the messages that don't appear to be personal. Yes, you can delete messages immediately, but we'd recommend first putting them in a folder, so you can skim through and make sure there's nothing in there that really is for you.

So, work out where you want mail for different people to go; create folders for



## workshop: spam



Screenshot 6

them, and then set up the filters. Here's how to do just that to catch spam in three of the most popular programs.

### Eudora 4

We've used the latest beta version of Eudora, in Sponsored Mode, which has good filtering facilities. It's worth upgrading from Eudora Lite, but you will see adverts in a window on the screen.

You can create a filter by choosing Filters from the Window menu. Click on New, and set the options for your filter. First, choose To as the field, and then 'does not contain' and type in your email address (screenshot 1 on the first page).

Add a second condition, selecting 'and', and set it identically to the first, except for the header field, which you should set to Cc. For action, select Transfer, and then choose a folder from the Transfer menu – we've created a new one called Potential Spam.

If you selected 'Manual' as well as 'Incoming' for the filter, you can test it by selecting all the messages in your 'in box' (screenshot 2), then choosing 'Filter' from the Special menu. If everything's working OK, you'll see suspect messages moved out to a folder of their own.

We've not used the option to check 'Any header' as some ISPs will include your email address in the Received: lines.

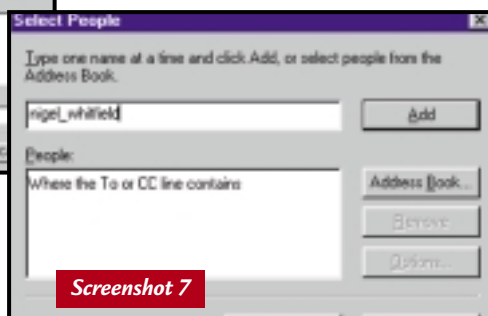
You can also use other rules. For example, checking for messages with the phrase ADV in the subject (which is short for 'advert').

### Netscape Communicator

From the Edit menu in Netscape Messenger, choose Message Filters (screenshot 3). This is the screen you'll see if you've not set up filters already. If you have multiple filters, you can change their order – make sure the spam filtering is done last, after you've sifted out

mailing lists you subscribe to, and personal messages from regular correspondents.

Netscape allows you to search the To and Cc fields of your message in one go, with the 'To or CC' option, so select that, then choose 'Does not contain', and type

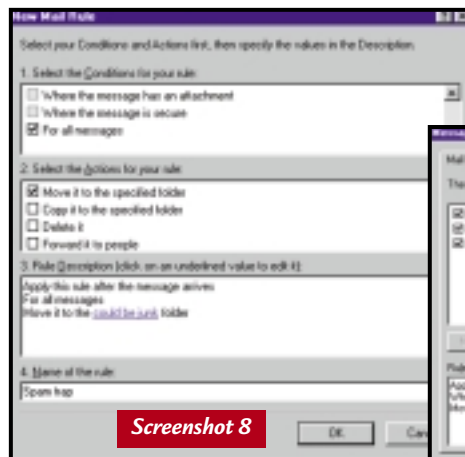


Screenshot 7

your email address (screenshot 4).

If there's only one set of rules you're using, it doesn't matter if you choose the 'Match any' or 'Match all' options. Select a folder for the junk mail, and type a description of the filter if you like (screenshot 5).

We're also going to filter messages that have the word 'ADV' in the subject.



Screenshot 8

Some spammers reckon this makes them magically immune from complaints because, by identifying the mail as an advert, they are alerting you to the content before you open the email. Click the More button beneath the first rule you entered, choose subject, then contains, and type ADV.

Make sure that the rule is set to 'Match any' of the criteria, rather than 'Match all'. Click OK when you're done, and Communicator will filter messages as they are downloaded from your ISP.

### Outlook Express 5

Outlook Express 5 has rather peculiar

rules in that there isn't a straightforward way to look for something that isn't in a message header. Instead, we'll need two rules to do the job.

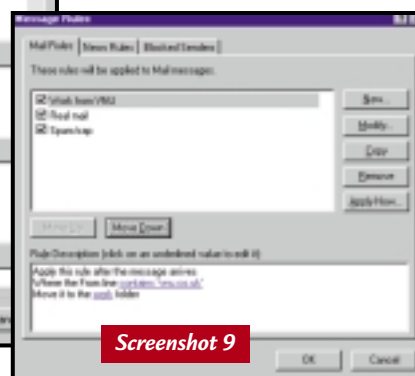
From the Tools menu, choose Message Rules, then Mail. Create a rule by choosing 'Where the To or CC line contains people'. Under actions choose 'Stop processing more rules' (screenshot 6).

At the bottom of the window, Outlook will be building up a description of the rule. Click on 'certainpeople' and type in your address here, click Add, and then OK (screenshot 7). Give the rule a name such as 'Real mail', and then click on OK.

Now we need another rule to move messages that didn't fit the criteria of the first one to a new folder. First, click on New from the list of rules, and choose 'For all messages', then 'Move to a specified folder'. Next, create or choose a folder for junk mail, and then save the rule as 'Spam trap' (screenshot 8).

This is the list of rules we have installed – you'll need all your other rules at the top of the list, and the two to catch spam right at the bottom. Use the move buttons to change the order if necessary (screenshot 9).

The reason we have not used



Screenshot 9

the Blocked Senders option is that it's not really much use for spam – you can stop someone who regularly sends you mail from a specific domain – such as Microsoft.com – however, if you don't know who is going to be sending you junk mail, you will have to use rules such as the ones we created instead.

## CONTACTS

Nigel Whitfield welcomes your comments. Contact him via the PCW editorial office or email [internet@pcw.co.uk](mailto:internet@pcw.co.uk)