

Short guide to preventing unwanted emails and getting the most out of Mail Washer

First some simple definitions.

Spam – Unsolicited email

Spammer – Sender of unsolicited email

Spam is every bit as unwelcome as circulars in your post box or telemarketers who call at meal times. Fortunately there are ways to decrease or eliminate the amount of spam you receive in your daily email.

Why is spam bad?

1. Theft of resources – The amount of time it takes to filter out unwanted email from legitimate email stops you doing other productive things.
2. The receiver pays – You pay for receiving spam, through your online charges and time.
3. You never asked for it – it is an invasion of your privacy.
4. It's garbage.
5. The offerings are most probably fraudulent or illegal.

Tips

The following are straight forward tips to help you overcome or prevent spam and viruses in your email.

1. Be private. Do not give out your email address in the first place. In many instances if you are required to give your email address in order to receive something off a website, give an email address that you have set up specifically to receive junk.
2. You can also set up a fake email address at such places as www.hotmail.com or www.yahoo.com, these email accounts are free.
3. Look for options to opt out of receiving promotional mailings when you have to give your address.
4. Treat every email you preview as being of a suspicious nature, many harmless looking emails with attachments may contain viruses. Many people succumbed to the "I love you" email that contained a virus. Use Mail Washer to preview your emails by double clicking on the email.
5. When you receive a forwarded email asking for help or money from someone, and in return you will have eternal good luck (or bad luck if you don't forward it). Do not forward it on, it is likely to be a hoax and is a great way for spammers to cultivate email addresses. Many virus warning emails are a hoax as well.
6. When forwarding emails to groups of people, send them via the BCC field, this shields their address from others. Ask others to send emails to you this way too.

7. Use the filters function to filter out unwanted emails that do, or do not meet certain criteria – further info on how to use the filters properly is below.
8. Keep your name off mailing lists, chat rooms and newsgroups by not giving out your correct address in the first place.
9. If your email address is on a website, ask your web designer to transform it in to a picture. Otherwise it is very easy for automated ‘robots’ to come and cultivate your email address and put it on to a mailing list. But if it is displayed as a picture then it won’t be recognizable as an email address to the ‘robot’.
10. Many spam messages have instructions at the bottom of the message asking you to reply to the message if you want to be removed from their mailing list. Don’t do this, as it will only confirm that your address is valid and active and you will most likely be hit with more spam. Use Mail Washer to bounce the message back to the spammer so it looks as though your address is not valid.
11. Check the email address of the sender – do you recognize it? If not, then double click on the header in Mail Washer and you will see a preview of the email.
12. Watch out for fake headers. These are in the subject line and are commonly – ‘Dear Friend.....’ or ‘Here’s the information you requested.’
13. Never buy anything from a spammer’s email, even if it is something you want as it is likely to be fraudulent.
14. You can complain to the spammers internet service provider by sending an email to abuse@[The domain in particular] or postmaster@[The domain in particular].
15. Don’t reply to contests in your email, offers of free websites or send money to anti-spam organizations as it will most likely be a hoax.
16. Don’t submit your address to Opt-out or removal lists as these are a hoax and you will end up getting more spam.
17. It is still advisable to have antivirus software installed on your computer. While you may be able to recognize an email with a strange attachment, a picture or word document may harbor a virus.
18. Use Mail Washer to delete any unwanted emails directly off your internet service providers server before you receive them.
19. Use the blacklist function in Mail Washer to instantly recognize previous spammers or to delete the message off the server instantly.
20. Finally, one option that will get rid of the spam (for a while) is to change your email address. It may take some time to notify others of your new address, but at least you will not get spam.
21. Filter out potentially harmful attachments (.vbs .exe etc) by adding a filter to recognize these files. This can be done by setting MailWasher to recognize these files in the body of the message. ie The body of the message contains .vbs – further information below.
22. Set to automatically bounce blacklisted messages as soon as they are recognized by MailWasher so you never have to see them.
23. Add your own existing blacklist quickly by adding to the blacklist text file where the MailWasher program file resides.
24. MailWasher works very well if you have a permanent connection to the internet, you can just set MailWasher to check for new email every 10 minutes or so.

25. Email us at support@mailwasher.net if you have any questions, or feedback@mailwasher.net if you would like to offer feedback.

More tips on using MailWasher

1). Using filters

If you want to block out a whole string of words, instead of trying to write a filter for each word, use regular expressions instead. Regular expressions are powerful tools that make writing filters easier. Lets say you wanted to be notified of the following words in an email – free, money, casino, deal, credit, and \$. Instead of writing 6 separate filters – regular expressions lets you put them in one line.

Like this – ‘The Body’ ‘contains reg expr’

```
free|money|casino|deal|credit|$\n
```

This will filter out any emails with these words.

2). If you find that you get a lot of emails and most of them are junk, here’s a quick way to sort through them.

One way to deal with a whole lot of email is to change the friends list in this way - in the friends list options tab (Tools, Options, Friends/blacklist tab – Friends Options button), untick 'Display emails received from friends' so people in your friends list won't be shown - this allows you to go through your list very quickly and right click to mark all for deletion then you can go through what is left and unmark those from friends. After a while you will have lots of people in the friends list (which won't be shown) and all the junk shows up which can be marked for deletion by right clicking and selecting ‘mark all for deletion’. You can then go back and tick the ‘show emails from friends’ box to see what your friends have sent you, or simply download them.

3). Here’s how to make mailwasher recognise an attachment (This might be a bit complicated for some users)

here is the header of an email with an attachment:

```
=====  
X-Mozilla-Status: 9001  
X-Mozilla-Status2: 00000000  
Message-ID: <3C170241.EB2F627B@bobbuilder.com>  
Date: Wed, 12 Dec 2001 20:07:45 +1300  
From: Bob Builder <Bob@bobbuilder.com>  
X-Mailer: Mozilla 4.73 [en] (Windows NT 5.0; U)  
X-Accept-Language: en  
MIME-Version: 1.0  
To: Nick Bolton <nick.bolton@clear.net.nz>  
Subject: 1.30  
References: <011f01c17eef\$74c16740\$ee4c56d2@carolyn>  
Content-Type: multipart/mixed;  
boundary="-----1E35701F7A8E081B531FC710"
```

=====
the second to last line is :
Content-Type: multipart/mixed;

this line is in emails which have file(s) attached to them.

So, a simple filter to determine if there is an attachment would be to see if the string "multipart/mixed" is anywhere in the header - you don't want to search for "Content-Type: multipart/mixed;" as that won't match a malformed header like "Content-Type:multipart/mixed;"

To match it properly you could search the header with a regular expression instead, eg
Content-Type:\s*multipart/mixed;

* So your filter would read as follows*
'The entire header' 'Contains RegExpr' Content-Type:\s*multipart/mixed;

However, the name and type of the attachments are specified in the body,
eg

```
-----1E35701F7A8E081B531FC710  
Content-Type: application/octet-stream;  
name="MailWasher.exe"  
Content-Transfer-Encoding: base64  
Content-Disposition: attachment;  
filename="MailWasher.exe"
```

and this is the part that the built-in MailWasher regular expression is checking for. Since mailwasher as a rule only previews the first 20 lines of a messages (for speed) it may not pick up attachments at the bottom of lots of lines of text. Viruses are a bit different, in that they usually do not contain much text, if any at all. You'll soon be able to alter how many lines mailwasher automatically previews (speed vs security).

4). If you own your own domain name, this will be useful.

If you get bounced emails returned to you then read on....

When mailwasher sends a bounce email, it sends it via the postmaster of your internet service provider so it looks exactly like it is a genuine bounced email. If the message that you are trying to bounce has a false return address then you will receive a non deliverable bounced email which will further clutter your inbox – this is because you own your own domain and all the mail is fed in to that domain. This doesn't happen if you have an address from a internet service provider – they get the non deliverable bounced email back to their inbox.

To stop the non deliverable emails coming back in to your inbox, enter the address MAILER-DAEMON@mydomain.com in the blacklist and set it to auto delete.
(where mydomain.com is actually the domain you own)

- 5). To get your email program to check automatically when it starts.
If you have your email program set to not check mail at all (unless specified by you), then after you have finished processing mail with MailWasher it will open up your email program, but will not check mail for you until you press the receive button yourself.
To get around this, and have your email program automatically check mail when it is opened (but not at other times), set the "Check for new mail every xx minutes" to a very high number, say 9999. This will prevent your email program checking while it is up, but WILL permit it to check when initially started.
- 6). Get a free personal fire wall.
These will notify you if any programs try to contact an external address. Have a look at:

Zone Alarm	www.zonelabs.com
Tiny Personal Firewall	www.tinysoftware.com
Outpost.	www.agnitum.com/products/outpost/

VIRUS ALERT

A recent virus doing the rounds is the BadTrans Virus, so here's a tip on how to trap it so you can delete it off your server.

Go to the Tools menu, click on Options and click the Filters tab.

Click on Add, now you can add a filter name and description to the filter. I just called it 'Suspect attachment'

Action: click on mark for deletion

Apply this filter when 'all of the rules below are satisfied'

Rules:

'The body' 'contains RegExpr' doc.scr|doc.pif|mp3.pif|.doc.pif|zip.pif|zip.scr|mp3.scr

The last part you can just copy and paste in to the filter.

This should pick up the virus attachment. The size of the virus is about 39.6k or 39.7k and usually has the subject line Re:

Another virus that has been spreading havoc around the world is the Goner virus and comes with an attachment called gone.scr which can also be filtered in a similar way, although the built in mailwasher checker should identify it.

If you do get these viruses, then you can use a fix from several software antivirus companies. For example, Panda Software (www.pandasoftware.com) have these available for download.

Quick tip on halting .vbs viruses

You may recall the 'I Love You' or 'Kournikova' virus. These were Visual Basic scripts that attached themselves to your emails and sent messages automatically to the contacts in your address book. These are known as .vbs bugs or worms.

Here is an easy way to stop .vbs bugs from running automatically if you accidentally download them.

In Windows Explorer, open **Folder Options** under the **View** menu (**Tool** menu in Windows ME).

Select the **File Types** tab and scroll to **VBScript Script File**.

Click on the **Edit** button (**Advanced** in Windows ME). A new window will open showing the possible file actions, with the default action shown in bold face type, which is likely to be set to **Open**.

Highlight instead the word **Edit** and click on the **Set Default** button. **Edit** should now appear in bold face.

If you have an older system and the **Edit** function doesn't appear, select the **New** button and enter **Edit** in the action field and **Notepad.exe** in the application field.

Once **Edit** appears, make it the **default** action. While you're in the **file-type** screen, make sure the boxes for **Always Show Extension and Enable Quick View** are checked. Click **OK** to close the open windows.

Making this change will cause the VBS file to harmlessly open in Notepad, rather than execute the script and activate the virus.

If it's not clear why you need to always see file extensions, it's because things like the Kournakova virus spread using a vbs file called something like kournakova.jpg.vbs, so if you suppress the .vbs extension it looks like a jpg

Follow this link if you would like to know more about fighting spam.
[Link to anti-spam site](#)