Mailgate Ltd.

THE CRASH DUMMY'S GUIDE TO
SpamWeasel Free

SPAM
Weasel

Microsoft is a registered trademark and Windows 95, Windows 98, Windows 2000, Windows NT and XP are trademarks of Microsoft Corporation.

Copyright © 2002 Mailgate Ltd.

Written by R. A. Hall

Contents

Getting Started

Welcome to SpamWeasel

Introduction

SpamWeasel ™ contains a full user's manual together with context-sensitive help text. In addition, there are FAQ's on the Mailgate Web site to assist with installation. But this guide is different. It's for anyone with problems understanding software manuals and computerspeak. And computers, come to that.

If this doesn't apply to you, congratulations: we already wrote a manual for you, so go read it!

If you haven't already, you'll want to download the program. Go to the SpamWeasel's hide-out at: **http://www.mailgate.com/products/spamweas/sw_feat.asp** and download it. You'll find you can't invoke your browser simply by clicking on this URL, so copy & paste it into your browser's Address field instead. Oh, and before you do, if you are one of the 30 million AOL users, products like SpamWeasel will not work for you. Why? Because AOL opted out of the standard POP3 email protocol adopted by the other 500 million of us Internet users.

OK – you've got the program. This guide helps you get SpamWeasel to analyse your incoming mail and bin spam. If you haven't printed it out & are reading it on-screen, print it! Otherwise you'll be juggling screens and guide like a one-armed decorator papering a ceiling.

The software comes with standard settings, but you need to personalize it the better to junk your spam. That's all it does. We do sometimes get mail from people who want to know why SpamWeasel doesn't stop Windows from crashing and also bring democracy to Cuba. We're always polite to them. But if you just want less spam, here's how to.

Getting Started with SpamWeasel

Installing SpamWeasel

To install SpamWeasel for the first time, find the file named sweasx86.exe and double click on the file icon. This displays the licence - we're keen you read it because tho' the product's free, we still like to think it's ours. Scroll down to the very end of the licence and click on 'Accept'. This starts the installer program, which asks you the questions it needs answered to know where to install itself, reasonably enough. If 'Accept' stays greyed out you haven't scrolled far enough down – it'd surprise you how many calls we get on that one.

SpamWeasel first asks where you want to install it – leave this at our suggested setting and click 'Next'. Then it asks if you want Shortcuts and Autostart. Again, leave these settings as suggested and click on 'Next'. If this gets you dithering around like a learner at a busy five-way crossing: stop, get out, climb into the back seat and wait for help.

By the way, If you already have SpamWeasel and are updating it - and before you ask, yes it will keep your existing settings – FIRST stop SpamWeasel by right clicking on the icon and selecting 'Stop SpamWeasel' or 'Exit'. Then proceed as above and it will over-install. All you need do then is accept the licence, as above, do a re-start - see next paragraph - and SpamWeasel will run as smoothly as before.]

OK - I'll assume that the installer wants you to click on 'Finish'. Do this. And then re-start your computer. You probably think I mean by that, hit the "on/off" switch, which is a reboot: I don't. Use the mouse to close down and re-start the computer operating environment after first closing any active programs. This distinction needed pointing out to me so if you knew that already, you're ahead.

SpamWeasel runs automatically when you re-start your computer, provided you've left the settings alone like I told you, and it will place an icon in your system tray. If you don't know where that is, look at the bottom right corner of the screen next to the time display. See it? Now double click on the SpamWeasel icon – he's the weasely little fellow staring out from the envelope.

If the program isn't yet registered it nags you to, but can be ignored for now by clicking on Continue.

Once you have completed the install routine I recommend you look at the SpamWeasel logfile to see if any errors are reported. If so, SpamWeasel isn't going to happen until it's put right. Usually the error is simply due to another program hogging the same communications port SpamWeasel wants and can easily be resolved.

You already should have done a 'restart' as described previously. If not, you should do it now to generate the logfile that tells you if it's working OK.

You'll need to use NotePad to view the logfile. To invoke NotePad, left click on the Windows 'Start' button (bottom left corner of the screen). Hover over 'Programs' and left click on 'Windows (your version here, eg. 98) Explorer'. Double click on the 'Program Files' folder, on the 'SpamWeasel' folder, and finally on the 'log' folder. The SpamWeasel log you want is named 'SW' followed by today's date, displayed year-month-day, and is at or near the end of the folder you've just opened. Open the logfile and scroll down to the last lines, which should look something like this:

```
spamweas I 17:29:42 0x000000bd SpamWeasel version 1.0.16 initializing
spamweas I 17:29:42 0x000000bd spamfltr: Extension version 1.0.32 starting
spamweas I 17:29:42 0x000000bd spamfltr: Parsing C:\Program Files\SpamWeasel\spamfltr\userpre.sfr
spamweas I 17:29:42 0x000000bd spamfltr: Parsing C:\Program Files\SpamWeasel\spamfltr\system.sfr
spamweas I 17:29:42 0x000000bd spamfltr: Parsing C:\Program Files\SpamWeasel\spamfltr\userpost.sfr
```

If you see a similar entry to this, SpamWeasel is happily installed and you can move on. If instead, an error looking something like this is displayed :

```
spamweas E 17:47:52 0x000000e9 Unable to bind to port 110, error 10048
```

you can resolve it using the method shown in our FAQ at :

http://www.mailgate.com/support/faq/swfaq023.asp

You now need to configure your email client program.

Configuring your E-mail Client.

Changing your POP Settings

Your email client is the software that collects & displays your email. To configure your client to work through SpamWeasel you normally need make only two changes to your email client. If you want more detail than you find here, go to the Mailgate site and look up your email client in our FAQ section and follow the instructions at : **http://www.mailgate.com/support/swfaq.asp** There are many different releases of each different type of email client we describe, so you may need to exercise your judgement when entering the recommended changes. Here's what to do:

First, look under your Mail Account Settings to locate your POP Server address. If necessary, consult your email client manual. Now write down your current Incoming POP Server details. On a piece of paper, for instance HERE :

Now change this setting to 127.0.0.1

Secondly, locate your current POP Account Name. Change this by adding an @ to the end of your account name and then type in, right after the @ sign, your Incoming POP Server details (you've just written them down!] Then check it – the example below should help.

Then – and only then - click on OK, which closes the window and saves your new settings.

Example

Your *original* email client settings (aka Mail Account Settings) looked something like this *before* you changed them:

Incoming POP Server: pop.my_isp.net

Account Name: jdoe

Password :   pass_word

After making the recommended changes your email client settings should look something like this:

Incoming POP Server : 127.0.0.1	(Yes, just so: 127.0.0.1)
Account Name : jdoe@pop.my_isp.net	(If this *is* your name and ISP, you get the prize!)
Password : pass_word	(Use *your* password, this one's *mine...*)

Now right click on the SpamWeasel icon, select 'Configure' and at the bottom of the next screen is a dropdown 'Logging:' menu. Select 'Detailed with protocol'.

You are now ready to run a test session to Send/Receive mail. It doesn't matter whether there *is* any mail in your Inbox / Outbox to run this test, since we're only looking to find if SpamWeasel can communicate with the email client. So ask your email program to go look for mail – Send / Receive - and then view the results in the same logfile as before, like you did after running the install programme.

Scroll down the logfile entries as before and the last lines at the bottom of the file should look something like this (if you actually did process mail, this entry will be a little higher up in the file):

```
spamweas * 17:36:47 0x00000076 >c +OK SpamWeasel
spamweas * 17:36:47 0x00000076 <c USER jdoe@pop.my_isp.net
spamweas * 17:36:47 0x00000076 <s +OK pop server ready
spamweas * 17:36:47 0x00000076 >s USER jdoe
spamweas * 17:36:47 0x00000076 <s +OK jdoe welcome
spamweas * 17:36:47 0x00000076 >c +OK jdoe welcome
spamweas * 17:36:47 0x00000076 <c PASS <secret>
spamweas * 17:36:47 0x00000076 >s PASS <secret>
spamweas * 17:36:47 0x00000076 <s +OK mailbox is locked
spamweas * 17:36:47 0x00000076 >c +OK
```

You are looking for the characters 'c' and 's' after the prompts < and > . These indicate the c: (Client – your E-mail Client) is talking to the s: (Server – your ISP, or the network server if you're using one). If they are present, all is well.

If instead you see something like this:

 –ERR Permission denied

go over the email client settings to make certain they're set exactly as described already. IF they are absolutely correct, read Things to Watch For (below) or go to the FAQ page at :

http://www.mailgate.com/support/swfaq.asp for some more hints on where your problem may lie.

If all else fails, you can email **support@mailgate.com** with the problem. Our techies are usually busy so you won't always get top priority, but they try to help you between making coffee /recycling Internet jokes/dissing each other /cracking the boss's passwords. Only joking.

Things to Watch For

- Leave your original Password setting unchanged or your ISP will knock you off your mailbox account.

- A few email clients use different separators from the @ sign. If you find nothing else works, you may need to change this. Go to the dropdown 'Separator Char.' on the Action tab in SpamWeasel 1.0.16 to change the '@' separator to another character – we recommend you use the question mark: '?'

- You may need to re-start your e-mail client for the above changes to take effect. Don't ask me why, ask Uncle Bill.

- Some ISP's may require Secure Password Authentication for incoming (POP) mail, such as MSN (in N. America, anyway). For more information on this and other settings, go back to the relevant FAQ's at our Mailgate Web site.

Also, as I've mentioned, a full manual which goes into The Meaning of Everything is included with the SpamWeasel and can be downloaded from the Mailgate Web site. It's a real read, written by techies for people with entire lives yet to get. Best avoided.

Using SpamWeasel

Initial Configuration

Identifying Spam

All things being well, SpamWeasel is now able to collect your mail from your ISP and pass it to your email client. Out of the box, SpamWeasel's standard settings will allow all mail through, but it will also label most of it as Spam unless you change some settings. This may seem odd but it's just a starting point 'cos everyone has different ideas about what spam is. So SpamWeasel starts by saying everything more or less *is* spam, until you tell it otherwise. We could've done it the other way around but the Internet is a tricky place & full of junk so we leave it for you to tell SpamWeasel where and how big to make the doors in your mailroom.

Just in case you didn't know how context-sensitive help works (and I didn't, for one) click on the 'Configure' option on the SpamWeasel menu and then left click once on the little '?' character at the top right of the SpamWeasel screen. Then position the mouse pointer (which is now accompanied by a '?') over any of the configurable data fields and left click again. The appropriate help message will appear. Click again and it disappears.

I describe two philosophies for using SpamWeasel here. First, the easy way, then a slightly more sophisticated approach. I prefer to combine both methods but it's best you discover what works for you and not be told how to, even by do-good dummies like me.

To get mail from friends passed to your inbox, click on the Patterns tab and then double click on 'Friendly From Addresses'. You'll find that you already have some friends in there, because it contains the entry : *@mailgate.com - the '*' means literally any character. SpamWeasel will allow as a friendly 'from' address anyone with a mail account domain of '@mailgate.com'. So, for instance, a mailbox called spamweasel@mailgate.com can send you a message. [If you don't want to be friends with us, that's ok - you can shut the door by cutting (save & delete) & pasting the '*@mailgate.com' entry to the 'Unfriendly From Addresses' list. Thus, we would become *not* your friends. Just don't then ask us for email support 'cos it probably won't reach you.]

By the same token, *@* in the 'friendly from' list will make anyone from anywhere your friend, so don't do it unless you're a very sad person. Enter just the individual addresses which you definitely want to receive mail from. It helps if you update the friendly from list whenever you exchange addresses with someone, obviously, or you may not get their mail. If you don't know an exact address you can start by using the part you do know plus '*' and tighten up later. Incidentally, the * is called a wild card, which is a card every poker player wants, but maybe you don't approve of poker so I'll move on and talk to the nice folk over there.

Before I do, I need to give you some tweaks to set up SpamWeasel to KILL spam, which is the real aim.

Go to the 'Unfriendly From Addresses' list and put in the addresses you don't want mail from, obviously. For instance, addresses of those pesky people who promise to stop mailing you if you only click on - or reply to - the 'unsubscribe' , 'remove' or 'de-list' address they give. Use the '*' character freely as the unfriendlies will morph their address slightly just in order to confuse you. For instance, if they hide their from address and only give a huge URL with instructions to click on this to de-register,
http://www.SpamULike.net/yeeuuch8475_yahdy_yah.asp then try using the wildcard trick to prevent further mailings by blocking the 'From:' address: *@SpamULike.net* If that doesn't work (because for instance, they're spamming you from one address but sending your de-list request elsewhere) you need to look into this further, and maybe speak to a spam sophisticate. Which ain't necessarily a bad thing to do and you'll learn a lot your grandmother never knew.

Then, and this is important so pay attention, turn OFF the next two Rules. Rules are listed under the 'Rules' tab and are turned on and off by left clicking on the green check symbol to the left of each Rule. The turn-offs are: 'Spam if To or Cc address is not found in 'My Addresses'' and 'Pass if To or Cc address is found in 'My Addresses''. You'll know when they're turned off because you'll see a red cross appear in place of the green tick, or check. Both these rules are intended only for network users and power users. Turn them off or you'll run into problems that only the sophisticate can resolve.

Now you are indeed ready to KILL spam.

Killing & Archiving Spam

Click on the Action tab and uncheck the 'Allow through modifying 'Subject" field which will prevent spam mail reaching your inbox. 'Modifying 'Subject" means SpamWeasel adds a word or phrase to the subject line to tell you it's spam – you can choose the words yourself if it makes for interest. On the same tab there's a checkbox option to 'Archive message to' for each spam mail (that's like a 'Go to Jail' card). If you want some excitement, you can uncheck this box and delete it immediately (that's like a blow away option, so if you do this you can't bring it back just because you're really sorry).

You start by leaving checked the 'Allow through…' option in the 'Action' screen. This setting allows you to see in your inbox whether the mail *you* think is spam is marked in the Subject field as spam by SpamWeasel. When that is happening consistently, you can uncheck the 'Allow through…' box, while leaving the 'Archive message to' box checked. This will allow SpamWeasel to route the marked mail directly to archive, bypassing your inbox. You need to repeat this for each priority setting that you use to identify spam (see 'Using Rules and Priorities', below). You can then review the archives - I describe how to below. Leave the default folder setting alone unless you're sure you know what you're doing.

Provided you archive spam, for say 7 days, before auto-deletion occurs (the 'Tidy archive of messages older than' option on the 'Action' tab) you can pan through periodically, looking for any gold dust. I go through mine every day. To get into the Archive you right click on the SpamWeasel icon and click on 'Archive Viewer' and then open 'SpamWeasel Archives'. There the trapped spam is placed in neatly prioritised, date-ordered folders. Mail is removed from your Archive file by left clicking and dragging the individual mail icon across and releasing it into the 'SpamWeasel Pending Queue' (in the left column) from where it will go to your inbox. It's the 'Get out of Jail Free' card. Once you've initiated archiving (from the 'Action' tab) all becomes clear. It's worth trawling through your spam archives because occasionally good mail will get labelled as spam. It's up to you to decide why and take the appropriate action to give it free passage in future.

SpamWeasel will work OK if you set it up as I've described and then leave it alone, apart for updating the 'friendly froms' and the 'unfriendly froms'. It's rather a limited use of it, but good enough.

Finessing SpamWeasel

Using Rules and Priorities

If you want, you can now go play with SpamWeasel by prioritising the Rules governing 'Usual Spam Subject Phrases' and Usual Spam Message Phrases' and adding to the list of phrases.

First, go to any phrase list by clicking on the 'Patterns' tab and then double-clicking on the chosen phrase. This displays the complete list, which you can alter just as you would a shopping list. You must use the wildcard character '*' *before and after* each chosen word or phrase, otherwise SpamWeasel will not see the wood for the trees. If for example want to use 'promise' as a spam identifier, enter in the 'Usual Spam Message Phrases' list *promise* in order for SpamWeasel to recognize it when occurring within a larger sentence, like, 'If not absolutely satisfied with this offer I promise to make a huge donation to the Incurably Optimistic Society'.

To alter the priority level of a Rule governing a Pattern, go to the 'Rules' tab and right click on the 'Priority' level assigned to the rule (initially, these are set at 'Normal') and check the popup menu with a priority that *you* believe suits the importance of the 'Pattern'. To do this, right click on the text stating the priority of the rule, and click on the appropriate priority.

Each time you change the priority of a Rule you should also ensure the 'Action' tab is set to handle the priority in an appropriate way. To do this, click on the 'Action' tab and then on the dropdown menu 'Action for priority level:' to see if the action suits the new priority you've set for the Rule. Remember that if you change the action associated with a priority, it changes the action for every rule with that priority.

For example, 'Action for priority level: Highest' could be to uncheck both boxes, which will delete all mail in the 'Highest' category of spam. For the next level, 'High' you could uncheck 'Allow through modifying subject' and check 'Archive message to'. For 'Normal' you might check the 'Allow through etc' box (but not the 'Archive message to' box) and put a message in the field associated with 'Allow through etc' such as 'Normal Spam'. And so on for the lower priorities. The spam message chosen should indicate the level of priority you have assigned to the rule that governs it. If you then find lots of junk mail in your inbox marked with a 'Normal' priority you can consider raising the priority of the rule governing the pattern involved so that SpamWeasel archives the mail directly.

Be aware that if you leave the 'Friendly From Addresses' at it's standard setting of normal priority, but raise a spam identifier rule to a higher priority, this spam rule will over-ride the lower 'Friendly From Addresses' rule. For instance, if a friend's mail has features that are also typical of spam, like !! and ?? and $$, you'll need to ensure that you give *as high or higher* priority to the 'Friendly From Addresses' Rule as you do to the Usual Spam Message (or Subject) Phrases' rule, or their mail could be treated as spam. The solution here is to give 'Friendly Froms' a 'Highest' priority so such mail will always be passed to your inbox.

The 'Undesirable attachment marks' Rule (the last in the list of Rules) can be used for blocking certain known viruses that come as .exe files or which have an identifiable file name such as 'LOVE-LETTER-FOR-YOU.TXT.vbs' or 'valentin.scr'. Go to the Patterns tab and double click on the entry 'Undesirable Attachment Marks' and you'll see a few instances already included which you can remove or add to at will. But bear in mind that it all mail carrying attachments of the type listed will be treated as spam, so best archive it for a week or so before allowing SpamWeasel to delete it, in case you get valid mail incorporating a file with an undesirable attachment mark.

Oversized Messages & Reporting

In this context, you need also to look at the 'Action' tab. The item 'Don't check messages bigger than:' is set at a low 30k on the basis that most spam is short in length. This 'Action' bypasses any Rules that otherwise would apply to the message – even the 'Unfriendly From' Rule. So if spam mail is larger than 30k it will not be checked for spam content until you raise this setting.

For example, if you set SpamWeasel to identify something like a newsletter as spam, which could run to 100k in size if an .html version is included with the text version, the mail could bypass the SpamWeasel and go straight through to your Inbox unchecked.

Why did we set the 'don't check' limit so low? Because otherwise your computer will check out all large mails, few of which will prove to be spam. Usually spam mail is short. It's down to you to set the size limit of this bypass routine. I've put mine at 200k to hit the big newsletters, but my experience ain't necessarily yours.

The SpamWeasel can generate a regular report listing the mail it has labelled as spam, indicating why it has done this. Normally, the report is sent to your inbox every time mail is collected from the ISP, provided it has found spam. These reports are useful feedback while you are setting up SpamWeasel but can become a distraction once it's running happily. You can turn off the 'per collection' report and optionally even disallow the daily report 'tho I don't recommend the latter as occasional feedback is better than none. To turn off reporting uncheck the appropriate box in the lower part of the 'Action' screen.

You should also know that after some debate we decided if two Rules of the same priority conflict, one saying 'pass' and the other 'archive', the 'pass' option would prevail and the mail appear in your inbox marked as spam, not archived. This and related topics are more fully addressed in the manual that accompanies this product. It's a technical read so if you don't want to be a techie, don't go there.

More about Rules and Priorities

Rules are as we now know, listed under the 'Rules' tab and turned on and off by left clicking on the green check symbol to the left of the Rule. The Rule itself is displayed by double clicking on it's description but it's written in our own script language, which is indecipherable to me, and anyway, you can't change a Rule from within SpamWeasel. Editing Rules is only for power users and beyond me entirely. However, as you will now have gathered, many Rules refer to lists that you can easily edit within SpamWeasel. For instance, the 'Words' tab allows you to access three pre-existing lists by double clicking on the titles: Adult Words, Likely Spam Words and Usual Spam Subject Words. A few specimen entries are already there but our polite adult vocabulary was quickly exhausted so you'll have to exercise your creativity on this one.

We've created quite a lot of Rules for you already as you've seen and some of them are quite specific, like 'Check Mail Body GUARANTEE In Capitals', meaning that if the word guarantee appears in capital letters in the body of the message you can be pretty sure it's spam. I've set this rule to the highest priority level and directed everything caught by it to the archives. Similarly with BILLION/MILLION and FREE. In fact, if the subject heading is all in upper case (it's called 'SHOUTING' – don't do it!) we have a rule for that too. But if your friends shout a lot, not to worry, you've already set the 'Friendly From Addresses' to highest priority (haven't you?) and where two rules of equal priority conflict the mail gets labelled as spam & passed through to your inbox. Remember?

Likewise, if you like getting spammy newsletters you might try going to the Rule: 'Pass if Subject listed in 'Friendly Subjects'' (which is already ticked with a 'Highest' priority setting, right). Then enter the subject of the newsletter in the Pattern list matching the Rule, exactly as it appears in the newsletter subject header.

If the 'To:' or 'From:' fields are blank or missing in a piece of unwanted mail it's usually a good indication you're looking at a piece of spam and there's a Rule for that, too. Or you could instead use the 'Friendly From Addresses' and/or 'Friendly Subjects' Rule to let it through. We haven't included one to look for a reference to Senate Bill 1618 (which regulates spam) but if you choose to put that as a phrase into the list found in 'Patterns' and 'Usual Spam Subject Phrases' (don't forget to use the wildcard character '*' at each end of the phrase) you'd probably be right nine times out of ten.

Registering SpamWeasel

The nag screen appears whenever SpamWeasel operates, until you register at the mailgate.com site and the code you're given entered into the prompt box. Do this by following the SpamWeasel links on our index page at www.mailgate.com. Registering lets us send you interesting info about the SpamWeasel's life and times (which you can always block using SpamWeasel) and it lets you feel good about having this admirable little chap work for you unpaid. Any personal information you give to us will be used only to deliver, market and improve our products and our service to you and for no other reason.

Avoiding the Spammers

Keeping the Zombies Buried

Even if you do get the temptation to flame spammers – don't. Not politely, not rudely, not at all - it only encourages them. Treat them as you would a solicitous zombie. Hide. Your reply – that is, the From: address on your reply – is simply more meat for their smorgasbord. Flaming the spammer only adds to the amount of spam in the universe. And if the spammer eventually respects your de-list request a reply still gives them a confirmed as valid address to sell on to other spam zombies. So, more spam.

Besides, spammers often use a spoof or a one-time address and send spam mail from an unattended mail box which does not accept incoming mail. Their de-list URL often takes you to a site whose only function is to – you've guessed it – harvest validated email addresses. Worse, they may have hijacked an innocent party's mailbox, so you only see the hijacked 'From:' address and assume it belong's to the spammer when it's actually being used to relay spam from his hidden address.

We even get mail from the annoyed and the desperate because they've seen the ubiquitous term 'mailgate' somewhere in the header of tons of unwanted mail. 'Mailgate' is conventionally used by mail system administrators and ISP's to indicate a mail gateway and has nothing to do with its source domain. We have a standard email reply that explains this too.

You can take a look at the header info that contains the routing information in any of your incoming mail by clicking on the correct tab (next to 'Message' and labelled Options, in Outlook anyway...). But be aware that identifying the source of spam by analysing headers is a tricky subject that requires skill and persistence, things often not being as they seem.

So instead of replying, enter the spammer's address into the 'Unfriendly From Addresses' or the 'Known Spammer From Addresses' – whichever floats your boat. Go to the matching Rule and give it a 'Highest' Priority in the settings. Then click on the Action tab, set the Priority level at Highest and uncheck the 'Allow through modifying 'Subject'' field and you'll prevent this mail reaching your inbox. On the same tab there's a checkbox option to archive it or, if unchecked, to delete it immediately if you're that way inclined. Remember what I said earlier about the 'Don't check massages bigger than:' option (see Oversized Messages, above).

You can now go on to explore the flexibility of SpamWeasel. In time, you could, briefly, attain the spam-busters nirvana of 100% correct identification. I got to about 98% before satisfying my curiosity as to how spam mail is constructed, identified and blocked by SpamWeasel. I also discovered that I need to update my definitions occasionally as spam changes character rather like mutant viruses.

If you've read through this Guide without clicking through the software screens at the same time you may by now be slightly confused, but, hopefully, still eager to start. SpamWeasel is a fairly sophisticated utility, spun off from a larger mail server product we also produce (MailGate), so wasn't originally intended for the novice. So if you struggle a little it's really our fault, not yours. But once you start thinking about the effect of each setting and follow through the logic, the ideas embodied in the program should click with you as it did with this particular computer crash dummy.

Author's Note

The author takes full responsibility for all mis-spellings and other infelicities and he spells words the English way (mostly). All other mistakes are also of his own making but then again, what did you really expect from a crash dummy?