

SpamVault - a FREE spam filtering program from AJT. Simply login to your control panel and click on the SpamVault icon to begin setup. Be sure to read all instructions below carefully.

Getting Started with SpamVault

SpamVault allows you to block e-mail from spammers. Although SpamVault is very easy to use, it's also very powerful and **if not used properly can delete e-mail you may have wanted to receive**. Please read these instructions before using SpamVault as we cannot retrieve lost e-mail.

Begin by Adding an Entry:

You need to add an entry in the text box appropriately named, "Add an entry:". An example of an entry would be a spammer's e-mail address. SpamVault is not case sensitive, so you can use "ALL CAPS" or "Not All Caps" and it makes no difference. There are radio buttons called filters to the right of this box with the letters F,T,H,S & B next to them. These represent the area of the e-mail that is used to trigger the blocking of the e-mail. For instance, the "F" stands for e-mail "From" someone. In the example here, we want to block any e-mail coming "From" the e-mail address spammer@spam.com, so we would make sure the radio button next to the "F" is checked.

The following are the areas of the e-mail that can be blocked:

- F = From** (block e-mail 'From' someone or some network)
- T = To** (block e-mail sent 'To' someone at my domain)
- H = Header** (block e-mail with special text in the header section of an e-mail)
- S = Subject** (block e-mail with this word or phrase in the 'Subject' of the e-mail)
- B = Body** (block e-mail with this word or phrase in the 'Body' of the e-mail)

Caution: We thought this would be a good time to warn you. As a beginner, we recommend that you only use the following characters in your entries as other characters can cause very predictable results (*all bad*). You can use the following characters: A - Z, a - z, 0 - 9, period (.), dash (-), Underscore (_), and the At symbol (@).

Here is what your entry should look like

Type new entry here then click the Update Entries button at bottom						
New Entry:	Filter:					
	From	To	Header	Subject	Body	

After entering the information you wish to block press the "Add Entry" or "Update Entries" buttons:

Entries are sorted by the filter names so that all your "From" entries will be together, etc. Once entered, your entry will show up on the list and looks as follows:

#	Blocked Entry	From	To	Rec'd	Head	Body	Block on/off	
01		F	T	R	S	B	Block	DELETE

It is very important that you allow the entire page to load before pressing the "Add Entry" button at the top of the page when adding or editing an entry. If you fail to do this, the entries that have not loaded yet will not be submitted

to the system and therefore will be eliminated.

Editing an Existing Entry:

Once an entry is entered, you can change it by editing the existing entry. For instance, if you wanted to test this entry to see if you were still getting e-mail from this particular address, you might wish temporarily turn off this filter by unchecking box next to the word Block. We do recommend that you try to keep the quantities of your entries as small as possible. However, it's not unusual for someone to have 100 entries before long. You can edit as many entries as you wish but be sure to press the 'Update Entries' button after you're finished editing.

#	Blocked Entry	From	To	Rec'd	Head	Body	Block on/off	
01		F	T	R	S	B	Block	DELETE

Configuration Section:

You can show or hide the configuration data of SpamVault by checking or clearing the box appropriately called "Show Configuration Data" located below the 'New Entry' section at the top and then click the Update Entries button.

Sample Configuration Data Section

Configuration Info	
Total Spams Blocked: 33739	
51 of 82 emails were filtered since log was cleared 7 hrs 3 min. ago.	
Send Spam to Never Never Land! (recommended unless you're testing new entries.)	
Or check this box to save and manage your spam via webmail	
Check box to clear the 624415 byte repository file and conserve your disk space.	
E-mail Log Info:	
Keep an e-mail log	
Check box to clear the 16911 byte log file and conserve your disk space.	
White List:	
Check box to turn on Whitelist	
Advanced Filtering Tools. See the Help File before using these options.	
Block Base64 encoded emails.	Break web-bug and web-based images.
Prevent multiple exact duplicates.	
Block these types of executable attachments.	
Bypass address --> Destination mailbox file name: -->	
Width of Text Boxes:	

Let's review the configuration section.

Total Spams Filtered: 33739 This is the number of spams that have been filtered on your account. Note that some spams aren't blocked with SpamVault as you'll see in the Advanced Filtering Tools section below.

Send Spam to Never Never Land! You can delete your spam (AKA send it to Never Never Land) or send it to a special repository file by placing a check in the box labeled, "Or check this box and manage your spam via webmail". As this file grows it uses disk space, so it is always a good idea to clear this file regularly by placing a check in the box next to "Check box to clear the ##### byte repository file and conserve your disk space." It is also best to avoid saving email to the repository unless you're testing new filters to make sure you don't accidentally lose any email. You must press the 'Update Entries' button for these changes to take place. The most effective way to view your spam repository is to click on the link that reads "webmail". See below on your **spam email box** which may help you recover any spam that should not have gotten blocked. If you want to see the raw repository file, you can click on the link by the same name.

Email Log Info. SpamVault can keep a log of all the e-mails that have gone through your account. As the log file grows, it also uses disk space, so it is always a good idea to 'Clear this file' regularly or uncheck "Keep an e-mail log" which turns off the logging feature. You must press the 'Update Entries' button for these changes to take place. To view the log simply click on the "e-mail log" link. There is more information on viewing the log files further down in these instructions.

When logging is on, SpamVault logs all email and is then able to keep tabs on how many spams it has blocked. This feature is guaranteed to provide a personal sense of satisfaction.

Note: there is a limit to the size (set by your host) that SpamVault will be allowed to use for the repository and log files. If you reach this limit, the next time you open SpamVault you will see a warning notifying you of this that directs you to clear your log and repository files. Until the logs are cleared, SpamVault will then stop blocking spam and logging.

White List. A White List is a list of email addresses that you never want blocked. There may come a time when you're blocking the term, "Click Here" to avoid spam that want you to click to buy something. However, you may also subscribe to a mailing list that uses the same term to get you to see the full text of their newsletter by clicking on the same term. All you would have to do to is add their email to your White List to make sure that their email is never blocked. Turn the White List feature on by putting a check next to the text that reads, "Check box to turn on White List". Then click on the words White List to add entries to your White List in the window that will pop up.

Advanced Filtering Tools.

Block Base64 Encoded Email: Spammers use special encoding called Base64 to bypass text based email filters. Virtually all Base64 encoded email is spam. This option stops all Base64 email from getting into your email box. Note: Email attachments such as Word files are encoded with the email as Base64 but SpamVault will allow these to pass through. While most do not, some email programs such as AOL create Base64 emails when you attach files. As a result, you may want to be careful when using this tool and turn it off if you have a lot of people sending you attachments.

Break Web-Bugs and Web Based Images: When a spammer sends HTML based email, they can include images that are pulled in from the internet when you open the email. Using special code these images can alert the spammer that you have opened the email and they have hit a live target. Unfortunately, these images can also be legitimate images such as logos in a letter from a business. SpamVault does NOT block these type of emails. It simply attempts to break the code referring to the image, leaving everything else intact. This option also does NOT block images sent as attachments.

Prevent Multiple Exact Duplicate Emails. It's amazing how many times a spammer will send you emails just to

get his point across. Often these are exact duplicates. For instance, they might try sending to info@, support@, sales@, and help@ your account in hopes of hitting a live email box. This kind of trash can be blocked with this filter. The first one, if not blocked by your regular entries, will be the only one that you will need to deal with.

Block Executable Attachments: Many viruses are delivered via executable email attachments. When checked, SpamVault will block email with executable attachments. This does not guarantee that you will not catch a virus or that SpamVault will catch every possible executable attachment. However, this is just another safeguard in your toolbox to prevent damage to your computer. This is not a replacement for virus protection software which we recommend you have installed on your own computer.

Because different people have the need to block or allow different types of files, you can use the text boxes to designate which types of files you wish to block. Enter the file extension. Separate entries with a pipe symbol.

Example: . Note, do not put a pipe symbol at the beginning or the end. Just use it to separate the entries. For example:

Types of files that are executable and known to be able to carry viruses and email worms. File extensions are in (parens)									
Application (exe)	Batch file (bat)	Compiled HTML Help (CHM)	Control Panel Extension (CPL)	HTML Application (HTA)	Internet Communications Settings (INS ISP)	Internet Shortcut (URL)	JScript Encoded Script (JSE)	JScript File (JS)	MS Access Add-in (MDA)
MS Access Applications (MDB)	MS Access DB (MDE)	MS Access Project Extension (ADE)	MS Access Project (ADP)	MS Access Wizard Template (MDZ)	MS Common Console Doc. (MSC)	MS Outlook Profile Settings (PRF)	MS V-Foxpro Table (DBX)	Outlook Express Folder (NCH)	Photo CD Image (PCD)
Registry Entry (REG)	Screen Saver (SCR)	Security Cert. (CRT)	Setup Info (INF)	Shell Scrap Object (SHB SHS)	DOS Program Info File (PIF)	Shortcut (LNK)	VBScript Encoded File (VBE)	VBBasic (VB)	VBScript File (VBS)
VB Class Module (BAS)	Visual Test Scrote File (MST)	Windows Explorer Command (SCF)	Windows Installer Package (MSI)	Windows Installs Patch (MSP)	Windows Medial (ASX)	Window Media Skins (WMS)	NT Command Script (CMD)	Script Component (SCT WSC)	Windows Script (WSF)
Windows Script Host Settings (WSH)	Windows Help (HTP)								

Bypass Address. The Bypass Address is similar to a White List except that it is a special single address that when people send email to it, it will not get filtered. You can change this address regularly and give it out only to people who need it. For instance, you might choose sales@yourdomain.com as your Bypass Address that should never get filtered just in case a prospective customer writes in. You can make the Bypass Address 'sales@yourdomain.com'. The Bypass Address doesn't even have to be a valid email box on your account. It's just an identifier to SpamVault that you want all email sent to this address directed to an email box name on your account.

Width of Text Boxes. Depending on the screen resolution you use and the length of your entries, you may wish to change the width of the text boxes used in the list of blocked entries. Changing this number merely changes the width of these boxes. You must press the 'Update Entries' button for these changes to take place.

Spam Email Box

When you installed SpamVault on your account there was a new email box added to your account called spam (assuming that there wasn't one by that name there already). This new box is not like other email boxes in that you should not use it as an address for people to send email to. Instead, the special box enables you to use the webmail on your account to review and manage the spam that has found its way into your spam repository. For instance, let's say you notice in the email log that SpamVault has blocked a piece of email that you wish to recover. Click on the WebMail link in the line "Or check this box to save and manage your spam via [webmail](#)" to open your webmail interface. The user name to type in is "spam." Note: Before you can gain access to this email box, you must set the password using your Control Panel - Mail Manager tool.

Viewing the Email Log.

This is actually a very rewarding experience even if you're not a propeller head because it will quickly show you the spam that is being blocked and help you figure out which email filters are working for you. The SpamVault Log is also helpful in diagnosing why (heaven forbid) an email you wanted was blocked. Here is a sample of what the log looks like. All of the entries that start with "===**SpamVault: Part_of_Email contains [spam trigger text]**" tell you that this email was successfully filtered based on your preferences. The text in [brackets] tells you the actual word or words that triggered a block of the email. One item to keep in mind when reviewing your logs. As soon as SpamVault discovers that the email is spam, it filters it out, logs it and moves on. Therefore, it may find that the that some text in the subject triggered the block when it's clear that the subject line also has elements in it that are being blocked. However, it will not only the first item that triggered the block, not all the items.

When SpamVault filters an email it will also log the true designated recipient of the email. Many spammers send email to one address and then BCC the email to your address in a little slight of hand. The true recipient's address isn't shown in the header of the email. SpamVault will reveal this information in red in spite of the spammer's efforts to hide it. This will be very helpful in finding out if there is a pattern of email boxes that the spammers are trying to send to. You will also see a little \geq next to the "Subject" line in the table below. This is a handy tool if you should see a subject that you're interested in and want to view. Clicking on the \geq will take you to webmail where you can log in and view all the email that SpamVault has captured.

SpamVault Log
View spam in log Go to WebMail
From john@CLEVELANDCAN.COM Tue May 27 12:38:01 2003 \geq Subject: Get Traffic Now - Promised Hits Folder: bitbucket 1014
=== SpamVault: Subject contains [Mortgage] Recipient: someone@yourdomain.com From 9dnz9wwd09kt@aol.com Tue May 27 13:02:30 2003 \geq Subject: Body Part Enlargement Pill for your Toes Folder: /home/user/www/sv/spamvault 1567
=== SpamVault: Duplicate Message Recipient: bob@yourdomain.com From 9dnz9wwd09kt@aol.com Tue May 27 13:02:30 2003 \geq Subject: Mortgage Approved... get the home loan you deserve - lowest rate / be Folder: /home/user/www/sv/spamvault 1567
From list-request@chicago.org Tue May 27 16:35:37 2003 \geq Subject: [ChiECTF] MD5 and Journalled FS Folder: myemailbox 3411

===SpamVault: Body contains [Home Equity Loan]

Recipient: joe@yourdomain.com

From fj04zse55@netscape.com Tue May 27 13:59:09 2003

Subject: Rates are lower than ever and will go back up soon, REFINANCE TODAY!

Folder: /home/user/www/sv/spamvault 1856

===SpamVault: Subject contains [Prescriptions]

Recipient: bobby@yourdomain.com

From hjjjuhnjh@astr.ucl.ac.be Tue May 27 16:15:38 2003

Subject: Discreet Overnite Prescriptions- Easy & Secure

Folder: /home/user/www/sv/spamvault 4138

Note that by default, SpamVault does not show all email that has been received as the screen shot above shows. If you click on the link at the stop of the log that reads, "View ALL email in the log", you'll then be able to see all email -- filtered and non filtered. The shown that do not have "===SpamVault..." in them were emails that weren't filtered that have successfully found their place in an email box on you account.

Hidden Benefit of SpamVault:

Until now, your account used bandwidth twice when you received spam. Once the e-mail arrives at the server and again when you retrieve it from the server. SpamVault completely eliminates the spam at the server level so you will avoid using the extra bandwidth when you check your e-mail. The less e-mail traffic there is, the faster your website is served up when people visit it.

Maximum Entries:

The maximum amount of entries that you can put into SpamVault is 999 because the more you enter the more work your server has to perform while filtering each email. It is recommended that you purge as many entries as often as possible by either deleting them or allowing them to remain temporarily see if they are still required. This makes sure your email is working as efficiently as possible.

Understanding E-mail Header Information:

Every e-mail sent has a section called the 'header'. This section includes commonly known data such as who the e-mail is being sent from and who it is being sent to along with some other information that will help you manage your spam. The header is not usually viewable in the default settings of your e-mail program. You may need to read the documentation on your e-mail program to find out how to view the header.

An e-mail header can be broken down into some basic parts. Each part is identified by a title such as "From:". Rather than getting into too much detail about all the sections, we'll just focus on the ones SpamVault looks at to filter out spam. We've highlighted the data that we'll be focussing on in red.

SAMPLE e-mail HEADER:-----
X-POP3-Rcpt: you@your-mailaddress.com

Received: from welove.spamnet.com (spammers_isp.com [209.90.160.156])

by youre-mailserver.com (8.10.2/8.10.2) with SMTP id g05HX0N10982

for <me@youre-mailaddress.com>; Sat, 5 Jan 2002 12:33:04 -0500

Message-Id: <200201051733.g05HX0N10982@spammers_isp.com>

Content-Type: text/html; charset=US-ASCII

Date: Sat, 5 Jan 2002 09:33:13 -0800

To: you@your-mailaddress.com

From: Bob Spammer <bob@phonyaddress.com>
X-Mailer: Version 5.0
Subject: You may have already won \$10,000!!!
Organization:

The "To:" Section. Info in this section shows where the e-mail was delivered to. Often, this is a weak place to put a block because spammers take advantage of catch-all e-mail boxes. They send it to Anybody@yourdomain.com and whoever has the catch-all e-mail box will get it. So you might set up a block on anything sent to Anybody@yourdomain.com. Tomorrow they'll use Nobody@yourdomain.com and get by the block of "Anybody@yourdomain.com" that you'd set up. One thing this section is good for is to stop mail from going to someone who's left the company.

The "From:" Section. In short, this is easily forged and can be changed as easily as the "To:" address. This is useful to block out those annoying friends who keep sending you chain letters. Blip, you'll never have to look at those again.

The "Subject:" Section. Now we're getting some power. Want to stop the e-mails with XXX or SEX or Work At Home in the subject line? This is the place to do that. Be careful about blocking short words such as "sex." What if the subject were, "Life is great in Essex Park"? It might be better to put a space before and after the entry so that it doesn't include anything other than the single word sex.

The "Header:" Section. Info in this section is blocked using the H (Head) trigger in SpamVault. This is one of the most powerful areas for blocking because you can block an entire network in one fell swoop. (Please note that "Powerful" does not mean easy. It means, if you use it incorrectly, you can easily block all of your email.)

There are some services that are friendly to spammers; they even encourage spamming. They permit or profit from spamming on their server network. Often, you'll get many different looking spams from one network and not realize it, because the return addresses are phony. Before we decide what to block, remember to block as little as possible by using a well targeted entry. Casting too wide a net or making a lot of unnecessary entries just makes the server work harder for no reason and will block email you will have wanted to receive. So, looking at the Received: section, here are some potential candidates for blocking in order of preference. 1) spamnetwork.com 2) spammers_isp.com (but be careful, if the guy's on America Online, you've just blocked everyone on AOL). Also, there are often more than one Received: entry, use the last one ONLY.

Spammers and Their Tricks:

We have to confess that SpamVault is not the end of all spam, but it will give you better control over your circumstances. In our test and experience we've been able to reduce spam by well over 95%. Still, spammers are always devising tricks to work around all spam-blocking software and we're constantly trying to prevent them from doing so. One way they may get around SpamVault is to trick you into blocking the wrong section of the e-mail header. Technically speaking, it's easy to fake almost all but the Header section of an e-mail. And without a trained eye, it's hard to sort out truth from fiction. You might block everything coming from one e-mail address and all they have to do is fake you out by using another e-mail address. Using this trick it can look like they're sending from a hotmail.com address today and a different address tomorrow. Here is where the power of the 'Received' section of the header comes in and why it's important to review the header of your e-mail rather than the default to and "From:" sections.

A spammer typically is not be able to change the information in the 'Received' section of the header. So, using that as a filter can be the strongest method of blocking e-mail. Please do not just paste the entire 'Received' section into SpamVault. You need to review the header for a specific server name and sometimes an IP number (but these change regularly so it is not recommended). In the example above, the network that the spam is coming from is

welove.spamnet.com. We would recommend that you only use the last and second to the last section of the network name: spamnet.com.

Spammers are using HTML-based email more and more lately. Unfortunately for them, while it's often easy to fake parts of the headers, when it comes to the body of the email, they almost always provide some method of contacting them and thus, give you something to block. It's especially hard to hide the references to their domains and IP addresses in the links of the source code. The trick is to view the source code of the email (usually by right clicking on the email itself) and then search for the text "<href=...". There is usually more than one of these. Following this is a reference to the server that the page links to. Grab just the domain name and block that. SpamVault will read that in the source code of the email as it passes through and block those emails in the future.

Many companies get duped by professional spamming companies into thinking that there's some money to be made in massive emailings. Maybe for the spammer there is. The one common theme in this type of email is that the advertisers links will probably always change in the body of the email but the "unsubscribe" link is probably directed right at the spam provider since they're the ones doing the spamming. When given a choice, I'd take the unsubscribe link domain name over the one in the body of the letter.

Error Messages:

There are several error messages that may appear while using SpamVault. Most of these are self explanatory but some may need a little further explanation.

User ID Authentication Failure: SpamVault performs a security check to make sure you arrived here from your control panel. Unfortunately, your browser is not showing the proper information. Note: This error occurs if you're blocking cookies or browser history via a firewall or within your browser configuration or if you are not accessing this program from your control panel. You should correct this and then press the line below to reload SpamVault.

If you're using ZoneAlarm Pro the best way to prevent this error is very easy and it won't compromise your security. Click the Privacy tab on the left > Select the Site List tab at the top > place a check mark in the column labeled "Private Header".

Warnings and Cautions:

When someone uses the term 'powerful program,' this is code for 'you can really mess things up with this program if you're not careful.' ***SpamVault is a powerful program*** and therefore you should be very selective in the entries you make. Adding an entry that only contains the letters '.com' in it will block all e-mail coming from any e-mail address that has '.com' in it. ***If all of a sudden your e-mail doesn't work, check your entries in SpamVault before you contact support.***

Illegal Characters. Only use the following characters in your entries as other characters such as a bracket "[" will cause very predictable results (all bad). You can use the following characters: A - Z, a - z, 0 - 9, period (.), dash (-), Underscore (_), and the At symbol (@).

Only if you are one of the very few people in the world who understand "Procmail" escape characters can you use backslash (\), forward slash (/), dollar sign (\$), exclamation point (!), quotes (" or '), and the question mark (?).

Advanced features of SpamVault

This section is a special tutorial for advanced SpamVault users. The features shown here may **not be supported** by our tech support staff and therefore you are using them *at your own risk*. The reason for this is that any mistakes in this document or in your email entries can cause you to block all of the email going to your account. Now that you've entered all the dirty words in your vocabulary and are still getting spam, here are some tips.

New Entry Filters

SpamVault works by integrating itself with the email software (called Procmail) on the server. It is Procmail that actually blocks the email and SpamVault that tells Procmail what to block. The Procmail syntax has some special characters that when used in an entry take on special meaning. SpamVault checks each new entry for illegal and sensitive characters in an effort to prevent novice users from unintentionally blocking email. This document will show you some tips on blocking emails using some of the special characters.

When you use special characters, such as those that are not "A-Z", "a-z" and "0-9", you may get a warning that notifies you that there might be a problem with some of the characters in your entry. For instance, an entry with a "%" sign will trigger such a warning even though your entry is accepted. If you use characters that have special meanings for Procmail your entry will be rejected outright.

To enable you to work with these characters, you have to edit an existing entry. Existing entries are not screened for illegal characters. For example, enter this: "Save 50%" (w/o quotes) and you'll get a caution as follows:

CAUTION: The string you entered contains characters that if not used properly can cause problems with your email. Unless you are sure you know what you are doing, try using a-Z, 0-9, period (.), Underscore (_), and the At symbol (@).

Entry Accepted but may cause trouble: [Save 50%]

Advanced users will need to use characters that if not used properly will cause problems. When these characters are entered, your entry will not be accepted through normal means and you'll get the following warning:

WARNING: The string you entered has illegal characters in it. Try using a-Z, 0-9, period (.), Underscore (_), and the At symbol (@).

Offending Entry not accepted: [!@#\$\$%^]

To get around this message you simply have to first add an entry that will be accepted. For instance add, "abcdefg" and then edit it after it's been accepted.

Feel the power...

Here are a few tricks that you can use to screen out even more spam.

Let's say you want to save space by putting several entries into one line. For instance: dog, cat and mouse. Just enter "dog|cat|mouse" (without quotes but with the pipe symbol) into one entry. This will work on the other options as well for instance the from address of more than one person: "junkmail.com|spamco.com|hateemail.com". Note: entries are taken as a whole when SpamVault looks for a duplicate and sorts them. Therefore, in the above example, if you added "dog" as a new entry, it would not be considered a duplicate.

Regular Expressions

The term "Regular Expressions" is a programming code that does not mean expressions that regular people use. It's actually a pattern-matching language. If you've ever used wild card characters, you've had some experience with Regular Expressions. There's not enough space in this help page to make you an expert in Regular Expressions. If you do study Regular Expressions in another source, make sure you're using Regular Expressions for "Procmail" (the

mail program on the server) rather than Unix or Linux. Perhaps some expressions and samples will help you catch on. Be warned, this is a very specialized field that is not common knowledge among our techs and the following items are not strongly supported.

Using the example above of "Save 50%", what if you get another email that reads, "Save 70%" or "Save 79%?". Instead of making 100 entries to cover most of the possibilities, you would edit the "Save 50%" to read "Save .*%". The period-asterisk combination mean "any character or characters". From now on, if I use {brackets} it means the meaning of the word in the brackets not the literal words. For instance, to type in {space}, meaning a space, you press that long horizontal key at the bottom of your keyboard. Therefore this entry now blocks any entry with the letters "Save" + {space} + {any character or characters} + "%". Be warned, this is a good filter for the subject line but not the body of the email because the body (or even the header) might contain "I thought this would save money but I'm just not 100% satisfied". Note that the entries are not case sensitive and this client who needs immediate attention may get lost in the shuffle.

Here's a quick and general tutorial on Regular Expressions.

A dot '.' matches *any character except a newline*. So, the expression

.ob Jones

will match the string "Bob Jones", but also "Rob Jones" and "Qob Jones", too.

Any character followed by a star '*' matches that character repeated 0 or more times. Thus,

Bob* Jones

matches "Bo Jones", "Bob Jones", or "Bobbbbbbbbbb Jones". The expression ".*" matches any number of unspecified characters.

Related are the '+' and '?' modifiers. The expression "a+" matches *one or more* a's. The expression "a?" matches *zero or one* a.

You can use parentheses to group an expression for use with a modifier. So, the expression

B(ob)+

matches "Bob", and also "Bobobobobobob".

If one character in a pattern could be one of several, you can use a *character class*. For example:

Part [abcd]

matches "Part a", "Part b", "Part c", and "Part d". If the first character of a class is '^', the class matches anything *_not_* in the class. For example:

[^aeiou]+

matches any series of one or more non-vowel characters.

One more operator is the '|' (vertical-bar) character. It is used to match either of two expressions. For example:

Bob|Joe

will match "Bob" or "Joe".

The last two special characters I want to mention are '^' and '\$'. Incidentally, here I'm referring to a '^' that *isn't* inside a character class. '^' means the beginning of a line, and '\$' means the end of one. So,

Learning by example

One of the tricks used by spammers is to send HTML formatted email with links and pictures and other goodies. One work-around they've used to block filtering is the use of HTML `<!-- comments -->` that break up words like this. "To Unsub`<!--comment-->`scribe just cli`<!--comment-->`ck here!". When viewed in the browser the comments disappear and the sentence looks like this, "To Unsubscribe just click here!". Now when someone screens for the word "Unsubscribe" or "Click Here" the search fails because SpamVault is looking at the source code of the email. Since normal people don't use HTML comments in their letter, why not search for comments themselves? Just make an entry like this "`[<!--.*-->]`" and any email with hidden `<!--{any characters}-->` will be gone. Note: if the spammer uses a graphic button that reads, "click here" rather than an HTML text or input button, SpamVault will not read the graphic. As a general rule, always put your greater or less than `<symbols>` in square brackets like this `[<]` and `[>]`. Not doing so causes bad things to happen.

Another item to search for is the domain name within the source code of the email. Search for the @ symbol in the source code of the email and it will be followed by the domain name. Just use the "domainname.com" and not all the other stuff around it. So rather than blocking one address like someone@thespamnetwork.com, block everyone there by using "@thespamnetwork.com".

Many spammers use IP numbers as well. Just use the numbers themselves and not all the stuff around them. For example: 123.12.1.32.

And how about those emails that have "something silly for sale ie8383"? Let's use the above example to block a bunch of spaces followed by at least three characters. Use this: "`[< ...[]>`". This blocks any subject with a bunch of spaces followed by at least three characters at the end.

Many people have requested that I provide a default list of blocks in every new install of SpamVault. However, not everyone wants to block the same email as I do. So, I've included the chart below which is a series of advanced filters that I use and you may find helpful by adding them to your entries in SpamVault. In the chart, the left column shows which part of the email this was designed for, H=header, F=from, T=to, S=subject, and B=body. As you'll see, the body is one of the strongest areas used to block spam. The column on the right in bold is the entry you can put into SpamVault followed by a comment about this particular filter. Note the spaces, which are critical.

H	<code>.*@.*@.*@.*@.*@.*@.*@</code>
	Multiple CC'd names when someone CC's 7 or more people.
S	<code>...</code>
	Several spaces and 3 periods. Blocks a series of spaces followed by some characters in the subject line. "Something Silly for Sale ie84477"
S	<code>ADV: <ADV > ^ADV.</code>

	Several forms of ADV in the subject line. Make sure you put a space after it.
HS	00.*per day 00.*per week 00.*per month
	Block text like "Make 10,000 'per day' or 'per week' or 'per month'"
S	[0-9]*%
	Gets rid of text that contain a number then a %. "50% off" and "Save 80%"
B	[<]http[:]//.*[/remove/.]*[>]
	Gets rid of any links which include a directory named "remove" somewhere in the link.
BS	HGH H G H H-G-H
	Several forms of HGH
B	MLM
	{Space}MLM{Space}. Multi Level Marketing
B	8.5.2.-.2.7.8.0.-.3.2.5.7
	This is a phone number that may or may not be spaced out. Phone numbers are a prime target because they're hard to change.
B	po Box 914
	Phone numbers, addresses work well
B	@%77%77%77
	The equivalent of www in an email address in the body. However the spammer tried to obfuscate it.
B	A HREF[=]3D
	This is a link with "3D" in it to stop spam blocking software from catching it. Some HTML email created with MS Outlook Express will have these in them so be careful because your friends might not be able to send their email through.
B	[<].*MARQUEE STYLE.*[>]
	Scrolling marquee usually created by MS Front Page and I don't know very many people who write their email in FrontPage.
B	opt.in email
	The words "optin or opt-in" email. Very few of my friends ask me to opt-in to their emails.
B	S. 1618
	Senate Bill S. 1618 never passed to allow spam but they sure like to quote it.
B	[/]mortgage[/]

	/mortgage/ subdirectory
B	[/] mothersday [/]
	/mothersday/ subdirectory popular in June.
SB	[0-9] year fixed
	Any year fixed mortgage
B	[0-9][0-9][0-9][0-9][0-9].com
	A link with several numbers in the domain name. "494938.com"
B	[<] href..http..[1-9][0-9][0-9].[0-9][0-9][0-9].* [>]
	A link that uses an IP address rather than a real domain name.
B	[<].* bgcolor=..000000.*font color=..000000.* [>]
	If your back ground color and your font color are black, you're hiding something.
B	[<].* content..Microsoft FrontPage.* [>]
	Any email created in Front Page is probably not worth reading anyway.
B	[<].* target?._blank.* [>]
	A link that pops open another browser window.
B	[<] ROWSPAN.* [>][<] COLSPAN.* [>]
	Column span or row span tags. When was the last time you put those in your email?
B	[<] SCRIPT LANGUAGE.* [>]
	Java Script in email
B	[<] TABLE=.* [>]
	Commonly used in legitimate emails so you may need to watch your logs and make entries to your white list if you wish to use this very effective entry.
B	[a-zA-Z][<!-.*-->][a-zA-Z]
	Comment in the mi<!--comment-->dble of words.
B	[<] form.* [>]
	Never saw a form in an email that wasn't spam
B	[<] a href.*http[:]/*.*mortgage.* [>]
	Any link with the word "mortgage" in it.
B	[ÿ£ÉÓÑÔ]
	Any of several forign characters
B	.com.br [^ a-zA-Z]

	End of a domain name from Brazil and not followed by a space or letter
B	[<].*font color???ffffff?.*[>]
	Tag for Font color white
B	v[^a-zA-Z]i[^a-zA-Z]a[^a-zA-Z]g[^a-zA-Z]r[^a-zA-Z]a
	Viagra broken up by non alpha characters such as comments or whatever.
B	[<]href=.http://*%.*%.*%/.*[>]
	Obfuscated url is always spam

A small portion of this tutorial has been taken from <http://userpages.umbc.edu/~ian/procmail.html>.

Credits

As the writer of SpamVault, I wish to thank you for using my program. I originally wrote SpamVault for my own use and then found that there were a lot of people who had the same needs to block spam. I humbly would never claim that this is the best spam blocker program in the world, but I do hope you enjoy this tool as much as I have enjoyed writing it. I can successfully block about 98% of spam using this tool. No animals were harmed in the creation of this program.

If you have any suggestions or comments or, heaven forbid, you find a bug, please contact your service provider and they will notify me. They are also the first line of technical support and will contact me if there's a problem with this program.

SpamVault Copyright 2000-2004 and Trademark of GraphiComm Inc., Streamwood, IL. All rights reserved.