Using SPAVAS

Virus detection

When SPAVAS detects a virus, or any other threat, within an email, it will attempt to disinfect it and deliver it to you.

If disinfection is successful, the remainder of the email will be delivered to you, but with the word "VIRUS:" as a prefix to the original subject line. Information about the virus or threat that has been removed will be provided at the beginning of your mail. It is safe to open these messages.

When disinfection is not possible, SPAVAS will notify you that the infected email has been deleted. This notification will appear to have come from the original sender, but with the word "VIRUS:" as a prefix to the original subject line and will only contain information about the virus or threat found. It is safe to open these messages.

Please note that many viruses fake the sender's email address so there is often limited value in informing the sender that they may have a virus infection.

Spam detection

The SPAVAS system examines the characteristics of each email.

Emails, which are definitely spam are automatically discarded and those identified as legitimate are delivered unaltered.

Emails, which are probably spam, are held in quarantine for 28 days, just in case any of them are legitimate but have been misclassified.

When an email is quarantined as suspected spam, you will be sent a notification email which will appear to have come from the original sender, but with the word "SPAM:" as a prefix to the original subject line. The sender and subject line provides a good indication as to whether an email is spam or is a legitimate email that has been misclassified. If you decide that it is legitimate, the original email can easily be retrieved from quarantine by using the simple procedure below (these instructions will also be included in the notification email).

Retrieving mail misclassified as spam from quarantine

To retrieve a mail that has been misclassified simply "Reply" to the notification and SPAVAS will automatically deliver the original mail to your inbox.

The retrieved email will have the subject line prefixed with the word "RETRIEVED:".

Please note that retrieved emails may not appear at the top of your Inbox but may appear at a position corresponding to the date and time of the original message.

Reporting missed spam

Occasionally, the SPAVAS system makes a mistake and misclassifies a spam email as being legitimate and delivers it and retrieved quarantined items are often discovered to be spam after. These are usually messages which are borderline spam/legitimate which some people may want and others not. To optimise the accuracy of the SPAVAS system, it is important to report the mistake by clicking on the "SPAVAS: Report this message as spam" link at the foot of the message so that the SPAVAS system re-learns the message as spam.

Managing notification messages

The use of the prefix "SPAM:" in the subject line of notifications makes identification in your Inbox easy and creates the opportunity to use a sorting rule in your email program to automatically move them to a particular mail folder.

Most users create a message rule in their email program, which moves all mail with "SPAM:" in the subject line to a specific mail folder for junk email. It is important to include the ":" in the term to be searched for in the subject line (and only the subject line) otherwise messages which mention "spam" in the subject, or elsewhere in the email, will be moved in to the spam folder. Additional information about creating message rules for handling spam notifications can be found here.

White and black lists

Adding to the white list

If email from a legitimate correspondent is regularly misclassified as spam, you may wish to add them to your white list, so that future emails from that address will not be treated as spam.

There are three ways of adding an email address to your white list:

- Send an email to whitelist@spavas.net with the email address as the subject line; the mail body can be empty.
- Forward an email from the person you wish to add to your white list to whitelist@spavas.net
- When retrieving a misclassified spam from quarantine, "cc" the email to whitelist@spavas.net.

You can white list all email addresses under a domain name by sending an email to whitelist@spavas.net with "DOMAIN:" followed by the domain name as the subject line; the mail body can be empty.

In all cases above, you will receive an email in response, to which you must reply to confirm the addition.

Adding to the black list

If spam from a particular email address regularly reaches you, then you may wish to add it to your black list so that future emails from that address will be treated as spam and automatically discarded.

There are two ways of adding an email address to your black list:

- Send an email to blacklist@spavas.net with the email address as the subject line; the mail body can be empty.
- Forward an email from the person you wish to add to your black list to blacklist@spavas.net

You can black list all email addresses under a domain name by sending an email to mailto:blacklist@spavas.net with "DOMAIN:" followed by the domain name as the subject line; the mail body can be empty.

In all cases above, you will receive an email in response, to which you must reply to confirm the addition.

White/ black list management

You can obtain a list of email addresses and domain names contained in your white list by sending a blank email to whitelist@spavas.net with the subject line "list". A similar list of those on your black list can be obtained by sending a blank email to blacklist@spavas.net with the subject line "list"

You can move an email address from your white list to your black list and vice-versa by adding the email address to the appropriate list.

If emails from a number or correspondents are falsely classed as spam or more than a few spam mails are not detected, then you may wish to alter the spam score threshold at which emails are classed as spam or legitimate. You should contact the person with responsibility for the SPAVAS system in your organisation in order to do this.

FAQs

I used to get lots of spam mails, why am I getting so few spam notifications now?

Every email processed by the SPAVAS spam filters is assigned a spam score. Those messages that are assigned a very high spam score are extremely unlikely to be legitimate and are automatically discarded.

For messages which are assigned lower scores (between your spam threshold, normally 50%, and the discard threshold, normally 99%) you will receive spam notifications to enable you to decide if they are legitimate or spam. Most people receive up to five notifications per day.

I still get some spam, why isn't it all being stopped?

It is impossible to stop all spam without misclassifying legitimate messages as spam. The aim is to minimise both the number of emails misclassified and the number of spam notifications sent to the user, to minimise the time wasted dealing with them. SPAVAS, when properly tuned, should detect more than 99% of spam. This means that the average user can expect up to three spam messages per week to be undetected and about one legitimate message per fortnight to be misclassified as spam and quarantined, requiring retrieval. Most of these will be automated, usually promotional messages from organisations which you may have a previous connection with which some people will regard as legitimate and other as spam. If you are receiving significantly more undetected spam or have to retrieve a lot of messages from quarantine, then please contact the person within your organisation with responsibility for the SPAVAS system for assistance.

What is a spam score?

The spam score is a rating generated by the SPAVAS spam filters to indicate how likely an email is to be spam. The score is based on a number factors including its origin (i.e. does it come from a known source of spam?) and technical aspects about the mail as well as its composition and content.

You can view the score assigned to each mail in the internet mail headers of the message. Access to the internet headers is to be found in:

- **Microsoft Outlook**: by opening the message in its own window and selecting "Options" from the "View" menu.
- **Microsoft Outlook Express:** by selecting "Properties" from the "File" menu and clicking on the "Details" tab.

Some legitimate emails, other than SPAVAS spam and virus notifications are ending up in the Junk E-mail folder, what is happening?

SPAVAS spam and virus notifications are easily recognisable by the "SPAM:" and "VIRUS:" prefixes to the subject lines. Their message bodies are replaced with information about how to retrieve the complete message from quarantine. For efficient management of these notifications, most people use email or messages rules within their email programs to automatically sort them into the Junk E-mail folder. There are two reasons why this may be happening:

1. The email/ message rule is being triggered and the email is being moved to the Junk E-mail folder because the rule has been created to match the words SPAM or VIRUS without the colon (:) and the messages contain spam or virus elsewhere within the subject line. You

should modify the email/ message rule to include the colon character to solve the problem.

2. Your email program or mail server has built-in spam protection and it is misclassifying legitimate email as spam and moving it to the Junk E-mail folder.

   For example, some versions of Microsoft Outlook have built-in spam protection which is enabled by default. It is considerably less effective than SPAVAS at both detecting spam and can misclassify significant numbers of legitimate emails as spam. To avoid this problem, we recommend that it you disable this filter altogether or switch it off for email addresses which are protected by SPAVAS. Continuing its use is extremely unlikely to catch any spam missed by SPAVAS and is only likely to cause problems by misclassifying legitimate emails as spam.

   In Outlook versions 2002(XP) and 2003, this can be done by opening the "Actions" menu, selecting "Junk E-mail" and then clicking on the "Junk E-mail Options" item to open the "Junk E-mail Options" dialog box.

   To disable Outlook's spam filter select the "Options" tab and click on the "No Automatic Filtering" radio button and press the "OK" button to finish.

   To restrict the use of Outlook's spam filter to addresses protected by SPAVAS, select the "Safe Recipients" tab and enter the list of those email addresses or domain names before clicking the "OK" button to finish. You should leave the settings on the "Options" tab unchanged.

   In Outlook 2000, spam filtering is not enabled by default and is configured on a per folder basis. For example, to disable it for the Inbox, select the "Inbox" and open the "Ways to Organise Inbox" pane by opening the "Tools" menu and selecting "Organise". Click on the "Junk E-mail" tab and press the "Turn Off" button to disable Junk E-mail filtering for the Inbox; you may have to do this for other folders if email is automatically moved there using email/ message rules.

   Some networks may be configured so that users may not have permission to change these settings, which can only be done by the network administrator.