



SPAM & Virus FAQ

SPAM filtering service

Can I still use your service if I have my own mail server?

Yes. This service is available for customers with their own mail servers. This service also gives the added security of masking your mail servers from the Internet.

What exactly is SPAM?

The Internet community has adopted the term SPAM to identify unwanted / unsolicited junk email. It is estimated that 36% of all Internet email traffic is unwanted SPAM mail.

Why is [SPAM]: showing up in the subject line of my emails?

Your email account or domain has been enrolled in the SPAM filtering service. If your email account ends in @sterling.net or @sterlink.net the SPAM filtering service is enabled by default. If you have your own custom domain, the SPAM filtering service has been enabled by your company.

I received a legitimate email with [SPAM]: in the subject line. What should I do?

Our spam filters are very effective at detecting SPAM email, however, like most technology it is not perfect. If you received an email that has been incorrectly tagged, please forward a copy of the email to nospam@sterling.net and note that this email should NOT be marked as spam. We will place the senders email address in the "never mark as spam" list.

I received an email that SHOULD have been marked as [SPAM]:. What should I do?

Our spam filters are very effective at detecting SPAM email, however, like most technology it is not perfect. If you received an unsolicited SPAM email just forward a copy to nospam@sterling.net and include the full email header. If you are unfamiliar with obtaining the full email header please go [here](#) .

Why do you just tag the email rather than delete it?

Email has become an essential form of communications that relies on the guaranteed delivery of messages. At Sterling Communications the integrity of the email system is very important and the likelihood of deleting a false positive, even though very small, is unacceptable. We have taken the position to allow our customers to determine what to do with spam mail. By identifying the mail as spam the customer can choose to delete the email or file it for later review.

We do take exception in the area of SPAM pornographic email. In the event that an email is determined to contain pornographic content, it is returned to the sender.



We do have an option that will delete the email before it is delivered. This option is recommended for accounts that are used by children. If you would like to enable this feature please send an email to support@sterling.net and request the delete option for SPAM filtering service. Please include the email address(es) for the requested accounts.

How do I setup my mail client to file the [SPAM] tagged email in another folder?

We are currently in the process of developing these instructions. In the meantime, please visit our [technical support page](#) or send mail to support@sterling.net.

I don't want SPAM or Virus scanning. How do I get it turned off?

If your email account ends in [@sterling.net](#) or [@sterlink.net](#), please send an email to support@sterling.net requesting to be removed from the SPAM and Virus filtering service. All other requests must come from an authorized agent for the email domain.

VIRUS scanning service

Why do I need your service, I already have a Desktop based virus Scanner?

Desktop-based virus scanners are a necessity in today's computing environment. However, it is not enough. New viruses are being created every day. It is impossible for any single virus scanning company to provide 100% virus protection.

The VIRUS scanning service offers the following advantages in conjunction with your desktop-based virus scanner:

- Provides the resources of two company's development efforts to detect viruses, thus giving you more protection. Think of a Desktop virus scanner as having a car with only a driver side airbag. Using the Sterling VIRUS scanning service would be like adding the passenger and side airbags for added protection.
- Gives added protection in case of a lapse in the management of the desktop-based virus-scanning product.
- Helps reduce the resource requirements on the desktop systems by offloading the initial virus scanning to the Sterling servers.

Am I guaranteed to never get a virus?

No virus protection method can guarantee that you will never get a virus. However, there are products, services, methods, and procedures that can be put in place to greatly reduce the risk. The VIRUS scanning service is one of those services. We use a highly effective virus-scanning product that is updated with the latest virus definitions every day. For the most comprehensive virus protection scheme we recommend utilizing the VIRUS scanning service in conjunction with a desktop virus-scanner.



Can I stop using my PC based virus scanner if we use the VIRUS scanning service?

No, The Sterling VIRUS scanning service only scans email messages for viruses. Email is only one of the ways in which a virus may be propagated. Using the Sterling VIRUS scanning service in conjunction with a desktop-based virus scanner is the preferred method for providing the most effective virus protection. The following is a list of added benefits:

- No single virus-scanning product is 100% effective. Using a desktop-based scanner along with the Sterling VIRUS scanning service gets you closer to that 100% mark.
- Desktop-based virus scanners are only effective if they are updated on a regular basis. The Sterling VIRUS scanning service gives you added protection for any lapse in on-going maintenance of the desktop product.

What if we have our own mail server, will the Sterling VIRUS scanning service still work?

Yes, the VIRUS scanning service works regardless of whether you use the Sterling managed mail servers or you have your own server. Besides the standard benefits of the VIRUS scanning service, the following are additional advantages for customers with their own mail servers:

- Provides a mail store-and-forwarding service. In the event that the customer's mail server is down or their Internet connection is unavailable, the Sterling VIRUS scanning system will store the message for up to 2 days for later delivery when the customer's mail server is backup up.
- Helps reduce the resource requirements on the customer's email system by offloading the initial virus scanning to the Sterling servers.
- Masks the true IP address of the mail server to deny hack attempts.

Why does the VIRUS scanning service choose to delete the virus-infected email rather than forward it on?

The approach we have taken with the Sterling VIRUS scanning service is to delete all virus-infected emails and to send a notification to the sender of the email. The reasons for this are as follows:

- Virus infected emails contain no beneficial information.
- Many viruses cannot be removed to create a safe email message. This may create a situation of forwarding an email that may still be infected.
- Provides for a higher level of protection and integrity of the virus scanning system.

How to get the full email header:

Outlook 97, 2000, 2002:

- Right-click on the message in your Inbox and select "Options..."
- In the "Message options" window select all the information in the "Internet headers:" and copy it using the mouse cut and paste feature.



Outlook Express (Windows):

- Right click on the message in your Inbox and select "Properties".
- Click on the "Details" tab.
- Copy all the information in the "Internet headers for this message" box using the mouse cut and paste feature.

Outlook Express (Macintosh):

- Select the message in your Inbox.
- Choose "Source" from the "View" menu. A new window will appear containing the email message with the full header.
- Press "Command+a" to "select all". This will copy the entire email and header information in the paste buffer.
- Create a new message and press "Command+c" to paste the full header and email.

Netscape:

- Open the email message.
- Click on "Message Source" in the "View" drop-down menu. A new window with the message header should appear.
- Copy all the information using the mouse cut and paste feature...

Eudora (Windows and Macintosh):

- Open the email message.
- Click on the button labeled "Blah Blah Blah".
- Copy all the information in the message window using the mouse cut and paste feature.