

## Mail Scanning Service FAQ

This list of Frequently Asked Questions is provided to help you understand the Mail Scanning Service.

- **Will spam be deleted before I retrieve my email?**  
Mail that is 99.9% certain to be spam is deleted although you can configure Mail Scanner to deliver that as well and it will be marked {Definitely Spam?}. Other email reported by the system as spam will have the subject line modified to include {Spam?} and header records added (tagged) to indicate them so that you can automatically filter them from your inbox and place them in a separate folder so that you can check them at a later time.
- **Should I tell you about incorrectly tagged spam?**  
Not unless it is an email from someone you regularly receive email from. The simplest thing to do would be to add an extra inbox rule in your email client to keep email from them in your inbox. Alternatively, you can add them to your whitelist in the cPanel MailScanner configuration.
- **Will all spam be detected?**  
No. All the email is scanned and assigned a score based on the likelihood that an email is spam. Thresholds (low scoring and high scoring spam) are used to determine whether an email should be tagged as spam: it is important that this is done to help avoid false-positives and false-negatives.
- **Is all email tagged as spam, spam?**  
Not necessarily. The system is not foolproof and there will be instances where legitimate email is tagged as spam and where spam is not tagged as such. This is why email is delivered, so you can filter them email in your email client and check through the spam to ensure there is no email that you actually need.
- **I don't need (spam/virus) checking, can I only have email scanned for one?**  
Yes, you can configure the service to either scan for viruses, spam or both.
- **Will viruses be deleted before I retrieve my email?**  
All emails and file attachments will be scanned for viruses. If one is found, the virus is removed from the email before it is delivered to your mailbox, a text file attachment will be added to the email notifying you of the virus infection. Removed viruses and dangerous file attachments removed from email may be stored in a quarantine area on the server for 30 days. You can request the file from quarantine as described in the text file attachments, or , preferably ask the sender to resend the file in a zip archive.
- **Will all viruses be detected?**  
No system can guarantee 100% detection, though nearly all infected files and dangerous file attachments should be detected using this service. The service scans all email received and sent through the server to help ensure that you do not accidentally start spreading a virus yourself.
- **Do I still need a virus scanner on my computer?**  
Yes! Not only can the service not guarantee that all email viruses will be detected, there are many other ways that your computer can become infected. You should always install an anti-

virus solution on every computer and ensure that it is constantly kept up to date.

- **How do I know whether and email has a virus or is a spam?**

There are two methods used to identify these emails to you. Firstly, the subject line of the affected email will be prefixed with one of the following:

- **{Disarmed}** - indicates that the email contained html tags that are considered dangerous, e.g. iframe and form tags
- **{Virus?}** - indicates that the email contained a virus and has had the attachment removed.
- **{Filename?}** - indicates that the email contained a dangerous file attachment which has been removed.
- **{Spam?}** - indicates that the email is likely to be spam - you should filter these emails into a separate folder in your email client.
- **{Definitely Spam?}** - indicates that the email is almost definitely spam because it got a very high detection score - you should filter these emails into a separate folder in your email client. [These emails are deleted by default for Cobourg Internet Clients – you can modify this if you want in Cpanel].

Secondly, additional headers are added to the email:

- **X-\_\_\_\_\_ -VirusCheck: Found to be clean** - indicates that the email passed the virus scanning tests.
- **X-\_\_\_\_\_ -VirusCheck: Found to be infected** - indicates that email email contained a virus which has been removed.
- **X-\_\_\_\_\_ -SpamCheck: spam** - indicates that the email is likely to be spam and contains information on how the score was reached.
- **X-\_\_\_\_\_ -SpamScore: sssss** - indicates the spam score for the email. Each s represents 1 point, so sssss indicates a score of 5. The service has a default threshold of 5 for {Spam?} and 20 for {Definitely Spam?}

- **Can the system simply delete all email marked as spam?**

We advise against this as it is possible that legitimate email will be deleted and the sender will never know that you didn't receive it. We recommend filtering the email in your email client and placing it in a separate folder so that you can check through it in your own time.

If you're happy that email marked as {Spam?}, and/or more suitably {Definitely Spam?} you can then configure MailScanner to delete that email.[Cobourg Internet default is to delete mail marked {Definitely Spam?}.]

Another alternative is to have all email marked as {Spam?}, and/or more suitably {Definitely Spam?} delivered to a specific email address. For example, spam@mydomain.com.

- **How do I configure my email software to filter spam into a separate folder?**

You should create a separate folder in your email client called Spam. You should then create an inbox rule to place any email containing the strings {Spam?} or {Definitely Spam?} into that folder.

We have instructions on how to do this with Outlook Express and Outlook in a separate document.

- **What can I do to prevent receiving spam?**  
Have a look at the self-help checklist below

### **Anti-Spam Self-Help Checklist**

Here is a list of things you can do to help prevent receiving spam in the first place:

- Do not use a catchall email account on your domain(s). Only list aliases and POP accounts that you actually use. This stops the frequent spams that fire off emails to a list of names on a domain. [No client of Cobourg Internet uses this].
- Obfuscate your email addresses on your website, i.e. replace them with JavaScript "trick" email addresses, or, switch to web forms for initial contact, rather than displaying an email address. [Most Cobourg Internet sites already have this option].
- Never, ever, click on any links in any spam - especially not to "unsubscribe". All this does is confirm to the spammer that they have a "live" address.
- Configure your client to read any incoming emails in plain-text, never html. Html spam emails contain links to graphics and scripts on spammers sites, confirming your email address.