CHAPTER 4

Troubleshooting

Why Spam Got Through

In most cases, the user receiving the message was not registered in the Email Control service. Follow these steps to determine what happened:

If too much spam is getting through to users' inboxes, follow these steps to determine why:

Step 1 Has the user been added to the Email Control service? If not, and Non- Account Bouncing is turned off for the user's domain, and no Catchall user is enabled for the domain, mail is delivered to the user without filtering.

Search for the address on the User's tab. If a user isn't found, add the address to the service:

- If the address is associated with another user that's already been added, add the new address as a user alias.
- If the service could recognize the address via domain aliasing, create a domain alias for the user's domain.

To ensure that all valid users are added to the service, consider enabling SMTP Autocreate for the user's domain, which adds users automatically.

Step 2 Is the user's spam filtering turned on?

Go to Spam Filtering on the user's Overview page and verify that the Filter Status is On. If it isn't, turn it on.

If the user has User Access permissions to turn their own filters on and off at the Message Center, and the filters have been turned off, instruct the user not to do this, and consider removing that particular permission.

Step 3 Is virus blocking turned on, and with a proper disposition?

Go to Virus Blocking on the org's Organization Management page and verify that Virus Blocking is On.

Also make sure the Virus Disposition is not set to Message Header Tagging, because if it is, all messages containing viruses will be delivered to your server.

Step 4 Are the user's category filters set high enough to catch spam?

Go to Spam Filtering on the user's Overview page and verify that the Bulk Email and other category filters are set high enough. If they aren't, adjust them accordingly. If they look OK, go to the next step.

Step 5 Was the message sent to a distribution list rather than an individual user?

If a message is sent to a distribution or mailing list that hasn't been added to the Email Control service as a user alias, it will pass through to users without spam filtering. Review the message's header to determine the TO address. Then search for that address on the Users tab. If the list isn't found, add it as a user.

Step 6 Was the message sent directly to, and accepted by your mail server, bypassing the Email Control service?

Sometimes users' email is delivered to them from more than one mail server. Messages from another server that isn't mapped to an email config in the service don't go through the ScanSafe data center and therefore aren't filtered. Many email clients put these messages in the same inbox as filtered messages, so users might believe they received spam from a protected server. Review the message headers to make sure they include an email server registered with the service. If they don't, please contact ScanSafe Technical Support for further details.

Step 7 Did a user within your organization send the message?

Unless you reconfigure your email server to send all email outside the server, rather than delivering to local users locally, messages exchanged among users on the same server aren't processed by the data center, and therefore aren't filtered for spam. Review the message headers to see if the email was sent from someone on the recipient's same server.

Step 8 Was the sender's address in an Approved Senders list?

If the sender or sender's domain is on an Approved Senders list - either the user's personal list, or a list defined for the user's org - messages from those senders will be delivered, regardless of spam-like content. This is also the case if the spammer has spoofed the sender address so it matches an Approved sender. Review the user- and org-level lists and delete any large and well-known domains that are often spoofed by spammers.

Remember that users don't have visibility of their org's Approved Senders list, so they might be confused as to why spam from a sender on this list would not be filtered.

Step 9 Has the user added their own address or domain as an Approved mailing list, at the Message Center?

If so, all spam addressed to the user, regardless of any spam settings, will be delivered to their inbox. In the Administration Console, go to the user's User Settings page and select Lists. If you have administrative privileges, remove the user's address or domain from the Approved Recipients list. Then let the user know why adding their address or domain here is not a good idea.

Step 10 Does the email content have enough spam characteristics to trigger filtering?

In general, if all prior steps have turned out to be false, the spam did not have sufficient spam characteristics to be filtered.

However, if a large amount of spam is still slipping through the filters, evaluate the spam score in the message header using the Support Portal's Message Header Analyzer. If the score is above 2.0000 and it has been through the security service,, please contact Technical Support.

Note You will be asked to enclose the message as an attachment to an email and send to Technical Support. By sending the spam as an attachment, analysis can be performed on copy of the original email with headers intact; otherwise, the message will be unusable. ScanSafe's service engineers evaluate these messages to make improvements to the filtering engine. The messages are used for statistical analysis.

Why a Virus Was Not Filtered

In most cases, the user receiving the message was not registered in the Email Control service. Follow these steps to determine what happened:

Step 1 Has the user has been added to the email protection service? If not, and Non-Account Virus Blocking or Non-Account Bouncing are turned off for the user's domain, mail is delivered to the user without filtering.

Search for the address on the User's tab. If a user isn't found, add the address to the service:

- If the address is associated with another user that's already been added, add the new address as a user alias.
- If the address could instead be recognized by the service via domain aliasing, create a domain alias for the user's domain.

We highly recommend turning on Non-Account Virus Blocking and also ensuring that allusers are automatically added to the service for virus protection.

Step 2 Is Virus Blocking turned on for the user's org, and with a proper disposition?

Go to Virus Blocking on the org's Organization Management page and verify that Virus Blocking is On. If Virus Blocking is Off, turn it On.

Also make sure the Virus Disposition is not set to Message Header Tagging. If it is, all messages containing viruses will be delivered to your server.

Step 3 Was the message sent directly to, and accepted by your mail server, bypassing the Email Control service?

Sometimes users' email is delivered to them from more than one mail server. Messages from another server that isn't mapped to an email config in the service don't go through the ScanSafe data center and therefore aren't filtered. Many email clients put these messages in the same inbox as filtered messages, so users might believe they received spam from a protected server. Review the message headers to make sure they include an email server registered with the service. If they don't, please contact ScanSafe Technical Support for details.

Step 4 Was the virus only recently discovered?

The email may contain a virus that the virus engine did not know about. There is a lag time between the initial outbreak of a virus and the implementation of an update to the antivirus definition file that allows the virus engine to detect (and thus quarantine) the virus. This time is usually very short, but on rare occasions, new viruses might get through in the meantime. Contact Technical Support to establish the date and time when the virus definitions were updated for this particulate virus.

Caution Cisco highly recommend that you configure Attachment Manager to quarantine or block executable and compressed files, which are typically the delivery mechanisms for viruses.

If the date of the infected message was before the protection date and time, this is the source of the virus delivery. Otherwise, proceed to the next step.

Step 5 Check the file size of the virus attachment.

If the virus was delivered after the protection date and time determined above, compare its file size with the documented size of the virus (contact Technical Support for details). If your virus is significantly smaller, the virus payload was truncated, making the virus inert and preventing detection. Viruses like this can be deleted since they pose no threat.

If after these steps you still haven't determined the source of the virus, submit a copy of the original virus-infected message as an attachment or as comments to Technical Support.

Why Good Mail is Quarantined

In rare instances, legitimate messages can be falsely filtered as spam. Use the Support Portal's Message Header Analyzer to determine why your message was quarantined. Some common reasons for legitimate messages being filtered as spam include:

- Filter levels are too aggressive.

  The message might have characteristics that make it look like spam, such as disclaimers, URLs, dollar signs, multiple exclamation points, and little or no body content apart from a link, image, or file attachment. The more such characteristics it has, the more likely it will be caught, depending on your filter levels.

  In particular, aggressive category filters can falsely tag valid messages as spam. Try lowering category settings, beginning with the Special Offer filter. Businesses tend to receive legitimate email containing commercial content, so false positives in this category are more likely. An aggressive Bulk Email filter can falsely tag valid emails, too, but should do so less often than a category filter.

- A listserv or news group server sent the message.

  Mailing lists share many characteristics of spam. If the sender address is always the same, for example, list_name@domain.com, add it to the user-level Approved Recipients list.

- The message was sent by an automated email service and appeared "spoofed."

  This might include a message from a group reservation or auction site. Add these addresses to your Approved Senders list.

- The sender appears on the org-level or user-level Blocked Senders list.

  Remove it from this list.

When Mail Is Not Flowing

In most cases, mail flow problems are related to the configuration of your email servers and the Email Control service, incorrectly configured MX records, or loss of connectivity to or from your email server.

Check the Delivery Manager Message Traffic Graphs

In the Administration Console, select the appropriate email server from the pull downlist.

Click the Inbound Servers tab, then the Delivery Mgr link. View the Message Traffic Graph:

- Gray Bars = Total attempted connections.
- Dark Red Lines = Failed connections.
- Light Green Lines = Spooled connections.
- Any other color lines = Delivered connections. See the legend on the graph for details about which line refers to which IP.