SpamCure from Mail-Filters.com, Inc.

Mail-Filters' Testing Options

There are four ways to test Mail-Filters' anti-spam technology. Option number 1 is the least intrusive. It does not require any changes to your environment. Option number 2 includes all 11 categories of tests and only requires a change in your DNS to redirect the email to our service. Option number 3 is the most comprehensive test. It runs on a server in your environment, includes all the categories of tests in option 2 plus our continuous and dynamic filter update process. Option 4 is for those environments where an embedded anti-spam solution is desired. This test requires integrating our technology into your software/hardware product and is accessed via our API. There is a separate document that describes this operation.

Option #1: You can filter a set of messages by forwarding them to a special mailbox on a Mail-Filters server. Mail-Filters will process the messages and divide the good mail from the spam. You can access the results on the web after we filter the messages to see how effective and accurate we are. This test would require about 5 minutes to set up in addition to the time needed to send the messages, and would provide a quick look at our effectiveness and accuracy. The messages can be of any size or volume. This technique of testing will only test our signature database, not any of the other 10 categories of tests we use to determine if a message is spam, since the header information is not available to the filter when forwarding mail.

Option #2: You can send messages directly to our in-house service, SpamRepellent. This option is similar to Option #1. The major difference is that this option will utilize all of the 11 different categories of tests included in our technology. SpamRepellent is easy to implement. It usually takes just 5 minutes to get running. To access the service takes three steps.

1. Change the MX record in DNS to have the mail flow through the SpamRepellent servers. To be clear, only inbound Internet mail flows through the SpamRepellent servers.
2. Tell Mail-Filters what you want to do with the spam:
a. Mark spam, but send it to the user for their client software to filter into folders.
b. Forward all spam to another account.
3. Give end users instructions on how to handle spam and how to customize their client filters as well as their SpamRepellent filters.

Option #3: We can provide you with a copy of the SpamCure server, our turnkey server technology, for installation in your environment to use for testing. This option allows you the freedom to put our technology through its paces by running messages on a local server to confirm its accuracy and effectiveness, utilize the signature update process and ease of administration, as well as monitor performance and scalability. SpamCure is very simple to install and maintain. Installation usually takes about 30 minutes and ongoing maintenance is almost zero. To get the system up and running takes four steps.

1. Install the SpamCure server software on a Windows 2000 Server (UNIX and Linux available soon) machine.
2. Configure the server to recognize where the e-mail server is and to handle spam as defined by the administrator. Spam can be handled in two general ways:
a. Mark spam, but send it to the user for his client software to filter into folders.
b. Forward all spam to another account.
3. Change the MX record in the DNS to have the mail flow through the SpamCure server.
4. Give end users instructions about how to handle spam and how they can customize their client filters as well as the SpamCure filters.

Option #4: We also offer our technology as an integrated service using our API. After you have had a chance to test our technology, we can talk about the benefits of using our API to implement an integrated solution.