

## **SpitShine™ Spam and Virus Filtering**

### **Email Solutions**

Spam is not only an annoyance to all who receive e-mail, but can also be a danger to your computer and/or network. Spam is often used to deliver viruses, Trojan horses, and malicious applications. MessageLabs.com reports that as of May 2003 spam now accounts for 50% of all business e-mail traffic. It's been predicted that by April 2004, spam will represent 70% of all e-mail traffic. To substantially reduce spam traffic and virus infection, your company must initiate a proactive prevention method.

LIHQ's SpitShine™ Spam & Virus Filtering is a comprehensive solution for the elimination of these annoyances, having proven to be 98 to 100% effective with our installed customer base. SpitShine™ Spam Filtering safely identifies, tags and (if you desire) quarantines spam, using a combination of heuristics, public and private spam directories, and spam signatures.

### **Features**

Whitelist / Blacklist - this works as a pre-configured method of identifying from whom you are receiving email. The whitelist identifies the sender as "safe", while the blacklist blocks any URL or email address you don't recognize or wish to reject.

Configurable options for processing the spam such as pre-pending the subject line of the email with an indication that the message failed a particular spam test, modification to the header of the email, a header or footer message placed inside the email, rerouting to a different email address or simply quarantining the offending emails all together so they never reach your users.

Web based interface for managing domain configurations and quarantine.

Up-to-the-minute virus updates to protect your users and your servers from email viruses (included free).

### ***Can my company try the service before we buy it?***

Absolutely! In fact we encourage it. Once you try the service for 30 days you will see how easy it is to setup and how valuable it is to your users.

*Can you assist me with my configuration or if there is a problem with my messaging server?*

Yes. We have certified system engineers available to assist you with any configuration problems should they arise.

*What if I have additional questions?*

Please feel free to contact us with whatever questions you may have.

Call 516-393-7800 or email: [info@pb.net](mailto:info@pb.net).

## **Auto-Whitelisting**

### **LIHQ's Challenge/Response system**

Challenge/Response is an old idea, and one which has been used by mailing list management software for years, but it's surprisingly effective against spam.

### **LIHQ's Whitelist-centric Strategy "*Deny everything that is not explicitly allowed*"**

With LIHQ's Whitelisting, unrestricted access to your mailbox can no longer be assumed, a premise which spammers rely heavily upon.

The way this thwarts incoming junk-mail is simple yet extremely effective. You maintain a "whitelist" of trusted contacts which are allowed directly into your mailbox. Messages from unknown senders are held in a pending queue until they respond to a one-time confirmation request or "challenge" sent by our whitelist server. Once they respond to the confirmation, their original message is deemed legitimate and is delivered to you. The system then automatically adds their address to your whitelist so they won't have to confirm future messages. To see what the confirmation process looks like, send me a test message, and then reply to the confirmation request.

This methodology has the advantage of being very selective about what it allows in, while at the same time permitting legitimate, but previously unknown senders to reach you.

## Long Island Internet Headquarters: SpitShine®; Spam & Virus Filtering

Optional use of the LIHQ Whitelist tagged addresses will greatly reduce the number of unknown senders who are actually sent a confirmation request.

### **Traditional Blacklist-centric Strategy "*Allow everything that is not explicitly denied*"**

Traditional anti-spam technical countermeasures are based upon maintaining a "blacklist" containing e-mail addresses, domains, and/or network subnets of known junk-mailers. Or worse, a "profile" of message headers and message body text that fits the software's idea of what a piece of spam looks like.

The problem with this approach is that spammer's intrusion techniques are evolving as fast as your prevention techniques are, so the battle is never ending. Maintaining the blacklist or spam "corpus" is often just as time-consuming as pressing the `Delete' key on the easily recognized junk messages. If wasted time is your biggest complaint with junk e-mail, you can see why these traditional methodologies are flawed.

The chance of accidental "false positives" is also significantly higher with this more complex approach. If you really want effective and reliable UCE control, you need something like LIHQ's Whitelist that doesn't rely on heuristics that spammers can work around.