




LanTech Spam Firewall

Welcome and thank you for choosing the LanTech Spam Firewall service. This service is easy to use, and a quick review of the highlights below will make it even easier.

What is the “LANTECH SPAM FIREWALL”? The Lantech spam firewall is a hardware device that filters all incoming email for spam and viruses by running a multitude of tests on every received email. Email sent from Verified Known Spammers (as determined by the industry) will be automatically blocked. A very large percentage of spam falls into this category. If the firewall determines an email is spam, it will be delivered to the user’s personal Quarantine Inbox on the firewall. If the firewall determines an email is not spam, it will be delivered straight into the user’s normal inbox.

Welcome eMail. Once the spam firewall delivers an email to a user’s Quarantine Inbox, it will send a “Welcome Email” with the subject “User Quarantine Account Information”. Each user should save this email as it contains a **username** and **password** that may be needed in the future.

Summary eMail. Any user who has received spam within the past 24 hours will receive an automated email with a summary of emails currently in quarantine. (If NO spam has been received within the past 24 hours, NO summary email will be sent.) A Summary email will show (1) a list of emails in quarantine, (2) who they are from, (3) the subject line, and (4) three options for how to deal with a quarantined email.



Account: **mcolgan@lantechllc.com**

This is your quarantine summary from the LanTech Spam Firewall.


You have **9** messages in your spam quarantine inbox.

- Click on the **Deliver** link to have a message delivered to your mailbox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that his/her messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine.

Messages older than 14 days will be removed

Time Received	From	Subject	Actions
01/02/07 01:15:46	Shafer Rosaline <bdzn@gccoull1.wan>	sophomoric	Deliver Whitelist Delete
12/31/06 00:11:25	amigliaccio@sonicwall.com	SonicWALL Service is up for Renewal - Q13767924	Deliver Whitelist Delete
12/29/06 14:23:23	"RegisterFly Specials" <list-serv@r>	RegisterFly.com - Happy New year Specials, 2 for 1 \$9.5	Deliver Whitelist Delete
12/29/06 14:14:51	"RegisterFly Specials" <list-serv@r>	RegisterFly.com - Happy New year Specials, 2 for 1 \$9.5	Deliver Whitelist Delete
12/28/06 11:31:16	"MCPmag.com News" <RMG@1105>	New-Gen SharePoint, Exchange Exams Go Beta: VMwar	Deliver Whitelist Delete
12/28/06 10:33:44	"Services" <skazcv@t-dialin.net>	Play and Win.	Deliver Whitelist Delete
12/27/06 12:07:18	"RegisterFly Specials" <list-serv@r>	RegisterFly.com - 2 for 1 \$9.99 SSL CERT SALE! SUPER	Deliver Whitelist Delete
12/27/06 11:46:18	"RegisterFly Specials" <list-serv@r>	RegisterFly.com - 2 for 1 \$9.99 SSL CERT SALE! SUPER	Deliver Whitelist Delete
12/27/06 09:38:25	"MCPmag.com News" <RMG@1105>	Windows Tip Sheet #130: Fast GPO Backups	Deliver Whitelist Delete

To view your entire quarantine inbox or manage your preferences, [click here](#).

Spam/Virus Protection By 

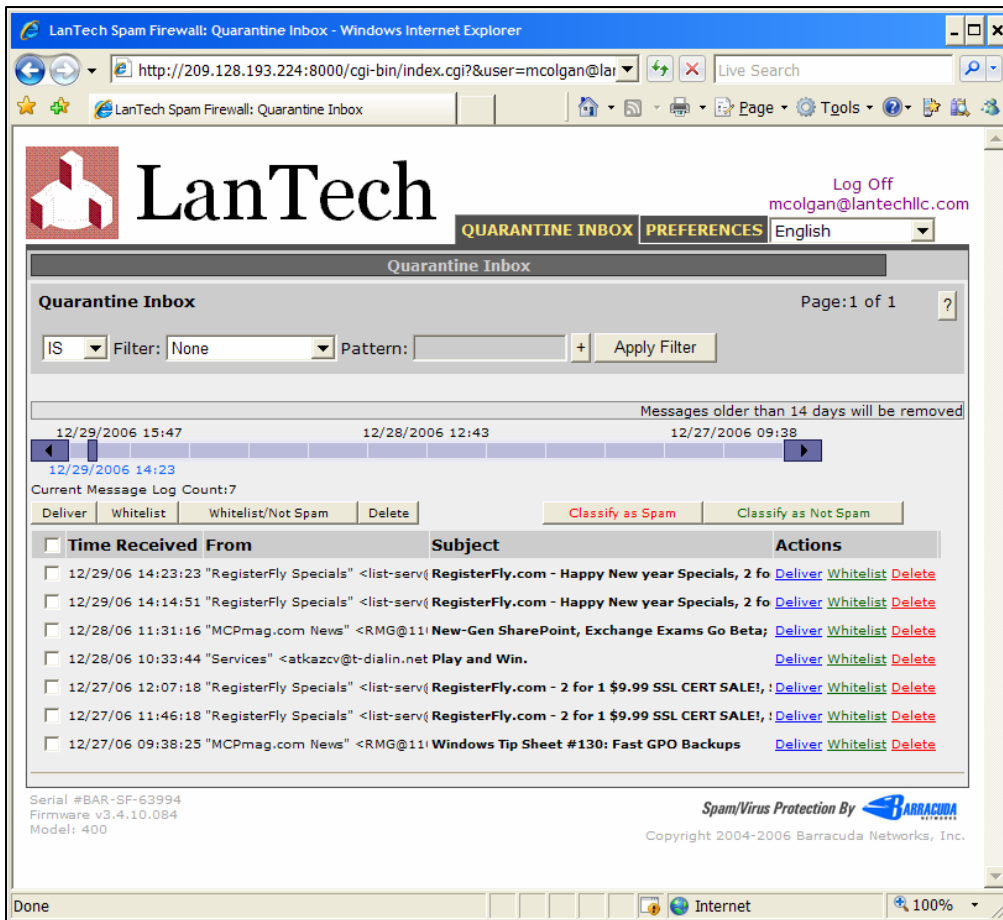
What if I WANT a Quarantined eMail? A quick glance at the list of quarantined e-mails should let you decide whether to take any action. If you don’t want any of the emails, no action is necessary. Quarantined emails older than 14 days will automatically be deleted. You have three actions for dealing with quarantined emails: **Deliver**, **Whitelist** and **Delete**. If you want the email, you must choose either **Deliver** or **Whitelist**.

Deliver will take the email from quarantine and deliver it to a user’s normal inbox.

Whitelist does the same thing but it also means that future emails sent from this email address will NEVER be quarantined.

Delete will delete an email from quarantine. However, the LanTech Spam Firewall will delete quarantined emails older than 14 days. We recommend letting the firewall do the work.


Reviewing Quarantined eMail. You can view your entire quarantine inbox at any time by clicking the link at the bottom of any quarantine summary email. If the quarantine summary email is less than 5 days old you will be automatically logged in. After 5 or more days, users will need to “log in” by entering the username and password sent to them in their Welcome eMails.



Classifying Spam eMail.

From within your quarantine inbox you will have the same three basic options for dealing with quarantined emails as you do on the quarantine summary email -- **Deliver**, **Whitelist** and **Delete**. In addition you can select more than one email at a time. For example, by clicking the box to the left of each email you wish to deliver to your inbox, then clicking the “Deliver” button above the email list, you can deliver all the “checked” emails at once instead of just one at a time.

Firewall Accuracy. Because the system removes quarantined emails after 14 days, no further action is necessary once users have quickly scanned their quarantine inboxes and delivered any “wanted” email to their regular inboxes. There is an option available, however, that can increase the accuracy of an individual user’s spam detection over time. By using the **Classify as Spam** and **Classify as Not Spam** buttons available in the Quarantine Inbox, a user activates a personal database (called Bayesian) that allows the system to be trained more accurately as to what an individual considers spam vs. valid email. Bayesian becomes effective after the user identifies between 200-400 emails as “Spam” and another 200-400 emails as “Not Spam.” (More than 400 identified emails in either category may reduce the effectiveness of Bayesian.) For more information about Bayesian and how it works, a user can view a 5 minute Flash Player video by clicking on <http://www.barracuda.com/ns/support/videos/How-Bayes-works.htm>.

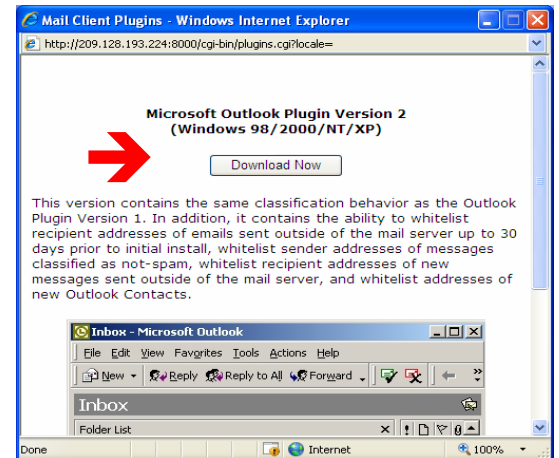
What if an UNWANTED eMail Slips Through? A handy optional item for dealing with the occasional spam email that slips through is the Outlook Plugin (which allows emails to be classified as Spam or Not Spam directly from Outlook). After installing the Outlook Plugin, two new buttons will appear on the user’s Outlook toolbar -- a green “**Add to the Not-Spam List**” button and a red “**Add to Spam List**” button.  These buttons serve the same purpose as the **Classify as Spam** and **Classify as Not Spam** buttons in the quarantine inbox. In addition, the Outlook Plugin will automatically **Whitelist** the sender of an email classified as **Not-Spam**, and will automatically **Whitelist** the email addresses of any new personal Outlook contacts created by a user after the Plugin is installed. We recommend using the **Classify as Not Spam** button to identify examples of “good” email when working in the Quarantine Inbox, and the **Classify as Spam** button to identify “bad” emails when working in Outlook.

How Do I Get the Outlook Plugin? To get the Outlook Plugin, you must be in the LanTech Spam Firewall Login. You can get there from the Quarantine Inbox or Welcome eMail. From the Quarantine Inbox, first click **Log Off** at the top right-hand corner. (Clicking on the link in the Welcome eMail takes you directly to the Login box.)



When the **Login** screen appears, click on the “**Get Mail Client Plugins Here**” link at the bottom of the page.

When the window pops up, click the “**Download Now**” button, then click “**Run**” or “**Open**” and follow the installation prompts.



If you would like to install the Outlook Plugin before you receive your Welcome eMail or Spam Quarantine Summary eMails, click the following link: <http://antispam.lantechllc.com:8000> to go to the LanTech Spam Firewall login page.

Questions? Need Help? Please call us at 916-564-5455. We’ll be happy to answer any questions and help you in any way we can to effectively use the LanTech Spam Firewall.