Barracuda Spam Firewall is an email gateway appliance that applies a combination of spam and legitimate message identification tests that are updated daily in order to check incoming mail messages for their probability of being SPAM. If the Barracuda Spam firewall scores the message as SPAM, it will be held in a queue and not delivered to the recipient of the message.

Quarantine Summary Report
A Quarantine Summary report is an email sent from the Barracuda Spam software listing all the messages that were held by the firewall as suspected SPAM. In order to allow end users to look for messages that were possibly incorrectly identified as SPAM, a daily Quarantine Summary Report will be sent at these times throughout the day.

7:05am 11:05am 4:05pm

These suspected SPAM messages will remain in the quarantine queue for a period of 42 days and up to a 10MB total quarantine inbox size.

You can access your quarantined messages via two methods:

1. Click the link in your daily summary report email that is sent to your inbox. This will automatically connect and log you in to the email quarantine interface page.
2. Open a web browser and type in the URL address https://barracuda.chaffey.edu
   You will then see the log on screen shown below:

   **Username:** Enter your Chaffey login (Firstname.Lastname)
   **Password:** Your current Chaffey email account password
Once you are logged in, you will see your quarantine inbox as pictured below:

Quarantine Inbox tab - Deliver/Whitelist/Delete email in the Quarantine Inbox

By default, the Quarantine Inbox is displayed. You can manage the items in the quarantine individually or as a group.

- **Individually**: To Deliver, Whitelist, or Delete individual emails, select the preference to the right of the email subject. (Area marked in purple)
- **As a Group**: To Deliver, Whitelist, or Delete all the emails in the quarantine at one time, click the small box next to “Time Received” and then make your choice above the box you just checked. (Area marked in green)

When you first start using the quarantine interface, view the list daily to classify as many messages as possible. Barracuda has a learning engine that learns how to deal with future messages based on the ones you classify as spam and not spam. The learning engine becomes more effective over time as you teach the system how to classify messages.

- **Deliver messages**– Delivers messages from a sender to your mailbox for that occurrence. The next time a message is sent from the same sender, the message will be quarantined.
- **Whitelist messages**– Once a message added to your Whitelist, all future emails from this sender are not quarantined unless the message contains a virus or banned attachment type.
- **Delete messages** - Removes the message permanently
Preferences Tab – Whitelist /Blacklist

- **Allowed Email Addresses and Domains**: This area will allow you to manually add or delete email addresses and domains from the Whitelist. When an email address or domain is added to the Whitelist from the Quarantine Inbox, the system automatically enters them to the list found here.

- **Blocked Email Addresses and Domains**: This area will allow you to add or delete users and domains from the Blacklist.

**Tips on specifying addresses**

When adding addresses to your whitelist and blacklist, note the following tips:

- Enter a full email address, such as *asjohndoe@yahoo.com*, to specify a user. If you enter just a domain, such as *yahoo.com*, all users in that domain are will be specified as either whitelisted or blacklisted.

- Mass mailings often come from domains that do not resemble the company's Web site name. Examine the **From: address** of an actual mailing that you are trying to whitelist or blacklist to determine what to enter.

**Logging Off**

When finished viewing your quarantine email, you can log off of the Barracuda system by clicking on the “Log Off” link found in the upper right-hand corner of the page.