

TABLE OF CONTENTS

The Spam Digest

- What is the Spam Digest?
- What do I do with the Spam Digest?
- How do I view a message listed in the Spam Digest list?
- How do I release a message from the Spam Digest?
- How do I delete the messages listed in the Spam Digest?
- How do I change the frequency that I receive the Spam Digest?
- Are there any other Spam Digest options?

Quarantined Messages

- What are quarantined messages?
- What username and password do I use to access my quarantined messages?

Personal Dashboard

- What is the Personal Dashboard?
- How do I get to the Personal Dashboard?
- Do I need a password to access my Personal Dashboard?
- How do I create my password?

Filtering Options

- How does filtering work?
- What are my filtering options?
- How do I view or change my filtering options?
- What are subject tags?
- How do I configure a subject tag?
- Why are blank messages flagged?
- What is an “Invalid Sender”, and why are these messages flagged?
- What is “phishing”?
- How do I select which foreign characters to filter or tag?



More Details About Your Spam Digest & Dashboard

- Why are attachments risky?
- How do I select which attachments to filter or tag?

Whitelists and Blacklists

- What are “Friends” (Whitelist) and why do I need to tell you about them?
- How do you add someone to the Friends whitelist?
- What are “Enemies” (Blacklist)?
- How do you add someone to the Enemies blacklist?

How it Works

- Is somebody at Red Condor reading my mail?
- Will the filtering delay my mail?
- How does Red Condor identify spam?
- Can I run Red Condor on my computer?

The Spam Digest

Question: What is the Spam Digest?

Answer: The Spam Digest has three main functions. It provides a:

- List of activity for your account of email identified by Red Condor as spam, junk, phishing, or containing a virus or other dangerous content since the last digest. These messages have been filtered and held in quarantine for your review. It shows a list off all quarantined email, the reason the message was filtered, the date, time, message size, sender's name, the sender's email account, and email subject line.
- Portal to the quarantined messages. There you can review a message and release it if needed.
- Portal to your personal dashboard where you can manage your account, customize views, and generate reports.

Tip! Click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen in your browser. Then bookmark this page in your browser for easy access.

Question: What do I do with the Spam Digest?

Answer: You don't have to do anything! The messages listed in the Spam Digest have already been filtered. The Spam Digest requires no user action to delete the spam/junk mail listed in the summary. They are deleted automatically after 35 days. The Spam Digest lists a summary of the filtering activities for your account since the last digest. The only thing you need to do is to review the summarized list of messages for any valid messages that were mistakenly filtered out.

Note: You will not receive a spam digest unless you have received messages that have been blocked or quarantined during the latest digest period.

Question: How do I view a message listed in the Spam Digest list?

Answer: Here is a picture of a sample Spam Digest, with Zones indicating Green, Yellow and Red areas. Click the **View** link on the left side of the Spam Digest of the message you want to view. The arrow in the screen below shows the **View** link. The **Preview Message** screen then opens in your browser with an HTML preview of the message.

| Green Zone — Bulk mail, including subscriptions and advertisements | | | | | | | |
|--|---------------------|---------------------------------------|---|--------|---------|------|---------|
| View | Sender | Mailbox | Subject | Date | Time | Size | Type |
| View | Dell Small Business | <del@smallbusiness.dell.com> | Customized desktops starting at \$469, plus savings on net... | Feb 26 | 3:43PM | 47KB | Junk |
| Yellow Zone — Suspicious mail quarantined by policy settings | | | | | | | |
| View | Sender | Mailbox | Subject | Date | Time | Size | Type |
| View | Kathy Olesen-Tracey | <svmpa@cait.org> | [GED_Illinois_Admins_Teachers] Teaching and Learnign Orli... | Feb 26 | 12:50PM | 19KB | Enemies |
| View | Spiegel | <bob15d3d4a9fmdjovdyd1f_@e.e.sei.net> | Best of the Brands: Designer Swimwear in fits that flate... | Feb 26 | 9:00AM | 13KB | Enemies |
| Red Zone — Spam, public groups and other potentially suspicious mail | | | | | | | |
| View | Sender | Mailbox | Subject | Date | Time | Size | Type |
| View | Register Login | <rtf@redcom@coatlans.com> | Louise OlsenMegan Joan | Feb 26 | 1:08PM | 14KB | Spam |
| View | Onyx | <gptina@ozarkhour.com> | Show | Feb 26 | 3:45AM | 13KB | Spam |
| View | Rosalind Carrier | <maltimegeh@rcma.com> | Top listed medications 4 you. | Feb 26 | 2:00AM | 8KB | Spam |

Question: How do I release a message from the Spam Digest?

Answer: Simply click the **View** link in the Spam Digest next to the message you want to release, as described above. When the Preview Message screen opens in your browser, you can determine if it is a valid message.

If the message is valid, you can release it by clicking the **Release** button on the bottom right of the screen. The message will be immediately sent to your regular email inbox.

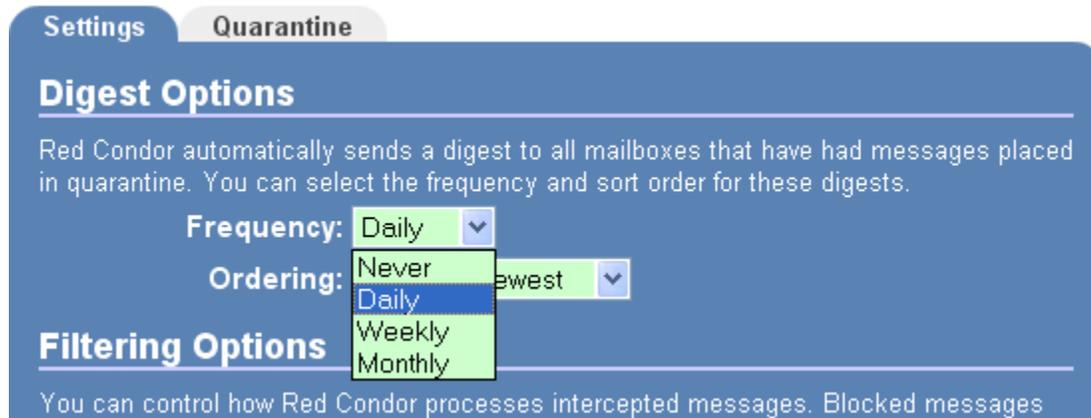


Question: How do I delete the messages listed in the Spam Digest?

Answer: There is nothing to do. The spam messages listed in the Spam Digest have already been filtered. These messages will automatically delete after 35 days. Each digest you receive lists only the new filtered mail, while the older filtered mail is not shown.

Question: How do I change the frequency that I receive the Spam Digest?

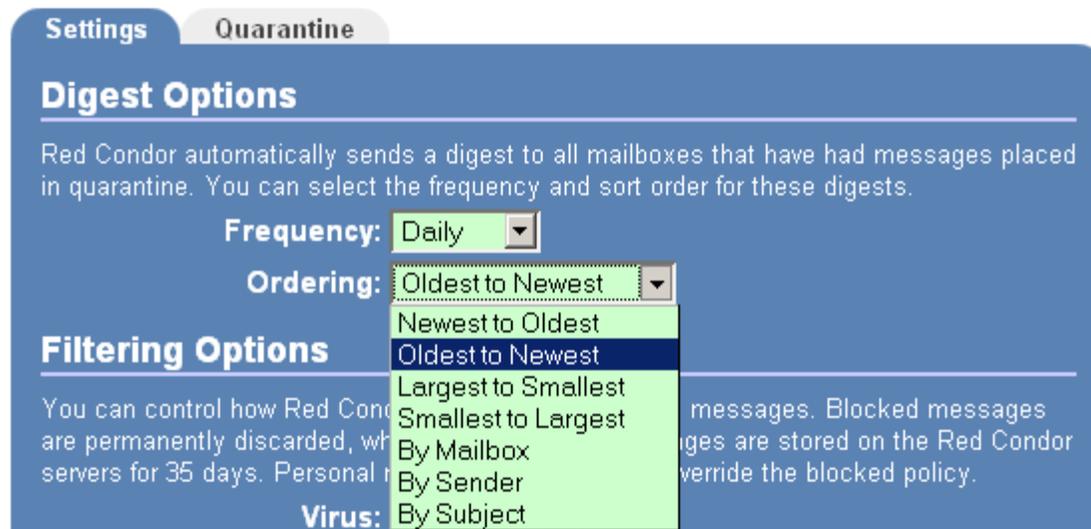
Answer: The digest delivery frequency can be set to daily, weekly, monthly, or never. By default, the Spam Digest is sent out daily. Click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen. At the top of this screen, click **Settings**.



The screenshot shows the 'Settings' tab selected in a navigation bar. Below it, the 'Quarantine' section is active. The 'Digest Options' section has a heading and a descriptive paragraph. The 'Frequency' dropdown menu is open, showing options: 'Daily' (selected), 'Never', 'Weekly', and 'Monthly'. The 'Ordering' dropdown menu is also open, showing 'Newest' (selected) and 'Oldest'. Below these is the 'Filtering Options' section with a heading and a descriptive paragraph.

Question: Are there any other Spam Digest options?

Answer: You can also change the sort order of messages in the Spam Digest by selecting an option from the **Ordering** drop down list.



This screenshot is similar to the previous one, but the 'Ordering' dropdown menu is open, showing options: 'Oldest to Newest' (selected), 'Newest to Oldest', 'Oldest to Newest', 'Largest to Smallest', and 'Smallest to Largest'. The 'Frequency' dropdown menu is closed and shows 'Daily'. The 'Filtering Options' section is visible at the bottom, with a 'Virus:' label and a dropdown menu showing 'By Mailbox', 'By Sender', and 'By Subject'.

Quarantined Messages

Question: What are quarantined messages?

Answer: Quarantined messages are the messages that the system has filtered out based on your filtering options. The Spam Digest posts a summary of the quarantined messages for your account for the previous day. Quarantined messages are archived for 35 days online.

You can run reports through the **Personal Dashboard** for your quarantined messages. You can set the reporting period



and select the sorting order of the messages.



Click **Find** to generate a report. The report displays a list off all quarantined email, including the reason the message was filtered, date, time, message size, sender's name, the sender's email account, and email subject line.

| | Reason | Date/Time | Size | Sender | Mailbox | Subject |
|--------------------------|--------|----------------|------|-------------------|---------------------------------------|---|
| <input type="checkbox"/> | Spam | Mar 28 7:01 PM | 14KB | Womens tipsSearch | <kwunfyp@anacia.net> | Igor Suoside Jonny |
| <input type="checkbox"/> | Spam | Mar 20 9:16PM | 11KB | Borbely Crofut | <borbely.crofut@2crsolutions.com> | lines |
| <input type="checkbox"/> | Spam | Mar 20 9:05AM | 10KB | Sengorn Seisan | <sengornseisan@antaresrealestate.com> | myriad message wont |
| <input type="checkbox"/> | Spam | Mar 19 7:14PM | 16KB | fausto Rukman | <fausto-rukman@arronline.com> | lighting up |
| <input type="checkbox"/> | Spam | Mar 12 6:22AM | 14KB | Dyrell Clary | <clary@app-haefrner.de> | Month Ray Lum |
| <input type="checkbox"/> | Spam | Mar 11 12:13PM | 12KB | Dung Kiran | <dung955@pmhh.com> | Analysis PDF Smith December |
| <input type="checkbox"/> | Spam | Mar 8 11:45AM | 4KB | Kevin Lee | <bounce@etrigue.com> | Industry Analyst Webinar - NAC as a Critical Security Process |
| <input type="checkbox"/> | Spam | Mar 6 8:20AM | 4KB | Kevin Lee | <bounce@etrigue.com> | Gartner webinar - NAC as a Critical Security Process |
| <input type="checkbox"/> | Spam | Mar 2 11:38AM | 54KB | Rodger Malmas | <rodger.malmas@acemagnetics.com> | Interviews Biography |
| <input type="checkbox"/> | Spam | Feb 28 3:34AM | 25KB | Kawoh Klair | <kawoh254@4venicehomes.com> | honest generous Loves kisser |

Question: What username and password do I use to access my quarantined messages?

Answer: By default, there is no username / password authentication. Click the **View** link on the left side of the Spam Digest for the message you want to view. Or, run a report from your **Personal Dashboard**, as described above. Then select the check box or boxes of the messages to access and click **View**. That's it!

Personal Dashboard

Question: What is the Personal Dashboard?

Answer: The Personal Dashboard allows you to create and change your password, select your digest options, configure your mail filtering preference settings, manage your whitelist and blacklist, and to run reports on quarantined messages.

Question: How do I get to the Personal Dashboard?

Answer: Click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen. The **Personal Dashboard** screen opens in your browser.

Question: Do I need a password to access my Personal Dashboard?

Answer: Your Personal Dashboard does not require a password. Red Condor authenticates your access to the Personal Dashboard through the secure, encrypted link you click from your Spam Digest. You can create a password for your account if you choose for added security.

Question: How do I create my password?

Answer: Open your Personal Dashboard screen. On the top left of the screen, click **Change Password**. Enter your new password in the **Password** and **Confirm** text boxes. Click **Save** to save the changes.

Note: Your new password must contain at least 6 characters.

The screenshot shows a web interface for changing a password. On the left, a vertical navigation menu contains three items: "Dashboard" (highlighted in white), "Change Password" (highlighted in dark red), and "Help" (highlighted in blue). The main content area has a blue header with the title "Change Password". Below the header, a message reads: "Please provide a new password consisting of 6 or more characters." There are two text input fields: "Password:" followed by a pink box, and "Confirm:" followed by another pink box. A yellow tooltip with the text "Enter your new password" is positioned over the first input field. A blue "Save" button is located at the bottom right of the form area.

Filtering Options

Question: How does filtering work?

Answer: Red Condor flags messages that have suspicious content and sorts them into one of the following categories:

| | | |
|----------|------------|----------------------|
| Virus: | Block | |
| Porn: | Block | |
| Spam: | Block | |
| Junk: | Markup | Subject Tag ADV: |
| Blank: | Quarantine | |
| Forged: | Markup | Subject Tag FORGED? |
| Foreign: | Markup | Subject Tag FOREIGN: |

| | |
|---|--------|
| Blocked Attachment: | Block |
| <input type="checkbox"/> *.bat <input type="checkbox"/> *.inf <input checked="" type="checkbox"/> *.pif <input type="checkbox"/> *.wsc <input type="checkbox"/> *.com <input type="checkbox"/> *.lnk <input type="checkbox"/> *.reg <input type="checkbox"/> *.wsh <input type="checkbox"/> *.dll <input type="checkbox"/> *.msi <input checked="" type="checkbox"/> *.scr <input type="checkbox"/> *.zip <input type="checkbox"/> *.exe <input type="checkbox"/> *.ocx <input type="checkbox"/> *.vbs | |
| Attachment: | Markup |
| Subject Tag CAUTION: <input checked="" type="checkbox"/> *.asd <input type="checkbox"/> *.eml <input checked="" type="checkbox"/> *.nws <input checked="" type="checkbox"/> *.vbe <input checked="" type="checkbox"/> *.bat <input checked="" type="checkbox"/> *.exe <input checked="" type="checkbox"/> *.ocx <input checked="" type="checkbox"/> *.vbs <input checked="" type="checkbox"/> *.cab <input checked="" type="checkbox"/> *.hlp <input checked="" type="checkbox"/> *.pif <input type="checkbox"/> *.vcd <input checked="" type="checkbox"/> *.chm <input checked="" type="checkbox"/> *.hta <input checked="" type="checkbox"/> *.reg <input type="checkbox"/> *.vcf <input checked="" type="checkbox"/> *.com <input checked="" type="checkbox"/> *.inf <input checked="" type="checkbox"/> *.scr <input checked="" type="checkbox"/> *.wsc <input checked="" type="checkbox"/> *.cpl <input checked="" type="checkbox"/> *.lnk <input checked="" type="checkbox"/> *.sct <input checked="" type="checkbox"/> *.wsf <input type="checkbox"/> *.dat <input checked="" type="checkbox"/> *.msi <input checked="" type="checkbox"/> *.shb <input checked="" type="checkbox"/> *.wsh <input checked="" type="checkbox"/> *.dll <input checked="" type="checkbox"/> *.msp <input checked="" type="checkbox"/> *.shs <input type="checkbox"/> *.zip | |

Question: What are my filtering options?

Answer: Depending on how aggressively you want to filter your email, you can configure each of the filtering categories to block the messages (delete them immediately), quarantine the messages for review, forward the messages to your mailbox with a tag in the subject line, or allow the messages to pass directly to your mailbox without a tag.

Question: How to I view or change my filtering options?

Answer: Click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen. At the top of this screen, click **Settings**. The **Filtering Options** section shows your current settings. Change a setting for a filtering

category by selecting a different from the drop-down list to the right of the option. Then click **Save** at the bottom of the screen to save your settings.

| | | |
|--------|------------|---|
| Virus: | Block | ▼ |
| Porn: | Block | ▼ |
| Spam: | Block | ▼ |
| Junk: | Allow | |
| | Markup | |
| Blank: | Quarantine | |
| | Block | |

Question: What are subject tags?

Answer: Subject tags are short bits of text (up to twenty characters) prepended to the subject line of an email message to alert you that a message has been flagged as suspicious. For example, you can configure the mail from invalid senders (the Forged: field) to say “Fake:” to alert you that the message is not from the sender it claims to be from. So, the tagged message in your mailbox might read “Fake: Your New Macys Gift Card!”

Note: Red Condor recommends ending the subject tag with a colon. When sorting on the subject line, most mail programs ignore the text before a colon and sort on the content of rest of the subject line.

Question: How do I configure a subject tag?

Answer: Open your Personal Dashboard screen. Click **Settings**. For each filtering option that you want to tag, select **Markup** from the drop-down list. A new text box appears on to the right of the drop-down list. Type your text entry into the box, then click **Save** at the bottom of the screen. The screen below shows some common subject tags:

| | | | | |
|----------|------------|---|-------------|----------|
| Junk: | Markup | ▼ | Subject Tag | ADV: |
| Blank: | Quarantine | ▼ | | |
| Forged: | Markup | ▼ | Subject Tag | FORGED? |
| Foreign: | Markup | ▼ | Subject Tag | FOREIGN: |

Question: Why are blank messages flagged?

Answer: Blanks messages are a spammer technique.

Question: What is a “Forged” message, and why are these messages flagged?

Answer: Forged mail is an email message that was not sent from the domain in the “From” field of the message. These messages are often from phishing or other potentially dangerous sources.

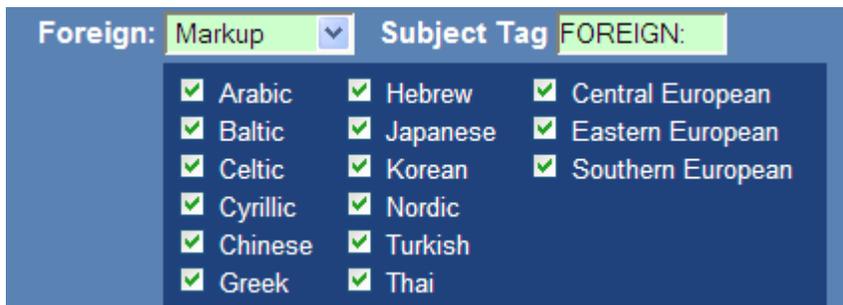
Question: What is “phishing”?

Answer: Phishing is activity that fraudulently attempts to lure the user into giving up personal information such as credit card numbers, passwords, and social security numbers. Phishing messages appear to originate from banks, department stores, online merchants, and other trusted sources.

Question: How do I select which foreign characters to filter or tag?

Answer: Open your Personal Dashboard screen. Click **Settings**. In the **Foreign** section, select the check box or boxes of the characters to filter out. Deselect the check box or boxes of foreign characters you want to pass without filtering or tagging. Click **Save** at the bottom of the screen.

The screen below shows settings that tag all types of foreign characters, and prepend the word “FOREIGN:” to the subject line.



| Foreign: | Markup | Subject Tag | FOREIGN: | | |
|-------------------------------------|----------|-------------------------------------|----------|-------------------------------------|-------------------|
| <input checked="" type="checkbox"/> | Arabic | <input checked="" type="checkbox"/> | Hebrew | <input checked="" type="checkbox"/> | Central European |
| <input checked="" type="checkbox"/> | Baltic | <input checked="" type="checkbox"/> | Japanese | <input checked="" type="checkbox"/> | Eastern European |
| <input checked="" type="checkbox"/> | Celtic | <input checked="" type="checkbox"/> | Korean | <input checked="" type="checkbox"/> | Southern European |
| <input checked="" type="checkbox"/> | Cyrillic | <input checked="" type="checkbox"/> | Nordic | | |
| <input checked="" type="checkbox"/> | Chinese | <input checked="" type="checkbox"/> | Turkish | | |
| <input checked="" type="checkbox"/> | Greek | <input checked="" type="checkbox"/> | Thai | | |

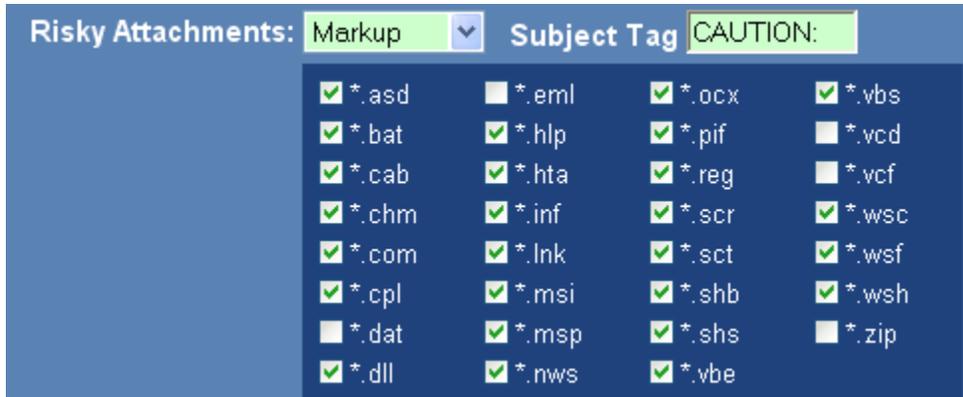
Question: Why are attachments risky?

Answer: Some attachments can contain potentially harmful programs, such as viruses, spyware, and keyboard loggers that can cause loss of data and/or personal information. Red Condor recommends that you never open an attachment from senders you do not know, or those from senders you DO know that you were not expecting a file from.

Question: How do I select which attachments to filter or tag?

Answer: Open your Personal Dashboard screen. Click **Settings**. In the **Risky Attachments** section, select the check box or boxes of the file extensions to filter out. Deselect the check box or boxes of file extensions you want to pass without filtering or tagging. Click **Save** at the bottom of the screen.

The screen below shows settings that tag most types of file extensions, and prepend the word “CAUTION:” to the subject line.



| Risky Attachments: | | Markup | Subject Tag |
|---|---|---|---|
| <input checked="" type="checkbox"/> *.asd | <input type="checkbox"/> *.eml | <input checked="" type="checkbox"/> *.ocx | <input checked="" type="checkbox"/> *.vbs |
| <input checked="" type="checkbox"/> *.bat | <input checked="" type="checkbox"/> *.hlp | <input checked="" type="checkbox"/> *.pif | <input type="checkbox"/> *.vcd |
| <input checked="" type="checkbox"/> *.cab | <input checked="" type="checkbox"/> *.hta | <input checked="" type="checkbox"/> *.reg | <input type="checkbox"/> *.vcf |
| <input checked="" type="checkbox"/> *.chm | <input checked="" type="checkbox"/> *.inf | <input checked="" type="checkbox"/> *.scr | <input checked="" type="checkbox"/> *.wsc |
| <input checked="" type="checkbox"/> *.com | <input checked="" type="checkbox"/> *.lnk | <input checked="" type="checkbox"/> *.sct | <input checked="" type="checkbox"/> *.wsf |
| <input checked="" type="checkbox"/> *.cpl | <input checked="" type="checkbox"/> *.msi | <input checked="" type="checkbox"/> *.shb | <input checked="" type="checkbox"/> *.wsh |
| <input type="checkbox"/> *.dat | <input checked="" type="checkbox"/> *.msp | <input checked="" type="checkbox"/> *.shs | <input type="checkbox"/> *.zip |
| <input checked="" type="checkbox"/> *.dll | <input checked="" type="checkbox"/> *.nws | <input checked="" type="checkbox"/> *.vbe | |

Whitelists and Blacklists

Question: What are “Friends” (Whitelist) and why do I need to tell you about them?

Answer: The Friends whitelist contains email addresses and domains of those organizations and individuals that you trust. You only need to add an entry to the Friends whitelist if they send you spam that you actually want to receive. For example, you may be on a large mailing list that would be flagged as a bulk mailing.

Question: How do you add someone to the Friends whitelist?

Answer: There are two ways to add someone to the Friends whitelist:

- If the mail has already been filtered, simply click the **View** link next to the message. The **Preview Message** screen then opens with an HTML preview of the message. At the bottom of this screen are two check boxes: **Add user@domain.com to whitelist** and **Add domain.com to the whitelist**. The first adds that specific address, while the second adds the entire domain. Select the appropriate check box and click the **Release** button. The message is released to your mailbox, and the user or domain is added to the Friends whitelist.
- If the mail has not yet been filtered and you are adding the address as a precaution, click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen. At the top of this screen, click **Settings**. Then scroll down to the **Friends aka Whitelist** section to add email addresses, domains, IP addresses and more. Click inside the box to display the instructions and valid options.



More Details About Your Spam Digest & Dashboard

Note: Red Condor strongly advises using the system for a month or more before adding anyone to your whitelist. Our extensive testing has found that using the whitelist introduces more problems than it solves.

Domain Friends aka Whitelist

Enter the email addresses, domain names, or IP addresses of the individuals and organizations that are trusted by **barnun.com**. Mail that is received from these addresses will **not** be subject to spam filtering. Only add entries for individuals or organization that send email that may be mistaken as spam.



Question: What are “Enemies” (Blacklist)?

Answer: If you have a legitimate sender that you do not want to receive further email from, you can add an entry (email address or domain) to the Enemies blacklist.

Question: How do you add someone to the Enemies blacklist?

Answer: Click the **Personal Dashboard** link in the second paragraph of the Spam Digest to open the **Personal Dashboard** screen. At the top of this screen, click **Settings**. Then scroll down to the **Enemies aka Blacklist** section to add email addresses, domains, IP addresses and more. Click inside the box to display the instructions and valid options.

Domain Enemies aka Blacklist

Enter the email addresses, domain names, or IP addresses of the individuals and organizations that refuse to honor unsubscribe requests.

Valid entries include:

- email address
- domain
- IP address
- IP address / mask
- country code

Each entry must appear on a separate line. You can remove entries that you no longer need by deleting the line.

```
spam@badguys.net  
www.badguys.net|  
192.168.0.2  
10.1.2.3.0/24
```

How it Works

Question: Is somebody at Red Condor reading my mail?

Answer: No. Red Condor filters mail through a series of rules-based programs to flag suspicious messages. The only time a person looks at a specific message is if it has been sent to a decoy account or a wrong address, or is flagged by a user and sent to us for analysis.

Question: Will the filtering delay my mail?

Answer: The filtering process typically introduces a delay of less than one second.

Question: How does Red Condor identify spam?

Answer: Red Condor investigates bulk email that is captured from numerous decoy mailboxes worldwide. When these mailboxes receive a suspected message, they classify the content. Messages that do not pass the filter are quarantined. Red Condor uses the following filtering techniques:

- Signature filtering for virus detection
- Real time blacklists
- Message rate throttling
- Reputation scores
- Message finger print analysis
- Graphic image analysis
- Verifying recipient account name
- String based text rules



More Details About Your Spam Digest & Dashboard

- Pattern rules
- Human review

Question: Can I run Red Condor on my computer?

Answer: No, Red Condor is a hosted solution without client software. Users manage their account settings through a Web browser. This means there is no software on your computer to install, configure, or maintain.