# Email Spam and Virus Protection Guide

Great Plains Communications consumer Email offering includes built in Spam and Virus scanning with many customizable options. This guide will explain these features and give instructions how to manage and change them. The features discussed in this guide can be accessed through the web mail interface at https://webmail.gpcom.net.

If you need additional assistance, please contact the Great Plains Communications Internet Service Center at 1.888.343.8014.

# Contents

# Anti-Virus

Virus protection is essential, and since most viruses are spread through email, this feature is permanently set to enabled. All incoming and outgoing email will be scanned for viruses.

This will be reflected in the email interface:

# Spam Management

All email is scanned for spam messages regardless of whether you use Webmail or a client like Microsoft Outlook.  By default, the spam filter quarantines spam messages in a folder called "Spam". Once activated, this folder is viewable in your webmail and email clients. It is recommended that you routinely check this folder to ensure no legitimate email is getting quarantined as spam. **All quarantined email is automatically deleted after 5 days.**
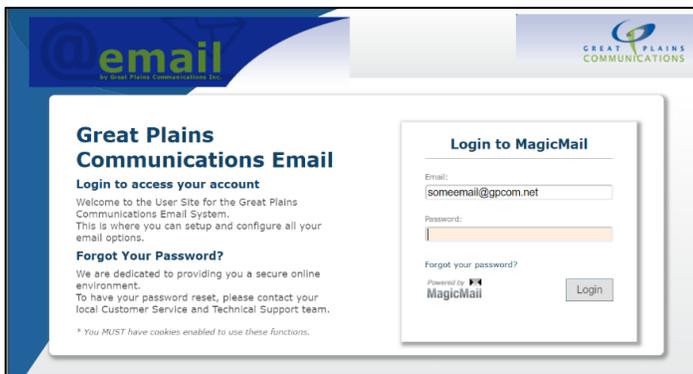
## Accessing Spam Management Console

1. Open an internet browser like Chrome or Firefox. In the address bar type:
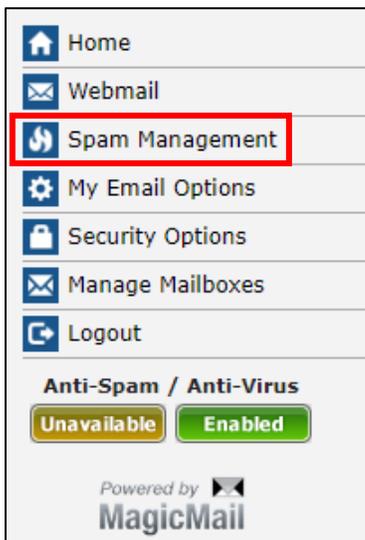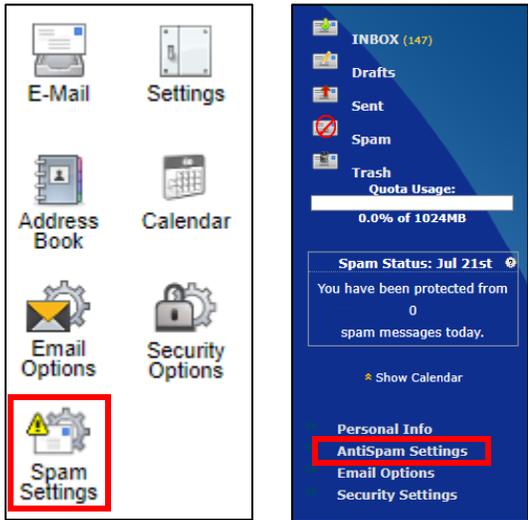   https://webmail.gpcom.net
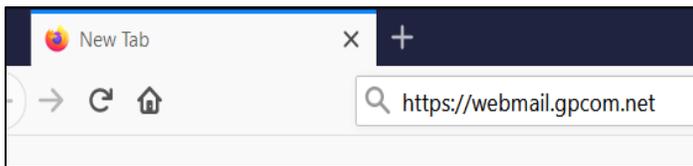
   

2. Login using your full email address and password:

   

3. Click on Spam Management:

   

4. The console can also be accessed from Tuxedo and Webmail Light by Selecting Spam Settings and AntiSpam Settings respectively in the left panel:

# Spam Management Options



There are four levels of spam management that can be selected on this screen by simply selecting the radio button next the option you prefer. A description of each level of spam protection is below:

## Normal
This is the recommended setting for most customers; it will stop most spam email.

## Normal, (w/Quarantine)
This uses the same settings as Normal, but also allows the customer to watch for messages that might come from servers that are not correctly configured. Incorrectly configured email servers can be caught by spam filters. This is only recommended for advanced users.

## Strict
This is a very advanced setting and only recommended for customers being targeted by a sustained spam attack. Use this setting with caution, as it requires that senders conform to Internet Standards and many servers are not set up correctly. You may need to 'whitelist' many email addresses so people can send you email.

## Block All, except on Whitelists
CAUTION! This WILL block ALL EMAIL until you expressly allow email via a whitelist. It is not active or recommended by default, however, some advanced users may need this setting.

This banner will be displayed when your selection is made:

## Disable Spam Filtering

Although not recommended, spam filtering can be disabled. Anti-virus scanning remains active even if you disable spam filtering. To enable or disable spam filtering, simply click the green/red button on the main webmail screen:



## Personal Spam Lists

Spam lists can be personalized to allow or block emails from specific senders or block emails with specific subjects. Whitelisted addresses will always be allowed, and Blacklisted addresses or subjects will be sent to the spam folder. There are three spam lists available:

### Subject Blacklist

When a message is delivered to your mailbox that has a subject line that matches an entry in this blacklist, it will be automatically blocked as spam. This allows you to specify common spam message subject lines. From the "Spam Management" page:

1. Click on Subject Blacklist in the Edit spam Lists in the Spam Management window
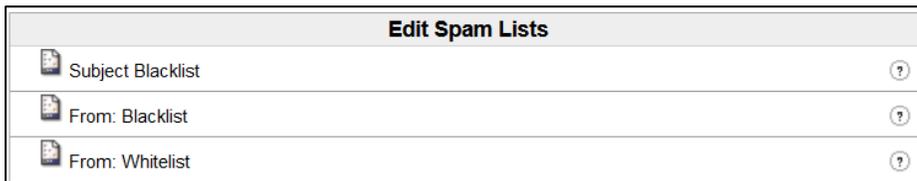


2. Enter the subject to be blocked and click Add. The [subject] can consist of only alphanumeric characters and the following symbols: ('!@#,_=-?(){}%|*.$\)
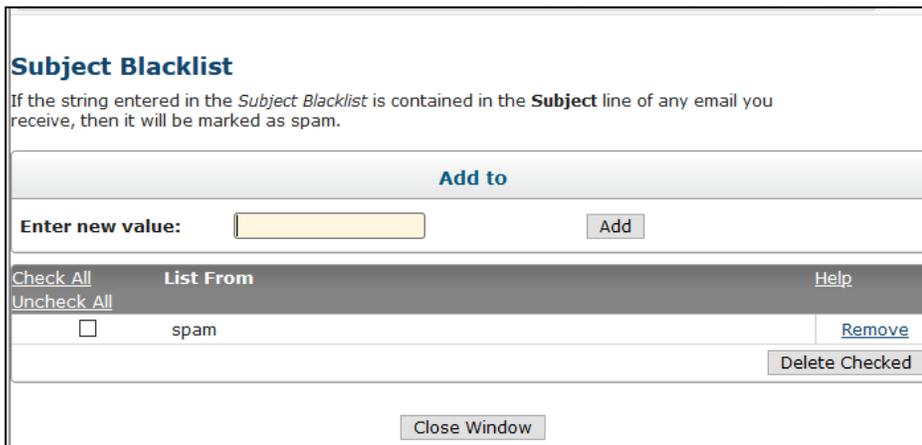
## From Blacklist

When an incoming email matches your blacklist, the message will never be delivered to your mailbox. However, remember that a whitelist match always takes precedence over other email rules. From the "Spam Management" page:

1. Click on "From: Blacklist" in the Edit spam Lists in the Spam Management window

| Edit Spam Lists | |
|---|---|
| Subject Blacklist | ? |
| From: Blacklist | ? |
| From: Whitelist | ? |

2. Enter the email address or domain to be blocked and press add

MagicMail can blacklist senders at 2 different levels:

Server Level
Mailbox Level

Note: You can filter either a portion of or all of the email address. For example entering **@domain.com** will filter all mail from that domain (it will filter both joe@domain.com and jane@domain.com). You may also choose to use the full email address which is the preferred option -- it prevents "false positives", which are matches you did not intend.

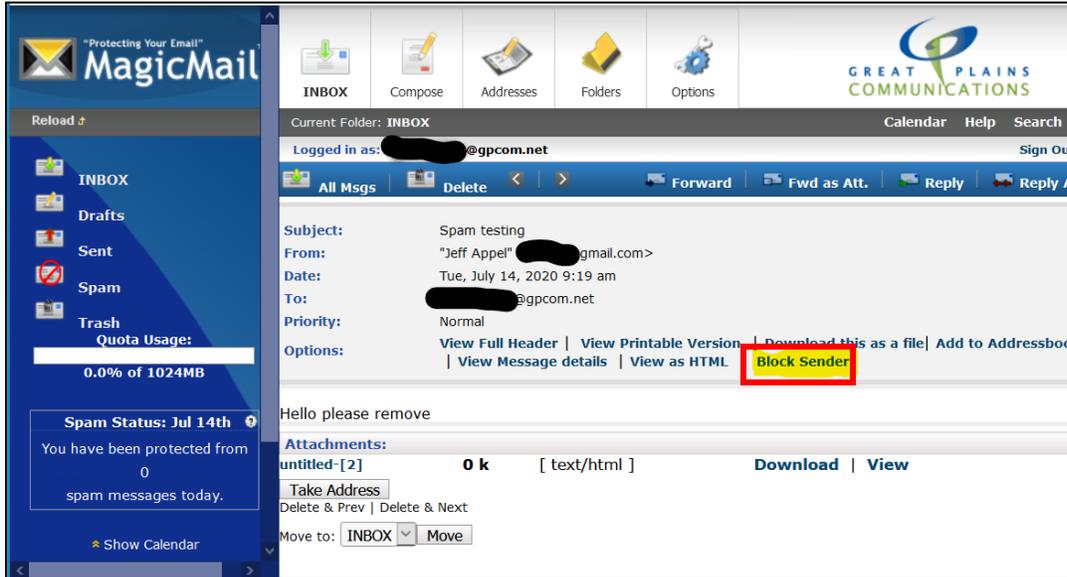**Add to Blacklist**

| Enter new value: | | ☑ Server | Add |
|---|---|---|---|
| | | ☑ Mailbox | |

| Check All Uncheck All | List From Blacklist | | Help |
|---|---|---|---|
| ☐ | spam@spam.com (Mailbox, Server) | | Remove |
| | | | Delete Checked |

Messages can also be added to the "From: Blacklist" directly from the Webmail Lite and Tuxedo interfaces. This can be done by clicking the message and selecting the Block Sender option.

**Tuxedo Interface:**



**Webmail Lite Interface:**
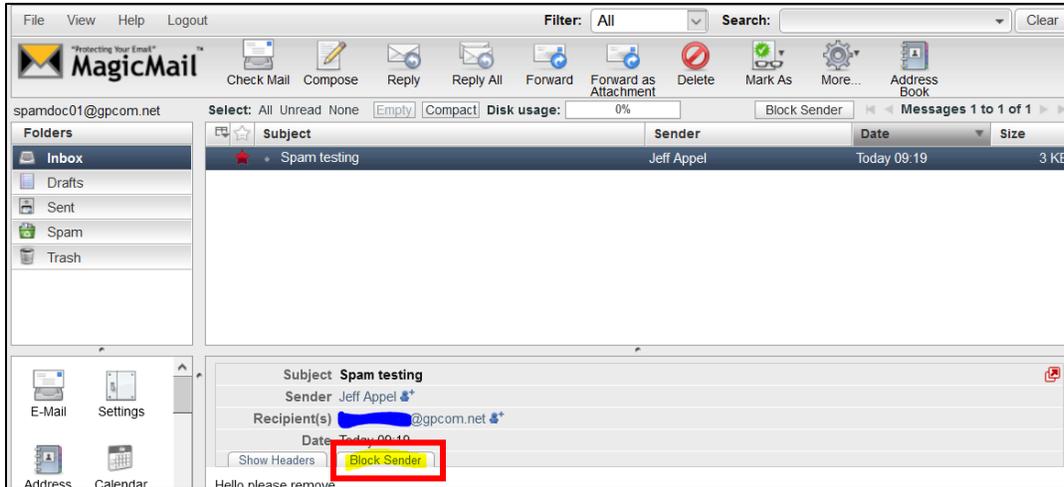
## From Whitelist

When an incoming email matches your whitelist, the message will always be delivered to your mailbox. A whitelist match always takes precedence over other email rules. From the "Spam Management" page:

1. Click on "From: Whitelist" in the Edit spam Lists in the Spam Management window

| Edit Spam Lists | |
|---|---|
| 📄 Subject Blacklist | ⑦ |
| 📄 From: Blacklist | ⑦ |
| 📄 From: Whitelist | ⑦ |

2. Enter the email address or domain to be allowed and press add

Note: You can filter either a portion of or all of the email address. For example entering @domain.com will filter all mail from that domain (it will filter both joe@domain.com and jane@domain.com). You may also choose to use the full email address which is the preferred option -- it prevents "false positives", which are matches you did not intend.

| Add to | | | |
|---|---|---|---|
| Enter new value: | notspam@notspam.com  ☑ Server  ☑ Mailbox | | Add |
| Check All  Uncheck All | List From | | Help |
| | No entry found | | |
| | | | Delete Checked |

# Quarantined Mail Management

If the Normal (w/Quarantine) option is selected in the Spam Management Console, messages marked as spam by the system will be saved in "Quarantined Mail" for 5 days. These messages can be managed under the Spam Management Console in the Quarantined Mail section

## Accessing Quarantined Mail

1. Open an internet browser like Chrome or Firefox.
2. In the address bar type: https://webmail.gpcom.net
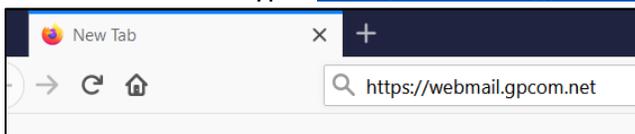


3. Login using your full email address and password:
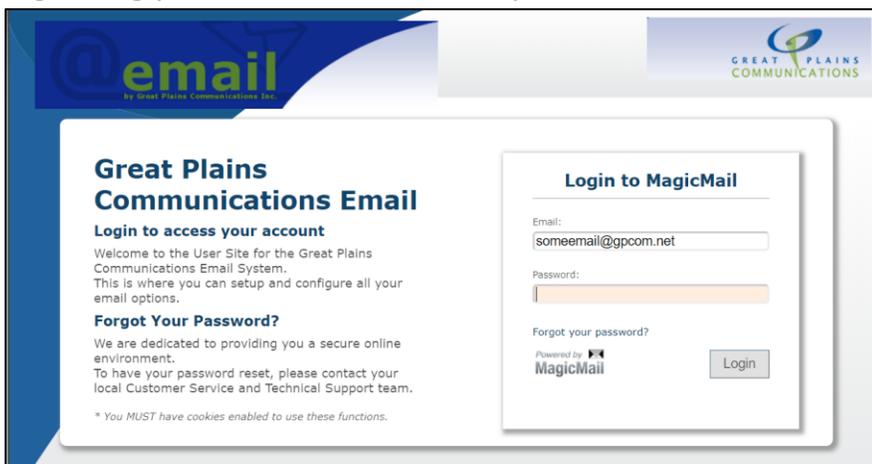


4. Select "Spam Management" then select "Quarantined Mail"

## Release Quarantined Mail to the Inbox

1. In the Quarantined Mail window click the box next to the message to be delivered to the inbox.

### Quarantined Mail

Select the message(s) you would like to delete or move, and then click the corresponding button.
To view the message click on the subject.

| Search Messages | | |
|---|---|---|
| Find messages | From ▼ 🔍 [          ] | Search |

| Quarantined Mail | | | Show All |
|---|---|---|---|
| **Check All Uncheck All** | **From** | **Date Sent** | **Subject** |
| ☑ | Jeff Appel | 11:45 AM | Spam |

| Delete selected messages permanently | Deliver selected messages normally |
|---|---|

| Advanced |
|---|
| Delete all quarantined mail messages. |
| **Warning**: This will mark all of the messages in your Spam Folder for removal |

2. Select the "Deliver selected messages normally" option:

   Deliver selected messages normally

3. A banner will appear confirming the message was delivered to the Inbox.

   The selected message(s) were delivered to your Inbox.