Introduction

Demo site address http://www.wessex-hosting.co.uk/mailguard/login.php

User demo@demo-wessexhosting.uk

Password demo123

The mail server you're using is a sophisticated system designed not only to deliver and route your e-mail, but to scan it for viruses and filter out unwanted UBE (Unsolicited Bulk E-mail), coloquially known as "spam". To get the most out of this system you'll want to read this document in full.

Maia Mailguard is your interface for controlling the way the mail server processes your mail. As you're aware by now, you login using your e-mail address and the same password you use to check your mail. You remain "logged in" for up to ***24 minutes*** between page accesses (each time you access one of the Maia Mailguard pages this timer is reset). If you let this expire you'll be logged out automatically, and will have to login to access your mail filter controls again. If you want to logout explicitly when you're done, of course, you can click the [Logout] link on the toolbar above, or simply close your browser.

Welcome Page

This page is the first page you see when logging into Maia. It contains a quick overview of all the activity Maia has done on your behalf. It also has a simple way to select various levels of protection for your email account.

These levels have been chosen by your system administrator for the needs of your own site, but it should be safe to choose "High" and hit Submit. Once this is done, Maia will begin to filter your email. Look at the Settings page below for more information on how to check the exact scoring of email.

A list of all the categories of email Maia scans for is listed, along with how many items are suspected to be in that category. This is where you can help fight against unwanted email. More information about these categories can be found below.

Statistics

Your status page displays a statistical summary of the mail that Maia has processed for you, divided into categories by type. By clicking the[View Systemwide Statistics] link you can see the same kinds of statistics for the system as a whole. The categories are:

Unconfirmed Non-spam is mail that Maia thinks is *probably* legitimate mail (so-called "non-spam"). To view this mail and confirm (or deny) this diagnosis, visit your "non-spam cache" by clicking the [Report Spam] link.

Confirmed Non-spam is mail that you have already "confirmed" to be legitimate.

False Positives occur when Maia mistakenly thinks that a piece of legitimate mail is spam, and blocks it. These are errors, in effect, and considered by most people to be the worst kind, since it blocks legitimate mail. Fortunately Maia lets you rescue this kind of mail from the[Quarantine], so this mail is not actually lost.

Suspected Spam is mail that Maia thinks is *probably* spam. To view this mail and confirm (or deny) this diagnosis, visit your [Quarantine]area.

Confirmed Spam is mail that you have already "confirmed" to be spam.

False Negatives occur when Maia mistakenly thinks that a piece of spam is legitimate mail, and lets it slip through to your mailbox. These are annoying mistakes on the part of the spam filter, but not as troublesome as false positives. The spam filter is biased heavily toward false negatives, and away from false positives, so it's normal to expect it to make more of this type of mistake. When this happens, you can use the [Report Spam] link to point out the spam and help Maia learn from the mistake.

Whitelisted Items are mail items received from senders on your whitelist. These items are not spam-checked, so they will *always* be delivered to your mailbox.

Blacklisted Items are mail items received from senders on your blacklist. These items are not spam-checked, so they will be discarded, and*never* delivered to your mailbox.

Viruses/Malware are mail items that contain identified "malware"--viruses, worms, Trojans, spyware, and so on. Maia quarantines these items for you, just in case you should want to force one of these items to be delivered to your mailbox for some reason.

Banned Attachments are "suspected malware". Maia tries to be proactive by blocking attachments of certain types, typically executable files, which have been known to disguise viruses and other forms of malware. While no specific malware was identified at the scanning stage, these file types are quarantined as a precaution. You can rescue these items from your [Quarantine] area if you wish.

Invalid Mail Headers are items with "broken" mail headers--mail that does not comply with Internet standards regarding electronic mail. This happens when spammers use certain non-standard mail programs designed specifically to send out bulk mail. These poorly-written programs generate invalid mail headers, and while most mail servers are lenient about allowing this mail to be delivered, Maia considers this a suspicious symptom and quarantines such mail. As always, you can rescue such items from your [Quarantine] area if you wish.

Oversized Items are mail items larger than **20000000 bytes**. These items were **accepted** by Maia without being scanned or processed in any way.

Mail Filter Settings

Maia allows you to maintain different mail filter settings for each of the e-mail addresses you have access to at this site. You can consolidate all of these addresses under one Maia user account to make it easier to manage them all from one interface.

E-mail Addresses

Your **Primary Address** is the first e-mail address associated with your Maia login. Any mail that Maia sends you will be sent to this address, except for items rescued from your quarantine (which will be delivered to you at the original destination address). If you have more than one e-mail address linked to this account, you can use the **Make Primary** button next to each non-primary address to make it the new primary e-mail address for your account.

To link a new e-mail address to your account, supply the login credentials for that account and press the **Add E-Mail Address** button. If you authenticate successfully, the new address will be added to your account immediately.

Miscellaneous Settings

Send quarantine reminder e-mail? tells Maia to send you an e-mail once a week whenever you have ***100 or more items*** in your quarantine area that need to be dealt with, or items ***totalling more than 500000 bytes***. If you neglect your quarantine, of course, the contents will ultimately be deleted after ***30 days.***

Display graphic charts? determines whether your [Stats] page should include graphic charts in addition to the standard tables of statistics. The graphs can help visualize the data more easily, but they do slow the page down somewhat, so if you'd prefer to do without them, you can disable the charts here.

Is this a spam-trap account? lets you tell Maia that *all* of the mail you receive at *all* of the addresses linked to this account is spam, because you don't use these addresses for any legitimate mail. These addresses are only used as spam-bait for automated address harvesters, and should only be advertised in ways that human beings will not mistake for a legitimate address. Use this setting with caution, and only if you know what you're doing--if you activate this feature, ***you will not receive any mail at any of the addresses linked to this account, since everything will be reported automatically as spam.***

Add senders of rescued mail to your whitelist? tells Maia to automatically add a sender's e-mail address to your whitelist when you rescue one of his e-mails from your quarantine area. This is a convenient way to make sure that sender's mail will never be blocked again.

Mail items to be displayed on each page? determines how many mail items appear on a single page in your quarantine area and non-spam cache. If you have a slow Internet connection (e.g. a dial-up modem, etc.), you'll probably want to set this page size relatively low (e.g. 20). If you have a fast connection, you may find it more convenient to set a much larger page size (e.g. 100, 500, or even more), so that you can scan many items at a time. Since you can only confirm items one page at a time, larger page sizes make the process much faster.

Display Language lets you specify the language you'd like Maia to use for all of its output.

Display Character Set lets you specify the character set Maia should use for all of its output.

Per-Address Settings

Virus Scanning enables the mail server to inspect every e-mail you receive to make sure it does not contain any harmful viruses, worms, trojans, or dangerous macros. If you disable this feature, your mail will not be scanned for viruses. Most users will want to enable virus scanning, but if you have some special need to collect viruses (e.g. you're testing an antivirus program installed on your computer, etc.) you can disable virus scanning here to make sure everything gets through untouched.

Detected viruses should be... lets you specify whether virus-infected files should be quarantined, or whether they should be explicitly labeled with special headers as viruses and delivered to you anyway. If you set this to **Quarantined**, the virus-infected e-mail will be placed in your quarantine area, where you can review it at your leisure, and recover any items that contain important information (in spite of the virus). In almost all cases you'll simply want to delete these virus-infected e-mails. Selecting **Labeled** instead causes the mail to be delivered to you, but with special headers inserted to warn you about the status of the mail, so that your mail program can filter on the basis of these headers and deal with it appropriately.

Spam Filtering lets the mail server try to determine whether e-mail you receive is legitimate mail or whether it is spam. A number of different spam-detection mechanisms are used, and an overall score is assigned to each e-mail, with higher scoring items more likely to be spam. By adjusting the various score levels, you can define the level at which mail should be declared to be spam, and the level at which it should no longer be delivered to you. If you'd like to take advantage of spam filtering, enable this feature. On the other hand, if you'd rather receive your mail unfiltered, feel free to disable this feature.

Detected spam should be... lets you determine what happens to e-mail that the spam-checking tools identify as spam. If you select**Quarantined**, any mail that exceeds your quarantine threshold score will be placed in your quarantine area, where you can review it at your leisure, and recover any items that were mistakenly classified as spam. Selecting **Labeled** instead causes the mail to be delivered to you, but with special headers inserted to warn you about the status of the mail, so that your mail program can filter on the basis of these headers and deal with it appropriately.

Add a prefix to the subjects of spam will mark the "Subject:" header of any e-mail classified as spam with a distinctive tag, so that you can more easily create filters in your mail program to catch such items and deal with them accordingly.

Add X-Spam: Headers when Score is >= lets you specify the minimum score a spam-filtered e-mail must achieve before it has 'X-Spam:' headers inserted. These headers provide information about the scoring process, including the list of rules that were used to score the e-mail, so this can be useful for figuring out why a particular e-mail did (or didn't) qualify as spam. The default configured by your mail administrator is probably fine, but if you'd like to see the headers on *every* e-mail, try a setting like -999. Conversely, if you don't want to see the headers at all, set this value to a higher figure (though not higher than the **Consider mail 'Spam' when Score is >=** score, below).

Consider mail 'Spam' when Score is >= lets you specify the score level at which an e-mail is considered to be spam, and labeled as such in the X-Spam headers. Note that this does not prevent the spam from being delivered to you, it merely marks the headers in such a way that your mail client can be configured to filter such mail (e.g. have your mail client look for "X-Spam: Yes"). This value should not be any higher than the **Quarantine Spam when Score is >=** score, below.

Quarantine Spam when Score is >= specifies the minimum score required to take action against spam. This value should be set at least as high as the **Consider mail 'Spam' when Score is >=** level. Any e-mail with a score at or above this level will not be delivered to you. This e-mail will instead be placed in your quarantine area, where you can inspect it at your leisure. If you're afraid of having valid mail filtered, increase this value; if you find you're still receiving too much spam for your liking, decrease this value.

Attachment Type Filtering tries to protect you from potentially malicious files included as attachments to incoming mail. Attachments that include executable files are particularly dangerous, and due to bugs and vulnerabilities in popular mail clients like Microsoft Outlook and Outlook Express, some of these file types can even execute automatically when an e-mail is received. Enable this setting for maximum protection; disable it if you're having trouble receiving certain file types from legitimate correspondents.

Mail with dangerous attachments should be... lets you determine what happens to mail that contains banned attachment types. If you select **Quarantined**, the mail will be placed in your quarantine area where you can review it at your leisure, and recover any items you decide are safe after all. Selecting **Labeled** instead causes the mail to be delivered to you, but with special headers inserted to warn you about the status of the mail, so that your mail program can filter on the basis of these headers and deal with it appropriately.

Bad Header Filtering looks for broken mail headers--basically e-mail that is malformed and in violation of various Internet standards. Legitimate e-mail clients generate valid and complete header information, but the software spammers use often does not, so with this setting enabled you can further protect yourself against such e-mail. There aren't many good reasons to disable this feature, but if you want to be absolutely sure you're not blocking anything on the basis of broken headers, you can always disable this.

Mail with bad headers should be... determines what happens to mail that arrives with malformed headers. If you select **Quarantined**, the mail will be placed in your quarantine area where you can review it at your leisure, and recover any items you want to salvage. Selecting**Labeled** instead causes the mail to be delivered to you, but with special headers inserted to warn you about the status of the mail, so that your mail program can filter on the basis of these headers and deal with it appropriately.

Whitelist and Blacklist

Your **whitelist** lets you specify that mail coming from specific senders (or entire domains) should not be spam-checked, and should be delivered to you regardless of its content. It's a way of making sure that you don't inadvertently block mail from people you know and trust.

Your **blacklist** is effectively the opposite of your whitelist--it lets you specify that mail coming from specific senders (or entire domains) should *never* be delivered to you, under *any* circumstances. Senders on this list will be blocked, regardless of the content of their mail.

Initially, your whitelist and blacklist are both empty. To add an address to either list, go to your [W/B List] page and enter the address (either in "user@domain" form for a specific sender, or "@domain" or "domain" for an entire domain), select the list (Whitelist or Blacklist) and click the **Add to List** button. When you reload your Whitelist and Blacklist page you should see the new entry in the table.

Once you've got an address in your whitelist or blacklist, you can move it from one to the other, or remove it completely just by making the appropriate selection in the table, and clicking the **Update** button at the bottom of the table. The changes will appear the next time you reload the Whitelist and Blacklist page.

TIP: Don't add your own e-mail address (***you@yourdomain***) or your entire domain (***@yourdomain***) to your whitelist. Spammers often supply fake addresses in the mail they send, claiming to be the recipient--*you!*. If your address (or your entire domain) is in the whitelist, this mail will not get spam-checked, and will be delivered to you as if it were from a whitelisted sender.

In general, it's best to start out with an empty whitelist and build it one entry at a time whenever you encounter a "false positive"--a legitimate e-mail that gets flagged incorrectly as spam. When you rescue such an item from your quarantine area, you'll be offered a chance to add the sender's address (or entire domain) to your whitelist.

False Positives

Your quarantine area is where any captured spam and virus files will be stored, awaiting your review, along with any banned file attachments or mail items with invalid mail headers. These are broken down into several tables by type:

Suspected Spam items (if any) are listed first on the page. The list of potential spam items is sorted by score in ascending order, so that the items most likely to be legitimate mail are near the top of the list, and the items near the bottom are almost certainly spam. The list contains the sender's (supposed) e-mail address and the subject line of each item, so you can often spot legitimate mail on the basis of a quick scan, but if you aren't quite sure, you can click on the subject field and take a look at the contents of the mail, using the Mail Viewer.

Each row in the quarantine area represents one mail item. At the right-hand-side you'll see that Maia has already guessed that these items are spam, but if she's made a mistake, you can change the status of that mail item by selecting the **[Non-spam?]** option. The **[Delete]**option lets you just delete the mail item without confirming or denying that it's spam. At the bottom of the page, you can then confirm the status of all the items on the page by pressing the **[Confirm the Status of these Items]** button.

Virus/Malware items (if any) are listed after any spam items. This list is sorted by date, and includes the name of the virus(es) that were found in the mail, along with the sender's (supposed) e-mail address and the subject line. The Mail Viewer is safe to use if you want to look at the text portion of the e-mail, since it will only decode text and HTML elements, not binary attachments.
There *is* a **[Non-spam?]** option in case you really, really want the virus-infected mail sent to your computer (presumably for special processing of some sort). Obviously use the **[Non-spam?]** option with great caution, or not at all. Generally all you should be doing with these virus items is clicking the **[Confirm the Status of these Items]** button at the bottom of the page.

Banned File Attachments (if any) are listed after any virus items. This list is sorted by date, and includes the names of the file attachments that were found in the mail, along with the sender's (supposed) e-mail address and the subject line. You can use the Mail Viewer by clicking on the subject line of the mail, if you want to check out the contents of the mail itself, and you can use the **[Non-spam?]** option to have the item redelivered if you wish. The **[Confirm the Status of these Items]** button at the bottom will clear the list for you, and rescue all of the items you requested.

Invalid Mail Headers (if any) are listed after any banned file attachments. This list is sorted by date, and simply lists the sender's (supposed) e-mail address and subject line. You can use the Mail Viewer by clicking on the subject line of the mail, if you want to check out the contents of the mail itself, and you can use the **[Non-spam?]** option to have the item redelivered if you wish. The **[Confirm the Status of these Items]** button at the bottom will clear the list for you, and rescue all of the items you requested.

As a footnote, when you "confirm spam", you're not just deleting the mail, you're effectively helping to prevent others from receiving that spam in the future. The confirmed spam items are studied by Maia's learning engines, and then passed along to other spam-filtering networks on the Internet. Similarly, when you use the **[Non-spam?]** option to rescue an item from your spam quarantine, you're helping the learning engine recognize what legitimate mail looks like, so that it's less likely to make the same mistake in the future.

You'll want to check your quarantine area regularly to make sure you haven't missed any important mail, and of course to clear out the items that have accumulated since the last time you checked in. ***Items that go unconfirmed for 30 days are automatically deleted, and cannot be submitted to the learning engines***, so please try to keep your quarantine area up-to-date.

If you don't have time to confirm the items in your quarantine area, or there are simply too many of them to bother with (e.g. you just got back from a two-week vacation and there are thousands of items waiting to be confirmed, etc.), you can use the **[Delete ALL Quarantined Items]** button to delete all the items in the quarantine area without reporting them. Obviously this isn't very helpful to Maia's learning process, but it's better to just delete items than to "confirm" items blindly and have Maia learn the wrong things.

False Negatives

While Maia quarantines "bad" or "suspicious" things like viruses, spam, dangerous attachments, and malformed e-mail, she also maintains a short-term *non-spam cache* that keeps track of the "good" mail you receive as well. This serves two purposes: first, it lets you "confirm" that the mail was legitimate, so that Maia can learn what legitimate mail looks like, and second, it lets you correct Maia when she mistakenly lets spam through.

Your non-spam cache looks very similar to your quarantine area, aside from the distinctive gold colour of the table, and the fact that the items are sorted in the opposite order--higher scores are listed first in the list, since these are the most likely to be "false negatives" (spam that got through the filter).

You can use the Mail Viewer to look at a mail item, the same way things work in the quarantine area, but this time your options are simpler--if any of the items in the list are actually spam, report them by clicking on the **[Report this SPAM]** link for the offending items.

Each row in the non-spam cache represents one mail item. At the right-hand-side you'll see that Maia has already guessed that these items are non-spam, but if she's made a mistake, you can change the status of that mail item by selecting the **[Spam?]** option. At the bottom of the page, you can then confirm the status of all the items on the page by pressing the **[Confirm the Status of these Items]** button.

Items in the non-spam cache are automatically deleted after 5 days. If these items are not confirmed, they cannot be used to train Maia's learning engine, so please try to inspect these items regularly.

If you don't have time to confirm the items in your non-spam cache, or there are simply too many of them to bother with (e.g. you just got back from a two-week vacation and there are thousands of items waiting to be confirmed, etc.), you can use the **[Delete ALL Cached Items]** button to delete all the items in the non-spam cache without reporting them. Obviously this isn't very helpful to Maia's learning process, but it's better to just delete items than to "confirm" items blindly and have Maia learn the wrong things.

Mail Viewer

The **Mail Viewer** lets you take a look at a quarantined or cached mail item, either in its "raw" form or in its decoded HTML form. The mail is first displayed in its decoded form, but you can click on the **[View Raw]** link to switch to Raw Mode, and the **[View Decoded]** link returns to Decoded Mode.

At the top of the page, you'll see a report that lists all of the spam-testing rules that were triggered when the mail was scanned. This helps you understand why a particular mail item was (or wasn't) flagged as spam. The rules are sorted in descending order by score, so the ones at the top of the list had the most influence on Maia's decision.

The **Mail Viewer** is safe to use for all types of mail--even mail that contains viruses, since Maia only decodes text and HTML attachments. Other attachment types are be noted, but not displayed. In fact, even images are blocked by Maia, since most of the images that you find in spam contain hidden tracking codes that tell the spammer that you've opened his e-mail. Instead you'll see a placeholder image that says "Image Blocked". Any links in the e-mail remain untouched, however, so if you really want to visit any of those sites you can still do so by clicking on them.

The **Mail Viewer** also offers you the opportunity to report the mail item as spam, delete it, or rescue it to have it redelivered to you. This is equivalent to taking action on the item from the quarantine area or non-spam cache, except that it's done on a single item rather than a whole page of items.

Administrator Console

The Administrator Console has its own Administrator Help Page.

For Further Assistance

If all else fails and your questions haven't been answered here, your local mail administrator (postmaster@greenfrogsys.co.uk) probably has the answers you're looking for.

Credits

Maia Mailguard was written by Robert LeBlanc & David Morton, as a web-based mail filtering system based on the AMaViS Mail Virus Scanner (amavisd-new) and SpamAssassin. Virus-scanning is performed using McAfee