

OnyxServers Web Hosting SPAM Protection Guide

Revision date: 2007-09-04

Hide your e-mail from spambots

If you put an e-mail address on a web page without taking special precautions, spammers will steal it. They use automated programs called spambots which scour websites looking for e-mail addresses to add to their lists. It's not that they might lift the address, they will lift the address. Usually, it won't take long. If you're putting e-mail addresses on your web site, you should take precautions to prevent this.

Once an address has been stolen by spammers there's no way to get them to "un-steal" it. Like so many things in life, if you wait until something becomes a problem, then often there's no easy solution.

There are a number of different methods to hide an e-mail address from spambots. Some of the simpler methods, such as encoding the e-mail as unicode characters, are not very effective as spambots are getting better at getting around these tricks. Using JavaScript to display your e-mail address is a fairly safe solution. Here's an example:

The traditional way of displaying an e-mail addresses using HTML:

```
<A HREF=mailto:jack@mydomain.com>jack@mydomain.com</A>
```

The same e-mail address displayed using a small block of JavaScript code:

```
<script language=javascript>
<!--
var email1 = "jack";
var email2 = "mydomain.com";
var linktext = email1 + "@" + email2;

document.write("<a href=" + "mail" + "to:" + email1 + "@" + email2 + ">" +
linktext + "</a>")
//-->
</script>
```

In this example, you simply need to edit your web pages and replace the HTML code with the JavaScript one. This is a fairly safe and easy solution, but for added security, we recommend that you visit the two links below and choose one of the two more secure JavaScript based solutions explained:

<http://www.bronze-age.com/nospam/encode.html>

<http://www.jracademy.com/%7Ejtucek/email/download.php> (very secure)

To learn more, try googling for the keywords "email", "hide", and "spambots".

Turn off e-mail “catch-all”

E-mail “catch-all” determines what happens to an e-mail sent to an address which you have not created a mailbox, forwarding entry, or auto-responder for. In other words, it "catches" mail going to a non-existent address. What happens to those e-mails depends on the setting specified in the ‘Default Address’ page of your webcontrol panel.

Managing: All Domains Go

Set Default Address

The default email address will “catch” any mail that is sent to an invalid email address for your domain. All mail that is sent to an address that does not exist will go to the default email address. To send all default mail to the main mail account, simply type the user name of your cPanel account in the email address input field.

Default Address Maintenance

Send all unrouted e-mail for:

kimiauranus.com Current Setting: :fail: No such person at this address

Forward to email address

Forward to email address

Discard with error to sender (at SMTP time)

Failure Message (seen by sender):

Advanced Options »

Screenshot of ‘Default Address’ page in the cPanel webcontrol

The first option (Forward to email address) will forward mail sent to non-existent addresses according to what is specified in the ‘Forward to email address’ field. Selecting the first option **is a very bad idea** as you will likely receive a large volume of junk mail sent to random addresses at your domain (e.g. **somethinghere@yourdomain.com**). For this reason, we recommend that all customers set the default address behavior to ‘Discard with error to sender (at SMTP time)’.

As of July 11th, 2007 new accounts have the default address behavior set to ‘Discard with error to sender (at SMTP time)’. This measure was taken to reduce the accumulation of junk mail in customer mailboxes.

The first step in fighting incoming junk mail is to turn off e-mail “catch-all”. This is done by setting the default address behavior to ‘Discard with error to sender (at SMTP time)’.

Please examine the setting in your ‘Default Address’ page and if it is not set to discard, follow these steps to make sure you do not lose any legit mail:

Step 1:

Make a list of all e-mail addresses at your domain you expect to receive legit mail at.

Step 2:

Click on the 'Forwarders' icon in your webcontrol panel and create an entry for each address you expect to receive legit mail at.

Example:

Email Account Forwarders

Forwarders allow you to send a copy of all mail from one email address to another. For example, if you have two different email accounts joe@domain.com and joseph@domain.com, you could forward joe@domain.com to joseph@domain.com so you do not need to check both accounts. Note that the mail for a forwarded email address will still be delivered to that address as well.

ADDRESS	FORWARD TO	FUNCTIONS
david@kimiauranus.com	to kimia	Trace Delete
james@kimiauranus.com	to kimia	Trace Delete
john.doe@kimiauranus.com	to john@kimiauranus.com	Trace Delete
kimia@kimiauranus.com	to kimia	Trace Delete
support@kimiauranus.com	to kimia	Trace Delete
webmaster@kimiauranus.com	to monica@somewhere..com	Trace Delete

[Add Forwarder](#)

Looking at the above example, mail for four addresses will be placed into the default mailbox (kimia@kimiauranus.com). When specifying the 'Forward To' entry, enter your main user ID (as opposed to the address of your default mailbox) in order to have e-mails placed into your default mailbox. If you are not forwarding the mail into your default mailbox, then you should enter an e-mail address for 'Forward To' entry.

Further examining the above example, we can see that mail to john.doe@kimiauranus.com is going into an existing mailbox john@kimiauranus.com and mail to webmaster@kimiauranus.com is being forwarded to an external e-mail address.

Step 3:

Go back to the 'Default Address' page in your webcontrol panel and set the behavior to 'Discard with error to sender (at SMTP time)'.

You will now receive only mail sent to existing addresses and any other mail will be rejected with an error message.

Use SpamAssassin

About SpamAssassin

SpamAssassin is a powerful and effective e-mail filtering system which can detect most junk mail by examining their content. SpamAssassin performs numerous tests and assigns a score to each incoming e-mail which reflects the likelihood that it is SPAM. The SPAM score is recorded in the e-mail headers as such:

```
X-Spam-Status: No, score=2.6  
X-Spam-Bar: ++
```

By default, SpamAssassin will tag an e-mail as SPAM if it receives a score of 5 or more (the higher the score, the more likely it's SPAM). In the above example, the e-mail is not tagged as SPAM because it received a score of 2.6.

```
X-Spam-Status: Yes, score=8.2  
X-Spam-Bar: ++++++++
```

In the above example, the e-mail received a score of 8.2 so it is tagged as SPAM.

When an e-mail is determined to be SPAM, the key phrase *****SPAM***** is inserted into the e-mails subject line. This allows you to setup a custom filter in your e-mail application which filters out mail tagged as SPAM. For example, you can create a folder called 'junk mail' in your e-mail application and create a filter to place any e-mails with the keyword *****SPAM***** in the subject into the junk folder.

Enabling SpamAssassin

Before activating SpamAssassin, we strongly advise you to turn off e-mail "catch-all" by following the instructions from the previous section.

To enable SpamAssassin for your account, login to your webcontrol at <http://YourDomainHere/cpanel> and click on the 'SpamAssassin' icon followed by the 'Enable SpamAssassin' button.

SpamAssassin is currently Disabled.

[Enable SpamAssassin](#)

Automatically deleting mail marked as SPAM

If you turn on SpamAssassin, by default, all that will happen is that mail labeled as SPAM (score of 5 or more) will have *****SPAM***** inserted into the subject line. You may want to automatically delete e-mails determined to be SPAM so you don't even have to download them. To do this, select the

SpamAssassin icon in your webcontrol panel and click on the 'Auto-Delete Spam' button under 'Filters'.



Filters

You can automatically delete messages marked as spam. First set the number of hits required before mail is considered spam.

(Note: 5 is the default setting. The higher the number, the more conservative the setting.)

Score

You may also disable auto-deletion of spam.

If you change the score, you are changing the minimum SPAM score an e-mail must receive in order to get deleted. For example, if you set the score to 10, you will not receive any e-mails with a SPAM score of 10 or more, but you will still receive e-mails marked as SPAM which carry a score between 5 and 10 (they will carry ***SPAM*** in the subject line).

TIP: If you are worried about false positives, try setting the auto-deletion score to 7 or 8 which are very conservative.

Configuring SpamAssassin

You can instruct SpamAssassin to white list or black list specific sender addresses. You can also modify the default score of 5 which is used to classify an e-mail as SPAM. To configure SpamAssassin, click on the 'Configure SpamAssassin' button found in the SpamAssassin page of your webcontrol.

SpamAssassin™ Configuration

You may also configure the different settings for Spam Assassin.

If you find that an e-mail was incorrectly marked as SPAM, you can add the senders address to SpamAssassin's white list so that any future e-mails from them is not filtered. You can also white list (or black list) e-mails originating from a specific domain name. For example, you might want to white list all e-mail addresses at your company. You can use an asterisk (*) as a wildcard. For example, to white list all e-mail addresses @MyCompany.com, add the following to the white list: *@MyCompany.com.

Spam Box

Spam Box sorts mail marked as SPAM into a server-side folder named 'spam'. By server-side, we mean an IMAP folder (refer to our [e-mail FAQ](#) to learn about the IMAP protocol).

If you have chosen to auto-delete all mail marked as SPAM, or have setup custom filters in your e-mail application to sort suspect SPAM into a local folder, turning on Spam Box will not benefit you.

To turn on Spam Box, login to your webcontrol panel and click on the ‘SpamAssassin’ icon followed by the ‘Enable Spam Box’ button.

Spam Box

SpamBox will deliver any emails identified as spam by SpamAssassin into a separate mail folder named "spam". This "spam" folder will fill up and should be emptied regularly.

Spam Box is currently Disabled.

[Enable Spam Box](#) [Clear Spam Box](#)

Since the spam folder is an IMAP folder, customers accessing their mailbox using the POP protocol will not be able to see the ‘spam’ folder in their e-mail application. However there is a way to download the contents of the SPAM folder via the POP protocol. This is done by adding /spam to the POP username. For example, if the POP username is ‘myusername’, connecting using the POP username ‘myusername/spam’ to download the contents of the SPAM folder.

If you access your mail via the webmail interface, the ‘spam’ folder is visible only in Horde webmail interface. This is because SquirrelMail does not support the IMAP protocol.

If you turn on Spam Box, the ‘spam’ folder will not be created until an instance of SPAM is received.

IMPORTANT: Customers using Spam Box must periodically check and flush the contents of their ‘spam’ folder. The ‘spam’ folder takes up space from the mailbox and not flushing it will eventually fill up the mailbox resulting in incoming mail bouncing back.

Setup E-mail Filters

E-mail filters allow you to instruct the mail server to discard, forward, or reject incoming e-mails for your account based on one or more conditions. For example, you may want to discard any e-mail which contains the keyword 'viagra' in the subject line.

To create e-mail filters, login to your webcontrol panel and click on 'Account Level Filtering' or 'User Level Filtering' icons.

Account level filters work for all mailboxes. User level filters work for a specific mailbox only.



Here are three sample filters being setup:

Example 1: Discard any e-mail with the keyword 'viagra' anywhere in the subject or body.

Filter Name:

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

Subject	contains	-	+
<input type="text" value="viagra"/>			

Actions

Discard Message	-	+
-----------------	---	---

Example 2: Reject and bounce any e-mails from Annoying.Person@somewhere.com with the custom error message 'Sorry, this e-mail address no longer exists'.

Filter Name:

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

From	contains	-	+
<input type="text" value="Annoying.Person@somewhere.com"/>			

Actions

Fail with message	Sorry, this e-mail does no longer exist	-	+
-------------------	---	---	---

Example 3: Forward any e-mails sent to *john@mydomain.com* or *sales@mydomain.com*, which contain the keywords 'urgent' or 'immediately', to *MyCellPhone@MyPhoneCompany.com*.

Filter Name:

The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.

Rules

Any recipient	contains	or	-	+
<input type="text" value="john@mydomain.com"/>				
Any recipient	contains	or	-	+
<input type="text" value="sales@mydomain.com"/>				
Subject	contains	or	-	+
<input type="text" value="urgent"/>				
Body	contains	or	-	+
<input type="text" value="urgent"/>				
Body	equals		-	+
<input type="text" value="immediately"/>				

Actions

Redirect to email	<input type="text" value="MyCellPhone@MyPhoneCompany.com"/>	-	+
-------------------	---	---	---