



Technical Support

Administrator's Guide to Reporting Spam

March 01, 2007

Last modified March 10, 2006.

COPYRIGHT

Copyright 2006 Tucows, Inc. All rights reserved.

Contents

	Identifying and handling spam	1
	Reporting spam	3
	Reporting receipt of a spam message	3
	Reporting a filter blocking issue	3
	Managing spammers in your environment	4
	Getting full email headers	4
	Getting full headers from Tucows Presentation Server (Web Mail)	6
	Getting full headers from Mozilla	6
	Getting full headers from email clients for Microsoft Windows	6
	Microsoft Outlook	6
	Microsoft Outlook Express	7
	Netscape Communicator	8
	Eudora	8
	Getting full headers from email clients for UNIX.	9
	Mutt	9
	Pine.	9
	Elm.	9
	Getting full headers from Mail for Mac OS X	10
APPENDIX A	Acceptable Use Policy	11
	Unsolicited bulk e-mail (popularly known as “spam”).	11
	Filtering of incoming e-mail	12
	Illegal activities	12
	Right to damages	12
	Definitions used in this document.	13
	Selected bibliography	13
APPENDIX B	Mass Mailing Policy.	15
	Policy objectives	15
	Definition of mass mailing	15
	Reminder	15
	Mass mailing requirements	15

Administrator's Guide to Reporting Spam

Your email service includes spam blocking, which prevents most spam messages from reaching you. However, a spam message may occasionally appear in your inbox. This is because spammers continuously invent new ways to circumvent spam filters. These filters must be updated whenever a new type of spam appears.

You can help make your spam blocking service more effective by reporting spam whenever it appears in your inbox. When you report spam, Tucows uses that information to update its spam filters, preventing similar spam from reaching users in the future. This guide explains how to report spam effectively.

Identifying and handling spam

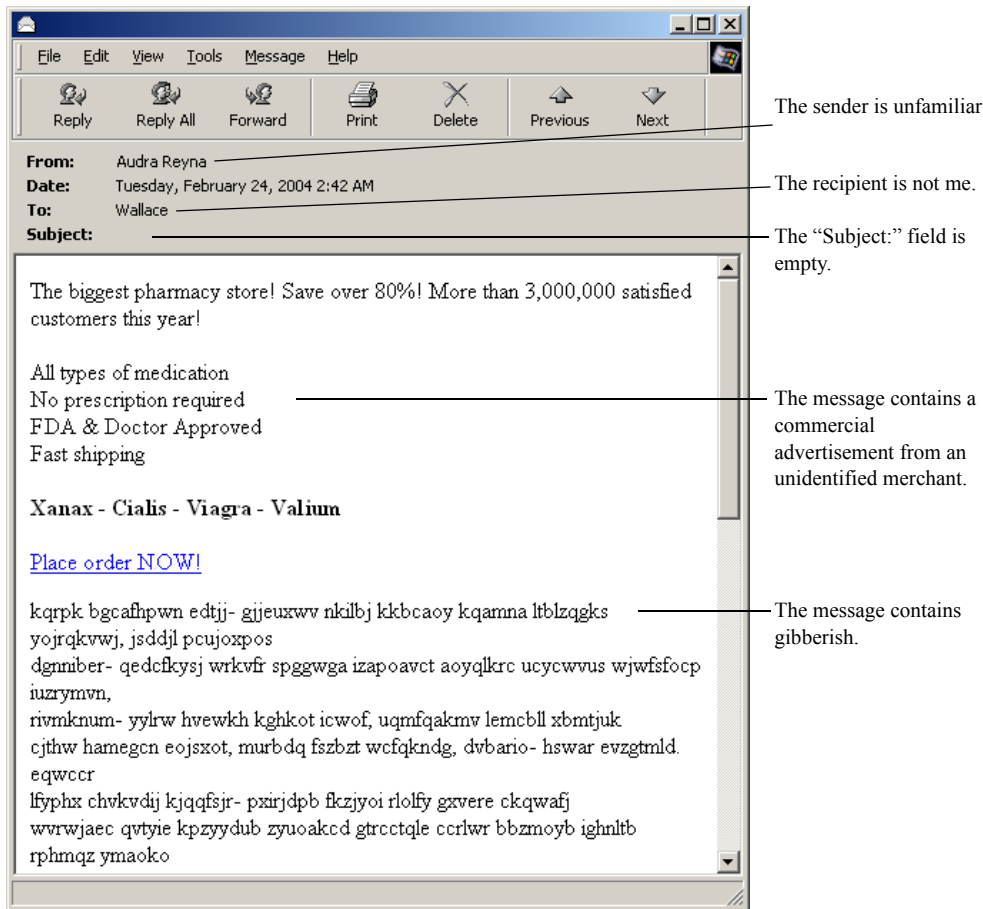
Spam is unsolicited, bulk email. A single message is sent to hundreds or thousands of users without their permission. A spam message usually consists of a commercial advertisement. Less common but more dangerous forms of spam include computer viruses or requests for personal information such as credit card numbers.

A message *may* be spam if any of the following are true:

- The message consists of a commercial advertisement by a merchant from whom you have never purchased products or requested information.
- The message consists of explicit sexual text or images.
- The Subject field or the body of the message contains gibberish, all capitals, or many exclamation marks (!) or dollar signs (\$).
- The From or Subject field of the message is empty.
- The recipient is not you.
- The sender is unfamiliar.
- The sender appears to be someone you know, but the message does not make sense considering the sender.

Some spam messages are obvious, while others are subtle. Figure 1 shows an example of an obvious spam message.

Figure 1 *Example of a spam message*



These are some general guidelines for handling spam:

- Never open attachments that are associated with a spam message. Computer viruses are commonly distributed as spam attachments.
- Do not respond to the removal addresses contained in spam. They rarely work and may encourage more spam.
- Report spam promptly, as explained in "Reporting spam" below.

Reporting spam

In order for you to effectively report spam to Tucows, your end-users need to report occurrences of spam to you. This section explains how to take action by submitting this information to Tucows and includes the following topics:

- “Reporting receipt of a spam message” on page 3
- “Reporting a filter blocking issue” on page 3
- “Managing spammers in your environment” on page 4

Reporting receipt of a spam message

If a Tucows user receives a spam message, send a complaint to our spam complaint address:

`abuse@abuse.tucows.com`

Always include the original spam message, *including full headers*. Full headers are required for analysis of any email problem, especially spam. See “Getting full email headers” on page 4.

Reporting a filter blocking issue

If a legitimate message is bounced back to the sender by the Tucows spam filtering system, then there may be a filter blocking issue. This means that the Tucows spam filters have mistaken an innocent message for spam. When you report a filter blocking problem, we can adjust our filters to prevent similar problems in the future.

TO REPORT A FILTER BLOCKING PROBLEM

- 1) Send the original message to the following email addresses:

`abuse@abuse.tucows.com`
`emailabuse@tucows.com`

Sending the original, undelivered message to this address allows us to observe how it interacts with a variety of filter configurations. If the original message is unavailable, construct a similar message from the same sender.

- 2) Send a copy of the bounce message, *with full headers*, to `emailabuse@tucows.com`.

Include the following addresses in the Bcc field:

`abuse@abuse.tucows.com`

For more information about obtaining the full headers of a message, see “Getting full email headers” on page 4.

- 3) Send a new message to abuse@abuse.tucows.com with the following information:
 - The “To”, “From”, and “Subject” lines that were blocked.
If you later changed those fields and the message was subsequently delivered successfully, explain what you changed the fields to.
 - The date and time, including the time zone, that this failure occurred.
 - Any other relevant information.
For example, tell us the size of the email and any attachments, the program used to send the email, whether this was part of a bulk mailing, and so on. The more information you send, the more efficiently we can address the problem.

Managing spammers in your environment

If you or Tucows receive a complaint about spam that is being sent by one of your users, then we will help you investigate the incident. Make sure that you have provided us with an abuse contact within your organization. That person will be contacted by the Tucows abuse team to coordinate the investigation. Before determining an appropriate course of action, the team will determine whether the spamming is accidental (for example, the user is infested with a virus that sends spam) or deliberate.

Getting full email headers

When you view an email message, most email clients normally show you just the few headers that are likely to interest you, as in this example:

```
From: Matt Gonzalez <matt@example.com>  
To: Sam Johannsen <sam@example.org>  
Date: Mon, 16 Feb 2004 10:45:10 -0800  
Subject: Thank you for your interest
```

Your email messages also contain additional headers that provide more detailed information, like this:

```
From matt@example.com Mon Feb 16 10:45:40 2004
Return-Path: <matt@example.com>
Delivered-To: sam@example.org
Received: from gate.ci.sf.ca.us (gate.ci.sf.ca.us [209.77.149.2])
    by phoenix.example.net (Postfix) with ESMTP id D1186B
    for <sam@example.org>; Mon, 16 Feb 2004 10:45:39 -0800 (PST)
Received: from chhub01.example.com (client-172-31-01-
67.example.com [172.31.1.67])
    by gate.ci.sf.ca.us (8.11.7+Sun/8.11.6) with ESMTP id
i1GIjdt17780
    for <sam@example.org>; Mon, 16 Feb 2004 10:45:39 -0800 (PST)
X-Priority: 3 (Normal)
From: Matt Gonzalez <matt@example.com>
To: Sam Johanssen <sam@example.org>
Message-ID: <OF88256E3C.00670338-ON88256E3C.00670338-
88256E3C.00670337@example.com>
Date: Mon, 16 Feb 2004 10:45:10 -0800
X-MIMETrack: Serialize by Router on lnh02a01/SFGOV(Release
6.0.2CF1|June 9, 2003) at 02/16/2004 10:45:12
MIME-Version: 1.0
Content-type: text/plain; charset=US-ASCII
Content-Length: 335
Lines: 5
Status: RO
X-Status:
X-Keywords:
X-UID: 4972
```

The full headers include information about the true origin of the message. Unlike the information in the normal headers, most of the information in the full headers cannot be forged by deceptive spammers.

When forwarding a spam message to Tucows, always forward it with full headers. These are required in order to modify the spam filters so that they can block any further spam from the same originator.

Most email clients allow you to display the full headers of any email message. The topics below explain how to display full headers using some common email clients:

- “Getting full headers from Tucows Presentation Server (Web Mail)” on page 6.
- “Getting full headers from Mozilla” on page 6.
- “Getting full headers from email clients for Microsoft Windows” on page 6.
- “Getting full headers from Mail for Mac OS X” on page 10.

For information about displaying full headers using other email clients, see your email application's documentation.

Getting full headers from Tucows Presentation Server (Web Mail)

Follow these steps to display full headers in Tucows's Web-based email interface, known as Presentation Server or Web Mail.

TO DISPLAY FULL HEADERS WITH PRESENTATION SERVER

- 1) In the message list, select the message whose headers you want to display.
- 2) In the message pane, click **Show All Headers**.
The message is displayed again, this time with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.

Getting full headers from Mozilla

Mozilla is a popular open-source email client available for a variety of computing platforms.

TO DISPLAY FULL HEADERS IN MOZILLA

- 1) Select or open the message whose headers you want to display.
- 2) From the **View** menu, select **Headers > All**.
The message is displayed again, this time with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.

Getting full headers from email clients for Microsoft Windows

This section explains how to display full headers using the following email clients:

- Microsoft Outlook
- Microsoft Outlook Express
- Netscape Communicator
- Eudora

Microsoft Outlook

TO DISPLAY FULL HEADERS WITH MICROSOFT OUTLOOK

- 1) From the message list, right-click the message whose headers you want to view.
A menu appears.
- 2) Select **Options**.
The Message Options window appears.

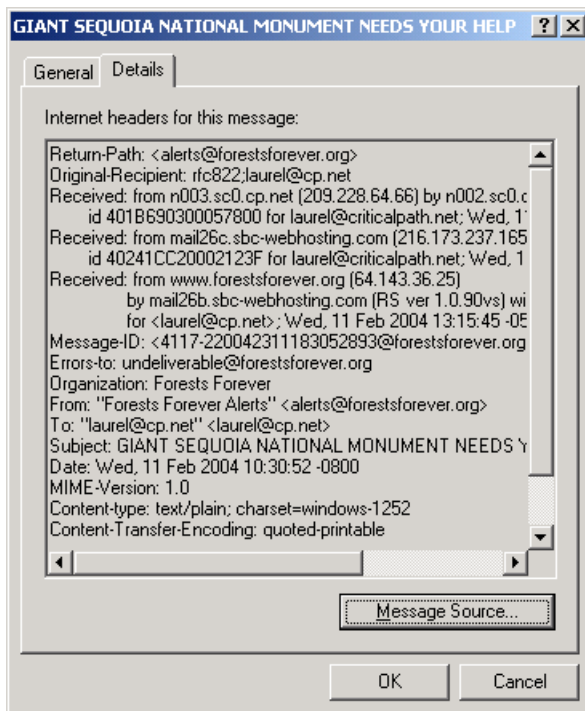
- 3) Copy the contents of the **Internet headers** field.
- 4) Forward the spam message to your spam prevention administrator, and paste the full headers into the forwarded message.

Microsoft Outlook Express

TO DISPLAY FULL HEADERS WITH MICROSOFT OUTLOOK EXPRESS

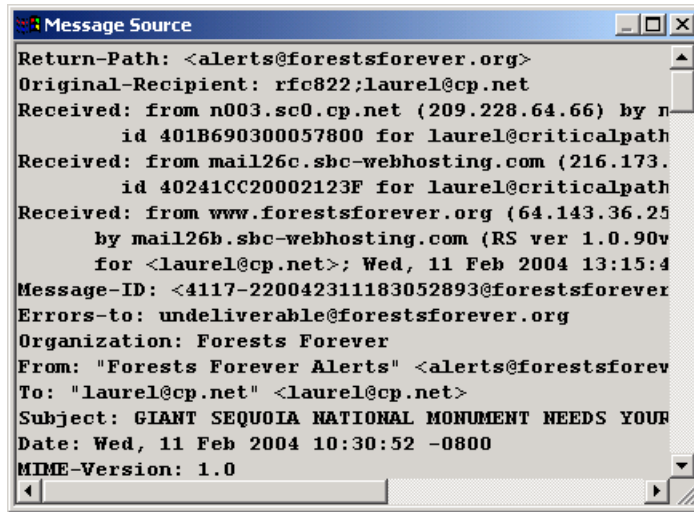
- 1) From the message list, select or open the message whose headers you want to view.
- 2) From the File menu, select **Properties**.
The message properties dialog appears.
- 3) Click the **Details** tab.

The **Details** tab displays the full headers of the message:



4) Click **Message Source**.

The message source window displays the complete contents of the message, including full headers:



5) Copy the entire text in the message source window and send it to your spam prevention administrator.


Netscape Communicator

TO DISPLAY FULL HEADERS IN NETSCAPE COMMUNICATOR

- 1) Select or open the message whose headers you want to display.
- 2) From the **View** menu, select **Headers > All**.
The message is displayed again, this time with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.

Eudora

TO DISPLAY FULL HEADERS IN EUDORA

- 1) Select or open the message whose headers you want to display.
- 2) Click the **BLAH BLAH BLAH**  icon.
The message is displayed again, this time with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.

Getting full headers from email clients for UNIX

- Mutt
- Pine
- Elm

Mutt

TO DISPLAY FULL HEADERS IN MUTT

- 1) Open the message whose headers you want to display.
- 2) Enter "h".
The message is now displayed with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.
- 4) To exit full header mode, enter "h" again.

Pine

TO DISPLAY FULL HEADERS IN PINE

- 1) Open the message whose headers you want to display.
- 2) Enter "h".
The message is now displayed with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.
- 4) To exit full header mode, enter "h" again.

Elm

TO DISPLAY FULL HEADERS IN ELM

- 1) Open the message whose headers you want to display.
- 2) Enter "h".
The message is now displayed with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.
- 4) To exit full header mode, enter "h" again.

Getting full headers from Mail for Mac OS X

TO DISPLAY FULL HEADERS IN OSX MAIL

- 1) Select or open the message whose headers you want to display.
- 2) From the **View** menu, select **Message > Long Headers**.
The message is displayed again, this time with full headers.
- 3) Forward the message with full headers to your spam prevention administrator.

Appendix A

Acceptable Use Policy

Without exception, Tucows decries the practice of mass-mailing unwanted e-mail solicitations of any type, regardless of content, and we will do everything within our power to reduce the flood of this type of traffic across the Internet.

Please read and understand the policies in the Tucows Mass Mailing Policy.

To this and similar ends, we have instituted the following policies (please also see our definitions below):

Unsolicited bulk e-mail (popularly known as “spam”)

Any Tucows Customer who sends unsolicited advertisements or solicitations, commercial or otherwise, may have their account disabled and be disallowed further service.

The Customer is responsible for ensuring that the services obtained from Tucows are used in an appropriate manner by their End Users. Therefore, the Customer must take steps to manage the use of the services obtained in such a way that network abuse is minimized. The Customer must also make contact information publicly available, and must respond in a timely manner to any complaints. Tucows shall consider any complaints regarding the Customer's End Users to apply to the Customer.

In extreme cases, Tucows operations personnel have the option to immediately disable any account in order to forestall further abuse or damage to e-mail systems. Should this occur, the Customer shall be notified as soon as possible.

Unsolicited advertisements or solicitations sent from other networks which reference e-mail accounts hosted at Tucows shall be treated as if they originated from the account referenced, unless there is sufficient reason given for Tucows operations staff to believe that the message truly originated with some unrelated party.

Likewise, postings made to the usenet newsgroups or other online forums, such as blogs, which reference e-mail accounts hosted at Tucows, and are deemed to be inappropriate according to the local ethical standards of that forum, may be treated in the same manner as unsolicited bulk e-mail above.

Filtering of incoming e-mail

As owner of the equipment and other resources utilized to provide services, Tucows has the legal right to block electronic communications from other entities on the Internet.

Customers should be aware that such blocking or filtering may take place if deemed necessary by designated members of the Tucows operations staff (or a third party chosen by Tucows and made known to the Customer.) Whenever possible, the party being blocked shall be made aware of such action before it occurs.

Illegal activities

Services offered may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of federal or of state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or any other statute.

Tucows reserves the right to cooperate with law enforcement and other legal authorities in investigating claims of illegal activity.

Tucows will not release any information regarding our Customers (excepting that which is public knowledge, such as the InterNIC's WHOIS database) or their End Users to any third party except upon presentation of a valid court order from a government or legal entity with proper jurisdiction. The Customer agrees that Tucows judgement as to the validity of any such order shall be considered proper and final.

Right to damages

Tucows considers most instances of unsolicited bulk e-mail to be a theft of services and reserves the right to prosecute originators of same in a court of law.

Tucows reserves the right to collect damages (software, hardware, and man hours) if any harm is done to our network or equipment which requires repair or reconfiguration of any kind.

If deemed appropriate by Tucows, the Customer will be billed not less than USD 500 per individual complaint received by Tucows staff.

In addition, Tucows reserves the right to collect punitive damages in recompense for any perceived loss of brand reputation.

Nothing contained in this document shall be construed to limit action Tucows may take or remedies available to us in any way with respect to any of the described conduct. Tucows reserves the right to take any additional actions we may consider appropriate with respect to such conduct, including without limitation taking action to recover costs and expenses of identifying offenders and removing them from our network or systems, and levying

cancellation charges to cover costs in the event of disconnection for the causes outlined in this Policy document. In addition, Tucows reserves at all times all rights and remedies available to us with respect to such conduct at law or in equity.

Non-enforcement of any policy or rule herein does not constitute consent or waiver, and Tucows reserves the right to enforce such policy or rule at its sole discretion.

Definitions used in this document

"Customer" refers to the business entity which has contracted with Tucows for e-mail services. Each Customer may have multiple domain accounts and each domain account may have one or more End User.

"End User" refers to the person, persons, or entity using a specific account (designated by a unique e-mail address) within a domain controlled by the Customer and operated by Tucows.

Selected bibliography

- RFC 1855 "Netiquette Guidelines"
(the "unwritten" rules)
<http://www.cybernothing.org/cno/docs/rfc1855.html>
- *Fight Spam on the Internet!*
(the central site for the anti-spam activist community; includes filtering methods, example policies, and much more)
<http://spam.abuse.net/>
- Coalition Against Unsolicited Commercial E-mail
(the world's largest online organization)
<http://www.cauce.org/>
- *The Net Abuse FAQ*
(mainly deals with Usenet)
<http://www.cybernothing.org/faqs/net-abuse-faq.html>

Appendix B

Mass Mailing Policy

Tucows has updated the Acceptable Use Policy to include guidelines for all mass mailings by customers, or a third party contracted on behalf of customers to send mass mailings to Hosted Email end users.

Policy objectives

The Tucows Mass Mailing Policy covers the following issues:

- Controlling mailing rates that stress systems.
- Eliminating service degradations.
- Mitigating the thousands of bounce messages in mail queues that delay mail delivery.
- Mitigating invalid return address information.
- Eliminating mass mailings during peak business hours.

Definition of mass mailing

“Opt-in” mailings are those email messages that are sent to more than 250 users by either Tucows customers or their third party partner to any group of end users. Opt-in means that the end user has signed up for mailings voluntarily. “Opt-in” implies that the mailing is not Spam.

Reminder

Spam is defined as “unsolicited bulk email that includes advertisements or solicitations, commercial or otherwise, regardless of content.” Without exception, Tucows prohibits the practice of mass mailing unwanted email solicitations of any type, regardless of content, and will take action to prevent this practice.

Mass mailing requirements

Mail send rate Mass mailings are done at a maximum rate of 10 messages/second.

Use of appropriate servers for originating mailings Use of Tucows Hosted SMTP servers for mass mailings is strictly prohibited.

Delivery of mass mailings All mass mailings (mass mailing sent by a domain, whether hosted or not hosted by Tucows, to domains hosted by Tucows) must be delivered through Tucows inbound MX machines. All mass mailing sent through Tucows SMTP servers will not be delivered.

Allowable send times Mass mailings must be started and completed between 0500 and 1200 UTC.

Valid "From", "Reply-To", "Return-Path" and "Error-To" headers If the following values are included in your mail header, they must contain valid addresses and each email address must accept any bounces at the rate that they occur.

- "From",
- "Reply-To",
- "Return-Path"
- "Errors-To"

The Tucows mail servers are not set up to process bounce messages for mass mailings. Therefore, none of the above addresses should deliver the bounce messages to an account on Tucows servers. Delivery of such bounce messages to a Tucows user account can cause service degradation and we will suspend the account involved to protect our servers.

Valid "Abuse contact" customers who send/receive mass mailings *must* supply Tucows with an emergency abuse contact in case there are any problems/complaints associated with the mailing.

Notifying Tucows of Mass mailing Tucows requires 48 hours notice for all mailings. The following information must be mailed to: massmailing@tucows.com

- Customer Name
- Number of recipients
- "From" domain
- "Target" domain
- Mailing Subject
- Mailing Date
- Mailing Start-End Times
- Rate of mailing (maximum of 10 messages per second)
- Valid "From", "Reply-To", "Return-Path" and "Error-To" addresses (please list the values used, if any)
- Copy of the message content
- Method for users to "opt-out" of mailings

Failure to comply with the conditions set forth above may result in:

- Blocking of the mailing currently causing the problems/complaints.

- Blocking of future mailings until the above requirements are satisfied. (Or until there is an agreement or special dispensation made by the Tucows Abuse Administrator.)
- If no “abuse contact” is provided to Tucows, Tucows reserves the right to block mailings without notifying the customer.

