



GFI White Paper

***Greylisting:
Decrease junk mail,
increase productivity***

Contents

The basic premise.....	3
How greylisting works.....	3
Impact on mail flow.....	3
Enabling greylisting.....	3

The goal of GFI MailEssentials Complete Online™ is to improve business productivity by reducing the volume of junk mail and time spent managing it. Achieving this goal is akin to duplicating what email users experienced back in 1994-95, when almost all email messages were 'legitimate' and extremely little time or effort was spent dealing with junk email. While MailEssentials Complete Online detects a vast majority of today's junk email, we are continually working on new approaches to combat the increasing sophistication of spammers and reduce time spent managing whitelists and blacklists, reviewing quarantines and digests and other tasks. Greylisting is one of the ways MailEssentials Complete Online reduces junk mail and saves you time.

The basic premise

The concept is simple. The first time a given mailbox receives a message from a given sender, we respond to the sending mail server with a temporary rejection message, asking the server to try again. (This happens during the SMTP conversation and is transparent to end-users.) With legitimate email, the sending mail server tries again a few minutes later, at which time we accept the message. Most spam messages are sent using software that will not retry the delivery. These messages will never arrive in MailEssentials Complete Online's quarantine or the user's inbox. With Greylisting, you'll save valuable time once spent scanning the quarantine, daily digest or a user's spam folder thanks to a greatly reduced volume of spam messages.

How greylisting works

For each incoming message, three elements are examined in the early part of the SMTP conversation: the sender IP address, the sender email address and the recipient email address. If this is the first time this email 'relationship' has been identified, a temporary deferral message is issued to the sending mail server – before the DATA portion of the email is sent. That relationship is then "greylisted."

If or when within a finite time period that same set of sender IP address, sender email address and recipient email address is seen again – as would be expected with any legitimate email – the combination is "whitelisted", so that the message, as well as future messages with that relationship, are accepted immediately, without temporary deferral. The whitelisting remains in place for upwards of a month.

After a message passes through the greylisting, it's processed as usual. Any spam message that is greylisted and re-tried will be subjected to the same stringent message analysis techniques as in cases where greylisting is not used.

GFI Software conducted a greylisting test of one million messages and found that less than 75,000 spam messages were retried – meaning over 90% of junk mail was blocked by greylisting alone.

Impact on mail flow

Greylisting by its nature can introduce delays in message flow, but these delays are generally brief and non-recurring for a given recipient-sender combination.

The length of delay is dependent on how long a sending mail server waits before re-sending a message. While a few sending mail servers – typically those used for high-volume mailings – will have a relatively long retry interval of an hour or more, most mail servers will automatically re-send a temporarily deferred message in 15 minutes or less.

Additionally, since the email 'relationship' described above (sender IP address, sender email address, and recipient email address) is whitelisted after a single temporary deferral, there should be no subsequent delays after that initial message.

Last but not least, any sender addresses that are whitelisted by a user or domain administrator are not greylisted.

Enabling greylisting

Greylisting can be enabled or disabled at any time on a domain-wide basis, via the MailEssentials Complete Online control panel.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit <http://www.gfi.com/contactus>



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.