



# **Greylisting Simple Concept, Highly Effective Technique**

**GFI MAX MailProtection™**  
Hosted Email Security and Continuity

# Greylisting

## Simple Concept, Highly Effective Technique

The goal of GFI MAX MailProtection™ is to improve people's productivity not only by decreasing the volume of junk mail that people receive, but also by reducing the amount of time that administrators and end users spend managing their junk mail. Achieving this goal is akin to duplicating what early Internet users experienced back in 1994 or 1995 – almost every email message was 'legitimate' and extremely little time or effort was spent dealing with junk email. While GFI MAX MailProtection detects a vast majority of today's junk email, we are continually working on new approaches to both combat the increasing sophistication of spammers and to reduce the amount of time that people need to spend managing whitelists and blacklists, reviewing quarantines and digests, and other tasks. Greylisting is one such technique that can reduce the volume of junk email while also saving 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 sending mail 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 re-try the delivery – thus those junk messages will never be re-sent, and will never arrive either in the GFI MAX MailProtection quarantine or in the user's inbox. And, because those messages won't be in the quarantine, the daily digest, or a user's spam folder, greylisting can save time that would normally be spent scanning those messages.

### How Greylisting Works

For each incoming message, three elements are examined in the early part of the SMTP conversation: the IP address of the sender, 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 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 – that combination is "whitelisted", so that that message, as well as any future message with that relationship, is passed through without the temporary deferral. The whitelisting remains in place for upwards of a month.

After a message passes through the greylisting, that message is processed as usual, so that any spam message that is re-tried will still be subjected to the same message analysis techniques as in cases where greylisting is not used.

In a test of greylisting that GFI Software conducted, of a million messages that are temporarily deferred, less than 75,000 messages were re-tried – meaning that upwards of 90% of junk mail was blocked using this technique alone.

# Greylisting

## Simple Concept, Highly Effective Technique

### 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 the delay is dependent on how long a sending mail server waits before re-trying after we defer the message. While a few sending mail servers – typically those used for high-volume mailings – will have a relatively long re-try 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 address, and recipient address) is whitelisted after a single temporary deferral, there should not be any subsequent delays after that initial message.

Last but not least, any “From” addresses that are whitelisted by a user or domain administrator are not subjected to the greylisting.

### Enabling Greylisting

Greylisting can be enabled or disabled at any time on a domain-wide basis, via the GFI MAX MailProtection control panel or by contacting GFI Software’s technical support.

© 2010. 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.