Q How does graylisting work?

A Graylisting functions at the mail relay level of the mail transfer process. When an SMTP communication between a remote mail server and KENDRA's mail relay server is initiated, three pieces of information are passed to KENDRA's mail server early in the communication: the IP address of the remote server, the mail recipient's address (ex. john.doe@Kendra.edu), and the sender's address (ex. spammer@spamhouse.com). This "triplet" of information is checked against an internal database of previous mail communications.

If this specific triplet has not been successfully passed by the graylisting system before, a temporary failure message is sent to the remote mail server. If the remote mail server is properly configured according to RFC 821, which specifies the SMTP protocol standard, the remote mail server will attempt to resend the message after a brief delay (usually within 1 hour of the original attempt). Resent messages containing this same triplet of information will be passed immediately to the KENDRA recipient to whom they are addressed.

Spam, on the other hand, is typically not resent, commercial spamming programs tend to not retry messages that are temporarily failed. In addition, automatically generated e-mail sent from virus-infected computers is also typically not resent, making graylisting one extra level of protection against these viruses. Finally graylisting benefits KENDRA's network by reducing unnecessary traffic. Since graylisting rejects e-mail before any of the message body or attachments are sent, a large portion of the traffic generated by spam never makes it into KENDRA's mail server or onto KENDRA's network.

While over time spammers will likely adapt to graylisting techniques and develop software that does resend, requiring a resend on bulk mailings will eventually help to make other techniques, like real-time blocking lists (RBLs) more effective by allowing more time for spammers to be added to RBL blacklists before their spam is passed onto KENDRA's network. In addition, any resending required of spammers can dramatically increase their operating costs, draining some of the commercial motivation behind most spamming.

Graylisting is not a replacement for spam-tagging, anti-virus programs or safe computing practices by users. KENDRA is employing graylisting as an additional measure in our battle to eliminate as much spam as possible from KENDRA's network. It is likely that a small amount of spam will continue to filter into user's mailboxes, and users should continue to be vigilant in managing their e-mail, and avoid opening unexpected attachments, or those sent by unknown users.

(this answer relies on information taken from Evan Harris' explanation of graylisting located at http://projects.puremagic.com/greylisting/whitepaper.html, and on the Slashdot discussion of graylisting located at http://slashdot.org/articles/03/06/20/168203.shtml?tid=111&tid=126)

Q Will graylisting cause me to not receive legitimate e-mail?

A Kendra believes, based on our research and on the design of the graylisting system, that it is very unlikely that any legitimate mail will be ultimately prevented from delivery. Graylisting works by taking advantage of characteristics of the SMTP protocol that is the universal standard for mail delivery over the Internet. While graylisting does initially reject mail from previously

unknown senders, properly configured mail servers forwarding legitimate mail will simply resend the e-mail after a relatively short delay. Please note that e-mails from KENDRA users will be automatically passed by the graylisting system and are thus unaffected by it.

However, it is possible, though unlikely, that the mail server at a remote location could be improperly configured and thus either fail to resend the message altogether, or resend the message either too soon or after too long of a delay to be accepted by the graylisting system. In this case, the message would continue to be rejected, and ultimately the remote mail server may cease delivery attempts.

Even in these unlikely circumstances, the remote mail server will typically notify the user sending the e-mail that it has been unsuccessful in its delivery attempts. Thus, the person sending the e-mail will be aware of the fact that you did not receive his/her message, and may contact you by other means.

If you are notified by an individual who says that his/her e-mail to you was bounced/rejected, please contact Kendra Support (support@kendra.com)

Q Will graylisting slow down the delivery of e-mail?

A In general, graylisting will not slow down the delivery of e-mail at all. Only the initial e-mail from an unrecognized sender will be delayed by the graylisting system, typically for a period of less than 1 hour. After this initial e-mail is passed to you, further messages from that recipient will be passed automatically by the graylisting system without delay. Mail sent by KENDRA users using the Kendra e-mail system will be passed automatically by the graylisting system and thus not subject to delay.

The records of senders maintained by the graylisting system do expire after a certain period of time. If you receive e-mail from a particular sender less frequently than once a month, these e-mails may be repeatedly subject to delay by the graylisting system. If you receive time-critical e-mails from certain sources at this level of infrequency, please contact Kendra Support (support@kendra.com)

Q What if I have questions or comments?

A Graylisting is only one of several new anti-spam initiatives that was deployed during the Fall quarter 2007. KENDRA welcomes questions, comments, of feedback concerning the new Graylisting service, the Kendra spam tagging system, or any other e-mail related service or support provided by KENDRA. Please e-mail these questions, comments, or feedback to Kendra Support (support@kendra.com)