

UC Davis Anti-spam Program Overview

EXISTING MEASURES

The following measures, which were implemented between spring 2003 and fall 2004, have helped reduce the number of spam messages that land in individuals' campus email inboxes.

- **Scanning and Tagging Possible Spam**
 - Since 05/03, Spam Assassin has scanned all email passing through the campus email servers
 - Purpose: Determine how likely it is that a message may be unsolicited commercial email ('spam').
 - Scoring & tagging:
 - SpamAssassin compares a message's characteristics to common characteristics of spam messages (e.g., use of certain words in subject line, use of graphics and links in body).
 - Points are assigned to each of these spam characteristics.
 - Messages scoring 5 points or higher are tagged as possible spam.
 - The higher the score, the more likely the message is spam.

- **Filtering Spam**
 - Opt-in service provided since 05/03; works in conjunction with scanning and tagging program.
 - Allows individuals the option of:
 - Having messages that are tagged as spam automatically deleted, or
 - Diverting those messages to a *ucd-spam* folder (created for them and accessible via the Web-based email program in MyUCDavis, or Geckomail).

- **Allow/Deny Lists**
 - Available since Fall 04.
 - Allows individuals who have opted in to spam filtering to personalize the service.
 - Messages from addresses individuals add to these lists are allowed through the spam filtering system (or denied) regardless of their spam score.

UPCOMING ENHANCEMENTS

To further reduce the number of unsolicited commercial (spam) email messages passing through the campus email servers, planning is underway to enhance the existing spam filtering service. Some enhancements under consideration include:

- **Temporary quarantine of high scoring messages**
Messages scoring 15 points or higher would be sent to quarantine message folders automatically created for all campus email users. Quarantined messages will be saved in those folders for XX days.
- **Real-time black list**
This feature identifies spam by running a script on campus email logs and identifying the IP addresses from which spam is sent. If a particular IP address sends more than 20 messages identified as spam **and** over 85% of messages sent from that address is identified as spam, the IP address is added to the campus blacklist. All messages originating from IP addresses on the blacklist will be rejected by the campus email servers. Bob, what can users do to be removed from the blacklist? Also, will they be notified that they've been added to the blacklist?
- **Bayesian filtering and Distributed Checksum Clearinghouse (DCC) – Are there any user-friendly terms to describe these enhancements? I'm not sure I understand what new functionality they'll translate into. . .?**
Both of these enhancements are intended to refine the spam scoring system and, aside from the improved scoring accuracy, will be transparent to campus email users.
- **Campus Email RFI**
Bob, can we say a few words about the long-term plans for the campus email architecture? Results of the RFI?

For additional information about spam filtering or to set up filtering on your campus email account, see <http://security.ucdavis.edu/spam.cfm>.