

## ISP Services :: What is dSpam?

### Why do I need an email anti-virus/anti-spam solution?

"Spam accounts for 45% of all e-mails, or 15 billion messages every day, and costs business world-wide a total of \$20 billion a year in lost productivity and technology expenses, according to the Radicati Group, a market research firm in Palo Alto, CA. The firm predicts the number of daily spams will rise to more than 50 billion by 2007, and costs will reach almost \$200 billion per year."

--Wall Street Journal, August 2003

There is no dispute that email has become a key communications tool for corporations. However, with spammers quickly filling your company's inboxes with unwanted messages, email has become a less efficient means of communicating. In fact, according to predictions by industry analysts, a third of your inbox will be spam by the end of the year, if not already. What is dSpam?

Dial Media Group's solution to this is a product we call 'dSpam', an award winning Anti-Virus and Anti-Spam firewall that checks all incoming email at the Internet level and intercepts unsolicited email and viruses before they reach your network. The Anti-Virus engine and Anti-Spam service will stop viruses and filter the remaining emails to ensure that only relevant emails enter your network, thereby increasing employees' efficiency and productivity and reducing stress on your email infrastructure.

The dSpam Anti Virus and Spam firewall handles a massive amount of email, over 10 million messages a day, without bogging down your own email servers. How can dSpam help?

The dSpam anti virus and anti spam service is unique in that it allows you to set up your own filtering criteria - a combination of public and internal company blacklists and whitelists. Additional functionality allows you to specify how all spam and suspect e-mail should subsequently be handled. It can handle over 10 million messages a day - filtering out both spam and viruses without adversely affecting your email servers. In fact, the dSpam service actually reduces the load on your email servers because it operates independently. As a user of the dSpam service you no longer need to worry about changes and trends in spam and virus attacks as new definitions and defenses will be added to the system automatically.

- Uses filtering and award winning technology
- Fully managed service, freeing your internal IT resources
- No need for additional hardware or software
- Reduction of incoming e-mail by up to 55%, enhancing efficiency and operation of your e-mail system
- Increased employee efficiency and productivity, due to reduced number of irrelevant and wasteful e-mails

Key features of our dSpam service

### Suspect emails get quarantined

There are three main types of emails: emails that you want, emails that you do not want (spam), and emails that are suspect. The dSpam service will tag suspect emails for delivery into a quarantine area on the dSpam servers. You can then either have the end user or another designated person be the final judge of what to do with these suspect emails. If after 30 days no action is taken, the message is deleted.

No software to install

No modifications to your existing email system

Deploying the dSpam service is easy. There is no software to install. There are no modifications to your existing email system. Simply let us know the domain name you would like scanned and we can advise you on adding dSpam to your domain.

### Blocks spam using proven methods

By using all the best methods to block spam, the dSpam service provides comprehensive spam-blocking for your company. Below are the primary algorithms we employ to block spam. We generally expect approximately 97% success. However, we provide a number of parameters that can be adjusted if necessary.

- Blacklisting of websites and domains: Central services maintains an up to date list of the largest and most aggressive known spammers. This list is maintained by both our suppliers and other anti-spam groups. This list is automatically updated on the dSpam service.
- Keyword scanning of emails: This can be configured on a per user basis. Our scanning methods include a scoring system such that emails are scored based on a number of criteria. If the score is above a threshold, then that email is flagged as spam.

- Checksum technology: Central services monitors email traffic through the Internet and uses checksum technology to keep track of the number of times a particular message has appeared on the Internet. If a message has appeared over a certain number of times, it is categorised as known spam. Checksums of known spam messages are utilised by the dSpam service to block spam messages.
- Message authenticity checking: Several algorithms are utilised to verify the authenticity of a message. Some of these are simple checks to verify that the 'from address' is authentic. Some are more complex relating to SMTP protocol.
- Blacklists and Whitelists: Domains, IP's, and email addresses can be blocked or whitelisted (allowed through). These lists may be maintained on a per user basis.
- Rate controls: Utilised to stop denial of service attacks as well as dictionary based spam attacks. These are integrated and automatic in the dSpam service.
- File type attachment blocking: we will block certain types of files, such as vbl scripts, from entering your company.