

How vendors protect organizations from spam

Organizations face a significant threat from spam and viruses, but how do organizations select a solution to face these threats? While there are a few established virus vendors, there are still dozens of anti-spam solutions. This article discusses the critical components of spam detection solutions required to effectively manage the spam threat and minimize the impact of spam on an organization's operations.

To be effective, spam protection vendors must innovate more quickly than the spammers who are evolving their attacks. Effective spam protection vendors have anti-spam labs dedicated to the analysis and improvement of the spam solution and advanced technology designed to enable the labs to rapidly adopt and deploy advanced detection techniques.

Anti-spam solution vendors help organizations manage the spam threat in three ways:

Spam detection technology

Vendors place spam detection technology at the email gateway to detect and remove spam messages from the organizations message stream.

Anti-spam labs

Vendors provide ongoing updates to both the anti-spam technology and the supporting data used by the filters to detect spam messages.

Spam filter management

Vendors provide tools to help organizations manage the disposition of spam messages, manage any quarantined messages and adjust the filtering to meet their organizations specific needs.

Effective spam filtering solutions excel in all three key aspects of spam protection: spam detection technology, anti-spam labs, and spam filter management.

Spam detection technology

In most cases, new anti-spam techniques are highly effective when first introduced but their effectiveness diminishes over time as the spammers create new techniques to overcome them. Better filtering systems recognize that different technologies are more effective against particular spam activity and deploy multiple filtering technologies at the gateway, combined in different ways, to maximize detection while minimizing false positives. Effective spam detection:

- Combines multiple detection technologies into one solution
- Provides a framework to incorporate new technologies
- Demonstrates innovation with unique detection technologies
- Is frequently updated to avoid testing and compromise by spammers

Anti-spam labs

Anti-spam technology provides organizations with the infrastructure needed to protect their users from spam, while the vendors anti-spam labs provide the technology with data necessary to protect against evolving spam activity. Solutions must provide both, as the vendor's anti-spam labs hold the key to

maintaining effective, ongoing spam protection. Only through the analysis of current campaigns and the development of new techniques based and evolving spam tactics can vendors maintain their effectiveness.

Five key spam detection processes:

Collection of spam messages	Vendors must have visibility into the current spam affecting the markets they serve. Enterprise anti-spam vendors should have enterprise spam traps to ensure the vendor is detecting the same campaigns as their customers receive.
Analysis of new spam methods to identify key spam indicators	Automated generation of spam tests is helpful, but vulnerable to compromise by spammers. To combat this, leading solutions rely on analytical processes to determine the strong spam indicators that separate spam from legitimate messages.
Tuning spam detection to suit current spam campaigns	While statistically insignificant, a few examples of a new spam technique represent the leading edge of current spam. Effective anti-spam labs combine analytical and automated tuning processes to highlight and focus the spam detection on current tactics. These semi-automated processes result in a faster, more reliable and effective method for tuning multiple spam tests than fully automated spam detection, which tends to highlight older, historically common spam tactics.
Testing the spam detection to ensure effectiveness in blocking spam without introducing false positives	New detection techniques and changes to the tuning must be tested for effectiveness and false positive level prior to updating. Alternate approaches such as automated rule generation are less effective, as they are more vulnerable to compromise and other unintended side effects.
Updating the rules to protect customers from spam	Vendors must have a simple, automated mechanism to keep rules synchronized that respects the customer's configurations and preferences.

Spam filter management

Once detected, spam must be disposed of appropriately. For some organizations this may mean discarding of messages, while for others it is tagging of messages. For most organizations spam disposition includes quarantining of spam messages for a period of time, which allows users to review quarantined messages and avoid the potential impact of false positives. Effective spam management includes:

- Flexible spam handling with the ability to set multiple spam disposition thresholds and actions
- The ability for end users to review quarantined messages on a scheduled or on-demand basis
- The ability for administrators to configure the detection criteria to meet the unique message filtering needs of the organization
- Global and end-user whitelisting capabilities to support both the efficient central management of whitelists and personal preferences
- Quarantine management capabilities sufficient to handle multi-million message quarantines

For more information, visit www.sophos.com/spaminfo

SOPHOS
WWW.SOPHOS.COM