

WHITE PAPER

What You Can and Should Do About the Rising Cost of Spam

Sponsored by: MessageGate Inc.

Mark Levitt

Brian E. Burke

Robert P. Mahowald

Christian A. Christiansen

March 2004

IDC OPINION

Spam is the latest scourge of the Internet, second only to viruses and other malicious code in the anger and frustration that it evokes. Filling networks, servers, and inboxes with unwanted and often offensive content, spammers continue to wreak havoc by frequently changing spam's appearance and masking its source to avoid having spam be identified and blocked before reaching its target: email inboxes. Since 2001, IDC has tracked a remarkable surge in spam volume and the resulting lower business worker (LOB) and information technology (IT) staff productivity and higher IT infrastructure and other costs. Spammers take advantage of the email model's ease and low cost with which mass email broadcasts can be sent, and from the fact that, similar to the cell phone model, it is the recipient of the phone call or the spam message who incurs costs for receiving, reviewing, and storing inbound messages. As the cost of spam rises along with the increase in the volume of spam, businesses, service providers, governments, and individual email users are only beginning to realize the need to take action against spam by separating spam and other types of unwanted email from legitimate and mission-critical inbound email and shifting the costs of spam to the spammers in ways that protect the future of email as an effective and efficient form of online communication.

METHODOLOGY

Determining exactly how much time and money spam costs users and their organizations is required to help convince decision makers of the magnitude and scope of the problem. To measure the cost of spam and the value of antispam solutions, IDC surveyed 1,000 LOB and IT mid- to upper-level managers representing organizations of various sizes (starting at 500 employees) and industries in North America in October through December 2003. IDC also interviewed 30 senior IT executives at organizations with more than 1,000 employees representing a range of vertical industries to capture their perspectives in greater detail.

The analysis presented in this IDC White Paper reflects research conducted in an IDC multiclient study. IDC designed, conducted, and analyzed the research to develop our conclusions on the true cost of spam and the business value of antispam solutions. A number of vendors offering antispam and related security and messaging solutions subscribed to the study.

IN THIS WHITE PAPER

This IDC White Paper identifies the cost of spam on worker productivity, IT, and other corporate resources, and explores the value of antispam solutions. It presents key findings from the 1,000+ surveys and executive interviews that IDC conducted among LOB and IT managers in fall 2003 as part of an IDC multiclient study and recommendations on how the problem of spam should be managed.

SITUATION OVERVIEW

What Is Spam?

If only there was a simple answer to this question, solving the spam problem would be a lot easier. IDC has divided all email traffic into three categories:

- ☒ **Person-to-person emails** are typically sent one message at a time from one email user to another. These emails contain content that for individual recipients can range from highly relevant and mission critical to somewhat relevant and low priority. Examples may include press releases and other information sent to a targeted list of recipients based on their positions or activities.
- ☒ **Email alerts and notifications** are typically sent automatically by an application or system to individuals or groups that originate from a preexisting relationship or arrangement with identifiable and legitimate sources. Examples of email alerts and notifications relate to email delivery, availability of new content on Web sites, links to news items and newsletters, and project updates.
- ☒ **Spam** is "unsolicited bulk email" sent by both legitimate direct marketers offering commercial products and services as well as less reputable firms and individuals offering illicit, offensive, and even nonexistent products and services or using email to deliver viruses. "Bulk email" is automated, mass email mailings that tend to have lower costs and response rates relative to traditional postal mail and telephone direct marketing campaigns.

The problem in defining, identifying, and separating spam from other email lies in the subjectivity inherent in what constitutes "unsolicited." At a basic level, "unsolicited" means that spam has been received by an owner of the email inbox who has not consented to receive it. To be "solicited," ideally email would have explicit consent to receiving specific content through an existing relationship or an opt-in process (e.g., "I give you permission in advance to send me email of this kind."). However, in the absence of such explicit consent, email marketers often rely on implicit consent based on recipients having purchased products or opted in to receive information in the past (e.g., a retail-customer relationship, group membership, Web site, or newsletter registration, etc.) for similar offerings. The degree to which emails containing new offers or information sufficiently resemble what was previously received with consent can vary greatly. While illegitimate email marketers do not typically care about consent and often rely on randomly generating or harvesting email addressees or buying email addresses from third parties, legitimate marketing firms may push the

envelope in relying on implicit consent from recipients, who often have an entirely different perspective about what emails they consented to receive.

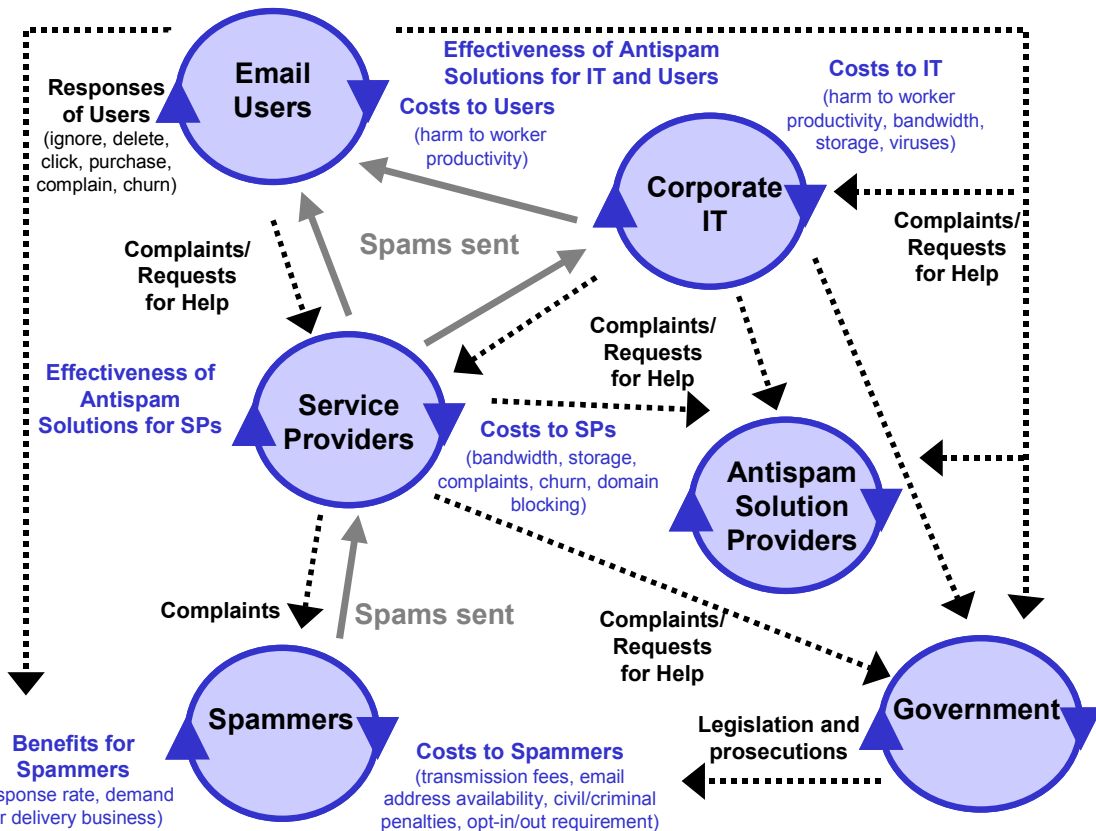
Clearly, the devil is in the details of how to apply definitions of spam to specific email traffic. While some emails containing fraudulent offers or scams would be nearly universally recognized and rejected as spam, other emails seen as annoying wastes of time and resources by some people could be welcomed as legitimate commercial offers by other people, even if the emails were in fact unsolicited.

Understanding the Spam Model

Let's take a look at the players and factors responsible for spam. IDC has created a spam model made up of multiple feedback loops representing the economic market ecosystem in which spam rises or falls (see Figure 1).

FIGURE 1

Spam Model



Source: IDC, 2004

In this model, the circles represent a combination of the players in the spam market and the feedback loop that affects whether spam increases or decreases. Factors such as costs, benefits, and effectiveness of antispam solutions, appear near the feedback loops, which they affect. Lines with solid arrows represent the flow of spam, while the dotted arrows, such as complaints and legislation responses, represent the responses or feedback from one player/feedback loop to another loop affected by it.

Spammers

Starting with the spammers' loop at the bottom left, we see that they are motivated to send spam to service providers by benefits such as acceptable response rates from spam recipients and demand for delivering third-party spam. When these benefits *increase* as the result of real or perceived successes in reaching valid email addresses with at least a small percentage of favorable responses from users, the number of spams sent also tends to *increase*. When benefits *decrease*, the number of spams sent tends to *decrease* in the long term. (This is a positive feedback loop since the two elements move in the same direction.) In the short term, spammers may attempt to adapt to *decreasing* benefits by *increasing* the number of spam sent to boost the number of favorable responses.

A counterbalancing factor to spammer benefits is the rising costs of doing business as spammers, such as transmission fees, availability of email addresses, civil and criminal penalties, and opt-in and opt-out requirements. Currently, these costs are very low, which translates into lower customer acquisition costs for spammers marketing products or services over the Web. As these costs *increase* as the result of complaints from service providers and legislation and prosecutions from governments, the number of spams sent will tend to *decrease* in the long term. (This is a negative feedback loop since the two elements move in opposite directions.) In the short term, spammers may choose to absorb *increases* in costs and not *decrease* the amount of spam sent in the hopes that nonresponsive but valid email addresses will pay off in the future either from favorable responses or revenue from selling email addresses confirmed to be valid.

Service Providers

Following the solid arrow showing the path of spam from spammers, we see that the amount of spam that service providers relay to email user direct subscribers and corporate IT departments depends on the effectiveness of antispam solutions. This in turn affects the costs of spam for service providers, such as network bandwidth, storage requirements, subscriber churn, complaints about spam, and blocking of their domains at least temporarily for relaying spam to other service providers. As this effectiveness *increases*, the number of spams relayed *decreases*. As the number of spam messages and complaints from email users and corporate IT departments *increases*, service provider costs *increase* as well. In addition, service providers respond to these *increases* by threatening or cutting off known spammers and requesting help from governments and antispam solution providers for more effective antispam solutions and initiatives, which if successful leads to *decreases* in the number of spams sent.

Corporate IT and Email Users

For both corporate IT and email users who receive email either directly or indirectly from service providers, costs and effectiveness of antispam solutions play similar roles to the ones they play in the service provider feedback loop. One factor that plays a more significant role among users and corporate IT is worker productivity. *Increases* in the number of spams that are delivered from service providers and evade antispam solutions lead to *increases* in costs especially harmful to worker productivity.

At the top left, we see how email users respond to spams that have reached their inboxes can affect the spam in the long term. By ignoring spams, email users *reduce* the response rate in the long term, thereby *reducing* one of the key benefits that is needed to motivate spammers to send spam in the long term. By *increasing* the number of complaints to or requests of help from corporate IT, service providers, antispam solution providers, and governments, email users *increase* those parties' costs, thereby motivating them to respond with more effective antispam solutions against spam or actions against spammers. On the other hand, email users who open or preview spam, which spammers can detect even if the recipient does make a purchase or provide private information requested, have taken actions that can *increase* response rates and other benefits for spammers, which tend to *increase* the number of spams sent in the long term as the result of higher profits to the spammer involved and word of favorable response rates and the availability of valid email addresses reaching other potential spammers.

Antispam Solution Providers and the Government

In response to *increases* in complaints and requests for help in dealing with spam, antispam solution providers and governments can *increase* the effectiveness of antispam solutions and other measures, thereby *increasing* costs for spammers and *decreasing* the costs of blocking spam for service providers, IT, and email users. Legislation requiring commercial advertisements labels in subject lines for quick and easy filtering by antispam solutions is an example of how government and antispam solution providers can work together to fight spam.

Costs of Spam

Now that we have an understanding of how the spam ecosystem works, let's take a closer look at the real costs of spam to enterprises according to the IT and LOB managers surveyed who deal with spam everyday. We will use the hypothetical example of a business with 5,000 email users and 10 IT staffers involved with spam. Please note that because the following cost estimates are based on averages of the firms surveyed as well as other information and assumptions about spam in the aggregate, actual costs may vary.

Email Users

Lost worker productivity among email users is far and away the largest cost of spam. For organizations without antispam solutions, the average amount of time lost by email users each day due to spam is 10 minutes, including time spent reviewing emails to identify which are spam and possibly tracking down valid emails that may

For organizations without antispam solutions, the average amount of time lost by email users each day due to spam is 10 minutes...This translates into a total of \$4.1 million in lost productivity each year for the firm with 5,000 email users.

have been deleted by users or IT by mistake. This translates into a total of \$4.1 million in lost productivity each year for the firm with 5,000 email users. This takes into consideration that only a portion of the time lost would likely have been used productively.

Corporate IT Staff

Lost productivity among IT staff dealing with spam, including email user complaints about spam, can be very costly as well. For organizations without antispam solutions, the average amount of time lost by IT staffers each day due to spam is 43 minutes. This translates into a total of \$85,800 in lost productivity each year from dealing with spam and viruses carried by spam for the firm described above.

Other Costs

Other costs, such as those for transmitting and storing spam, will vary depending on the speed at which spam is deleted from desktops and servers. The relatively small size of spam messages (several kilobytes) is a factor as well.

Spam can cause organizations to incur other costs that are harder to measure. For example, pornographic and other offensive content in spam can lead to time spent by human resources and legal departments dealing with employees complaining about spam or threatening to bring "hostile or offensive work environment" lawsuits against employers for not having effective antispam solutions that could prevent the spam from reaching their inboxes. In light of the high volumes of spam, and the extensive press coverage of the spam problem, employers would have a hard time defending against such suits by proving that they were not aware of the offensive content being delivered to employees on a daily basis. Another example of costs caused by spam is the harm done to the reputation of organizations whose servers are hijacked by spammers to relay spam to other organizations.

Antispam Efforts

For most organizations, spam has only recently emerged as a high-priority problem requiring high-priority attention and resources. Nearly 70% of the organizations surveyed had antispam solutions in 2003 and nearly 20% more expect to have one in place in 2004. This leaves only 10% without antispam solutions by the end of 2004.

More than 85% of the antispam solutions in use at the respondents' organizations have been in place for less than two years, and more than 50% for less than one year. Prior to 2002, spam was seen by most organizations as a nuisance that could be handled by individual email users along with basic homegrown email filters and domain name blacklisting of known spam sources. Corporate IT departments were too busy with other projects, including battling viruses and other malicious code capable of bringing down entire networks and damaging servers and personal computers, to invest time and money in fighting spam.

More than 85% of the antispam solutions at the respondents surveyed by IDC have been in place less than 2 years, and more than 50% are less than a year old.

What a difference two years make. During that time, spam has grown into too difficult and costly a problem for most IT departments to ignore or leave to email users. As one utility executive commented about the rise of spam in corporate email, "The

amount of email has probably tripled in the past two years, but the amount of spam has gone from 30% of that email to 50%."

Ballooning costs that spam imposes on email user productivity, IT staff availability, and other limited resources have made fighting spam a top priority. The frustration and cost of dealing with rising flood levels of unsolicited, largely unwanted, and often offensive emails is evident. As the CIO of a global food retail operation put it, "It's ludicrous that we should have to spend money on fighting spam, even though I see the benefit such spending delivers." The fairness of the situation aside, 60% of the firms surveyed consider spam to be a higher priority than it was last year, 37% consider spam to be of the same priority, and only 3% consider spam to be a lower priority.

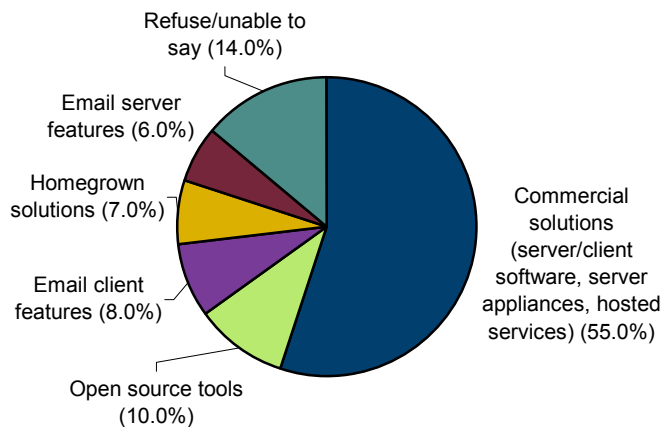
So why were there still 30% of organizations without any antispam solutions in place at the beginning of 2004? According to the IT managers surveyed, the two top reasons are that spam is not a problem or that there is no budget for a solution. These responses can be understood to mean that either in reality or perception there are other higher priority projects that consume all of the available budgets and other IT resources. As the problem of spam continues to worsen, the number of firms without antispam solutions in place will continue to drop.

Looking at the antispam solutions in place at the beginning of 2004, the majority were commercial solutions, followed by open source tools, email client features, homegrown solutions, and email server features (see Figure 2). This points to a recognition that fighting spam can be very time consuming and difficult and is most often best handled by experts who spend all of their time and resources focused on developing even more effective ways to block spam.

FIGURE 2

Types of Anti-spam Products, Services, or Methods in Use

Q. What antispam products, services, or methods does your organization use?



Source: IDC's Spam Survey, 2003

Benefits of Antispam Solutions

According to the organizations surveyed, the biggest benefits of antispam solutions are in higher worker productivity (see Table 1). Please note that because the following cost-savings estimates are based on averages of the firms surveyed as well as other information and assumptions about antispam solutions in the aggregate, actual cost savings may vary.

TABLE 1

Average Productivity Cost of Spam and Savings of Antispam Solutions for Firm with 5,000 Email Users

Workforce Segment	Description	Without Antispam Solution	With Antispam Solution
Email Users	Daily time spent by each user	10 minutes	5 minutes
	Average annual cost/savings to firm	\$4.1 million	\$783,000
IT Staff	Daily time spent by each user	43 minutes	19 minutes
	Average annual cost/savings to firm	\$85,800	\$13,000

Source: IDC's Spam Study, 2003 []

Email Users

Antispam solutions reduce the average amount of time lost due to spam each day for email users down to 5 minutes, a 50% reduction. This translates into a total of \$783,000 in email user productivity gains each year for the 5,000-email user firm described above. Note that having an antispam solution does not entirely eliminate the time email users spend dealing with spam because of the spam that avoids detection and reaches email inboxes and the fact that organizations choose solutions that involve email users reviewing suspected spam before deletion.

Corporate IT Staff

Antispam solutions reduce the average amount of time lost due to spam each day for corporate IT staffers down to 19 minutes, a 56% reduction. This translates into a total of \$13,000 in IT staff productivity gains from reduction in time spent dealing with spam and viruses carried by spam for the 5,000-email user firm described above. Note that even after an antispam solution is deployed, there may continue to be a fair amount of spam-related work for IT staffers to do, such as administering servers, updating spam patterns and software, and responding to email users about spam that evaded detection and false positives (legitimate emails incorrectly identified as spam).

Other Benefits

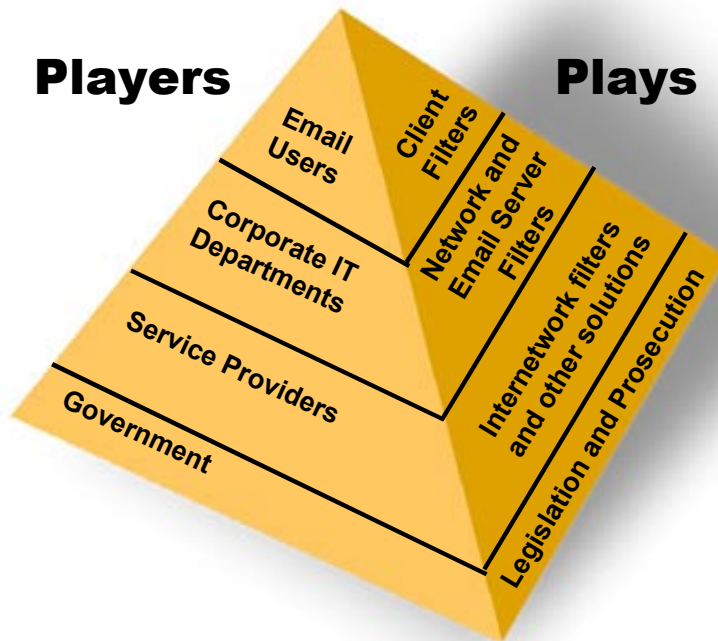
Other benefits from anti-spam solutions include reductions in network and storage costs, which will vary depending on whether spams are deleted immediately or saved in spam folders for email users to review. Corporate liability for offensive spam content and harm to corporate reputations for relaying spam unknowingly will decrease due to less spam being delivered and the organizations ability to demonstrate steps taken to block spam.

Antispam Players

A coordinated multilayer approach is necessary to have a chance of controlling spam that is constantly changing. Each layer adds protection that is necessary but not sufficient to do the job by itself (see Figure 3).

FIGURE 3

Layered Approach to Fighting Spam



Source: IDC, 2004

Governments

A growing number of government agencies are joining the fight against spam by targeting spammers with legislation that specifically criminalizes and provides penalties for the act of spamming. In response to antispam state laws being enacted around the country and the world, the U.S. federal government passed legislation known as the CAN SPAM Act of 2003, which preempts U.S. state laws. This Act walks a fine line between the interests of legitimate direct marketing firms on one side and the email users, IT departments, and service providers on the other, not surprisingly without pleasing either group entirely. It specifically criminalizes fraudulent subject lines and prohibits pornographic material to be placed in the body of emails. It charges the Federal Trade Commission (FTC) with the task of establishing standard content to be placed in subject lines to identify emails containing links to pornographic content and those containing advertisements and reviewing the effectiveness of the Act on controlling spam. The Act reflects a balancing of interests by the federal government. For example, the Act includes an opt-out requirement for email supported by the Direct Marketing Association rather than an opt-in requirement desired by antispam advocates. While the Act could have been more aggressive in battling spam, that would have risked making it more difficult and costly for legitimate firms to do business over the Internet and more time consuming for individuals who wish to receive legitimate business communications by email.

For the Act to have a significant impact on spam, the government cannot rely on spammers taking it upon themselves to comply. Aggressive enforcement of the Act through investigations and prosecutions of violators are required. Only visible, public actions will directly stop some spammers and deter many others from violating the Act.

Service Providers

The first line of defense against spam itself consists of service providers that are asked to relay huge volumes of email, which may include spam to other service providers, organizations, and email users. Close to the source of spam, service providers are in a unique position of being able to either stop or at least slow down the rate at which spam enters the Internet by watching the behavior of parties attempting to submit large volumes of emails for routing to subscribers or other service providers and by watching large volumes of spam for suspicious characteristics based on email meta data or actual content.

Corporate IT Departments

Corporate IT has the primary responsibility for determining, with input from business management, what communications are appropriate to be transmitted and delivered across business networks and computer systems. Determining how aggressive to be in classifying email as spam is often left in the hands of IT staffers who evaluate, deploy, and configure solutions that may or may not have email user involvement. However, this centralized approach to overseeing policies in fighting spam sometimes needs to be modified to allow for greater email user involvement in categorizing suspected spam, such as in businesses that deal with sensitive communications and

content. IT departments should avoid pinching pennies by relying on email server filters and open source antispam software, which may save a little money up front but will nearly always cost a bundle in terms of the large amount of time typically needed to keep these up to date with the latest spam and in the terms of the spam that will evade detection without frequent updates from commercial antispam solutions firms spending all of their time keeping up with spammers. IT departments never rely on homegrown solutions to fight viruses. The same appreciation for outside expertise should be applied to fighting spam.

Email Users

The intended recipients of spam, email users, have the final say and therefore the much of the responsibility regarding whether spammers are successful. To reduce spam, users must act responsibly to avoid encouraging spammers. Never make a purchase or supply personal information in response to spam. While there may be exceptions on occasion that prove the rule, such as legitimate commercial offerings from known companies that are sent without expressed consent, avoiding any positive response to spam can help discourage spammers from sending more spam. Avoiding even opening or previewing spam can also help avoid confirming the validity of the address that can lead to more targeted spam that more easily evades detection. A second key rule is that users should try to prevent their email addresses from falling into the wrong hands. For example, when supplying email addresses on Web sites, be sure that that sites are reputable and have a policy of not sharing or selling addresses with third parties. In addition, users should be more selective when opting in to receiving information or offers.

Antispam Approaches

There are many different approaches to identifying spam. No one approach has proven to be 100% successful detecting all forms of spam without unacceptable levels of false positives. As a result, many antispam solutions rely on a combination of approaches.

Honey Pot Signatures

"Honey pots" or decoy email mailboxes, created on service provider and enterprise networks to act as spam catchers or traps, are used to provide the basis for generating signatures or patterns of spam received that are used for testing other inbound emails sent to real mailboxes. This approach focuses on the "unsolicited aspect of spam by relying on the fact that any email sent to a mailbox that does not belong to a real person could not have been solicited and is spam by definition.

A key advantage of this approach is that only actual spam is blocked, resulting in no false positives. A disadvantage is the flip side of the coin that only spam exactly matching known spam already caught can be blocked. Since spammers are constantly changing spam, signature-based solutions such as this are always playing catch up. Inherent in the design is a delay from when patterns for new forms of spam can be created and distributed before spam can be blocked. During this delay, new types of spam can make their way into user mailboxes. Overall, signature-based tools continue to be a good way of identifying and repelling known threats that currently

represent a significant portion of all spam and of reducing the amount of email that needs to be scanned using other techniques.

Content Analysis

One or more content analysis techniques are used to analyze everything about the content of inbound email by service provider or gateway or email server or even client antispam solutions. This approach focuses on the "commercial" aspect of spam by relying on the suspicious characteristics of legitimate and illegitimate offerings or information requests that spammers try to hide from spam filters and email users at least until they open the emails. There are many content analysis techniques in use including;

- ☒ **Keyword analysis:** This approach involves analyzing the text section of an email for specific keywords and phrases (e.g., sex, profanities, Viagra, etc.) that are unlikely to appear in legitimate business correspondence. Keyword filtering, when used as a standalone spam solution, is a very primitive technique and often produces a high risk of false positives.

- ☒ **Lexical analysis:** Lexical analysis works by analyzing the context for all of the words and phrases in a particular message. Unlike Keyword analysis, the presence of a particular suspicious word or phrase by itself does not necessarily mean that the message is spam. Instead, each word or phrase is assigned a weight depending primarily on the context in which they are found.

- ☒ **Bayesian analysis:** The basis of bayesian logic uses the knowledge of prior events to predict future events. When used to detect spam, a bayesian filter examines a set of emails that are known to be spam and a set of emails that are known to be legitimate and compares the content in both emails in order to build a database of words that will, according to probability, identify or predict future emails as spam or legitimate email. Although bayesian analysis is a new technique used to fight spam, the bayesian logic theory was actually first published in 1763.

- ☒ **Heuristics:** Heuristics is a technique that looks for spam-like characteristics in an email message. Each characteristic is assigned a spam probability, and the message is given a cumulative probability score based on the overall test results. If a certain probability threshold is reached, the email is determined to be spam and is blocked.

- ☒ **Header analysis:** These products examine headers, looking for such items as the validity of the sender's address, whether the same information is found in the "sender" and "from" fields of an email, and whether a specific message contains information not common to normal email.

- ☒ **URL analysis:** Spammers are increasingly embedding URL links inside of emails to direct users to specific Web sites. URL analysis looks at the embedded links in email messages and compares the link to a list of URL rules or known spam URLs to determine if the message is spam.

An advantage of content analysis is that new threats can be identified by directly examining emails for suspicious characteristics based on previously identified spam. In simple terms, this analysis looks for spam that looks like other previously known spam. A disadvantage of content analysis is that it can produce false positives when perfectly innocent emails are suspected of looking like spam because they resemble spam. To maximize the effectiveness of content analysis in blocking spam, antispam solutions are increasingly using combinations of different types of content analysis to generate aggregated scoring of emails representing the likelihood of their being spam. This score can be used by email servers and clients to either delete, quarantine, folder, or tag emails, depending on the score and suspected spam category, according to settings chosen by email users, IT departments, or service providers taking into consideration individualized or corporate preferences and requirements.

Blacklisting/Whitelisting

Blacklisting and whitelisting rely on the identification of senders of email to determine whether messages are spam. Blacklisting relies on lists of domain names or email addresses maintained by antispam Web sites, service providers, IT departments, and even individual email users that block all email from known spammers.

An advantage of this approach is that all content from known bad senders is blocked and all content from known good senders is passed through. A disadvantage of this approach is that spammers can change their identifying information and even hijack legitimate domain names and individual email addresses to make spam appear to come from good senders. Whitelisting relies on similarly maintained lists that allow all email from known legitimate "good" senders. By adding all business partners, customers, and suppliers to whitelists, companies can ensure that those firms' legitimate email will not be blocked by automated filters that know not what they do.

Sender Authentication

Following in the footsteps of blacklisting and whitelisting, sender authentication is promising to identify spam by checking the identification of named senders of email based on either sender email or IP addresses. Emails with sender information that cannot be authenticated with the sending domains can be blocked or identified as suspicious for further scanning. An advantage of this approach is the prevention of email fraud. A disadvantage of this approach is the time and will needed to incorporate compatible sender authentication tools into all of the message transfer agents (MTAs) routing email at Internet gateways.

Challenge/Response

Challenge/response techniques detect emails sent as part of mass email broadcasts by requiring senders of email to provide confirmation like a real person, rather than an automated machine, before emails are delivered to user inboxes.

An advantage of this approach is the ability to accept only person-to-person emails and dramatically reduce the amount of emails automatically sent to email users. A disadvantage to this approach is the way it treats legitimate senders of email as suspected spammers until they prove otherwise, at least for the first time that they

attempt to send emails to the named recipient after which time they are no longer challenged. This can frustrate email users and their customers, suppliers, partners and other legitimate senders or at a minimum delaying legitimate email from senders who may not have the time or the means (as is the case with automated newsletter or account information sent by email) to respond to the challenge.

Mass Mailing Detection

Spammers sending huge numbers of spam messages at a time create a pattern of behavior that can be detected. Service providers can close or slow network connections when mass emailings are attempted by suspicious senders. Email filters can identify emails connected with mass emailing. This approach focuses on the "bulk" aspect of spam by relying on suspicious mass mailings. An advantage to this approach is the content-independent focus on stopping spamming behavior and only blocking emails that are specifically tied to spamming behavior. A disadvantage is that spammers may alter their behavior, such as by sending smaller faster bursts of spam that would be harder to detect and stop.

Reverse DNS Lookup

Reverse DNS lookup runs DNS queries on the IP addresses of the incoming email to determine if the host name identified matches an actual host name for those IP addresses of the sender. Since many spammers use spoofed hosts to disguise the source of the spam, a query that doesn't recover a matching host and IP address is a good indication that the message is spam.

Which Is Best?

So which of the spam detection techniques list above is the best method? The best answer would be that no single approach is 100% effective and accurate in detecting spam. IDC believes incorporating a combination of these methods in a layered approach is the best way to detect the highest percentage of spam (effectiveness) and the lowest percentage of false positives (accuracy).

Antispam Solution Options

Antispam solutions are available in many forms, including server software, client software, server appliances, and hosted services, either as standalone solutions or as modules or features of broader content or messaging security solutions. Due to the updates that most antispam solutions require to be effective against the latest forms of spam, antispam solution providers must provide quick and easy ways to keep their solutions up to date.

Server Software

With most corporate email systems consisting of internally managed server software, deploying server software to fight spam is a common choice. Advantages include the many add-on products that can be installed and managed alongside email servers and Internet SMTP servers and that can be customized and integrated according to customer needs. Corporate IT staffers are very familiar with evaluating, buying, and installing server software and may see server software as the most cost-effective

option for larger firms. Disadvantages include the administrative costs and expertise required to keep the solution running with the optimal settings and the latest software and pattern updates.

Client Software

Antispam filtering at the desktop is growing as the result of a plethora of email and security client add-ons and built-in capabilities. Advantages include the ability for individual email users to determine the settings and actions for filtering spam. Disadvantages include the reliance on individual email users to decide what is best and the higher costs of installing and supporting software on every desktop and the risks of allowing spam, which could be carrying viruses, to reach desktops before being scanned. In addition, email users may end up spending more time than they should dealing with spam that could have been blocked at the network perimeter.

Server Appliances

Like other appliances, appliances that fight spam are designed for firms that want to avoid installing and managing software but that want an onsite solution. Advantages include an optimized hardware/software combination that requires minimal effort to get up and running and to administer. Disadvantages include the need to buy hardware when other hardware may be available and the real or perceived limitations on the amount of customization and integration that can be done.

Hosted Services

The availability of hosted services that fight spam Advantages in outsourcing anti-spam include the ability to get up and running quickly and rely on expert third parties for maintaining the solution for maximum antispam effectiveness. One firm identified another reason to let a third party do the job: "We just didn't want to have a committee on dirty words." Disadvantages include the real or perceived limitations on the amount of customization and integration that can be done and the need to trust third parties to ensure that confidential, mission-critical email is neither disrupted nor compromised.

FUTURE OUTLOOK

Impact of Spam on Email

Will spam result in the death of email? Despite the availability of real-time and structured collaboration tools, 90–95% of all collaboration occurs in email. Spam would need to bring email to a standstill after several vigorous rounds of defenses and counterattacks before significant numbers of companies would consider giving up on email. This is due to the myriad of business processes reliant on and increasingly integrated with email and the massive investments in hardware and software infrastructure, expertise, and training supporting email.

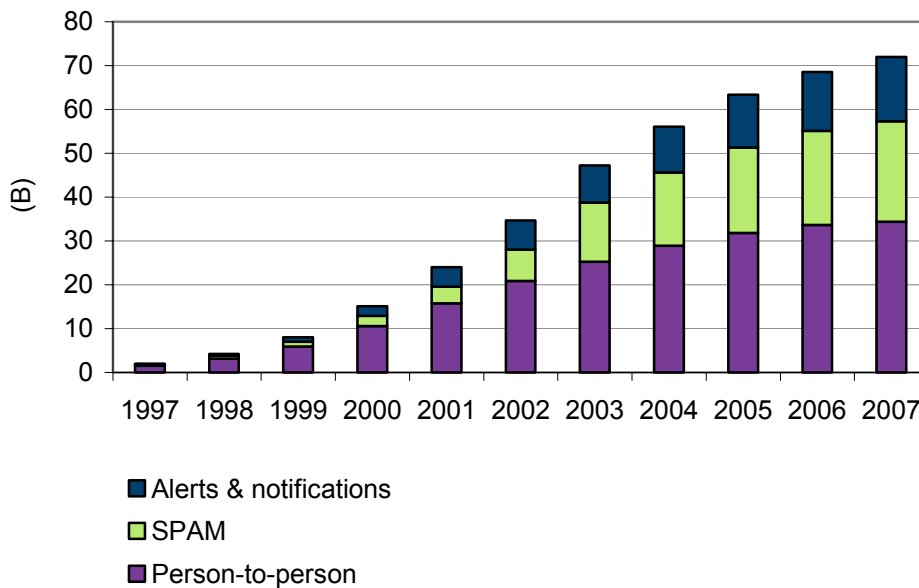
Moreover, there currently is no effective market substitute for email. Instant messaging (IM), short-message service (SMS), Web conferencing, and team workspaces lack the benefits of standards-based store-and-forward messaging to inboxes that are nearly always open to receive emails. In addition, there is still limited

experience in using and managing widespread use of these other collaboration tools and building up competence and confidence in these tools will take time. In addition, spam targeting IM and SMS users has only just begun and is expected to grow along with usage.

So while email has been weakened and remains under attack from spam, email in the form of person-to-person emails and email alerts & notifications email will continue to be a mission-critical communications and collaboration tool for the vast majority of businesses and other organizations (see Figure 4).

FIGURE 4

Worldwide All Email Messages (Alerts & Notifications, Spam, and Person-to-Person) Sent Daily



Source: IDC, 2003

CHALLENGES AND OPPORTUNITIES

Effectiveness of Antispam Efforts

Will antispam efforts successfully eliminate spam once and for all? Not likely. Both legitimate and illegitimate spammers will continue to create new ways to communicate their offerings in email with confidence that a sufficient percentage of recipients will respond favorably. In addition, legitimate direct marketers and their target customer base — the general public — will want to continue to do business over the Internet and communicate using low cost, ubiquitous email.

To maximize effective spam control, antispam solution providers will need to integrate various layers of protection to allow for a greater degree of accuracy in detecting both known and unknown spam. In addition, while many firms currently choose standalone antispam products or services in the interest of getting a best-of-breed solution, a growing majority of firms will prefer integrated comprehensive secure content management (SCM) solutions with antivirus, firewall, encryption management, Web filtering, IM, and other capabilities. Even firms that have historically favored traditional best-of-breed purchasing strategies, tightening of IT budgets for purchasing, and managing solutions will translate into integration and business value taking precedence over best-of-breed. This is because it will not do customers any good if they have the best products in the world if the firms lack people who are skilled enough to manage the products. Even the most skilled IT people will welcome products that help correlate and analyze blended threat attacks that are increasingly in frequency.

Nearly all spam could be stopped from reaching email users but at the cost of unacceptable levels of false positives. According to one organization interviewed, "The key in dealing with spam is the old physician's adage 'first do no harm.'" A large pharmaceutical firm pointed out the danger of blocking legitimate emails on the basis of their containing certain medical terms or body parts, "We get emails from patients experiencing medical difficulties, and these messages cannot be blocked in any way." Antispam solutions need to be customizable for individual policies and requirements of each customer, which may not be the same as other firms in other industries, or perhaps even in the same industry. There is no "one size fits all" in the detection of unwanted email.

"The key in dealing with spam is the old physician's adage 'first do no harm.'"

CONCLUSION

Recognizing the true costs of spam will require getting all of the necessary parties to do their share in fighting spam — email users, corporate IT departments, service providers, and governments. Legitimate direct marketers will need to comply with antispam legislation and establish best practices that can reestablish trust in email and email marketing.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.