University of Mississippi
eGrove

Guides, Handbooks and Manuals

American Institute of Certified Public Accountants (AICPA) Historical Collection

1-1-2004

CPA's guide to understanding and controlling spam

Roman H. Kepczyk

American Institute of Certified Public Accountants. Information Technology Section

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides

Part of the Accounting Commons, and the Taxation Commons

Recommended Citation

Kepczyk, Roman H. and American Institute of Certified Public Accountants. Information Technology Section, "CPA's guide to understanding and controlling spam" (2004). *Guides, Handbooks and Manuals*. 199.
https://egrove.olemiss.edu/aicpa_guides/199

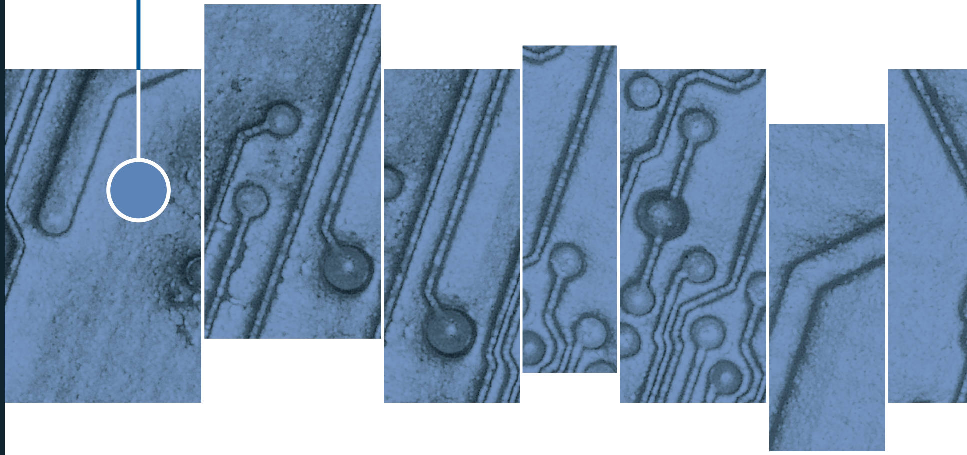
This Article is brought to you for free and open access by the American Institute of Certified Public Accountants (AICPA) Historical Collection at eGrove. It has been accepted for inclusion in Guides, Handbooks and Manuals by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

ISO Certified

091015

American Institute of Certified Public Accountants

Information
Technology Section

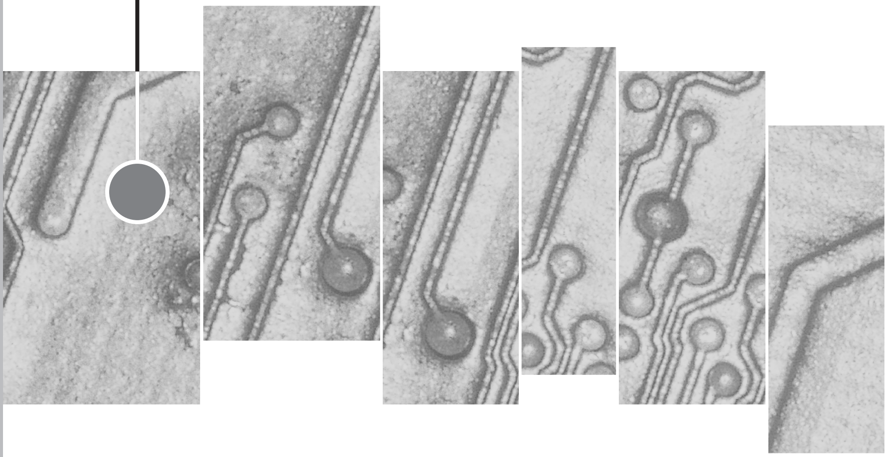


A CPA's Guide to Understanding and Controlling Spam

Roman H. Kepczyk, CPA, CITP

AICPA

Information Technology Section



A CPA's Guide to Understanding and Controlling Spam

Roman H. Kepczyk, CPA, CITP

American Institute of Certified Public Accountants

AICPA

Notice to Readers

A CPA's Guide to Understanding and Controlling Spam does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the author and the publisher are not rendering accounting or other professional services in the publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2004 by
American Institute of Certified Public Accountants, Inc.
New York, NY 10036-8775

All rights reserved. For information about the procedure for requesting permission to make copies of any part of this work, please call the AICPA Copyright Permissions Hotline at (201) 938-3245. A Permissions Request Form for e-mailing requests is available at www.aicpa.org by clicking on the copyright notice on any page. Otherwise, requests should be written and mailed to the Permissions Department, AICPA, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881.

1 2 3 4 5 6 7 8 9 0 MI 0 9 8 7 6 5 4

ISBN 0-87051-602-7

About the Author

Roman H. Kepczyk, CPA, is the President of InfoTech Partners North America, Inc., and the lead technology management strategist for the firm. His primary focus is helping firms throughout North America effectively use information technology by implementing best practices and directing them towards today's paperless or digital CPA firm.

He has spent the past eight years consulting exclusively with CPA firms and prior to that, ten years with the CPA firm of Henry & Horne (Arizona's largest regional firm), where he was the partner in charge of the firm's management advisory services and microcomputer consulting practices. Roman also served as the firm's administrative partner, overseeing internal accounting, marketing, human resources, and was responsible for the creation and implementation of the firm's technology plan and budget.

He is currently the chairman of the American Institute of Certified Public Accountants' (AICPA's) Information Technology Executive Committee and a member of the AICPA's Special Committee on Enhanced Business Reporting. He has also served as Chairman of the AICPA's Top Technology Task Force, as well as having been involved with the AICPA eBusiness, Best Practices, IT Research, IT Practices, and Group of 100 projects.

Roman was included in the *Accounting Today* Most Influential People list for the years 2000, 2001, 2002, and 2003, and was named a Technology Pathfinder by the AICPA's Vision Project.

Roman is also an advisory board member to the Association for Accounting Administration (AAA) and has served on the board of directors of the Arizona Society of CPAs. He has been a featured national and regional speaker to thousands of CPA firms on information technology. Recent speaking engagements include topics of Today's Digital CPA Firm, Strategic Technology Management, Security and Privacy, Technology Tools, and the impact of remote computing/virtual office.

On a technical level, Roman is an AICPA Certified Information Technology Professional. He has authored technology chapters for the PPC MAP Handbook, *PPC Guide to Paperless Engagements*, and sections of the AICPA *Management of an Accounting Practice Handbook* (Internet, Knowledge Management), and coauthored the *AICPA's Top 10 Technologies 2003 and Their Impact on the Accounting Profession* guide. He also authored the *AAA Guide to CPA Firm Intranets* and their *2003 Guide to Paperless CPA Firm Administration*.

Roman lives in Phoenix, Arizona, with Sylvie, Stephan, and Antoine. When he is not on the road consulting or grinding out projects in the local Barnes and Noble Café, he enjoys running, hiking, biking, and road trips with his family.

Special thanks go to David Cieslak, CPA, CITP from ITGUSA, and Nancy Cohen, CPA from the AICPA, for reviewing this guide and providing direction on completing it.

Table of Contents

Introduction

E-mail has become a mission-critical tool used by virtually every business and individual to communicate today. Nevertheless, some of the very features that make e-mail such a successful communication medium are now slowly draining its effectiveness. Unsolicited e-mail and dangerous attachments are clogging up inboxes and threatening the security of the computers receiving them. We are talking about the capacity of spam and virus-infested attachments to waste individual and organizational time, and erode productivity. This guide is designed to help you better understand the issue and share solutions that will help you regain control of your inbox. It is divided into the following sections:

- "Beauty of the Inbox" outlines the fundamental value of e-mail and other integrated tools in making users more productive. This section also describes tips and tricks to optimize the way individuals and organizations use e-mail.
- "E-mail Issues and Statistics" describes spam and other issues affecting productivity including current benchmarks on spam proliferation. This section describes why spam is so difficult to address, and why organizations must take a number of different approaches to combat it successfully.
- "Legislative Solutions" explains that spam is not just a North American issue; it is a worldwide problem that is being exacerbated by countries that choose "to look the other way." This section discusses the origin and definition of the term and the various legislative responses to the problem. Organizations must understand exactly what does and does not constitute spam in order to avoid being labeled spammers.
- "Lists, Lists, and More Lists" shows that one of the most effective tools for currently managing spam is to check all inbound e-mail against lists of identified spammers, as well as the addresses identified as trusted business associates. This section discusses the different types of blacklists and

white lists, and the ramifications of using them to reduce the volume of junk flowing toward the organization.

- "Understanding Filtering Options" explains that there are a number of options to filter out bad e-mail at the Internet service provider (ISP), server, and individual workstation level. This section describes a number of filtering options, as well as some practical guidance on using them.
- "People, Policies, and Procedures" describes what organizations can do to educate their people regarding the various issues and threats of spam, and how to minimize the associated risks of Internet and e-mail usage.
- "Planning Your Organization's Antispam Response" summarizes considerations for responding to spam, whether you are an individual, small business, or have to deal with unsolicited mail at an enterprise level.
- "Antispam Resources" and the "Glossary" herein are included because spam is such an ever-evolving issue that this guide could not have been developed without the information provided through a significant number of Web sites, periodicals, and resources. We identify these along with a listing of computer industry definitions and vendors of e-mail security solutions.

Disclaimer

This guide has been developed to educate CPAs about opportunities to optimize e-mail as a communication tool and minimize the impact of spam on their organizations and their own personal use. The products, solutions, and resources presented in this guide are those the author and other contributors have knowledge of and experience with as of April 2004, and are not to be taken as recommendations for products or endorsements made by the American Institute of Certified Public Accountants (AICPA) or InfoTech Partners North America, Inc. In all matters regarding this guide, it is recommended that CPAs consult with experienced technical and administrative personnel to provide current recommendations, guidance, and implementation assistance.

A CPA's Guide to Understanding and Controlling Spam does not represent an official position of the AICPA, and it is distributed with the understanding that the author and the publisher are not rendering accounting or other professional services in the publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Beauty of the Inbox

CPAs, at their very core, are information communicators. They receive data in the form of trial balances, spreadsheet schedules, and vendor statements, and convert these data into a useful form that can assist clients and shareholders in making optimal business decisions and meeting regulatory requirements. The faster CPAs can respond to requests and deliver information, the more effective and valuable they will be as "the most trusted business adviser." In this regard, e-mail has evolved into one of the predominant communication tools for business people, and organizations must make a concerted effort to optimize its use.

The beauty of e-mail is that it is an extremely cost-effective communications tool that addresses the needs of a very broad audience. Most simply, Web-based products, such as MSN® Hotmail and Yahoo®, or "thin" e-mail applications, such as Microsoft Outlook Express®, are extremely easy to utilize and are cost-effective, even for casual users. The most robust e-mail programs can be fully integrated with the predominant personal information management systems on the market today. Organizations using Microsoft Outlook, Lotus Notes®, Novell GroupWise®, or one of the other popular desktop e-mail applications already have a comprehensive product that integrates e-mail, contact management, task management, and a calendar in a single application.

Any user that would like to assign a task to another person or ask whether that person is available for a meeting can do so at their convenience via instantaneous electronic means, and also create a documented record of doing so. Contrast this to the time-consuming chore of calling or meeting with the individual, which often takes repeated attempts, and then having to enter the results of the contact manually into a calendar or task list. Groupware applications allow users to communicate at their convenience and to utilize the information that has been sent within the e-mail, eliminating the need to rekey everything.

Another benefit of e-mail integrated into groupware is that it allows organizations to identify best practices in utilization and develop effective education programs. Because groupware applications utilize a standardized menu structure, the commands learned within e-mail usually apply to the task and calendar functions, which reduce training time and make all users more effective.

All organizations should identify best practices and develop a training program to ensure that all employees understand and utilize these items effectively. Although the following list is not all-inclusive, note that standardizing the features discussed here goes a long way to optimizing the use of e-mail.

Also note that Microsoft Outlook is the dominant e-mail product utilized in business, and so the commands to implement each feature within Outlook are included in this discussion. For users of other e-mail applications, searching on the commands within the help screens should provide adequate instructions for implementing the suggested solutions within that e-mail product. Commands are listed as they would appear on the tool bars and separated by >. For instance, File>Open would require the user to select the File command from the tool bar first, which would open the menu allowing them to select the Open command below that.

The following are some of the predominant e-mail features that make e-mail usage more effective, and are features everyone should utilize:

1. *Organizing folders*. Most business professionals receive e-mails addressing a wide range of projects or tasks that can be difficult to manage when all mixed together in a single inbox. Today, most e-mail programs allow for the creation of custom folders that can be used to hold related e-mails together so they can be managed more efficiently. Within Microsoft Outlook, the File>New>Folder will allow the user to create a folder. Four types of folders to consider are the following:

   a. *Specific task or client*. Having an action folder set up for a specific task or client helps users be more organized. A folder marked *Prospects* allows the user to follow up with active marketing targets, while *To Be Printed* or

Internet Lookup means that the salesperson needs either a printer or Internet access to complete the task.

b. *Newsletters or distribution list*. Individuals receiving electronic newsletters will find that having them all in a single folder makes it easier to access and search for specific information. These folders can also be very effective for managing list serv e-mail groups in which every participant receives every response from every contributor.

c. *Committees or boards of directors*. For individuals serving in a fiduciary capacity, a committee folder allows all related e-mails to be sorted so they can be easily reviewed prior to meetings, which also creates a history of communications addressing the subject matter.

d. *Personal interest*. Folders can also be set up for topics of interest that may come from a variety of resources. Examples could include a folder for *Mobile Technology Tools* or *Security and Privacy*, which the author uses for collecting interesting e-mails.

2. *Setting rules for folders*. Although it is very easy to click and drag e-mails to a specific folder for storage, there are tools that can automatically move them to the appropriate folder. Often called *filters* or *rules*, these tools look at criteria such as keywords, the sender's e-mail address or subject, and automatically route them to the folder. This can be particularly effective for active Usenet groups that can easily receive a hundred e-mails a day on any one topic. As new e-mails are moved to the folder, they are identified as unread by being displayed in a bold font. If that folder is not expanded, the title is displayed as bold so the recipient knows there is a new e-mail. Within Microsoft Outlook, the Tools>Rules and Alerts>New Rule tab will allow the user to set up a new rule to route e-mail.

3. *Searching folders*. Unlike paper folders that have to be manually searched (which means that specific items are easily overlooked), e-mail folders can be comprehensively searched for a key word or resorted by any of the e-mail

criteria. For instance, if a tax professional kept a folder for federal tax bulletins, he or she can locate every e-mail that contains the word *AMT*. Within Outlook, this is done with the Tools>Find command, which allows the user to select which folders are to be searched; the results are displayed in a new view. Outlook also allows this information to be sorted again by clicking on the various headings such as date received, who the e-mail is from, or the subject line.

4. *Saving e-mails and attachments*. As e-mail becomes more prevalent for delivering information and requesting action, users will want to save e-mails for long-term archiving. For example, if a stock broker received an e-mail from a client requesting an investment be sold; he or she would want to save that e-mail in that client's file as a record of the request. Within Outlook, once the e-mail is open, the user accomplishes this with the File>Save As command and by designating the appropriate client folder. This command can also be used to save attachments via e-mail. With most auditors using digital working papers, more and more information is being delivered to them via e-mail. A spreadsheet schedule or a scanned image of a lease can be saved by "right clicking" on the attachment and using the Save As command to save it to the appropriate folder. The user can also open the document and save it to the appropriate application.

5. *Pacing e-mail receipts*. E-mail can be a distraction if a user is continuously bombarded with e-mail, particularly if their work requires concentration for an extended period. To minimize e-mail interruptions, the delivery of e-mails can be set to a predetermined delay such as 45 minutes. Within Microsoft Outlook, the Tools>Send/Receive>Send/Receive Settings>Define Send/Receive Groups allows you to determine the delay. In the event that a recipient is expecting a specific e-mail, the delivery schedule can be reset or manually overridden. In the case of Microsoft Outlook, the Tools>Send/Receive>Send/Receive All tab allows the user to immediately receive any e-mails in the queue each time it is selected.

6. *Setting up distribution lists*. When sending e-mails, most programs have a feature for setting up distribution lists for specific groups of recipients. When the group name is selected, every person on that distribution list will receive the e-mail. Examples of distribution lists include management groups such as owners, project teams such as the technology committee, work groups such as tax directors, and newsletter recipients, i.e., all contacts that receive the organization's electronic communications. A distribution list is created within Microsoft Outlook by using the File>New>Distribution List command, and selecting the members of this group. The list will then appear within Contacts, allowing the sender to select that one item rather than each individual recipient. Administrators should also be taught how to maintain the list so that it remains current. Also, if the organization would like to send an e-mail to a large number of users, without the other recipients being aware of the others receiving the e-mail (for a newsletter for instance), the organization can send the distribution list through the blind carbon copy (BCC) field.

7. *Adding attachments*. Because e-mail can deliver information to anyone with Internet access and an e-mail account, to almost anywhere in the world in a matter of seconds, it is an effective tool for delivering word processing documents and spreadsheets. E-mail can also effectively replace faxes or courier services if the organization has the capability to convert a physical document into a digital format, which can amount to significant cost savings, as well as more timely delivery. To attach a file to an e-mail within Microsoft Outlook, the sender would use the Insert>File command after they have written the e-mail. Attachments can include a number of other file formats including pictures, diagrams, objects, or hyperlinks to Internet Web pages. Please note that, when educating users on adding attachments, it is critical to take into account security considerations. Many documents have the ability to add a password or some level of encryption to minimize the risk of the document being accessed by unauthorized persons.

Another thing to keep in mind is that many recipients have restrictions in place that limit the size of the file attachments they are able to receive; a common limitation is 2Mb. If sending attachments in excess of a few megabytes, users may want to call ahead and confirm whether the recipient's system allows large file attachments, or make alternative arrangements for sending the attachments. Either way, the recipient should be asked to confirm receipt.

8. *Setting priorities*. When sending an e-mail, there are times when urgency must be announced to the recipient. E-mail systems have the capability of adding an importance level to highlight this urgency. Within Microsoft Outlook, selecting the exclamation point on the top of the menu will insert a high importance or low importance that helps the recipient prioritize his or her e-mail. But users should remember what happened to the boy who cried "wolf!" and not abuse the "Urgent" flag; otherwise, truly important e-mail may be ignored.

9. *Customizing e-mail with stationery and signature lines*. Organizations that want to enhance the look of their e-mail communications can do so with stationery. In addition to the templates provided by Microsoft Outlook, which can be added via the Tools>Options>Mail Format>Stationery Picker tab, companies can create their own stationery template. In addition, each user should also create a default signature line that automatically appears when writing an e-mail (found below the stationery picker tab described above). Users can create additional signatures if required, such as one containing additional contact information, including fax numbers or mailing addresses. In order to maintain a professional appearance, all companies using stationery and signature lines should standardize these items for all users.

10. *Developing a spellchecker*. Organizations should have the spellchecker turned on by default to verify that e-mails do not go out with misspellings, which is simply unprofessional. Users should also be trained to add technical or industry terms to the dictionary so they can also be used.

Spellchecking features can be customized within Outlook with the Tools>Options>Spelling tab and can incorporate features such as ignoring words that are uppercased or numbered and suggesting replacements.

11. *Deleting old messages*. As previously discussed, users may want to consider saving critical e-mail messages using the Save As function to make certain key correspondence is retained. Provided that key e-mail is separately saved, messages in the *Sent Items* and *Deleted folders* can usually be safely purged from a user's desktop e-mail program within 90 to 180 days. If this old e-mail is not deleted, these folders can become very large and prolong the amount of time it takes to search for recent messages and/or do folder maintenance and rebuilds, should those be required.

In summary, this section describes a number of features that make e-mail an incredibly easy communications tool, which CPAs must utilize to be effective. Unfortunately, the benefits of low cost, ease of use, and the extremely fast speed of delivery can be abused, which is the case with unsolicited e-mail, more commonly referred to as spam. In 2003, the volume of spam e-mail for the first time bypassed the number of legitimate e-mails sent worldwide, causing major problems for individual recipients and organizations alike. The next section explores the depth of the spam problem and the likelihood that the situation will get much worse before it gets better.

E-mail Issues and Statistics

E-mail has become one of the most prolific communications tools used by businesses and individuals because it is incredibly effective at delivering a message to the intended recipient regardless of external factors.

E-mail Design Leads to Simplicity for Users and Spammers

From the outset, during the Cold War, one of the priorities behind the development of the Internet was to establish an information system that did not rely solely on any one server and would allow information to move independently and reroute itself continually until it ultimately reached its destination. This led to the SMTP (Simple Mail Transport Protocol) that would encapsulate the necessary delivery address in the "envelope" or header of each e-mail package, so that any server handling it could forward it to the next server that was in the right direction (and could store it until it was successfully forwarded). At that time, the need to authenticate the sender was downplayed, despite concerns that a malfunctioning server could send out millions of messages by accident, which could cause other servers to be overloaded, in effect creating technical spam and a denial of service (DoS) attack. As the SMTP specifications rolled out, text was required only in the header, so that it could easily be read by servers running different protocols or operating systems. Also, as the Internet protocols were being developed, domains were set up and designed to allow for the local administration of the servers. This local administration included the capability of setting up and maintaining end-user e-mail accounts.

The ease with which an e-mail can be created and sent and the reality that a text-based header is not authenticated are vulnerabilities that play strongly in the favor of spammers. Spammers can easily create new e-mail addresses or fake the e-mail headers, concealing the true identity of the sender. Inserting fake headers, which is known as *spoofing*, give the appearance of legitimacy to e-mail that appears to come from someone the recipient actually knows or from an address that could reasonably exist, such as that of a well-known organization. Often, spammers (particularly those who are trying to distribute spyware or viruses) will spoof individual and corporate e-mail addresses or domains from previous spam targets.

Identifying the Cost of Spam

As described in "Beauty of the Inbox," e-mail is an amazing communications tool that can send information worldwide to an almost unlimited number of users for an incredibly low cost. These attractive features also make it an ideal medium for marketing products or services. But, whereas traditional marketing methods require the marketer pay for the creation and distribution of the advertisement, e-mail passes almost all of these costs on to the recipients and the file servers through which the e-mail passes. Once the marketer has a fileserver with an Internet access setup and an individual's e-mail address is entered into their marketing application, the cost to send that individual repeated e-mail is negligible, particularly if the marketer's distribution list contains thousands, if not millions of addresses. For organizations to effectively evaluate the impact of spam, they must not only identify the specific costs of the applications, but also understand the hidden costs.

The obvious cost of solving the spam problem is the purchase cost of solutions. Some organizations choose to outsource all of the filtering to a third-party provider, or individuals will utilize an Internet service provider (ISP) that provides spam filtering as part of their service. Other organizations, wanting more control over what gets filtered, purchase applications or hardware appliances that they maintain within their own organization. All of these solutions will have ongoing maintenance costs that need to be factored in. Please note that, in the long term, spam applications will most likely be merged with antivirus, outbound filtering, and groupware applications to create a new product suite of secured messaging applications that handle much more than spam. These application costs seem substantial until they are compared with the hidden or soft costs—then, they clearly seem insignificant. Hidden costs that organizations must evaluate include expanded infrastructure, lost productivity, the impact of viruses introduced by spam, and the far-reaching impact of identity theft and financial fraud.

Infrastructure Costs of Spam

The infrastructure required to send an e-mail successfully from one location to another is extensive and covers not only the servers and computers within the office, but also a vast network of cabling and routers dispersed all over the world. Every individual and organization that utilizes e-mail must use computer processor resources on a server or workstation to confirm that an e-mail was received. If spammers send hundreds or thousands of e-mails, the burden is on the recipient server to accept them or bounce them back to the sending server. For those e-mail addresses that were spoofed (and therefore not recognized by the server listed as the sender), both the sending and recipient servers must utilize processing power to resolve the communication. Once the e-mail has been accepted by a server, it is then stored in the hard drives until it is permanently deleted from the system. If this deletion has not occurred prior to the organization making its daily tape backup, the e-mail will then be backed up onto an archival tape and take up storage space there, until that tape is reformatted or overwritten. Again, the cost of the transmission, processing, and storage is all passed onto recipients.

In addition, to utilize e-mail, the organization must have a connection to the Internet, usually with a router directing traffic, and a broadband Internet connection that provides adequate bandwidth to deliver all valid and legitimate e-mail. As the volume of spam has increased to the point that the majority of all e-mail is spam, organizations have to pay for substantially more bandwidth than they need to handle their real e-mail requirements. An often-quoted statistic from America Online (AOL) is that, at any given time, more than 70 percent of all e-mails in their system consist of spam. Building an infrastructure that can provide subscribers with acceptable access speeds and still handle the additional spam overhead requires AOL to spend significantly more to manage this overhead.

The time spent by individuals addressing spam e-mail at the end-user level also must be considered. The more junk e-mails that are delivered to end users, the more the cost in lost productivity to the organization. According to one study done by Ferris Research, the average amount of time spent by individuals addressing the impact of spam on their e-mail was 9 minutes per day in those organizations that lacked a spam solution.[1] A quick calculation shows that the average person in such an organization would

[1] Cade Metz, “Can E-Mail Survive?” *PC Magazine*, February 17, 2004, www.pcmag.com/article2/0,1759,1473982,00.asp.

lose approximately one week of productivity per individual each year. Another study done by IDC in December of 2003 came up with similar findings that e-mail users in an organization that did not have an antispam solution spent on average 10 minutes per day addressing e-mail-related issues as opposed to 5 minutes per day in organizations that had an antispam solution.[2] According to that study, a large organization with 5,000 e-mail accounts would lose $4.1million in productivity if they did not have an antispam solution compared to $783,000 for those that did have an antispam solution. The study went on to say that the average cost of information technology (IT) staffing in organizations without an antispam solution would be $72,800 higher per year.

Based on the preceding disruptions and costs, it is easy to understand why management has become interested in reducing the impact of spam. It is suggested that organizations attempt to capture their costs for all of the above items and then compare these costs to the various solutions to determine an appropriate return on investment. There are also free tools available at industry Web sites that assist organizations in making quick calculations. These resources are listed herein under the heading of "Antispam Resources."

Spam and Viruses

Computer viruses are one of the most expensive and destructive forces in the business environment today with the cost of lost productivity measured in billions of dollars. Virus writers rely heavily on spamming techniques to fake e-mail headers, spoof sender addresses, and utilize open relays to spread their applications to other users. Once inside the system, they unleash their payload of damage, often capturing the e-mail addresses of other users and taking over those accounts to further spread the virus. According to a study on the MessageLabs Web site, the ratio of virus-infected e-mails increased by 85 percent in the past year and nearly two-thirds of all e-mail determined to be spam went

[2] Mark Levitt, Robert P. Mahowald, Brian E. Burke, and Christian A. Christiansen, *What You Can and Should Do About the Rising Cost of Spam*, IDC Whitepaper, sponsored by the SurfControl Web site, March 2004.

through systems taken over as open relays.[3] Because of the similarities in the processes required to analyze e-mails, many antispam applications were developed closely with or are integrated with antivirus applications.

Just as the antispam and antivirus applications improve, spammers and virus writers are getting smarter and utilize spamming techniques to capture complete directories of e-mail addresses from servers. One common trick is known as a dictionary or directory harvest attack (DHA) that adds the most commonly used men's and women's names to any known domain address, until they eventually hit a valid e-mail address that can be captured (and the computer infected), or sold to other spammers. Dictionary spammers send e-mails to, for instance, JohnSmith, JSmith, John, and JS at any domain; those not rejected are listed as valid addresses. This has a huge impact on the servers of an organization under attack because the server must respond to the invalid e-mail addresses. As spammers often use other unsuspecting servers that are acting as an open relay, that server is also burdened because it must address all of the bounced-back messages that eventually go back to the target of the original attack. If enough of these e-mails hit the server at one time, they can overwhelm that server, causing it to shut down and creating what is referred to as a DoS attack. The SQL Slammer, SoBig, and Mimail viruses, which were so devastating in recent years, used various spamming techniques to multiply themselves.[4]

Phishing With Spam

A relatively recent threat to e-mail is known as *phishing*, which describes how criminals and spammers capture confidential information from unsuspecting e-mail recipients. Phishing cons are based on sending an e-mail from a supposedly valid company and asking the recipient to verify account information on a Web site. This information can then be used by the con artist to steal from

[3] www.MessageLabs.com.

[4] www.Postini.com, *Special Report: Enterprise-Class Spam Solutions Buyer's Guide*, which also includes "Enterprise-Class Spam Solutions Work Sheets" and "Appendix."

those accounts or to propagate identity theft scams against the individual that gave away the information. Often, the e-mail will state that there has been a security breach or that the user's account will be shut down immediately unless the recipient responds. The e-mails, which can look remarkably authentic and can include valid links to the real Web site, also contain a link to a fake Web site where the user is asked to verify account information. This information can include items such as account numbers, personal identification numbers (PINs), addresses, Social Security numbers and mother's maiden name. Unless the users look up the specific uniform resource locator (URL) of the Web site, they think they are at the actual Web site "updating information." Customers of major financial institutions such as CitiBank, Fleet Boston, Paypal, and the FDIC have been victimized by this scheme, even though users are constantly warned that services offered via the Internet will never ask the user to disclose password or account information via e-mail.

E-mail users must be taught to never respond to such e-mails by clicking through the e-mail, as there is no way to confirm whether the e-mail is real or that the information they provide can be protected. If an end-user is concerned about receiving such an e-mail, they should only change information by logging directly onto the Web site through a browser with a secured connection (padlock in the bottom right corner). It is also advisable to limit the amount of information users provide a new Web site until they have established the legitimacy of that site. One variation of the phishing con sends an e-mail selling goods and services at a price that is "too good to be true." Extremely low-cost offers purporting to sell original equipment manufacturers (OEMs) or bulk software is common. As the user logs onto the site, they provide a significant amount of information to complete the purchase, which is then used by the con artists for fraudulent activity including financial and identity theft.

In addition to the impact of phishing schemes on the end user, the targeted organization, featured product provider, and all legitimate online retailers can be victimized. A user that has been scammed on the Internet is likely to question all Web transactions or stop doing business altogether in this way. End users that are targets of an invalid software sale can harbor a grudge against that application developer and a financial institution's reputation can be damaged because prospective customers determine that the organization is not trustworthy.

The Legal Impacts of Inappropriate Spam

Organizations must also evaluate the legal ramifications of inappropriate spam making its way into the workplace and creating a situation that could be construed by employees as a hostile work environment. As the spam issue has become widespread and solutions have become available, organizations are expected have a filtering system in place to ensure that offensive material cannot be received and distributed within the organization. Those companies that do not have a spam solution in place may face lawsuits from individuals who have been exposed (directly or indirectly) to such offensive content in e-mails. When the possibility of a lawsuit is mentioned or threatened, and the organization responds properly to such allegations, the time spent by management, human resources, and legal staff can become significant.

Spam Statistics

For organizations to effectively evaluate the spam threat, it is useful to consider industry statistics that help make the financial case to management for elevating and addressing the issue. First of all, most companies would agree that giving up e-mail is not a solution. Some studies suggest that smaller organizations might give up e-mail if spam becomes an unmanageable problem. Generally, however, e-mail is considered an essential communications tool. According to a study commissioned by Evergreen Assurance, 90 percent of businesses use e-mail in some fashion to conduct business transactions. The study also states that 70 percent of those surveyed believe that e-mail is directly tied to their organizations' means of generating revenue.[5]

[5] Cade Metz, "Can E-Mail Survive?" *PC Magazine*, February 17, 2004, www.pcmag.com/article2/0,1759,1473982,00.asp.

Only in the past few years has spam evolved from a minor problem that users just had to live with to a serious problem that is costing organizations of all sizes substantial amounts of money. Ferris Research estimated that the loss of productivity within the United States in 2003 was $10 billion.[6]

According to the FrontBridge Web site, the volume of spam has increased by 1,600 percent since they started tracking and managing e-mail in 2000.[7] Given that the Mail-Abuse Prevention System (MAPS) Web site states that the volume of spam is anticipated to increase at an annual rate of 600 percent to 700 percent, organizations will have to find a solution.[8]

According to the Brightmail Logistics and Operations Center (BLOC), which tracks all e-mails through its servers, the volume of spam compared to legitimate e-mail reached 50 percent in July 2003, which appears to have been the tipping point at which most organizations started taking the spam issue seriously.[9]

In December of 2003, IDC released a study that found 7.3 billion junk e-mails were being sent each day on a worldwide basis. Of these, 3.7 billion were sent to North America.[10] To put this in perspective, IDC estimated that in 2003, a 1,000-person organization would receive 2.1 million spam messages, the equivalent of each individual receiving and dealing with an average of 2,100 spam e-mails each year.[11] Another study done by Jupiter/Media Metrix estimated that number would increase to 3,900 per year by 2007.[12]

By April 2004, the percentage of spam e-mail had increased to 64 percent within the Brightmail system, which filtered over 96

[6] www.brightmail.com/pressreleases/091603_accuracy.html.

[7] www.frontbridge.com/services/spamfilter.php.

[8] www.ciphertrust.com/researchcenter/index.php.

[9] www.Brightmail.com, Brightmail Web site as of April 2004.

[10] www.globeinvestor.com/servlet/WireFeedRedirect?cf=GlobeInvestor/config&vg=BigAdVariableGenerator&date=20031201&archive=prnews&slug=2003_12_01_09_2243_1050247.

[11] www.ciphertrust.com/researchcenter/index.php.

[12] www.spamfighter.org/bb/index.php?5.

billion e-mails that month.[13] Within the CipherTrust system (Ironmail), the percentage of identified spam was over 79 percent at the same time.[14] Interestingly, according to the Brightmail Web site, 3.1 billion of the 96 billion e-mails filtered in April 2004 were fraudulent and could have led to financial or identity theft. Also on the Brightmail Web site, were statistics from the Federal Trade Commission (FTC) and the Gartner group stating that the cost of identity theft in the United States in the previous five years was $60 billion and that between June 2002 and June 2003 the number of victims increased by 79 percent. Clearly, the spam issue is having repercussions from the organizational level down to the personal level.

Another estimate from the Radicati Group, which is a messaging-analyst firm, estimated that on a global level, reduced productivity and increased IT resources in 2003 amounted to over $20.5 billion. Their study estimated that this cost would increase almost tenfold, to close to $200 billion in the next four years.[15] Another study released by the Radicati Group in May of 2004 stated that the cost of not having a spam-filtering solution (for organizations with approximately 10,000 employees) was just under $3,000 per employee in lost e-mail productivity. The study was conducted on 15 companies with over 155,000 users and found that after the implementation of antispam systems, these organizations were able to reduce the cost to just over $520 per user (averaged over three years).[16]

The increase in spam as an issue has led to an increase in the number of solutions providers that are addressing it. According to a reference to Gartner, Inc., in the Enterprise-Class Spam Solutions Guide from the Postini Web site, there were more than 40 enterprise-level spam applications on the market at the end of 2003.[17] The Guide goes on to say that Gartner estimated that

[13] www.Brightmail.com, Brightmail Web site as of April 2004.

[14] www.ciphertrust.com/researchcenter/index.php.

[15] Kevin Fogarty, "Block Spam! Save Millions! Feel Better!" *Baseline Magazine*, April 5, 2004.

[16] Thomas Claburn, "The Cost of Spam," *Information Week*, May 17, 2004.

half of them would be gone by the middle of 2004, so selecting an organization with long-term potential is critical. IDC, another well-known computer industry analyst, estimated the number of enterprise spam solutions to be closer to ten by the end of 2004.

The IDC study stated that in 2003, almost 70 percent of the surveyed organizations had an antispam solution already in place and that this number could be expected to increase to 90 percent by the end of 2004.[18] Gartner Inc., in a study dealing with the same topic, predicts that by the end of 2004, 85 percent of organizations will have some level of enterprise-caliber spam filtering.[19]

This information is also supported within the CPA industry. A study of 100 organizations done by the Association for Accounting Administration (AAA) in April of 2004 found that 85 percent of respondents had at least one antispam solution in place. The survey, which focused primarily on CPA firms, found that 34 percent utilized an external spam-filtering service, 44 percent had an internal filtering application, and 32 percent had a solution implemented at the workstation level. 5 percent of respondents had implemented a solution at all three levels (external, internal, and individual, while 25 percent of the respondents had implemented solutions at two levels.[20]

As spam has become a serious issue, a number of the Web sites listed above maintain live statistics that are updated on a monthly basis. For current information, it is suggested that readers of this Guide go to the Web sites, which are summarized in the section entitled “Antispam Resources.”

[17] www.Postini.com, *Special Report: Enterprise-Class Spam Solutions Buyer’s Guide*, which also includes “Enterprise-Class Spam Solutions Work Sheets” and “Appendix.”

[18] Mark Levitt, Robert P. Mahowald, Brian E. Burke, and Christian A. Christiansen, *What You Can and Should Do About the Rising Cost of Spam*, IDC Whitepaper, sponsored by the SurfControl Web site, March 2004.

[19] www.internetweek.com/breakingNews/showArticle.jhtml?articleID=15800271.

[20] www.cpaadmin.org, Association for Accounting Administration.

Legislative Solutions

Addressing spam requires a number of approaches including legislative action. This section describes solutions at the local, national, and international levels, as well as technical and financial proposals. It also provides a working definition of spam.

Defining Spam

Defining spam has been troublesome both for governments and for business. The only agreement is that most people have their own definition of what constitutes spam, and they know it when they see it. Because there is a wide range of definitions of spam, for the purpose of this guide, e-mail communications will be broken into the three categories of legitimate, bulk, and spam. *Legitimate communications* are those between parties that have either a relationship that is previously established or can be reasonably inferred based on past and related interactions. *Bulk communications* are those of online advertisers that follow the guidelines of the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act of 2003, which began as Senate bill S877), discussed later in this section, which includes opt-in newsletters or advertisements that the recipient has requested. All other unsolicited e-mails are considered spam, regardless of whether it originates from a legitimate or illicit organization.

The term *spam* first appeared in a list serv or chat discussion group, and the name stuck. Apparently, the then-new phenomenon of overwhelming e-mail reminded someone of a Monty Python skit set in a restaurant that primarily serves SPAM™ products. In the skit, whenever anyone ordered an item containing SPAM, a large group of boisterous Vikings (a common feature in Monty Python humor) broke into a deafening chant, espousing the virtues of SPAM, to the point of drowning out all other sounds. This, in effect, is what spam e-mail does—its sheer volume overpowers all other e-mail. (It is important to note that SPAM, in all capital letters, is a trademarked name of the Hormel Corporation referring to their brand of canned meat products, and all references to e-mail spam may not be spelled in this manner.)

United States Spam Legislation

Over the past decade, as unsolicited e-mail became more and more of a problem, various states addressed the issue. By the end of 2003, it was estimated that at least 36 states had enacted legislation. States such as Virginia and California enacted fairly strong laws that have stringent requirements including a convention to opt in to e-mail lists, criminal penalties for noncompliance, and financial fines for serious abusers. A summary of all legislation in place can be found at the SpamLaws Web site (www.spamlaws.com). The requirements of each state's individual legislation differed dramatically, making enforcement difficult in certain instances. To counter this, Congress worked to develop nationwide legislation throughout 2003, which was voted into law on October 23, 2003.

Thus, on January 1, 2004, the CAN-SPAM Act of 2003, went into effect to tackle spam. It outlined the basic rules for both individuals and organizations, and stipulated that noncompliance could mean penalties of up to five years in prison and fines of up to $2 million.

The basic rules of the CAN-SPAM Act can be summarized as follows:

- Spammers can no longer disguise e-mail header information, which was the primary method they used to hide their true identity and to route through servers that were not previously identified with spam.
- Spammers can no longer use misleading *From* or *Subject* lines that often trick people into opening e-mails for products or services not related to the subject or that contain offensive material.
- In the future, organizations must tag their e-mail to identify the type of e-mail (i.e., all advertisements have to include a subject of *ADV* in the subject line, while adult content must also be tagged as such).
- The harvesting of e-mail addresses is prohibited for any Web site and any of its Internet-based services provided a

notice that prohibits such activity appears on the site. Nevertheless, individuals posting their e-mail addresses to sites that do not have a digital rights policy can still be exposed to spammers collecting their addresses.

- Anyone sending an unsolicited commercial e-mail must maintain a physical mailing address that is valid and operational to ensure that the sender can be located.
- Commercial e-mail messages must also include a working return e-mail address, also intended to stop the use of fraudulent addresses and to allow the recipient to contact the sender.
- The CAN-SPAM Act also called for all unsolicited commercial e-mails to include a working method for a recipient to opt out of the e-mail list, in an obvious place at the top of the body of the e-mail content. The CAN-SPAM Act requires the sender of the e-mail to honor this request and discontinue any more spam to that address within ten days of the recipient completing the opt-out process.

Unfortunately, many organizations believe the CAN-SPAM Act does not go far enough, as it does not specifically prohibit any spammer from sending spam; instead spammers can send e-mails to recipients and then require them to opt out from that user's list. Most people are very suspicious of these lists as the very act of opting out confirms the address as being valid to the spammer, which could then be easily shared with other spammers or related entities. In addition, many spammers change e-mail accounts on a continual basis and rotate messages through a number of different servers, requiring recipients to opt out of a nonstop stream of e-mails.

Another problem that many people foresee is that the use of identifying tags, such as *ADV* in the subject line, could unwittingly label a legitimate business as a spammer. Antispam tools can be set up to capture such addresses automatically, and an organization that wants to legally comply with the law could end up having their organization listed on one of the blocking lists. These lists (discussed further in the section herein entitled "Lists, Lists, and More Lists") could lead to all e-mails from that sending organization being tagged as spam and automatically filtered out by a recipient's e-mail service. In effect, one e-mail listed as spam could block all communications from the sender, as well as to all other companies utilizing the same blocking list. The end result of a legitimate company being tagged as a spammer would have a significant impact on that organization's ability to communicate with any of its clients or prospects.

One of the stronger criticisms of the act is that it overrode the legislation enacted by the more than 30 states that had already addressed the spam issue locally, although some states will still be able to maintain the consumer protection and privacy capabilities of their local legislation. Some of these states have enacted much tougher laws and more stringent methods of enforcement. For instance, in California, where opt-out legislation was deemed ineffective, state legislators had just passed, in the fall of 2003, an opt-in anti-spam measure that banned all commercial unsolicited e-mail for which the recipient had not specifically signed up.

Some industry pundits went so far as to say that the CAN-SPAM Act gives spam the "congressional seal of approval" and "legalizes" it, its only real impact being to encourage spammers to set up shop outside of the United States, where the CAN-SPAM Act cannot be enforced. Some studies indicate that half of all spam is already coming from overseas, particularly from countries where antispam laws are insignificant, including Argentina, Brazil, China, Russia, and South Korea. In one report, AOL alluded to the fact that they registered a 10-percent increase in unsolicited commercial e-mail coming from overseas locations in the months following passage of the CAN-SPAM Act.

One additional provision of the CAN-SPAM Act was that it calls for the development of a national "Do-not-e-mail" list similar to the "Do-not-call" list imposed on telemarketers. The FTC is to make recommendations to Congress as to how such a list could be developed and implemented. Unfortunately, the development of such a list might only give offshore spammers easier access to a large list of valid e-mail addresses. In the early part of 2004, some groups fraudulently set up Web sites that claimed to be national "Do-not-e-mail" registries, a ploy that exposed signees to even more spam. In addition, other organizations such as CAUCE (Coalition Against Unsolicited Commercial E-mail) voiced their concerns with the act in that it relied on "overworked regulatory and law enforcement agencies, rather than giving consumers legal tools with which to protect their own inboxes."[21]

The first attempts to enforce the law occurred in March of 2004 as some of the major ISPs (AOL, Earthlink, Microsoft, and Yahoo) joined forces to sue the major spamming organizations under the provisions of the CAN-SPAM Act.

Antispam Legislation Around The World

Spam is as much a problem in Europe as it is within the United States; the European Commission (EC) estimated that unsolicited commercial e-mail cost European Union (EU) countries 2.25B euros in lost productivity in 2003.[22] In many ways, the 15 EU nations are ahead of the United States with regard to digital rights and privacy legislation. Italy was the first to enact antispam legislation in 1999 that called for criminal penalties and fines, while Austria, Denmark, and Sweden are well on their way with their legislation. On October 31, 2003, the EU passed a digital privacy law. In addition to making spam illegal, it outlawed spyware, severely limited the ability of organizations to download cookies without absolute consent, and disallowed the use of any locating software for mobile devices, except by the government and emergency services. One of the strongest provisions of the act was to require individuals to opt in to receive unsolicited e-mails from anyone that they did not previously have a relationship with, which many believe is the most effective way to legislatively ban spam. But the EU solution is not without its critics, particularly regarding enforcement since each country determines its own penalties.

Australia also enacted antispam legislation in 2003 that incorporated the opt-in provision favored by the EU and the banning of sending e-mails without having a previous business relationship.

[21] www.cauce.org, *Coalition Against Unsolicited Commercial E-mail.*

[22] CBC News Online, "Spam Around the World," November 24, 2003, and updated March 12, 2004.

Their Spam Bill 2003 legislation called for significant financial penalties to first-time offenders of up to A$44,000 for individuals and A$220,000 for organizations. Spammers that continued to send unsolicited e-mails could then be fined as much as A$1.1M per *day* that they violated the law. This legislation applied to spammers based in Australia or those that used servers that were physically located in Australia, which accounts for only 4 percent of the country's spam at the time of enactment. Nevertheless, Australian authorities plan to develop multilateral agreements with other countries based on their legislation that would eventually push spammers out of the collective countries within the agreements.

The Australian law is lenient toward violators who are not aware that their servers were being used or who can show that a mistake was made. The Australian legislation is criticized for including loopholes for charitable and religious organizations, as well as for allowing wording that permits companies to include factual information without a specific offer. An interesting note on the Australian legislation is that it defines a *commercial electronic* message as an "offer to supply, advertise or promote goods and services, land, or a business or investment opportunity; or by deception, assist a person to dishonestly obtain property or financial advantage from another person," whether or not the items actually exist, which would provide broad coverage (such as the Nigerian illegal funds transfer scams).

The Japanese enacted their antispam legislation in the spring of 2002, which also utilizes opt-out rules. Their legislation requires that all spammers include wording disclosing that the e-mail is unsolicited advertising. Penalties for violation in Japan could land spammers up to two years in jail and fines of up to $2.56 million.

In addition to legislative solutions, some organizations are promoting plans that would transfer the cost of sending unsolicited e-mail to the sender or make spamming significantly less profitable. One group sponsored by IronPort Systems created a program that has legitimate e-mail senders put up bonds with Bonded Sender (www.bondedsender.org) stating that they will adhere to strict e-mail guidelines in exchange for not being blacklisted. In the event that any of the organization's mail is deemed to be spam, the e-mail recipient, ISP, and real-time block list (RBL) could make a claim against the bond.

Another solution to pass the cost back to the spammers is called Penny Black. The term originates back to the early days of the British Postal system when all physical mail deliveries were paid for by the recipient, which caused a significant disparity in the amounts charged. To counter this, the British Postal system developed their stamp, called *Penny Black* that would transfer the cost to the sender, rather than to recipients. Penny Black works by responding to any inbound e-mail with a query to the sending server that would require that they calculate an algorithm (such as a cash total of all the ASCII characters in the e-mail). Once the sending server did the calculation and returned a correct response, the e-mail would be forwarded to the recipient. Although a short delay (8 to 10 seconds per e-mail) would not bother most individuals or businesses, it would add significant cost to spammers sending large volumes of e-mail, requiring them to pay significantly more for hardware.

Another proposed solution is to set up an infrastructure that would charge a nominal fee of a few cents for each e-mail sent. This works for physical mail, which imposes the cost on the sender by charging advertisers a bulk rate for their mailings. If every e-mail had a nominal cost of 1 to 2 cents, most businesspeople and individuals would still use e-mail, but spammers would have to reconsider. These charges would be used to set up the system to track the e-mails and collect for them. This has worked in the past; individuals that were part of the Prodigy e-mail system in the 1990s were charged $.25 for each e-mail sent.

Another common-sense solution is to just not buy anything from organizations that use spamming techniques. AOL has taken this step on behalf of its members and has blocked the ability of users to go to spammers' Web sites through their system. Spammers that are blocked will eventually filter out all of their AOL addresses because there is no possibility of return on those accounts. If the other major providers such as MSN, Yahoo, and Earthlink follow suit, the volume of spam to those individuals who are the major users of such services will dramatically decrease.

Legislation alone will not be effective against spam, and, most likely, will continue to push spammers offshore to other countries that have less stringent rules. Consequently, most industry pundits believe that, in the short term, organizations will have to utilize blocking lists (see the next section, "Lists, Lists, and More Lists") and filtering applications (see the section entitled "Understanding Filtering Options") to have any significant impact. In the long run, most of these industry analysts agree that a system that requires the senders to authenticate who they are will be the best solution, which is also discussed at the end of this section.

Lists, Lists, and More Lists

This section describes a variety of lists that organizations can use to minimize spam volume. Blacklists such as RBLs list known spammers, whereas white lists identify senders that the organization trusts to receive e-mail from, regardless of content. According to the Spamhaus Web site, 90 percent of United States and European spam e-mails are generated from a core group of 200 enterprise-level spammers and blocking e-mails from those sites can go a long way in reducing the volume of spam that an organization actually receives.[23]

Real-Time Block Lists

One of the more effective tools an organization can deploy to reduce the volume of spam is the use of RBLs, which block e-mail delivery of known spammers to the organization.

The RBL acronym usually stands for real-time block lists, but the terms *blacklist* or *boycott list* are also commonly used. The role of RBLs is to identify spammers at their root servers or those servers they use to relay spam, and to maintain a list, which is made available to the public either for free or a minimal fee. These lists

[23] Spamhaus statistic from Web site at www.spamhaus.org/rokso/index.lasso.

can then be imported into the organization's e-mail filters to block messages before they enter the organization. The RBL providers have found that by supplying the list to organizations, rather than specifically going after the spammers, they avoid litigation, so the model works fairly well for both the organization and the RBL provider.

Organizations can also utilize an RBL *honeypot* or *spamtrap* to identify spammers that use automated tools to capture addresses from the Internet. A honeypot is one or more e-mail addresses that are listed on the company's Web site or list servs that are not actually used by a valid employee. By definition, all e-mails sent to this address are automatically identified as unsolicited and added to the RBL and then blocked for all e-mail recipients within the organization.

To use RBLs, organizations import the list into their e-mail application, which compares every inbound e-mail against the list and then either automatically deletes the e-mail or moves it into a designated folder, where it is quarantined. Many organizations prefer to utilize quarantined junk mail folders that allow the organization the benefit of reviewing the e-mails prior to deleting them and also allows searching through the e-mails in the event that a valid e-mail has been tagged as spam.

RBLs can also be used by individual users locally by loading them into their own groupware application to identify spam. Individual RBLs work the same as organizational products, except the e-mails are usually delivered locally first and then automatically filtered to either a designated junk/spam folder or the deleted e-mails folder. Local delivery means that the individual still has to download all e-mails, which can be significant, particularly for dial-up users. Loading all e-mails locally leads to another spam "soft cost" in that these deleted e-mails still take up significant space on the user's hard drive and on any backup tapes they maintain.

To minimize this impact, filtered e-mails sitting in a junk/spam or deleted folder must be systematically deleted. This cleanup can be done either manually by the individual flipping through the list of e-mails, highlighting them and deleting, or by using the automated tools available in the groupware applications. For example, a user can do a search on all "unread e-mails" in their deleted folder, which would allow them to go through just those items, rather than valid items that they deleted in the normal course of business and may want to keep for archival purposes.

To counter the impact of the RBLs, spammers must continually find new servers and open relays through which to pass their messages, which are then identified and listed by the RBL, which in turn leads to more blocked sites. Thus, a cyclical process of continual updates evolves. Organizations that use RBLs must have a process to ensure that the lists they use are updated on a regular basis and that they know how to respond should they be targeted by one of the lists.

If an organization is listed as a spammer, the first step to clear their name is to contact the RBL and find out specifically why they were listed. For example, an overzealous marketing department or an individual workstation that has been commandeered as an open relay can cause an organization to be listed. After the organization clears up the misunderstanding and corrects any violating behavior, the organization should formally ask the RBL to remove it from the list. List providers must address a large number of such requests, so it can take days or weeks to update the information, during which time the company must be patient. If the organization's domain is targeted on multiple RBLs, it will have to work with each list provider; there is little coordination between them. In the interim period, the company may have to set up temporary e-mail accounts to make sure that users have some e-mail access.

As RBLs have become popular as a method of reducing the volume of spam, they have come under attack by some spammers. In 2003, a number of RBLs were victims of repeated DoS attacks in which the host servers were flooded with so many e-mails that they eventually shut down. Both Osirussoft.com and Monkeys.com were victims of this ploy.

White Lists

Another useful tool to fight spam is the use of white lists which work exactly the opposite of RBLs. *White lists* (also known as s*afe senders* in Outlook 2003) identify valid e-mail addresses from individual senders or domains that the organization normally corresponds with and allows through any e-mails from those organizations. The downside to relying solely on the white-list approach is that *all other* e-mails are blocked or placed in the junk mail folder. If using a white list, it is imperative that users be trained to update the list with every new contact or organization with whom they wish to communicate. This would include items such as e-mail newsletters and electronic subscriptions such as tax bulletins and RSS Feeds that may come from a different domain than the primary subscription. White lists can be extremely effective for individual users that only want to correspond with a select group of individuals, such as family members, or with specific organizations that they place on the white list. Should an e-mail user listed on the white list have to change their e-mail address for any reason, it is important that they notify the organization maintaining the white list, so it can be updated. Organizations can build white lists by including all e-mail addresses from those found within their employee's groupware or contacts list. They should also train users on adding e-mail addresses to the white list.

Another method of minimizing spam and populating white lists is the use of a *challenge/response system*. These systems direct all incoming e-mail to a Web server that stores the e-mail and automatically replies to the sender with a challenge that must be completed prior to the Web site releasing the e-mail to the recipient. Examples of a challenge would be to ask the sender to verify their e-mail address or to complete a simple task that a machine could not easily do. For instance, users of the iPermitMail E-mail Firewall (www.ipermitmail.com), must go to a hyperlink and retype their e-mail address and a message before being placed on the white list. A good example of a pictograph can be found on the GeekTools Web site (www.geektools.com), where users must identify a series of letters and numbers scrambled in a picture to allow access to their “who is” application. Spammers do not want to take the time or energy to respond to such a challenge, so the spam is eventually deleted.

An important consideration of using a third-party challenge/response system is the realization that the organization’s inbound e-mail will be available and possibly held up by an outside party. It is important for the organization to review that provider’s privacy policies and understand to what extent they have actual access to e-mails. This can particularly be a problem for companies that handle extremely confidential e-mails. In addition, it is important to confirm that providers’ redundant systems ensure that e-mails are still protected in the event that provider’s power is cut off or Internet access becomes unavailable for any reason.

A broad listing of RBLs can be found along with strengths and weaknesses at the Declude Web site (www.declude.com) or at Jorgen Mash’s DNS Database (www.moensted.dk/spam/). Nevertheless, the following lists some of the better known RBL providers, white list, and challenge/response systems uncovered during the research undertaken for the development of this guide:

- No cost or free providers include the following:
  - —DSBL or Distributed Sender Boycott List (www.dsbl.org)
  - —Not Just Another Bogus List (www.njabl.org)
  - —ORDB or Open Relay Data Base (www.ordb.org)
  - —SBL or Spamhaus Block List (www.spamhaus.org/sbl)
- Purchase or service-fee providers include the following:
  - —MAPS or Mail-Abuse Prevention System (www.mail-abuse.com)
  - —IPermitMail (www.ipermitmail.com) Challenge response system
  - —Choice-mail (www.choice-mail.com) Challenge response system
  - —Spam Lion (www.spamlion.com) Challenge response system
  - —SpamArrest (www.spamarrest.com) Challenge response system

Understanding Filtering Options

Another popular method of combating spam is to use software that evaluates incoming e-mail and filters out those that meet certain "offending" criteria that identify them as junk mail. These filters range from enterprise-wide applications that are managed by a third party or run alongside the organization's e-mail server, to rules filters running within an individual user's e-mail account. This section will describe the various filtering technologies available to organizations and individuals, as well as some new anti-spam proposals that could drastically reduce the volume of junk mail in the future.

Rules-Based, Collaborative, and Bayesian Filtering

One of the best analogies to understand how filtering software works is to compare the process to how a person's physical mail is sorted. When most people open their physical mailbox or sit down in front of their own mail stack at the office, they are confronting a pile of differently sized documents consisting of personal letters, bills from various vendors or clients, trade journals, and junk mail advertisements, which are interspersed with all the other important items. Most people quickly filter out the personal items and bills in one stack, trade journals in a "reading" stack," and throw out the advertisements in the circular file. There are always a few unusual pieces of mail that require a second glance or have to be opened to be evaluated, but the average person does this in a matter of moments and with a high probability of successfully "filtering" valid mail from junk. Most individuals have a predefined series of internal rules that allow them to do this chore, which is similar to what rules-based filtering does in identifying spam.

Rules-based filtering is probably the most common method of identifying valid e-mails and designating spam items as they are the easiest to use, and built into virtually all e-mail systems. Many people already use rules-based filtering to organize e-mail into various inbox folders automatically such as for list servs, committees, or newsletters as described in the section entitled "Beauty of the Inbox." These filters often consist of a series of rules that, when invoked, look through e-mail headers, subject lines, and content looking for specific key words that are representative of spam topics. According to the BLOC, as of March 2004,[24] more than two-thirds of identified spam e-mails concern the sale of products, financial opportunities, adult content, and Internet services. By setting up a rule to look for keywords (e.g., *Viagra, Mortgage, Adult*, and *XXX*,) or for common phrases to sell related services (e.g., *lower your interest rate* or *refinance now*), e-mails can be prompted to be routed directly into a junk/spam or deleted e-mail folder. These rules can also look for domains of sites known to send junk mail (those found in the blacklists) or for certain types of e-mail, such as those with embedded HTML (hypertext markup language) tags or images.

Unfortunately, rules-based filtering can lead to a high number of *false positives*, meaning that a valid e-mail is routed out of the recipient's inbox or deleted because it has characteristics that are targeted by one of the filtering rules. For instance, if a client forwards a product announcement that was written in HTML or has odd characters (such as those associated with foreign languages), and the organization has an all-encompassing filter to delete anything with those signal events, there is a definite risk that the e-mail will be filtered out. Should this occur, the intended recipient would most likely never know that an e-mail was sent and the sender may assume that the recipient was not being responsive, which could lead to a missed opportunity. Organizations that filter out all e-mails with HTML or linked images (such as photos), also risk blocking out all digital newsletters, so it is important that the individual or organization review the filtered e-mails occasionally to identify those organizations that should be placed on the "safe sender" list. It is particularly important to evaluate the filtered e-mails when the system is initially set up so they can be fine-tuned to filter properly.

[24] Brightmail Web site as of April 2004 (www.brightmail.com).

Rules-based filtering can be implemented at different levels within an organization, such as an individual's e-mail application or at the network level. At an individual level, rules-based filtering is usually part of the individual's e-mail client (Microsoft Outlook, Lotus Notes, Novell GroupWise). For instance, within Microsoft Outlook, under the Tools tab, there is a command for Rules and Alerts. This tab allows the user to create rules to check the subject line and content of all incoming e-mail for a variety of criteria, such as keywords or specific senders, and then determine whether to route the e-mail to a junk/mail or deleted folder. To understand how this is done within other groupware and e-mail applications, it is suggested that the reader search for rules or spam filtering within the help screen for that application.

Rules-based filtering can also be managed at an organizational level. The main advantage to companies is that the software is maintained centrally, which reduces the time required by individual users in updating and reviewing the filters. This also drastically reduces the amount of spam that flows to recipients, so the work of one person managing spam can have a significant impact on all the organization's e-mail users. Organizational spam filters are usually managed by a central information technology department, which allows them to have more technical capabilities that may not be available at an individual user level. In addition to key word filtering, many antispam applications utilize filtering techniques such as Internet provider (IP) address filtering, bulk counting, and timing techniques.

IP address filters work by comparing the IP address from an incoming e-mail to a real-time block list that the organization can either maintain itself or download from one of the RBL providers listed in the section entitled "Lists, Lists, and More Lists," herein. Any IP address on the list is automatically handled as spam. As this list changes regularly, organizations must have a process to ensure they are updated on a timely basis and the validity of the list is evaluated at least annually.

Antispam filters that utilize bulk counting basically evaluate the mass of incoming e-mails and delete large groups of e-mail that come in at the same time with the same content (and are not on an approved white list). This is done by running an algorithm that calculates a numerical hash total for each e-mail that could identify duplicate e-mails. This total is compared to other e-mails that have arrived previously and any e-mails with the same hash total are targeted as spam.

Timing techniques are somewhat similar to bulk counting, except that the system compares the time stamp for large volumes of e-mail that arrive into the organization's servers in rapid succession. Most e-mail requires a series of communications between the sending and receiving server that take a standardized amount of time. To increase their sending volume, spamming organizations bypass these communications by sending all the commands at once and without waiting for the standard communications response. By reviewing and comparing the timing receipts of an e-mail, the filtering application can very effectively determine whether an e-mail was sent in bulk to members within the organization.

Another form of filtering, which is a derivative of the real-time blacklists, is known as *collaborative filtering*, which relies on a community of users to identify spam e-mails that are reported to a central antispam organization. If enough people designate a specific sender's e-mail address as spam, it is added to the collaborative list and distributed to all users of that application, and all future e-mails are filtered out for all members of the collaborative. In this way, each member of the collaborative identifies any new spam e-mail for all the members, which drastically reduces the volume for everyone.

Bayesian filtering, an additional method, is gaining prominence among antispam vendors. Drawing on the work of eighteenth-century mathematician Thomas Bayes, this approach is predicated on the probability that an event occurring can often be predicted based on how similar previous events occurred and were resolved. An antispam product using Bayesian filtering analyzes the contents of an incoming e-mail and compares it to previous e-mails and how they were treated. If an e-mail has characteristics that were previously identified with spam e-mail, a probability that the e-mail is junk is calculated. The more items that are identified with spam, the more likely that it should be targeted as spam. For instance, if an e-mail that was previously tagged as spam contains the phrase *refinance now* or the similar wording, such as *ref!n@nce n0w*, it would most likely be identified as spam.

Another approach used by vendors is a filtering methodology based on heuristics. Usually, *heuristic filtering* is a proprietary method of spam identification that incorporates the different levels of the filtering previously described, along with that a given vendor's unique process to target spam with artificial intelligence or fuzzy logic. Most heuristic systems depend on a number of different criteria that they evaluate independently as part of an e-mail and by utilizing a scoring system. The more items that are flagged and add points to the overall score, the more likely that the item will be quarantined as spam. Vendors fiercely protect their heuristic methods simply so that the spammers cannot easily develop a countermeasure to bypass that vendor's antispam application.

External Filtering Services

Filtering rules must constantly be updated to keep up with the rapidly changing methods that spammers utilize to bypass them. This maintenance can be significant, so many individuals and organizations choose to let a third party be responsible for filtering. For large ISPs such as MSN, AOL and Yahoo, the volume of spam flowing through their systems is significant, so it is imperative that they filter out as much as possible to reduce the volume of and stress on their network infrastructure. Most of the major ISPs have incorporated spam filters into their e-mail that individual users can adjust to different levels. For instance, AOL allows users to set their Mail and Spam controls to only accept e-mail from *people I know*, which includes those e-mail addresses in the user's "buddy list" and address book. This setting effectively blocks *all* e-mails from everyone not on the recipient's specific trusted-user list. AOL also designates inbound e-mails with different icons that help the user identify whether the e-mail is from *someone you know*, a bulkmail sender (such as a newsletter, or an unidentified recipient that has an agreement with AOL) or an unknown sender (usually spam). Within AOL, users can also report spam as part of their collaborative filtering system, so that the users help AOL update their list of spammers. These features are not unique to AOL, so the easiest way to understand how to use the e-mail filtering service or change the tolerance level within an ISP managed service is to go to the help screens and do a search on spam filters.

For organizations that manage their own e-mail servers, there are a number of external filtering options. The benefit to organizations using a third-party filtering service is that the majority of spam e-mails are removed prior to being delivered to the internal e-mail server. These external service providers also usually include enterprise-level antivirus scanning, which can be more effective and timely than the organization's internal solution. Outsourcing spam filtering and antivirus processes eliminates a significant amount of internal maintenance, as well as drastically reducing the organizational resources needed to store and archive e-mail. These solutions have the added benefit of being able to be rolled out quickly and with a minimal impact on existing IT staff, who are already overworked in most organizations.

As stated previously, the downside to using an external filtering company is that the organization becomes very dependent on that provider. If that provider has any kind of server problem, loses its broadband connection, or is hit with a disaster such as bad weather or power outage, the company may not have access to e-mail during that time.

For internal antispam solutions (individual or organizational), some of the more popular antispam applications that incorporate filtering and blacklist technology are listed herein in the section entitled "Antispam Resources." For additional information on the process of selecting an antispam and e-mail security solution, see the section entitled "People, Policies, and Procedures."

The Future of Fighting Spam

Fighting spam is an ongoing game of cat and mouse between the spammers and the antispam solutions providers. As soon as one avenue of attack is shut down, spammers find another to exploit and the cycle goes round and round. Much of the overall problem lies within the fact that the Internet's SMTP (Simple Mail Transfer Protocol) was designed to be extremely easy to use, with minimal overhead, so that messages would have the best chance to make it to their destination, regardless of problems along the way. To make this efficient, very little information within an e-mail has to be verified before being forwarded to the next server on the delivery path to the final end user. Spammers take advantage of this by falsifying who they are and using other unsuspecting servers (called *open relays*) to forward their messages. To circumvent spammers, a number of organizations are developing and promoting solutions that require that e-mail senders authenticate who they are before their message can be forwarded. This process is known as *SMTP authentication*, and it is being approached by a number of vendors in different ways.

One of the most discussed approaches is called SPF (Sender Policy Framework), which over 8,000 organizations including AOL, Google, and Symantec[25] have adopted as of April 2004. SPF lists all the users of a domain in a format that other servers can verify prior to accepting an e-mail or forwarding it to another server. To be effective, the SPF solution would require that all open relays be eliminated, meaning that the sender of an e-mail has to log on to a specific server to send an e-mail. Spammers do not want to do this because it means that they can be easily identified, making blocking lists significantly more effective.

Another approach being touted by Yahoo is known as *Domain Keys*. This solution works with public key encryption rather than authenticating IP addresses. This means that whenever a message is sent, the server includes an encrypted private key in the e-mail. Prior to accepting an e-mail, the server receiving the message would have to access the sender's public key from their domain to authenticate that the e-mail is from a valid sender. Proponents of the Domain Key proposal say it is the only authentication scheme that does not break e-mail's "store-and-forward" capability. In addition supporting this proposal, Yahoo has incorporated Sendmail as one of the approaches available to their clients, which includes nearly three-fourths of the Fortune 1000.

[25] Larry J. Seltzer, "Stopping Spam," *PC Magazine*, April 20, 2004.

A third approach being touted by Microsoft is *Caller ID*, which also eliminates domain spoofing. The Caller ID proposal works on the e-mail address level with e-mail servers publishing the addresses of their outbound e-mail senders according to the Caller ID specifications. When a recipient server receives an e-mail, the header is examined to determine the domain from which the e-mail was sent. The recipient server then queries the sending server to verify that the specific e-mail is on that server's approved sender list. Although Caller ID looks similar to SPF, it analyzes the content of the message in order to see the headers, whereas SPF only looks at the SMTP envelope address. In addition to being put into Microsoft's Hotmail system, some of the major supporters of Caller ID include Amazon, Brightmail, and Sendmail. Caller ID is one component of Microsoft's overall response to fighting spam known as CSRI (Coordinated Spam Reduction Initiative), which also requires that an organization be set up to independently monitor the behavior of users in order to determine what is spam and what could be construed as acceptable direct marketing activities.

A number of other proposals have been discussed over the years including adding a security layer to the existing SMTP, such as SASL (Simple Authentication and Security Layer), specifically from vendors (such as BrightMail Inc.'s Reputation Service and IronPort's SMTPi). Two earlier proposals known as DMP (Designated Mailer Protocol) and RMX (Reverse Mail Exchange) were incorporated to create the SPF proposal touted above. All in all, it is not likely that any one of these solutions will become dominant in the near future, so it will require that the applications developers, ISPs, and organizational IT staff implement multiple solutions to ensure that e-mail can be authenticated regardless of the scheme used by the sender.

People, Policies, and Procedures

Effectively controlling spam not only incorporates the technical solutions outlined in previous sections, but also encompasses the people and procedural aspects within the organization. Companies must have effective computer and Internet usage policies in place that include efforts to minimize the impact of spam. In addition to the initial training provided on these policies, regular reminders must be posted and ongoing education provided regarding current e-mail issues and evolving computer threats.

One of the first steps an organization must do to address the spam issue through their policies is to distinguish the difference between what is considered spam and what is considered acceptable e-mail. Some organizations have policies against accessing of personal e-mail accounts through the company's Internet access, a practice that can easily introduce viruses or other malicious code. This policy is appropriate for internal employees with job responsibilities that rely only on other internal employees, but not for those who regularly interact with outside parties.

Organizations should also have a procedure on what to do when an individual receives an item identified as unsolicited e-mail. If individuals are given the authority to place an e-mail into the blocking list of their spam filter, they can inadvertently block appropriate e-mail destined for another recipient in the company. For instance, a blanket marketing announcement from an office supply company can be put on the blacklist for the organization and immediately begin blocking all e-mails from this company to the administrative department, which can lead to lost opportunities and communication. Such blocking is effective for individual users that maintain their own spam filtering, but in a larger organization that does its own filtering, it is better to centralize the maintenance of the internal blacklist.

If an organization decides to utilize an organizational spam filter, management should let users know the process by which it will be phased in. Most systems require monitoring and fine-tuning to be effective in meeting the needs of a diverse organization. If a phased-in approach is implemented, management should inform personnel that the software will initially be run in audit mode to identify normal e-mail flow within the organization. As the different levels of filtering are implemented (white list, blacklist, Bayesian filtering), management should inform personnel what is happening and how to respond if an expected e-mail is not received, as well as how to report spam. Organizations should make it easy for individuals to search through filtered e-mail to look for a specific item. For instance, larger enterprises can utilize an external e-mail filtering service that requires them to train personnel to search for such e-mails via a Web site or through the organization's IT department.

Organizations should also have a policy stating that although they are doing what they can about minimizing spam, there is no way that they can guarantee that this filter will block all unwanted or offensive content, especially if an individual goes through the blocked content looking for a missing e-mail. Procedures should be in place to outline how employees should respond if inappropriate or offensive content is received. Organizations must realize that there are a variety of situations in which e-mail can be viewed as creating a hostile work environment by either directly viewing an e-mail or indirectly viewing it by being present when it is opened. To minimize such hostile workplace environment issues, managers and owners must be shown how to respond appropriately.

Organizations should also consider polices for monitoring outbound e-mail because forwarding e-mails can provide e-mail addresses from the entire string of people that forwarded that content. Content management also allows the organization to monitor all e-mail to ensure that it follows company guidelines. For instance, it can scan the body of every e-mail to ensure that it does not violate any polices against profanity, inappropriate content, or sending confidential information.[26] Some applications can also monitor attachments that go out with e-mail to minimize the spread of viruses or the sending of huge files that can clog up the organization's (and recipients') servers. Content management filtering will have long-term appeal to CPAs as they can also be set up to archive e-mails that they deem to be critical, such as those to the Internal Revenue Service (IRS) or other government bodies.

[26] www.Postini.com, *Special Report: Enterprise-Class Spam Solutions Buyer's Guide*, which also includes "Enterprise-Class Spam Solutions Work Sheets" and "Appendix."

To develop an e-mail and Internet usage policy, a number of excellent templates are available from Web sites such as the SANS Institute (www.sans.org). Prior to implementing any policy, it is imperative that organizations review it with legal counsel to ensure that it meets the requirements of local jurisdictions. Some considerations to include within organizational policies are listed below along with various social engineering ploys that can lead to people being further targeted by spammers or other offensive parties:

- Define the purpose of the e-mail policy, including a statement that inappropriate e-mail tarnishes an organization's image either inadvertently or knowingly by the sender.
- Decide whether personal use is allowed and, if so, what usage is considered reasonable. Employees should be taught that access to personal e-mail accounts can introduce viruses or harvesting technology.
- Determine what settings should be in place on individual browsers, as many maintain personal information that can be captured when accessing a Web site. If an individual connects from a personal e-mail that is loaded through their browser, they could be providing the link with their e-mail address and become the target of more spam.
- Decide what types of business and nonbusiness e-mails or digital newsletters individuals are permitted to sign up for, given that these lists can be shared with other spammers.
- Provide guidance on the participation of employees in list servs and chat rooms as this can lead to the capture of their e-mail addresses. Individuals should consider the use of disposable e-mail addresses or "munging" their address to minimize the risk of harvesting:
  - — Disposable e-mail accounts (DEAs), often low-cost or free, are e-mail accounts that can be used for nonmission critical e-mail until they become the target of spam and then thrown out to use another. DEAs can be provided to nonprofit organizations from spamcon.org/services/dea/ and commercial vendors such as MailShell.com.

- — Munging entails a user inserting characters that make the address unusable for harvesting "bots" but effective for humans, such as john@DELETETHIScompany.com.

- Train users on the importance of carefully reading the boxes on a computer screen to ensure that the user does not inadvertently opt in to promotions or other lists (or respond to free offers or those that are "too good to be true.") It is better to deselect offers for more information and related offers, and contact the Web site directly. In general, the rule is, opt out unless it is a reputable organization with a privacy policy on the Web site.
- Train personnel not to open questionable-looking e-mails and not to click on links from within an inappropriate e-mail as this often confirms the validity of the e-mail address, making it a future target for spammers.
- Train users on creating e-mail addresses that foil DHAs.
- Teach personnel about e-mail threats such as phishing schemes and explain the most notorious Internet scams to them (such as the Nigerian money transfer scams).

From a management perspective, the organization should also decide whether they want to formally monitor the volume of spam. As CPAs, it is often useful to track the actual results of any technology investment to verify its validity. Some organizations track the volume of e-mail received, the percentage blocked as spam, the number of incorrectly blocked e-mails, and then estimate the time saved per individual. By monitoring these statistics, the organization can then translate the information into dollars saved for the organization, compared to cost to implement the solution. Many antispam products claim a return on the investment of less than a year, so it is to the organization's advantage to consider tracking this information.

Planning Your Organization's Antispam Response

Virtually all studies are finding that both the volume of spam and the effectiveness of antispam solutions is increasing, creating a cat-and-mouse game in which spammers need to send more e-mails and use new approaches to get results, while the antispam solutions are constantly putting in place stronger countermeasures to knock out more unsolicited e-mail. Within the Cloudmark system (provider of a collaborative antispam solution), spam accounted for 63 percent of e-mails in November 2003 and 71 percent by April of 2004. At the same time, the Cloudmark filters were effectively blocking 88 percent of spam in November 2003 and 97 percent by April 2004.[27] What this means to users is that everyone should have at least one solution in place to cope with the ever-increasing number of e-mails, and, as outlined by the statistics given herein in the section entitled "E-mail Issues and Statistics," the volume of e-mail is only expected to increase for the foreseeable future.

Selecting an Antispam Solution

To effectively address spam, organizations must develop a multitiered approach encompassing a variety of solutions; and including the use of filters, blacklists, white lists, and a slew of technologies that can be integrated at the workstation level, server level, or outsourced to a third party. Many of these tools are being combined and integrated into e-mail and security applications.

The ultimate selection of an antispam strategy is usually dependent on the profile of the user, the technical capabilities of the client, and the type of e-mail communications expected in the normal course of business. Many organizations will select a primary antispam strategy that will run either locally at the workstation or server, or externally at the ISP or through a dedicated third-party vendor. Although most organizations will initially select a product at one of these levels, it is anticipated that in the long run, a multitiered solution made up of a number of these approaches will be selected and eventually incorporated into a complete security solution that manages all inbound and outbound communications and Internet connectivity.

[27] Jon Swartz, "New Software, Laws Push Some Spammers to Log Out," *USA Today*, May 6, 2004.

Individuals

For individuals, a stand-alone or ISP-provided solution makes sense because these people usually are responsible for their own IT and maintenance. They are usually also used to being self-sufficient and making their own determinations as to policies or procedures (which is usually not the case as the organization grows beyond a few independent users). Those that are not technically proficient are probably best off going with an ISP that includes spam filtering within their system. Providers such as AOL, MSN Hotmail, and Yahoo have filters that are included as part of their regular monthly service fees. These filters can be turned on through mail controls and adjusted to various levels to meet the requirements of the individual user. Within MSN Hotmail, there are three settings including a standard default, an enhanced mode, and a white-list version (exclusive mode) that only allows e-mail from those on the list. Yahoo utilizes its own proprietary spam application (Spam Guard Plus) and also licenses Symantec antispam technology. Within AOL, the levels are expanded somewhat to include mail from all senders, only AOL members, individuals within your contact list, a customized list of names to block, and no senders whatsoever. Finally, AOL also manages its own advanced spam-filtering options.

The major ISPs also utilize collaborative methods to identify spam by having users report spam by clicking on a button at the bottom of the e-mail screen. If the ISP reviews the e-mail and determines it to be spam, it can then be blocked for all users using that service. For individual users, getting into the habit of reporting spam to the organization makes the spam filters more effective for everyone within the system.

For individuals with more technical capabilities who would like more control of their spam filtering, it is suggested that they review the filtering capabilities of their e-mail and incorporate an individual spam-filtering solution. Although filtering is improving within e-mail clients (particularly with the release of Outlook 2003), these solutions require additional maintenance. When a groupware e-mail filter and an add-on antispam application are combined, they usually provide users with more options and control than the generic e-mail service providers. This is particularly important for those that regularly receive e-mail inquiries from prospective clients and other unknown entities and do not want to leave the determination of what constitutes spam to a third party.

Beyond the built-in filtering capabilities of their e-mail client, there are stand-alone solutions that can be incorporated into the e-mail system. Below is a summary of a number of representative solutions that were available as of April 2004 and were garnering good reviews at that time. As previously noted, this list has changed dramatically from the top rated products in 2003 and is expected to change significantly in future years.

• Norton Anti-Spam 2004	www.symantec.com	($40)
• SpamBayes	spambayes.sourceforge.net/	(Free)
• SpamCatcher	www.alladinsystems.com	($30)
• SpamNet	www.cloudmark.com	($40)

Individual filters require that the end users be more involved with spam filtering and spend time doing maintenance. Although the cost of the application and maintenance time is expensive, it is still usually less expensive than a managed solution or external IT person and, therefore is suitable for a very small number of users such as those in home offices or individual practice. However, there is a point, particularly in professional organizations such as CPA firms, in which individuals have higher billing rates and cost factors, and a centrally managed or external solution would be more appropriate.

Again, the solution can be tied to the technical capabilities of the organization in implementing and maintaining solutions, as well as to the nature of e-mail within the company. Organizations that have technical resources that are good enough to manage a solution internally, as well as companies that want more control of all e-mail, will primarily choose an internal business solution. Larger enterprises, companies with less technical capabilities, or those that want to outsource antispam expertise will select externally managed solutions. Below, the considerations for these solutions are discussed.

Internal Business Solutions

Individual spam solutions are usually not as effective at the organizational or enterprise level as at a personal level, and are much more expensive than centralized solutions that can cover a multitude of users. The centralized management of e-mail also makes it easier for an organization to adhere to organization policies and apply them consistently to everyone, as opposed to depending on end users do this.

Internal business solutions can run on a dedicated server or within the organization's e-mail server. Today, there are many add-on products that integrate directly with Microsoft Exchange, Lotus Notes, and Novell GroupWise. This usually allows for easier maintenance as the commands and folders used are already familiar to network support personnel.

Some of the hardware solutions include dedicated hardware appliances. These devices are probably among the easiest to implement, but can be difficult to modify beyond the settings provided by the developer of the product, so they can lose effectiveness unless combined with an external support agreement to update on a continual basis (preferably automatically, such as antivirus software). In addition, there are gateway appliances that are set up to filter all inbound e-mail prior to entering the organization's e-mail system. Examples of internal business solutions would include:

• GFI Mail Essentials	www.gfi.com
• IronMail	www.ciphertrust.com
• Network Associates SpamKiller (McAfee)	www.nai.com
• SpamCop	www.spamcop.net
• SurfControl	www.surfcontrol.com
• Trend Micro Inter Scan Messaging Security Suite	www.trendmicro.com

One benefit of internally managed applications is that the organization has complete control of all e-mail, in that items tagged as spam are saved within the e-mail server and can be searched and retrieved from the organization's servers in the event that a legitimate e-mail is inappropriately tagged.

Internal applications also allow the organization to make their own determinations as to what is allowable and what is not, which makes it easier to enforce company policy. This is particularly helpful for organizations' confidential e-mails that must not be exposed to external parties. Finally, some organizations worry that depending on external third parties makes them susceptible in the event that third-party infrastructure becomes unusable for any reason.

External Solutions Providers

Organizations that do not want to incur the cost and the chores of managing their e-mail systems, or those that do not have the technical resources to do so, are often better served by outsourcing their antispam management and possibly all of their e-mail security needs. The best analogy is that using an external spam solution is like using the services of a water treatment plant.[28] Organizations would not think of building and maintaining their own water treatment system. Similarly, it is optimal for organizations to rely on a third party to filter out all the spam "impurities" prior to delivering legitimate e-mail. In addition to a central location being able to handle production in large volume at a lower cost, the company gets the benefit of a much higher level of professional expertise and experience, and is free from having to manage the handling and disposal of these "impure" e-mails. Unfortunately, in contrast, organizations with internal solutions have to receive, filter, manage, store, and delete spam items on their internal servers. One study states that as much as half of the increase in new e-mail servers will be caused by the need to handle increased spam and predicts that, in larger companies, many of these units will be dedicated spam servers.[29]

[28] www.Postini.com, *Special Report: Enterprise-Class Spam Solutions Buyer's Guide*, which also includes "Enterprise-Class Spam Solutions Work Sheets" and "Appendix."

[29] www.Postini.com, *Special Report: Enterprise-Class Spam Solutions Buyer's Guide*, which also includes "Enterprise-Class Spam Solutions Work Sheets" and "Appendix."

External solutions providers tend to do much more than just processing e-mail for spam. These services are often bundled with antivirus applications and can protect an organization from a number of Internet-based risks such as directory harvest or DoS attacks. Most of the external solutions providers, including those listed in the following, also incorporate multiple Internet access providers, as well as robust disaster recovery procedures that surpass the preparedness of most organizations, which usually translates to a much more stable e-mail system:

• Brightmail	www.brightmail.com
• FrontBridge True Protect	www.frontbridge.com
• MessageLabs E-mail Security	www.messagelabs.com
• Postini Perimeter Manager	www.postini.com

Evaluating Products

As mentioned above, the selection of a primary antispam solution is often dependent on the size of the organization, the mission critical nature of the organization's e-mail, the technical capabilities of internal personnel, and the comfort the organization has with using external services.

Between 2003 and 2004, a significant number of new players entered the market, as well as a number of players who left the market. Organizations should pay special attention to the market position of a provider as well as that provider's projected longevity. As discussed earlier in the section entitled "E-mail Issues and Statistics," two of the major industry analysts predict that consolidations and failures will dramatically reduce the number of major solutions providers from over 40 to less than half this number. The total cost of the solution is always a factor for CPAs, so it is imperative to calculate not only the purchase price, but the annual maintenance for both the service and the anticipated time that internal personnel will need to dedicate to managing the process. In the short term, it is expected that organizations will select the lower cost solutions that are managed internally. For the long term, it is anticipated that the most effective solutions will be those that block e-mails at the perimeter, prior to taking up internal resources and these products will be combined with antivirus, Internet security and both inbound and outbound content filtering.

Herein, the section entitled "Antispam Resources," describes various antispam products and resources. The "Glossary" gives the definitions utilized in the development of this guide.

Antispam Resources

Product	*Web Site*	*Notes*
Audiotrieve	www.audiotrieve.com	Antispam product that incorporates Bayesian filtering
Brightmail Antispam Solution	www.brightmail.com	Organization filter application
CAUCE-Center Against Unsolicited Commercial E-mail	www.cauce.org	Spam fighting organization
Choice-mail	www.digiportal.com	Antispam solution using challenge response
Distributed Checksum Clearinghouse	www.dcc-servers.net	Bulk counting hash total provider
FrontBridge True Protect	www.frontbridge.com	External filtering service
GFI Mail Essentials	www.gfi.com	Organizational level filter built into Microsoft Exchange
Imail Server	www.ipswitch.com	Blacklisting application
IronMail	www.ciphertrust.com	Hardware appliance solution and ROI Calculator
MailFrontier	www.mailfrontier.com	Antispam solution
MailShell	www.mailshell.com	Antispam solution
Mail Abuse Prevention System	www.mail-abuse.com	RBL provider
MessageLabs E-mail Security	www.messagelabs.com	External filtering service
Microsoft CSRI Inititiative	www.microsoft.com/mscorp/twc/privacy/spam.mspx	Microsoft Coordinated Spam Reduction Initiative
Network Associates SpamKiller	www.nai.com	Incorporate Bayesian filtering
Network Abuse Clearinghouse	www.abuse.net	Location to report Internet abusers
NetworkWorld Fusion Spam Calculator	www.nwfusion.com/spam/index.jsp	Spam cost calculator
Nokia Message Protector	www.nokia.com	Hardware appliance solution
Norton AntiSpam 2004	www.symantec.com	Individual spam protection
Open Relay Database	www.ordb.org	RBL provider
Postini Perimeter Manager	www.postini.com	External filtering service

(*continued*)

Product	*Web Site*	*Notes*
Praetor E-mail Content Security Spam Calculator	www.cmsconnect.com/ Marketing/spamcalc.htm	Spam cost calculator
Qurb	www.qurb.com	White-list software
SAPro	www.statalabs.com	Incorporates Bayesian filtering
Sophos/Activestate	www.sophos.com	Antispam solution
SpamArrest	www.spamarrest.com	Challenge Response solution
SpamCatcher	www.aladdinsys.com	Spam solution provider
SpamCop	www.spamcop.net	RBL provider
SpamFire	www.matterform.com	Spam solution for Macintosh
Spam Laws	www.spamlaws.com	Clearing house for local spam legislation
Spam Lion	www.spamlion.com	Challenge response system
SpamNet	www.cloudmark.com	Individual anti-spam solution
Spamotomy	www.spamotomy.com	Spam information and rating service
SpamSolutions	www.spamsolutions.net	Spam Information Web site
Sprint E-mail Protection Services (SEPS)	www.sprintbiz.com	Externally managed service
Symantec AntiVirus for SMTP	www.symantec.com	Organizational level filter built into Exchange
SurfControl	www.surfcontrol.com	Antispam solution
Trend Micro Inter Scan Messaging Security Suite	www.trendmicro.com	Organizational filter application
Trend Micro Spam Calculator	www.trendmicro.com/ en/products/gateway/ spam/evaluate/spam-calculator.htm	Spam cost calculator
Tumbleweed Communications	www.tumbleweed.com	Antispam appliance
Verity Messaging Control System	www.verity.com	Spam filtering solution

Glossary

Bayesian Filtering.[30] An analysis technique that has been applied to eliminating spam. It "learns" to differentiate real mail from advertising by examining the words and punctuation in large samples of both types of messages. It selects a set of words and numbers (called *tokens*) from the text and compares their ratio between good mail and spam. Using the tokens, the Bayesian approach looks at new mail and calculates the probability that the message is bogus.

Penny Black. An antispam proposal that would require e-mail programs to process a difficult computational puzzle before e-mail could be sent, which would add cost to the e-mail by using more CPU cycles.

Black List.[31] A blackhole list, sometimes simply referred to as a *blacklist*, is the publication of a group of ISP addresses known to be sources of spam, a type of e-mail more formally known as unsolicited commercial e-mail (UCE). The goal of a blackhole list is to provide a list of IP addresses that a network can use to filter out undesirable traffic. After filtering, traffic coming or going to an IP address on the list simply disappears, as if it were swallowed by an astronomical black hole.

Caller ID for E-mail. Microsoft's domain key proposal that looks at the IP address of the sending e-mail servers, and the sender's post in DNS. The receiving mail server checks the DNS for legitimate IP addresses that the mail should be coming from to determine if it is valid.

CSRI (Coordinated Spam Reduction Initiative). An initiative promoted by Microsoft that includes a roadmap for policy and technology infrastructure changes that can help stop the scourge of spam. One of the first technical recommendations outlined in CSRI is a Caller ID approach that takes aim at the rampant practice of sending e-mail with forged *From* addresses; commonly called *spoofing*.

[30] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[31] www.searchCRM.com.

Domain Keys. Yahoo's antispam initiative that authenticates the outbound domains of every e-mail message using unique embedded keys with e-mail message headers. The keys would be authenticated through comparison with public keys registered by the Internet's Domain Name System (DNS).

False Negative. Identifying spam as legitimate e-mail.

False Positive. Misidentifying legitimate e-mail messages as spam.

MAPS (Mail Abuse Prevention System).[32] A California-based nonprofit organization dedicated to eliminating spamming by maintaining the RBL (Realtime Blackhole List). The RBL contains the IP addresses of spammers, and companies and ISPs can use the list to reject incoming mail. If an offending spammer cannot be shut down, the spammer's ISP may contact MAPS with the subnet addresses allocated to the spammer so those specific addresses may be used instead of the IP address of the entire ISP.

Mung. Displaying e-mail address in a way that a machine cannot read it correctly. For example, JohnATcompany.com or **John-delete_this@company.com** would not be a usable address.

Opt in.[33] To purposefully accept some situation or condition ahead of time. For example, to opt in to an e mail campaign means that the user wants to receive periodic newsletters or information, which may include advertising from the publisher or third parties. An opt-in program implies that the user can cancel the service, or *opt out*. A lot of spam is sent out under the guise that, at one point, the user did opt in for the program, which may or may not be true.

RBL.[34] Realtime blackhole list; also referred to as block list and blacklist). A list of the IP addresses of known spammers.

[32] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[33] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[34] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

Spam.[35] E-mail that is not requested. Also known as unsolicited commercial e-mail (UCE), unsolicited bulk e-mail (UBE), gray mail and just plain *junk mail*, the term is both a noun (the e-mail message) and a verb (to send it). Spam is used to advertise products or to broadcast some political or social commentary.

Spam Filter.[36] Software that diverts incoming spam. Spam filters can be installed in the user's machine or in the mail server, in which case, the user never receives the spam in the first place. Spam filtering can be configured to trap messages based on a variety of criteria, including sender's e-mail address, specific words in the subject or message body or by the type of attachment that accompanies the message. Address lists of habitual spammers (blacklists) are maintained by various organizations, ISPs, and individuals as well as lists of acceptable addresses (white lists) that might be misconstrued as spam. Spam filters reject blacklisted messages and accept white listed ones.

Spam Relay.[37] Sending mail to a destination via a third-party mail server in order to hide the address of the source of the mail. For traveling users, it is common to use a local ISP to gain access to the Internet and send their mail to their home ISP, which forwards (relays) it to its destination. Nevertheless, ISPs can take precautions to prohibit spam relay. A mail server that is set up to relay mail is known as an *open relay* server or a server with an *open relay*.

Spam Trap.[38] A checkbox on a Web order form that defaults to *yes* or *I agree*, but positioned on the page so that you will most likely overlook it. Unless you change the default, you are unknowingly agreeing to accept more solicitations by e-mail from that company or from third parties.

[35] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[36] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[37] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

[38] Reproduced with permission from Computer Desktop Encyclopedia, © 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).

Spim.[39] Also spelled as spIM, spam over instant messaging (IM). Unsolicited advertising appearing in instant messages. Spim is even more annoying than spam. Unlike e-mail ads, which collect in the user's mailbox, an instant messaging ad pops up on screen whenever it is sent. Also referred to as instant spam or the less-intrusive sounding IM marketing.

SPF (Sender Policy Framework). An SMTP authentication scheme developed by Meng Weng Wong to require that the sending server verify that the e-mail came from it.

True Negative. Term used in spam filtering, when legitimate e-mail is correctly identified as legitimate e-mail (sometimes called *ham*).

True Positive. Spam properly identified as spam.

White List. A list of known parties to the recipient, often culled from existing groupware contact list.

[39] Reproduced with permission from Computer Desktop Encyclopedia, (c) 1981-2004 The Computer Language Co. Inc., (www.computerlanguage.com).