

Waging the War Against Spam



10100101011011010010101101010110110010101001
0100100110011001010100011100101010010
0100101110010010010101001001001
11101110010101001010101101010101
10100101011011010010101101010110110
01001001100110010101000111001010100100001010101

Waging the War Against Spam

The statistics are bleak, but far from surprising. According to a report released in the spring of 2007, American businesses spend a whopping \$712 per worker, per year, in the battle against spam.

"This isn't just a technology problem," says Rebecca Wettemann, vice president at Massachusetts-based Nucleus Research, the firm that authored the report. E-mail has become such an integral part of how businesses operate that spam "is now a business problem."

And the good guys aren't winning. "The best VC money that has been thrown at developing filtering technology has not met the mark yet," she says.

The Nucleus report, based on a survey of 849 users, found the following:

- Users are spending more than 1 percent of their time tackling spam in their inboxes.
- Even though 60 percent of companies deploy enterprise-wide spam filters, two out of three e-mail messages are spam.
- American companies are losing more than \$70 billion a year in lost worker productivity.
- Spam has risen sharply since Nucleus's survey in 2004.
- Nine out of 10 users are frustrated by spam, with one in 100 appearing to be "at the breaking point."

At the end of the survey, Nucleus asked users what punishment would be appropriate for spammers.

Eighteen percent said that spammers should see jail time, with more than 50 percent believing that junk mailers should be fined at least \$1 for every spam.

The survey also provided an "Other" option for how junk mailers should be punished. The responses were -- apparently in jest -- quite macabre. They included "the death penalty, slow hanging, public flogging, psychological assessment, and other suggestions that are inappropriate to print."

Concluded the report: "Spammers, watch your backs."

Three (Flawed) Solutions

On average, people spend 16 seconds per message deleting spam, according to the survey.

While this figure may sound high, Wettemann notes that it's an average; though many workers delete spam instantly, some -- shockingly -- actually read them fully before realizing they're from a Nigerian spam artist. (When Nucleus Research asked the same question in 2004, the average time was a 30 seconds. Fortunately, "People are getting more sophisticated," she said.)

Although the report's tally of the per employee cost of spam, \$712 per year, also seems high, it's down from a jaw-dropping \$1,934 a year in 2004. (The dollar amount is calculated by figuring productivity loss as a percentage of a 2,080-hour work year, at \$30 an hour).

Many firms are becoming ever more proactive in their battle against spam. However, this more aggressive filtering has a downside: "a growing number of legitimate messages are blocked as spam or deleted," the report found.

Waging the War Against Spam

The survey found three spam filtering methods that are common among enterprises:

- A confirmation process that delays the message until the sender confirms that it is a legitimate message.
- A quarantine strategy in which spam is placed in a directory to be reviewed by recipients.
- A delete strategy that automatically removes messages that the filter judges to be spam, without user review.

Each of these approaches has its pitfalls. The confirmation strategy slows down communication, at least initially (once correspondents become trusted, they aren't subject to this step).

In the quarantine strategy, Nucleus found that users spend an average of 4.5 minutes a week reviewing messages -- a minor expense that adds up over hundreds of workers. The costliest strategy, based on survey findings, is to delete apparent spam; staffers spend an average of 7.3 minutes per week searching for valid e-mails that have been lost.

In short, an ideal solution that bears no cost doesn't appear to be on the horizon.

In lieu of finding the perfect spam filter, business can demand greater accountability from related parties. Notes Wettemann: "Businesses need to go to their ISPs and the carriers of the spam, and have them take a closer look at 'What are they doing at the overall infrastructure level?' And maybe the FCC needs to be taking a closer look at how those public resources are being regulated and managed."

Spam Could Surpass Valid E-Mail

A report by technology research firm IDC says that spam could surpass legitimate e-mail in terms of volume in 2007 as unsolicited e-mail continues to explode and e-mail falls out of favor as a means of communication.

Text messaging and voice over IP (VoIP) calling, especially among younger consumers and workers, are becoming the communications means of choice. IDC estimates that the size of business e-mail volumes sent annually worldwide in 2007 will approach 5 exabytes, nearly doubling the amount over the past two years.

IDC predicts that nearly 97 billion e-mails will be sent daily worldwide in 2007, over 40 billion of which will be spam. Places like China, Eastern Europe, and Israel sport high percentages disproportionate to their populations, but there's also a large amount coming from North America, according to Mark Levitt, vice president for collaborative computing, enterprise workplace at IDC.

There has been a significant upswing in spam getting through since late last year, Levitt said, and the reason is two-fold: image-based spam, which is hard to impossible to detect by keyword filters, and increasing e-mail volume.

"Even if you get 95 percent of the spam with filters, if you double the output, that's double the amount getting through," he said.

It's certainly not getting any better. Panda Software reported that 87.5 percent of all e-mail scanned by TrustLayer Mail, its managed server for e-mail filtering, in March was spam.

The main problem with spam is that there are still too many naïve computer users who open it, click on links, or respond to the offers.

"The average user is unknowingly complicit in the issue and there is no clear delineation of authority over who can remediate it," said Adam O'Donnell, senior research scientist at Cloudmark, developer of spam filtering software.

Spam is a business, and the spammers keep doing it because people keep falling for scams like penny stocks or clicking on links to install key loggers. "If the market disappears for the products being pushed in spam, if spammers stop making money, then spammers will disappear," said O'Donnell.

Levitt said people get suckered into opening up spam fairly easily.

"Even by opening a spam you are confirming the e-mail address, you are potentially infecting your system, and unfortunately, too many people respond with info about themselves. They think if they just give their name that's safe, and it's not. It's not only monetary transfers that keep spammers going. It's the valid e-mail address they can sell or info that can be used for identity theft," he said.

In the 1990s, spammers like Sanford Wallace were easy to track down, but today, most of the spamming is done by botnets. Those botnets are on compromised computers, more often than not home users than corporate systems.

Spamhaus, which tracks spammers, lists Verizon as the worst offending network for spam, and AT&T as the third-worst.

"Spammers have taken the lessons of distributed computing and applied them to how to distribute their content," said O'Donnell. "They've built these large botnets of compromised systems to send out their spam. If the person is only sending out a couple messages a day they would never know."

Thus far, spam remains a nuisance for companies at large and has not brought down anyone's mail servers, according to Levitt. "I'm not aware of any company saying they won't use e-mail anymore because of spam. Most e-mails received by users are legit and most spams are blocked. So e-mail is still an efficient tool," he said.

Spammers Find New Ways Around Filters

The seemingly endless creativity and intense effort of spammers is as admirable as it is a waste of talent. As soon as spam filter vendors get the hang of blocking image-based spam, the spammers find a new method to completely invalidate it.

Image-based spam exploded in 2006 as a means of getting around the word filters used on client and server e-mail filtering software. Very quickly, image-based spam rose to account for 30 percent of all spam.

A managed security vendor noticed a significant drop in spam at the dawn of 2007, which it theorized could be due to many old, infected computers being replaced by shiny new systems given as Christmas presents.

SoftScan, based in the U.K., noticed a 30 percent reduction in traffic around the first week of January. The company speculated it could be either a major botnet going offline or possibly new Christmas computers replacing older ones that were unknowingly infected.

Gone are the days of Sanford Wallace, when spammers set up a formal organization and everyone knew where to aim. Now, it's all underground, with infected personal computers that pump out spam without the user knowing it.

Gartner estimates that 80 percent to 90 percent of all spam generated in North America comes from computers that are unknowingly infected.

"Today we have a situation where hundreds and thousand of machines are infected without their users' knowledge. It doesn't affect them directly, apart from perhaps the machine occasionally going slow, but that one machine in the right hands causes misery to thousands of others," wrote SoftScan CEO Diego d'Ambra in a posting discussing the issue.

Opinions are mixed as to what could cause such a drop in spam. Randy Abrams, director of technical education at antivirus vendor ESET, thinks it was a botnet disruption. However, Natalie Lambert, senior analyst for client security and client management at Forrester Research, believes the Christmas deployment theory is very plausible.

However, she adds "I also think that there's always a huge uptick of spam before any holiday. Given that it was Christmas, one of the biggest holidays of the

continued

Waging the War Against Spam

Rather than find weird ways to write "Viagra" or "mortgage" or stock symbols for pump and dump schemes, the text would be written in a JPG and the filters couldn't catch it.

So spam filter vendors went to work analyzing embedded images in e-mail files. Just as the products are making it to market, Secure Computing's labs have found that spammers are using image hosting sites and some HTML code to make the image appear in the e-mail.

Secure Computing's Chief Research Scientist, Dmitri Alperovich, said that because the image is hosted rather than embedded, image filters don't examine the file. And since HTML tags are used, the image appears within the e-mail just like an embedded image.

"As a result, they get a couple of benefits from this new technique," he said. "One is they no longer have to generate the image itself in their spam sending software, so they can increase the volume of spam they can send.

"Also, because of filtering technologies, spammers have had to introduce many randomizations and obfuscations into image spam, which reduces the readability. Now they don't need to do that, and they are even including logos of popular brokerage houses inside their image, directing people to these houses to place orders for the stock being promoted," he added.

There is good news in all of this. While it has been possible to embed actual malicious code into a JPG image, some hosting sites parse the image and will find hidden code and reject it. So at least this can't be used as a means to sneak malware onto a computer.

As of now, Secure Computing has only seen one hosting site, called ImageShack, being used in this manner. Unlike Yahoo's Flickr, you don't even need an account to upload pictures to ImageShack and then share links to it. But, Alperovich added, it would be a mistake to globally block all e-mails with links to ImageShack.

"These sites are used for legitimate images. People send out links to colleagues. So if you blindly block ImageShack, you may cause a lot of false positives that many individuals may not tolerate," he said.

For the end user, the solution is to set their e-mail client so it does not automatically display images embedded in e-mail. Microsoft has this feature defaulted on in Outlook and Outlook Express.

year, there's a lot of incentive getting that spam out there." The decline in early January could simply be the end of Christmas "promotions," for lack of a better word.

She thinks that just replacing infected machines isn't enough to take a 30 percent divot out of spam loads. It's likely a combination of new spam blockers, clean machines, and the end of the holidays.

Mike Irwin, COO for Webroot and formerly with Brightmail, doesn't believe new PCs played a part. "We've gotten to a point where PC churn is fairly normalized. There's seasonal PC buying, and I haven't seen that be attributable to any decrease in spam. We've been through five Christmas cycles where spam is still a problem, and we haven't seen a notable decline after the holiday," he said.

It's hard to determine the impact of new computers because the old systems they replaced might still be in use somewhere. "The question is how many were cleaned and how many are just repurposed or passed on with the malicious software intact?" said Abrams.

--Andy Patrizio, InternetNews.com

Image Spam a Server Threat

By spamming people with a small .jpeg or .gif file with the embedded text, spam blockers usually let the letter go through. The problem is these image-based spam letters are considerably larger in size than text-based spam, which wreaks havoc on the e-mail servers, and they take longer to process.

"This is the huge size increase in the size of spam. Even a small increase in image spam means a huge increase in the file size of spam being sent around," said Mikko Hypponen, chief research officer for antivirus vendor F-Secure.

Hypponen puts image-based spam at around 35 percent of all spam currently clogging the Internet. Fortunately, said Hypponen, e-mail accounts for very little of the total Internet traffic. So alarmist stories that image-based spam could bring the Internet to a crashing halt are unfounded.

"The Internet as a whole is not going to come to a standstill from e-mail, but e-mail of itself is a different thing," he said. The SMTP-based e-mail used today is the same design from the late 1960s when the Internet was born as a Defense Department project with a few dozen users.

It still has no real authentication, no security, and no guarantees of e-mail delivery in the protocol. "The only reason e-mail works as well as it does is the goodwill of the people, because they aren't trying to break things," he said.

Peter Firstbrook, security research director for Gartner, confirmed the explosive effect of image spam on e-mail servers. He said it went from 6 percent of all spam in Q3 of 2006 to 30 percent by Q4, a near sevenfold increase in one quarter.

"E-mail isn't the biggest bandwidth hog, but it is a CPU and MTA [Message Transfer Agent] hog," he said. He's talked to clients that had to turn off mail queuing to allow the backlog to be processed, and as soon as they opened up the mail servers, they got overwhelmed again.

The solution is not easy. Stopping to examine graphics files means a log jam at the mail server and MTA, which could mean lost or bounced e-mail. And while client-side spam blockers like Symantec's Brightmail and Cloudmark Desktop work well, the best place to block spam is at the edge of the network. Most developers of client-side spam blockers, including Symantec and Cloudmark, offer a server-side protection.

"It saves bandwidth between the server and user and doesn't pile up the user with image files. Most corporations don't even want [spam] in their e-mail servers. You've got to block at firewall, before the mail server," said Hypponen.

Firstbrook agrees. "You gotta drop this stuff at the boundary. You can't process everything. You gotta say, 'I can't trust this sender; I'm not accepting this message.'" That means if you get a dozen letters from a known spammer e-mail address or IP address, it's likely that future letters will also be spam.

To get around this, authentication and secure delivery are necessary, along with reputation-based systems at the firewall. But there's a simpler solution, too: check your own computer.

"Eighty to 90 percent of spam comes from bot-infected computers, and almost all North American spam comes from bots. There are more than 200,000 new bots every week. As a community, we're all less safe because of those people," said Firstbrook.

"Those people" are regular users, most likely home users, whose computers are infected and they don't know it, because they aren't using any form of security or malware detection.

Firstbrook said ISPs are in a position to know who is infected because they can see the traffic patterns, and they should warn customers, if not shut them off outright.

AOL originally sold McAfee VirusScan but found it was more economical to give it away to its customers. "They got fewer helpdesk calls and saw less bandwidth use," he continued. "Other ISPs need to follow this example and help their customers be more secure."

To Bounce or Not to Bounce?

What is the largest headache caused by spam? Many sites find that once you get decent filtering in place and start identifying spam, a new problem that crops up is just a disconcerting: Deciding what to do with it.

Software such as amavisd-new, a front-end for SpamAssassin and virus filters, leaves the ultimate decision up to the administrator. That is, what do we do with e-mail that has been identified as spam? The options are: use before-queue filtering to not accept it in the first place, send a delivery status notification (DSN) notifying the party that their e-mail was not delivered, or just silently discard the email. All of these options have consequences, and some are more hair-raising than others.

Option 1: DSNs, aka Bouncing

In this first scenario, a mail server will accept most e-mail, and then subject it to spam and virus filtering before delivering it to a user's mailbox. If the e-mail is determined to be spam, it isn't delivered to the user, and a DSN is sent to the address in the From: header, notifying the sender that delivery was not successful.

This is problematic for many reasons. Most critical, is the fact that the From: header in spam is rarely correct. In fact, it is possibly claiming to be from someone you know, since spammers have been known to harvest e-mail addresses from people's address books. Sending a DSN to someone who didn't send e-mail in the first place causes confusion, and results in support calls from the confused user who thinks their e-mail account has been compromised.

Even more detrimental to productivity, sending DSNs to addresses or domains that don't exist will cause the bounces to pile up on the mail server, since they can't be handed off to another server. Thousands of e-mail messages sitting in the mail queue will jeopardize system resources and can effectively clog mail services for legitimate mail. Most organizations find this to be the most difficult aspect of dealing with spam.

Option 2: Silently Discarding

Once a message has been accepted and eventually identified as spam, another option is to simply discard the message. This completely solves the problem of a mail server crumbling from having too much mail in the queue, but is perhaps just as problematic. If e-mail is falsely identified as spam, and the sender isn't notified that delivery failed, the sender will just assume everything was delivered as usual.

Clearly this is less than optimal, but when servers start falling over due to extensive resource consumption, many people turn to silently dropping spam. Oftentimes, silently discarding e-mail is an intermediate step between DSNs and before-queue filtering. David Ernst of HoosierNet said it was a question of keeping the mail flowing at all. "Well," he noted, "something had to be done. We can grind the service to a halt if we try to process all of those return-to-senders. So, it made the difference between working and not working."

Many people in this position opt to use a hybrid system of still sending DSNs, but cleaning the queue periodically to discard ones that cannot be sent.

Option 3: Don't Accept It At All

Ideally we want to identify spam while the sending server is still connected, and tell them that delivery isn't going to

happen. This means that the sending server has to deal with it, and in the case of a spammer, it simply means that sending failed. "Just don't accept it" is quite easy to say, but sometimes tricky to implement.

Some mail servers, such as postfix and sendmail, have the ability to hand messages to another program before sending them to the queue for final delivery. This provides the ability for the second program to scan mail for viruses and spam, and report the status to the mail server. If the message is identified as spam, the server, which has not yet reported to the sending server "delivery accepted," now has the option of reporting an error. There is no need to send a DSN, since we never accepted the suspicious message in the first place.

Best Practices

Implementing spam and virus checking isn't very difficult. Depending on the mail server, implementing spam filtering such that it is able to reject spam before the SMTP session is over can be difficult. Two widely used mail servers, postfix and sendmail, both have the ability to utilize amavisd-new.

Sendmail has the milter interface, which allows anyone to program add-ons to sendmail. The amavis-milter will hand off mail to amavisd-new, which in turn runs SpamAssassin and virus checking. Amavisd-new will also check attachments, and can extract data from zip files and many other types of archives to check for viruses and spam. Configuring this in postfix is even simpler, since it only requires one change in the configuration file, plus the addition of another smtpd process.

E-mail is increasingly frustrating to manage. We sometimes want to receive messages from people we don't know, so e-mail is designed to reflect that. People have implemented systems where a sender has to verify himself the first time they send e-mail, but that type of system doesn't always work. For instance, users always want to receive automated messages when they purchase things online, and those messages are normally sent from an address that people don't monitor, making "sender verification" impossible.

One thing that's clear is that sending DSN messages for spam is very bad practice. Users are confused when they receive a DSN for mail they didn't send, and dropping spam silently will lead to lost e-mail. The best option is to complete all virus and spam checking before accepting the mail for delivery, then report "success" to the sending server. Aside from the fact that this option tends to make the most sense, in most cases it also conserves system resources.

Tips for a Spam-Free Inbox

Most spam is recognizable without even opening it. Typically, the unwanted e-mail comes from someone you don't know and is about something you're not expecting, for example, offers for fake degrees, prescription drugs, or a moneymaking program.

Once you are on a spammer's mailing list, the volume of junk mail you receive will undoubtedly increase over time. Below is a nine-point guide on steps your users can take to prevent spam from overwhelming their inboxes.

1. Never respond to spam. If you reply, even to request removing your e-mail address from the mailing list, you are confirming that your e-mail address is valid and that the spam has been successfully delivered to your inbox. Lists of confirmed e-mail addresses are more valuable to spammers than unconfirmed lists, and are frequently bought and sold by spammers.
2. Check to see if your e-mail address is visible to spammers by typing it into a Web search engine. If your e-mail address is posted to any Web sites or newsgroups, remove it if possible to help reduce how much spam you receive.

Waging the War Against Spam

3. Disable in-line images, or do not open spam messages. Frequently spam messages include "Web beacons" enabling the spammer to determine how many, or which e-mail addresses have received and opened the message. Most current e-mail programs disable in-line images by default to prevent this from occurring.
 4. Do not click on the links in spam messages, including unsubscribe links. These frequently contain a code that identifies the e-mail address of the recipient, and can confirm the spam has been delivered and that you responded.
 5. When unsubscribing from e-mail, the main rule to follow is: if you didn't originally opt-in to receive it, or if you don't recognize the sender, then don't unsubscribe.
- Trying to unsubscribe from one e-mail can start a flood of mail from other sources, so if you are unsure, it is best not to unsubscribe and block the mail another way. When unsubscribing from e-mail, always check that the links go to the correct company Web site and not to a phishing site.
6. When filling out Web forms, check the site's privacy policy to ensure it will not be sold or passed on to other companies. There may be a checkbox to opt out of third-party mailings.
 7. Do not respond to e-mail requests to validate or confirm any of your account details. Your bank, credit card company, and the like already have your account details and would not need you to validate them.
- If you are unsure if a request for personal information from a company is legitimate, contact the company directly or type the Web site URL directly into your browser. Do not click on the links in the e-mail, as they may be fake links that will direct you to phishing Web sites.
8. If you have an e-mail address that receives a large amount of spam, consider replacing it with a new address and informing your contacts of the new address. Once your e-mail address is on a spammer's mailing lists, it is likely that you will receive increasing amounts of spam.
 9. Set up two e-mail addresses, one for personal e-mails to friends and colleagues, and use the other for subscribing to newsletters or posting on forums and other public locations. The more complex your e-mail address is, the less likely you are to receive spam.

This content was adapted from Internet.com's EnterpriseITPlanet and InternetNews Web sites and EarthWeb's Datamation and EnterpriseNetworkingPlanet Web sites. Contributors: Charlie Schluting, Guy Roberts, Andy Patrizio, and James Maguire.

Internet.com eBooks bring together the best in technical information, ideas and coverage of important IT trends that help technology professionals build their knowledge and shape the future of their IT organizations. For more information and resources on IT security, visit any of our category-leading sites:

www.esecurityplanet.com
www.antonline.com
www.internetnews.com/security
www.earthwebnews.com/security
www.enterpriseitplanet.com/security
www.insideid.com
www.smallbusinesscomputing.com
www.linuxtoday.com/security/

For the latest live and on-demand Webcasts on IT security, visit: www.jupiterwebcasts.com/security