

Spam: More Than a Nuisance

Spam – An Escalating Problem

Spam, or unwanted email, has become one of the largest side effects of the Internet, severely impacting email as a productivity tool. CipherTrust's research department estimates that spam accounts for 50% of corporate email and will increase to 60% by mid-2004. Judging from recent media coverage, spam currently stands out as the hottest Internet-related issue.

The increase in spam volume should come as no surprise – spam is a highly lucrative business. Spam profits are defined as revenues from sales of products or services generated from responses to spam, less the cost of sending spam. The cost of sending 10,000,000 messages is about the same as sending 100,000 messages. Assuming the response rate, profit margin per item and cost of sending spam remain constant, a spammer only needs to increase the volume of spam sent in order to earn more money.

Users at ISPs were the initial targets for spam, but over the last 18 months corporate mail systems have also been targeted. The rapid increase in spam at corporations leaves users frustrated, and overloads email servers and helpdesk organizations. According to Ferris Research, in 2003 the cost of spam is estimated to exceed \$10 billion for corporate organizations.¹

There is a symbiotic relationship between those who send spam and those who try to stop it. In the early days, spammers frequently relied on *open relays*– standard email servers that allow anyone to distribute email, either by design or oversight. This spurred the use of *blacklists* – lists of IP-addresses belonging to open relays used by spammers, for which connections should be rejected.

¹ FERRIS RESEARCH “Spam Control: Problems and Opportunities”; January 2003

Since then, spammers have learned to forge header information to deceive the email's origin; randomize text within words to bypass filters that look for specific words or expressions; hijack corporate email servers in order to distribute spam that looks like it's coming from a legitimate sender; make the actual message content look like a legitimate business email to fool statistical analysis tools, plus a range of other methods. As spammers develop new techniques, anti-spam vendors must respond with new detection techniques. This cat-and-mouse game has accelerated over the past 12 months and is likely to continue, rendering those organizations without effective anti-spam tools subject to increased spam abuse.

In addition to the dramatic increase in volume, spam content has become more graphical, sexually explicit and recently, more fraudulent. The most recent assault by the Sobig.F worm² demonstrates how spam is converging with malicious worms, creating a new type of threat against email systems.

Understanding Email Security Needs

The evolution of spam has had a direct impact on the email services delivered by Information Technology departments. It has breached the three essential security measures that must be present in order to provide secure email services.

Security Measures	Description
<i>Confidentiality</i>	Protection of email messages and systems from unauthorized access.
<i>Integrity</i>	Guarantee that email messages and systems are not distorted or destroyed in an unauthorized way.
<i>Availability</i>	Ensure email servers and directories meet the committed service level.

Failure by an organization to provide effective email security measures will compromise the value of email as a critical business tool.

Enterprises have deployed firewalls to enforce network level security, but they have limited means of analyzing the actual content of the email that is transmitted. Technically, a firewall sees email as data packages from outside the network directed to a dedicated email server on port 25 inside the network. These data packages receive only the most rudimentary scrutiny, leaving email vulnerable to a variety of threats.

² CIPHERTRUST "Sobig and Beyond: Defining Email Security"; September 2003

Spam Has a Direct Impact on Email Security

As the volume of spam increases, the content becomes more obscene and fraudulent, and spammers harvest corporate email directories and take control of corporate email servers, the spam problem develops into a serious security issue for enterprises. Email security is directly compromised by spam and spammers in several ways.

Security Measure	Type of Threat	Impact
<i>Confidentiality</i>	Mail server hijacking and directory harvest attacks.	Abuse of corporate assets and exposure of corporate user information.
<i>Integrity</i>	Mail server hijacking.	Abuse of corporate email systems by outsiders.
<i>Availability</i>	Spam floods and directory harvest attacks	Leads to denial-of-service and brings email servers to a halt compromising service.

To demonstrate how spam can compromise email security, consider the following two cases:

In February 2002, AT&T Worldnet's servers were crippled by a large spam flood, keeping their customers from sending and receiving email for several days.³

Trans Pacific Stores, Lakewood CO, was forced to take down the network for 36 hours in May 2002 after spammers began using their email server as a relay.⁴

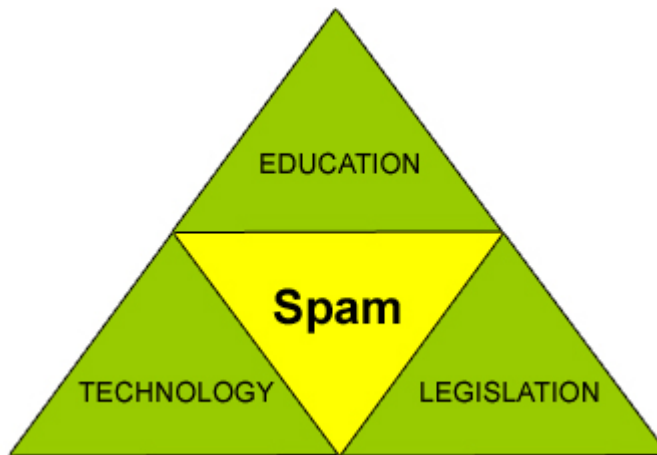
By recognizing that spam is a security issue, organizations can more effectively address the problem directly and deploy a solution that will guarantee the service level of the three critical security measures – *Confidentiality*, *Integrity* and *Availability*.

The Spam Problem Requires a Multifaceted Approach

While over 90% of spam can be blocked with filtering solutions at the receiving gateway, mail server or desktop, technical solutions alone won't be enough to eradicate spam. Since sending spam is a business with profit goals, dissolving the business model will make spamming economically unfeasible. This can only be achieved through a combined effort of user education, technology and legislation.

³ INTERNETNEWS.COM "Spam Attack Cripples WorldNet Servers"; February 2002

⁴ COMPUTERWORLD "Bottom Line Hit Hard by Need To Fend Off Spam and Viruses"; September 2003



User Education. Users must be educated to treat their email addresses as corporate assets and protect them accordingly. In addition, they must learn to manage the spam that makes its way into their inboxes.

Technology. Technical solutions must be able to distinguish spam from legitimate email while protecting the email system from intrusion, denial-of-service and other email related threats.

Legislation. Legislation serves as an important deterrent and can increase the spammers' overhead cost in the event they are sued for their actions.

With spammers' abilities to find new methods of sending spam and new techniques to masquerade the content, there is no silver bullet against spam. The industry has responded with a myriad of various detection techniques such as blacklists, whitelists, statistical analysis, signature-based filters, keywords, etc. Each technique has proven to be effective against certain types of spam, but have performed poorly against several other types, resulting in weak performance against the overall spam problem.

To address this effectiveness issue, anti-spam solutions should deploy techniques that answer four basic questions about a message:

1. *Who is the message from?*
2. *How was the message sent?*
3. *Where was the message sent?*
4. *What is in the message?*

The highest spam filtering success rate (a function of the spam detection rate and the false positive rate) can be achieved by combining results from multiple detection techniques into one aggregated score, which identifies the likelihood of a message to be spam. If the aggregate score meets or exceeds the threshold for what should be considered spam, an action should be performed on the message such as: quarantine, delete, log, subject-line insertion or x-header insertion.

With the rapid evolution of spam, anti-spam providers must deliver continuous detection technique updates to maintain the accuracy level. In addition, the solutions must have the flexibility of adding entirely new, innovative techniques against future spam that employs new spamming methods.

Conclusions

Any respectable anti-spam solution should detect and filter spam, but a more comprehensive solution is needed to address the overall email security threat. Protecting email servers from intrusion and being turned into spam-sending devices, and preventing corporate email directories from being harvested are also critical security concerns for enterprises.

Finally, true protection is only as strong as the weakest link in the system – a fact that hackers and spammers have learned to exploit. Security conscious organizations must be aware of all the email-related threats and prepare to address them appropriately.

About The Author

Marten Nelson is Director of Business Analysis and Strategy at CipherTrust. He was previously the lead analyst on spam and other content-related threats such as viruses at Ferris Research, the leading market research firm on email, messaging and collaboration. He has also conducted in-depth TCO studies on enterprise messaging solutions. Prior to that, Marten held senior marketing management positions at Brightmail and Lotus/IBM. Marten has authored numerous research reports on the impact of spam and the growth of the spam market, and has been a frequent panelist and speaker at industry conferences and seminars.

IronMail Is a Comprehensive Email Security Solution

CipherTrust's award-winning email gateway, IronMail, is an email security appliance designed from the ground up to provide high performance gateway protection for demanding messaging environments. IronMail is an innovative solution using the latest generation software. It is designed to evolve as new email security threats develop and can be tuned to meet the diverse needs of the enterprise.

To learn more about CipherTrust and IronMail, please visit our Web site at <http://www.ciphertrust.com>.