TRENDS IN SPAM MANAGEMENT (PART I)

EDUCAUSE Evolving Technologies Committee
Pablo G. Molina, CIO, Georgetown University Law Center Campus

THE (ANTI) SPAM CASE AT RIT (PART II)

EDUCAUSE Evolving Technologies Committee
Emilio DiLorenzo, Director Infrastructure & Technical Support Services, Rochester Institute of Technology

August 16, 2004

Trends in Spam Management Introduction (PART I)

It is 2004. Two things are certain in Internet life: spam and outages. Successfully dealing with the former may help reduce the latter. This article focuses on the state of spam and the efforts of higher education institutions to manage it from technical, legal, and social points of view.

What Is Spam Management?

As of April of 2004, the Oxford English on-line dictionary still defines spam as “1. The proprietary name of a type of tinned meat consisting chiefly of pork; also (with lower-case initial) applied loosely to other types of tinned luncheon meat.” Webster’s on-line dictionary offers a second definition: “unsolicited usually commercial e-mail sent to a large number of addresses.” This article focuses on managing spam email, the methods, processes, policies, and tools used to control the flow of unsolicited email messages.

Key Questions to Ask Yourself About Managing Spam?

University administrators and Chief Information Officers know that spam is a bad thing for their institutions. To know how bad spam is, they need to identify the costs of spam in terms of lost productivity, spoilage of technology resources, and user dissatisfaction. Once these costs are assessed, it is easier to gauge how much effort they should put into fighting spam.

In this context, decision makers need answers to three questions. What resources are necessary to develop and implement a spam management strategy? What funding resources, if any, are available to manage spam? What are the cultural values and expectations of campus members when it comes to dealing with spam?
Why Is Spam Management Important to Higher Education?

Spam Management is of great importance to preserve the technology resources of an institution, including but not limited to bandwidth, email infrastructure, support services, and information security defenses. The Georgetown University Law Center Campus recently implemented an outsourced spam management solution. In June 2004, a slow month for academic and computer virus activity, the service trapped more than 50% of incoming email messages as useless. 10% of the email traffic was trapped because it was infected with computer viruses. An additional 42.5% of all campus email traffic was identified as spam. For a campus of about 3,000 people, the number of monthly spam/virus email messages was over 500,000, an average of 167 messages per person per month. Considering that many community members have been using personal spam avoidance techniques for the last couple of years, the number is worrisome.

Similarly, the email system used by the majority of faculty, staff, and students at Georgetown University’s Main Campus was so overloaded with virus and spam messages that it was brought to its knees on several occasions during the first half of 2004. Fortunately, the technology team alleviated the problem with an overhaul of the email infrastructure. A working group continues to explore an institutional-wide spam management approach.

Spam management can help respect institutional values and meet community expectations. A clear example me was an alarming phone call from Sister Dorinda Young to the technology team indicating that she was receiving some “very strange emails about body parts that I do not have.” Associate Dean, James Feinerman expressed great concern when working at home and accidentally opening an offensive spam message received on his University account while family members were present. The Acceptable Computer Use Policy clearly states that “The University cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive.” Obviously, individual expectations differ.

What Are The Implementation Challenges?

The challenges are technical, financial, and cultural.

Technical challenges deal with the complexity of email systems and the need to maintain the systems running at all times. Hosted solutions, internal appliances, add-on email enhancement services, and personal computer software packages are technical tools available to manage spam. SPAM methods are adapting almost as fast as or faster than SPAM products. Best practices have not been fully documented and most vendors and tools are as immature as the spam problem itself.

Financially speaking, it is difficult to fund spam management at a time when technology funding is one of the most pressing concerns of CIOs. Are students willing to pay a spam management fee? How receptive are CFOs to fund these initiatives annually? For example, list pricing from some of the spam management outsourcers would put the price tag at $100,000 for a campus of 10,000 people. Other solutions may appear more affordable but carry hefty price tags once labor costs are factored into the equation. In desperation, cash-strapped technology organizations may feel tempted to rely on unorthodox financing such as the one proposed in a well-recognized email fragment. “I got your contact from my uncle who works with the chambers of commerce and industries during my search for a reliable or honest partner, to assist me carryout this transaction. first I will start by introducing myself. My name is John Bongo, the son of the late minister of power and steel, one of late Dr. Micheal C. Bongo. I and my 22 years old sister are orphans from the Republicof Laiberia…”

On the cultural front, the issues are many. According to Georgia Tech’s CIO, John Mullin: “At a university, [spam control] is not that easy because one person’s spam is another person’s research. It’s a cultural
issue and needs to be considered.” A Georgetown University student recently wrote about false positives trapped by a spam management system: “How am I supposed to know that I didn’t get an important message from my mortgage holder or from a prospective employer?”

What values should be considered when implementing spam management systems? The Georgetown University Law Center Campus uses a hosted spam control system run by MessageLabs. The IT team decided to configure the system in such a way that it would trap, without notification of any kind, incoming virus-infected messages. This approach places the technological responsibility on outside parties.

**Who Are The Major Spam Management Vendors?**

On February 17, 2004, a series of PC Magazine articles generically titled “The Email Mess” identified the following software products in the fight against spam. Listed in the category of filtering, or identifying spam by examining email contents, were iHateSpam, MailFrontier Matador, MailWasher Pro, and MacAfee Spamkiller, SAproxy Pro, SpamCatcher, SpamNet, and the Editor’s Choice product, Norton AntiSpam 2004. Listed in the category of whitelisting, or allowing email only from specified senders, were ChoiceMail, Qurb, and Vanquish Pro.

Gartner’s Magic Quadrant for Enterprise Spam Filtering First Quarter 2004 lists a large number of spam-filtering software, appliances, and managed services, including BlackSpider Technologies, Brightmail, CipherTrust, Clearswift, Cloudmark, FrontBridge Technologies, MailFrontier, MessageLabs, Mirapoint, MX Logic, NetIQ, Network Associates, Postini, Proofpoint, Sophos/Activestate, SurfControl, Trend Micro, Tumbleweed Communications, and Zix Corporation.

Most spam management products and services rely to some extent on blacklists used to identify the spammers on the Internet. One of the most popular blacklists is the SpamHaus Block List. "The SBL is a realtime database of IP addresses of verified spam sources (including spammers, spam gangs and spam support services), maintained by the Spamhaus Project team and supplied as a free service to help email administrators better manage incoming email streams. The SBL is queriable in realtime by mail systems throughout the Internet, allowing email administrators to identify or block incoming connections from IP addresses involved in the sending of Unsolicited Bulk Email. The SBL database is updated 24/7 by a dedicated international Spamhaus team (US, UK, NL, I, JP, AR) and is broadcast by 32 SBL zone mirror servers based in Australia, Belgium, Denmark, Germany, Greece, Italy, Japan, Netherlands, South Africa, UK and USA. Spamhaus also supplies direct hourly Datasfeeds of the SBL to many of the Internet's major Internet Service Providers, Corporations, Universities, Government and Military networks."

**What Are The Rules of Thumb for Judging Among Them?**

Not all solutions are suitable for all email systems. Once it is determined that a number of spam management systems can be integrated with an existing email infrastructure, the main criteria for selection should be reliability, performance, functionality, and cost.

Email is a mission critical system in academic institutions. If spam management applications negatively affect reliability, they become more of a nuisance than an aid. Certain tools are notoriously complicated to manage, and when improperly configured, can contribute to the instability of high-volume email systems.

Performance is difficult to judge because it takes into consideration various factors. First, it is important to consider the latency, that is, how long it takes for the system to filter email messages. A second consideration is the success ratio, that is, the percentage of correctly identified virus-infected and/or spam messages. The third issue to consider is the number of false positives, that is, messages that are not spam but incorrectly treated by the system as such.
Functionality is another key factor. The best products allow a great degree of personal customization, so that community members can establish their own thresholds for spam. The most important customization factor is an opt-out function for those users who are not interested in using the service at all. Useful functions are those that allow users to specify how often and in what format they would like to receive notifications about trapped email. It is also important to look into the functions that are designed to release or delete captured messages.

Annual total costs of operation is perhaps the most important factor. While custom-made, freeware solutions may be appealing at first, they could end up being more expensive than hosted solutions. This is particularly true for campuses where the email engineering team relies on telecommunication-class email systems or university engineers cannot absorb the workload required to manage spam. New companies tend to discount their services and products for the first few customers. As they become more popular, they slowly increase their prices. As of today, many of the companies in the business do not have clear pricing models for higher education institutions.

The weight assigned to each one of these variables depends on each organization's culture and values.

**How Should We Proceed?**

Student leaders, faculty members, and senior administrators are ideal agents to take the temperature of the community regarding spam tolerance. Annual technology satisfaction surveys may be used as a good starting point to collect inclusive data on community perceptions. Network engineers, together with support personnel, can produce information to paint an accurate picture of the volume of spam arriving at the gates of the university. Furthermore, they may be able to assess the cost of spam in terms of wasted resources.

A representative working group is another good approach for evaluating options and recommending a solution based on the culture of the institution. Technical members must be part of the group to ensure that integration with existing systems, vendor synergies, and support issues are taken into consideration. As previously mentioned, when several solutions are viable, it is useful to evaluate systems in terms of reliability, performance, functionality, and cost.

Once there is workgroup consensus, available funding, and signed contracts, it is time to engage in a communication campaign. Senior administrators must participate and endorse the initiative to ensure its success. Deans and their technology delegates can assist by sponsoring open forums, training sessions, web sites, flyers, etc. Like most other technology projects, the best time to implement a spam management solution is between academic years. Pilot implementations may prove useful in this type of project. For example, deploying the spam management system in a school or campus at first may help configure the system before university-wide delivery. A staged implementation may be suitable for certain environments. Under this approach, spam and virus-infected messages will be simply tagged at first. Community members will be given instructions on how to use their email clients and/or web interfaces to recognize the tags and delete or move the messages.

**When Will Spam Management Become Essential on Campuses**

For most institutions, spam management is essential today. Higher education officers who have not yet discussed the problem face increasing criticism from their communities, as spam problems are addressed in other organizations.
How Is Spam Management Evolving?

New technologies are being deployed to reduce spam. On May 5, 2004, the Wall Street Journal announced that “Microsoft Corp. is adopting an anti-spam tool that gives favored treatment to certified mass e-mailers, the first major operator to do so.” This technology was developed by a company called Ironport Systems. It is based on associating e-mailers with IP addresses to guarantee the authenticity of the messages and the legitimacy of the senders.

A second approach under research is the idea of charging a tax for every email message sent. The tax does not need to be assessed in monetary units. For example, the system would require that sender computers solve a mathematical equation for every email message sent. In the case of spammers, this would require significant computing power.

Legal and administrative actions are proving partially useful in controlling spam. Many states have passed spam laws over the last few years. Many of their provisions may be pre-empted by federal laws. Bill Number S. 877, which regulates interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial email via the Internet, was passed by the Senate on November 25, 2003, and agreed to by the House of Representatives on December 8, 2003. The bill was signed by the President on December 16, 2003, and took effect on January 1, 2004. This Act may be cited as the ‘Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003’, or the ‘CAN-SPAM Act of 2003’.

On April 28, 2004, the Washington Post reported that “U.S authorities charged four people in Detroit with e-mailing fraudulent sales pitches for weight-loss products, the first criminal prosecutions under the government’s “can spam legislation, which requires unsolicited e-mails to include a mechanism so recipients can indicate they do not want future mass mailings.”

On March 22, 2004, UT Austin VP for Information Technology, Dan Updegrove shared with other university CIOs the news that “United States District Judge Sam Sparks issued an important ruling supporting our university’s right to block unsolicited commercial email (spam), even if the email is judged to be legal under the recently-enacted CAN-SPAM Act of 2003. In this case a company obtained over 50,000 UT Austin student, faculty, and staff email addresses last spring, via a valid state open records request, then used the addresses to promote the company's business (a dating service, "LonghornSingles.com"). After the company did not comply with a request to cease and desist such email broadcasts, UT blocked the site. The company sought and received a temporary restraining order to remove the block in state court, which order was rescinded soon after by a federal judge. The company then sought a permanent injunction, which was denied last week.”

On June 15, 2004, the Federal Trade Commission announced that a “do-not-spam registry” service would not be created in the near future. The commission was obligated to consider this proposal under the “can spam” legislation signed by the President in December. The reason behind this decision was that the agency would find itself “largely powerless to identify those responsible for misusing the registry.”
What Are The Issues To Be Addressed?

Good information security practices suggest that email systems and protocols should eventually be modified so that the identity of a sender can be determined without doubt. Spoofed email messages should never reach their destination. This accomplishment would guarantee that techniques such as blacklisting, SpamHaus, or whitelisting would become truly useful.

Due to the open nature of the Internet, fighting spam with national and state laws will have limited success. Without international legislation and enforcement mechanisms, spammers will simply base their operations in countries where spam legislation is lax, or rarely enforced.

Where Are The Likely Impacts In The Coming One to Three Years?

Faculty, staff, and students will expect spam management solutions in place. This demand unfortunately spread limited resources even thinner. Some of the solutions, however, may bring higher reliability and better performance to email systems. Hosted solutions, for example, may reduce the number of processed messages.

Conclusion

In conclusion, most higher educations organizations should be developing and implementing interim strategies to reduce spam. At the same time, technology companies and government agencies must address the problem from technical, legislative, and enforcement perspectives.

Related EDUCAUSE 2004 Sessions and papers


The (Anti) Spam Case at Rochester Institute of Technology (PART II)

To be truly successful, SPAM defense should be considered just like virus defense is, at the gateway, in the server, and again at the desktop (multi-layered approach). Successfully integrating these tools within a complex email infrastructure is a challenge.

Rochester Institute of Technology (RIT), like Georgetown University Law Center Campus and many other Institutes across the country have experienced very similar situations.

Assuming no SPAM controls, and that it takes an average of 5 seconds to read and delete each SPAM message, and 6 SPAM messages per person daily, industry estimates are that an institution would be spending 2.53 hours per person per year to read and delete SPAM. In a corporate setting, this would equate to at least a $750,000 loss/year. These estimates are conservative and don't factor in time spent discussing the latest "creative" SPAM, contacting the Help Desk, etc. or loss of productivity when a spike slows or shuts down the e-mail server.
In late 2003, using an analysis of inbound e-mail traffic versus a combination of block lists - including Spamhaus, RIT identified 40+% as SPAM, 60+% on weekends with only partial success in identifying all of the SPAM between late 2003 and mid 2004. Sometimes, identification of SPAM is subjective at best. Spamhaus employs the idea of applying a "code of conduct" approach to SPAM sites. Spamcop employs the idea of a "collective reporting system", resulting in a purely subjective result. A combination of "blocking" and "tagging" may be necessary to put some of the control into the recipient's hands. Flexibility and speed are important here. SPAM methods change quickly, and products/solutions need to as well. How fast have they adapted in the past?

RIT has tracked a 3-4 fold increase in SPAM, partially due to a link between virus infected computers and SPAM. The combination of SPAM and viruses account for more than 75% of the mail inbound from the Internet. Today RIT is currently capturing 209 "bad" messages per person per month, 107 of those are designated SPAM. What was linear growth since 2001 is now appearing to be exponential growth in 2004.

Why are these statistics important to talk about? Well, let's look at some other key factors affecting higher education. Flat or decreasing operating and capital budgets. More services to support and no incremental headcount. The drive to be more operationally efficient. Finally, perhaps the most important thing we keep forgetting are the thousands of technologically smarter students than the previous year with a lot more time on their hands than all of us.

All of these points individually may not seem that tragic, however when you add them all up and throw Spam Management on top of the pile you have one great big mess to sort out.