


Spam E-mail and Its
Impact on IT Spending
and Productivity

Jonathan B. Spira
Chief Analyst

DECEMBER 2003





“Spam E-mail and Its Impact on IT Spending and Productivity”, copyright© 2003 Basex, Inc. All data, opinions, and projections in this report are based on Basex’ judgment at the time of publication and are subject to change. All rights reserved under International and Pan-American Copyright Conventions. No part of this report may be reproduced or transmitted in any form, by any means, without the express written permission of Basex.





CONTENTS

INTRODUCTION	1
THE FIRST SPAM	1
FIGURE 1: THE FIRST SPAM, MAY 3, 1978	2
FIGURE 2: OFFICIAL REBUKE TO THE FIRST SPAM	3
SPAM TODAY	3
AN INTERNET PIONEER'S PERSPECTIVE	4
THE COST OF SPAM	5
WHAT CAN BE DONE	6
THE FUTURE	7

Introduction

2003 was certainly no one product's year. Indeed, the year was filled with notable events around the globe. The designation of Basex:Product of the Year is given to a technology that has a tremendous impact on Collaborative Business Environments, one that changes the very fabric of how we work. This year, that "technology" is Spam.



The impact of the Internet has been, all would agree, far reaching. In a larger perspective, the world will never quite be the same. What networks of railroads, highways and canals were in another age, networks of information are today. Yet Spam is shaping a new era in the brief but poignant history of the Internet.

Even from one day to the next, it is easy enough to look at the world around us and conclude that the Internet has changed life dramatically. It is hard to imagine that, little more than 100 years ago, New York City streets were first illuminated by electricity, the German engineer Gottlieb Daimler built a gasoline-fueled internal combustion engine, and that 100 years ago, almost to the day, Orville and Wilbur Wright made powered flight a reality. These inventions changed the world

But what if the simplicity and ease-of-use of the Internet were to be neutralized by a sinister force?

The First Spam

Gary Thuerk, a marketer at Digital Equipment Corp, sent the first junk e-mail on May 3, 1978 (see Figures 1 and 2 on the following pages). He thought that Arpanet users would be interested in knowing that DEC had integrated Arpanet protocol support directly into the new DEC-20 and TOPS-20 operating system. He, with the help of a DEC sales engineer, Carl Gartley, sent a poorly-formatted message inviting people to two product presentations in California.

In the 1980s, the term "Spam" was used within the MUD (multi-user dungeon) environment, to denote one of several activities, including overwhelming a chat session by posting a large text file or files.

The term "Spam" itself comes from the Monty Python's Flying Circus spam skit, which takes place in a restaurant where every dish has spam as an ingredient. When a waitress repeats the word "spam" several times in describing a dish, a group of Vikings sings:

“spam, spam, spam, spam, spam, spam, spam, spam, lovely spam!
Wonderful spam!”

This continues until they are told to shut up. From this, Spam took on the meaning of something that keeps repeating to everyone’s great annoyance.

“Spam” was first applied to unsolicited commercial e-mail in 1994 when two lawyers (Canter and Siegel) posted a message advertising their services for an upcoming immigration lottery to every single newsgroup on USENET, several thousand in all. Users called this action a “spam” and the term stuck.

Figure 1:
The First Spam,
May 3, 1978

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM.

THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM HYATT HOUSE
(NEAR THE L.A. AIRPORT) LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM DUNFEY'S
ROYAL COACH

SAN MATEO, CA

(4 MILES SOUTH OF S.F. AIRPORT AT
BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW.
ALSO TERMINALS ON-LINE TO OTHER

DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET.
IF YOU ARE UNABLE TO ATTEND,

PLEASE FEEL FREE TO CONTACT THE NEAREST
DEC OFFICE

FOR MORE INFORMATION ABOUT THE EXCITING
DECSYSTEM-20 FAMILY.

Figure 2:
Official Rebuke To
The First Spam

ON 2 MAY 78 DIGITAL EQUIPMENT CORPORATION
(DEC) SENT OUT AN ARPANET MESSAGE
ADVERTISING THEIR NEW COMPUTER SYSTEMS.
THIS WAS A FLAGRANT VIOLATION OF THE USE
OF ARPANET AS THE NETWORK IS TO BE USED
FOR OFFICIAL U.S. GOVERNMENT BUSINESS
ONLY. APPROPRIATE ACTION IS BEING TAKEN TO
PRECLUDE ITS OCCURRENCE AGAIN.

IN ENFORCEMENT OF THIS POLICY DCA IS
DEPENDENT ON THE ARPANET SPONSORS, AND
HOST AND TIP LIAISONS. IT IS IMPERATIVE
YOU INFORM YOUR USERS AND CONTRACTORS WHO
ARE PROVIDED ARPANET ACCESS THE MEANING OF
THIS POLICY.

THANK YOU FOR YOUR COOPERATION.

MAJOR RAYMOND CZAHR

CHIEF, ARPANET MANAGEMENT BRANCH, DCA

Spam Today

Spam is the subject of many articles, news reports, and conversation, and such discourse is not limited to computer geeks. It is something everyone—from gardeners to grandmothers—is familiar with. Spam has been present in everyday life since the mid 1990s, when the infamous “King of Spam” Sanford

Wallace discovered how little it cost him to send millions of commercial e-mail messages per day, with the majority of the cost borne by the recipient.

AN INTERNET PIONEER'S PERSPECTIVE

Bob Kahn is the co-designer of the TCP/IP networking protocol, and is presently the president of the Corporation for National Research Initiatives, a not-for-profit organization that performs research in the public interest on strategic development of network-based information technologies. The very nature of the protocol he developed with Vint Cerf made the Internet open to all—including spammers. Kahn sees spam today as “hardly surprising.” During the early days of the ARPANET and Internet, the use of the network was limited to research and education groups. Commercial use was, of course, prohibited. “During most of that period,” Kahn relates, “close to 100% of the e-mail I received was relevant by some criteria...A few years ago, that figure became perhaps 50% and today it hovers around 10%. The rest is spam, or more accurately unwanted e-mail.”

Kahn is not at all “happy” about this situation, and suggests that a small fee for per e-mail for large bulk e-mailings would greatly reduce this traffic. “At even a fraction of a penny per e-mail above a free daily allotment,” he continues, “I think we would see a whole lot less spam.” He also thinks a “do not spam” registry might help where restrictive legislation is otherwise unavailable. “However, I have a hunch,” he says, “that there is a better solution waiting to be found, technical or otherwise. But until it is, we will likely have to cope with spam and other unwanted e-mail as best as we can.”

Today, such e-mail accounts for almost half of all Internet traffic, and can be as many as 15 billion messages per day. On December 16, 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) was signed into law. CAN-SPAM creates a uniform standard for e-mail marketers and provides for civil and criminal penalties for a variety of spam-related activities, such as the theft or harvesting of e-mail addresses from Web sites. To demonstrate how rampant the problem of harvesting is, U.S. Federal Trade Commission investigators recently placed 250 e-mail addresses on Web pages, news groups, chat rooms and online directories. After six weeks, the 250 addresses had received 3,349 spam messages. The first message came only nine minutes after the address had been posted in a chat room.

On December 18, 2003, Microsoft and New York State Attorney General Eliot Spitzer jointly announced that, as a result of a six-month long collaborative investigation, they had uncovered—and filed suit against— Synergy6, Inc., a spamming ring that was responsible for sending billions of illegal and deceptive e-mail messages, and Scott Richter, considered to be among the world’s top three spammers.

According to the investigation, Synergy6 and Richter are responsible for seven illegal spam campaigns, each in violation of consumer protection statutes in New York and Washington. These e-mail campaigns used false subject lines, designed to give the recipient the impression of a pre-existing business

relationship with the sender. They also falsified sender e-mail addresses, using over 100 different domains, including hotmail.com, aol.com, earthlink.com and yahoo.com. The messages were routed through ca. 500 Internet addresses throughout the world, in 35 countries spanning six continents, including addresses belonging to the Kuwait Ministries of Communication and Finance, several schools in Korea, the Seoul Municipal Boramae Hospital, and the Virginia Community College System.

With all of this activity, it is no wonder that spam, according to Brian Arbogast, Microsoft's corporate vice president and executive sponsor on the issue of spam containment, "is our customers' number one complaint concerning e-mail today." Many people, especially spammers, maintain that spam is a victimless crime. They hold that, since spam e-mail messages can be deleted with a press of the delete key, no harm is done. This would hold true if users received only one or two such missives per day. But spam is costly, to individuals, corporations, Internet service providers, and others. A recent Basex survey revealed that more than half of all e-mail received is spam. The survey also revealed that spam could overwhelm users, who spend ca. 15 minutes per day deleting such messages. Users can also inadvertently delete legitimate e-mails, either by misidentifying these as spam, or just due to their being lost in the sheer volume of spam.

The Cost Of Spam

Companies are looking at a variety of costs due to spam, including

- Lost productivity
- Clogged e-mail systems
- Bandwidth
- Storage costs
- User support
- Anti-spam software
- User training

Within the enterprise, the cost per user can range from \$600 to \$1,000 per year, based on these factors. This means a company with ca. 15,000 employees may be faced ca. \$12 million in spam-related costs annually. The cost of spam to companies worldwide is ca. \$20 billion and growing at almost 100% per year.

Microsoft, according to Arbogast, is incurring "exorbitant costs in lost-worker productivity and resources allocated to containing the problem."

When spammers spoof a legitimate user or corporate domain, that user or company may find its e-mail or domain name blacklisted, effectively sending e-mails from the user or company into a black hole.

Of course, there is also a cost to those sending out legitimate e-mail marketing pieces. Due to misconfigured anti-spam software, or user error, these may get deleted as well. As a result, the companies who send these mailings miss out on revenue, and the recipient may miss an important product or service that is actually desired. AOL and Microsoft each block over 2 billion suspected spam e-mails each day from reaching their subscribers; some of these, of course, are not spam but were blocked nonetheless.

More recently, spammers have taken a new tack: spoofing legitimate businesses (such as Citibank, PayPal or eBay) to gain access to personal information, including credit card details. These “phishers” create sites that are crude versions of the real thing, but have enough of a similar look and feel to gain the confidence of certain of their victims.

Given an environment where virtually anyone can purchase a list of 25 million e-mail addresses for \$25, and send e-mail to all 25 million at practically no cost, it should come as no surprise that spam has become such a scourge.

What Can Be Done

Companies that provide messaging applications, such as IBM and Microsoft, and those which provide hosted e-mail services, such as AOL and Critical Path, are committing substantial resources to technology solutions to combat the menace. Many companies are investigating and litigating against spammers

Users are taking spam-fighting into their own hands. No spam filter will stop all spam e-mails. In fact, it’s important to note that one man’s spam is another’s welcome offer. So individual users are refraining from giving out their e-mail addresses in many instances. Since one cannot reliably determine whom to trust, it is perhaps simpler to assume that no one will safeguard your information. This approach is, of course, somewhat impractical as many companies have a legitimate need to obtain an e-mail address. Examples include to confirm your identity when registering for a service, and to allow for shipping updates to be sent regarding orders placed via the Internet.

Other users are creating multiple e-mail accounts, reserving one address for chat rooms and another for e-commerce. This, of course, means that users must also check multiple accounts, and this may result in unplanned delays if an e-mail

account remains unchecked as well as lost mail in the case of reaching a message limit. Another alternative is a “disposable” or one-time use e-mail address, which allows a single e-mail to be sent to a user, after which the address is no longer valid.

Many corporations and individual users are implementing a variety of anti-spam software applications. Some companies deploying spam-scanning services, such as Postini or Brightmail, to block spam at the Internet gateway. Lotus Notes/Domino users can deploy solutions such as Granite Software’s SpamJam, which runs on the mail server. And Microsoft recently added spam-filtering SmartScreen Technology to Exchange Server, which uses feedback from millions of Hotmail users to determine what is, and is not, spam.

Basex estimates that companies spent in excess of \$600 million to deploy spam-fighting measures in 2003, and that this figure will grow to \$2 billion by 2005.

Additionally, some users take the whitelist approach, where only pre-approved e-mail addresses can get through to the inbox. Others use a challenge/response system, which sends a form back to the sender with a simple question to answer, or even a word that can be retyped. Human senders can respond; a computer-generated message from a spammer cannot. Another consideration is to avoid the use of actual e-mail addresses on corporate Web pages, using forms in their stead.

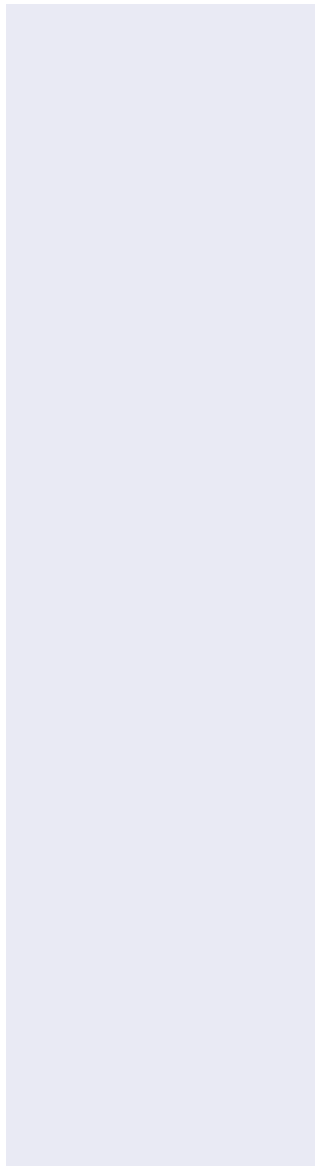
The Future

Does spam portend the end of useful e-mail as we know it? Hardly, as the Internet is far too resilient to succumb, even to what is really a major scourge. Researchers have been working on new standards and protocols for mail that will ensure safe and secure transmission of vetted e-mail, causing disreputable mailers to fall by the wayside. But it could take years before this becomes a viable product, and users will have little choice in the meantime but to improvise a more secure Internet based on the best tools and techniques available.

Companies have considered implementing a tiered e-mail system for years, one that basically replicated the airline system of first- and business-class travel versus economy class. AT&T is already planning a service that will let companies pay a subscription fee to provide guaranteed delivery.

The founding fathers of the Internet created the Internet predicated on a high level of trust, never anticipating firewalls and anti-spam software, let alone

e-mail sender spoofing. Now this trust has been betrayed, and the very foundation of the Internet is at stake. And it will be a form of trust, albeit via technology, that will restore the confidence of users in the network.



ABOUT BASEX

Basex is the independent research and analysis firm that pioneered Collaborative Business Knowledge research. Basex provides clients with expert intelligence on the technologies, benefits and best practices that facilitate the exchange of critical knowledge and information.

We are the recognized experts in Collaborative Business Knowledge, the intersection of content, knowledge and collaboration within the enterprise –with a 20-year track record of accurate research and visionary analysis that drives its clients to make the right technology decisions for their business.



**Knowledge. Analysis.
The Right Decisions
for Your Business.™**

The Empire State Building
350 Fifth Avenue / Suite 3304
New York, N.Y. 10118

☎ +1 212 725-2600

🌐 www.basex.com

✉ answers@basex.com

ABOUT THE AUTHOR

Jonathan B. Spira, CEO and Chief Analyst, founded Basex in 1983. He is recognized as one of the technology industry's leading thinkers and pundits, having pioneered the field of Collaborative Business Knowledge, which is the intersection of content management, portals, knowledge management, and collaboration. Mr. Spira, who directs all Basex research and analytic activities, is a founding board member of the Association of Internet Professionals whose columns are syndicated widely. A recognized expert in Collaborative Business Knowledge and related market segments, Mr. Spira makes frequent appearances speaking on the future of technology and has authored hundreds of papers on technology issues. He is the co-author of *The History of Photography* (published by Aperture), which was named a best book of the year by the New York Times, and a graduate of the University of Pennsylvania. He conducted graduate-level research at the Ludwig-Maximilians Universität (Munich).



The Empire State Building
350 Fifth Avenue / Suite 3304
New York, N.Y. 10118

☎ +1 212 725-2600

🌐 www.baseX.com

✉ answers@baseX.com