SPAM WARS

Our Last Best Chance to Defeat Spammers, Scammers, and Hackers

DANNY GOODMAN

SelectBooks, Inc.

This edition published by SelectBooks, Inc., New York, New York

First Edition
1-59079-063-4

Library of Congress Cataloging-in-Publication Data

Goodman, Danny.
Spam wars : our last best chance to defeat spammers, scammers, and hackers / Danny Goodman.-- 1st ed.
p. cm.
Includes bibliographical references and index.
ISBN 1-59079-063-4 (hardcover : alk. paper)
1. Electronic mail systems. 2. Unsolicited electronic mail messages. 3. Computer networks--Security measures. I. Title.
TK5105.73.G66 2004
004.692--dc22
2004010099

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

CHAPTER 1

Email Predators, Guardians, and Victims

Electronic mail—email—is under attack. I'm not talking just about your own email inbox, but the entire concept of email as a reliable, desirable, and speedy communications medium. Important mail you want to receive—if you receive it at all—is often buried among piles of unwanted email messages that do the following:

- Clog your inbox with offers for products you don't want (or wouldn't use even if you had the necessary body parts).
- Lure you to buy products that never come (and that might kill you if they did arrive).
- Trick you into infecting your computer with viruses and worms ("Check this out, Dude!").
- Dupe you into divulging personal identifying numbers to outright thieves ("Please re-enter your account details with our security department or we will terminate your account.").
- Embarrass or disgust you or your children with blatantly pornographic images ([blush]).

To defend inboxes from nonconsensual contact, you or your email provider may feel compelled to apply email filtering that blocks or quarantines spam and viruses. But aggressive filters are quite capable of inadvertently refusing or discarding messages you want, all without your knowledge. Less draconian filtering may instead divert suspect messages into a separate folder, whose

contents must be scanned with a human eye to make sure no "ham" gets tossed out with the spam—as if scanning through junk mail in batches were any less annoying or time-consuming than having it in your inbox.

Even if spam filtering were perfect, messages that appear to be from people you trust (and thus glide right past computer and human barriers) may actually be virus- or worm-laden, sent unknowingly from a computer owned by your best friend. If you then open the email attachment, you've just performed the computerized equivalent of exposing yourself, in one dramatic swoosh of your trench coat, in Times, Red, and Tiananmen Squares at the same time.

So we're now stuck with a broken system in which email you want to receive may never reach you, email appearing to be "from" people you know may be data-deadly, and tons of unwanted crap still comes through unless you use a service that literally blocks anyone you don't already know. Worse, you pay the "postage" for every piece of email that arrives at your inbox, just as if you were required to pay postage due on physical mail addressed to you.

I ask you: Is this any way to run a post office?

As much as my rant up to now sounds like a description of a traditional conflict between good and evil, the decay of the email system is not attributable to only two clearly defined sides. Numerous participants play vital roles in the drama, roles that fall into four main groups I've identified:

- **Originators**, who send the stuff
- **Facilitators**, who help Originators accomplish their goals
- **Guardians**, who try to protect us
- **Victims**, who suffer the most

Unfortunately, the systems and individuals throughout the email world have competing agendas and use different terminology relating to the problems and potential solutions. Some players even regard the solutions *as* the problems. That's why trying to clarify the issues surrounding email spam, scammers, and hackers is such a freakin' mess.

To help make sense of that mess, let me introduce you to the players, the *dramatis personae,* of the email tragedy.[1] These are the constituencies who wage wars—in tones ranging from inaudible whispers to violent rages—for their email causes. In all honesty, my sympathies lie with very few of these characters. You'll probably figure that out as we go along and as I discuss them in more detail throughout the book.

---

[1] *Dramatis personae* is Latin for "masks of the drama," otherwise known as the cast of characters. The primary meaning of *persona* is a full head mask, as worn by players of Greek and Roman (and probably other ancient) dramas. (See, I knew my college degrees in Latin and Greek were not in vain.)

CHAPTER 2

Grasping Spam (not SPAM®)

You can't accuse someone of sending it, you can't compose a law to limit or ban it, you can't issue a complaint about receiving it, and you can't sue someone for screwing up your system with it, unless you can precisely define what "it" is. And, because human languages tend to be imprecise (what with connotations, innuendos, and lies), the likelihood of all email constituencies voluntarily agreeing on a single, unambiguous definition of "spam" is zero.

This situation isn't anything new. I mean, take murder. You'd think that taking another human's life was murder, plain and simple. But it's not always either plain or simple. For example, depending on the circumstances and motivation of the killer, the offense may be treated as first-degree murder, second-degree murder, voluntary manslaughter, or involuntary manslaughter. Killing in self-defense or in an act of war (among other situations) disappears from the murder radar entirely, and is called justifiable homicide. And the French have this whole *crime passionnel* thing.

A suitable definition of spam usually starts out simple, but then becomes complicated with the addition of several conditions and subclauses to address human nature and the imprecision of language. If you try to keep the definition simple, then high-volume email senders will slither through loopholes and swear on a stack of Bibles that they do not spam.

Before I get to defining spam, it's worth looking into where the term originated. My love of Latin and Greek etymology doesn't help us here, because that one-syllable word didn't exist in the English language until New Year's Eve in the hours leading up to the year 1937. By the end of 1936, George A. Hormel & Company had 45 years' experience producing, packaging, and

selling pork and other meat products. Although the company had been selling canned hams since 1926, it developed a new product made from pork shoulder, other pork meat, and spices, all contained in an unrefrigerated tin can. The product was to be released in 1937, originally with the name Hormel Spiced Ham.

But the name didn't have quite the marketing zing a new product needed in the depths of the Depression, so Jay Hormel, second-generation president of the company, held a "contest" at his New Year's party to see if any of his guests could come up with a better name. I don't know what this party was like, but I have this vision in my head derived from 1930's movies, in which the wealthy classes who had managed to avoid the worst of the Depression motored around in Stutz Bearcats and lit cigars with $100 bills. The world existed only in shades of gray.

Attending this party was one Kenneth Daigneau, a Broadway actor and (nudge, nudge, wink, wink) the brother of one of the company's executives. Without too much wit, in my opinion, he compressed "spiced" and "ham" into "spam," winning himself a quick hundred bucks from Jay Hormel and eventual immortality on the Internet.[1]

The product, trademarked in all uppercase letters as SPAM, hit the market in the 1937. World War II, despite its ravages in many parts of the world, turned out to be a bonanza for Hormel and its new product. In the United States, meat was rationed and difficult to obtain. SPAM was not (not because it didn't contain meat, so put down your joke-making machine), and thus became a staple at home during wartime. It was available in Britain, as well. Former Prime Minister Margaret Thatcher once reminisced about how SPAM was, in her words, a "war-time delicacy" (poor sods). That the meat didn't require refrigeration was a boon to the military supply lines, which managed to keep the boys on the Allied front lines (western and eastern fronts, according to testimonials from Dwight Eisenhower and Nikita Khrushchev) supplied with SPAM. And SPAM. And more SPAM. Which brings us to the true start of the connection between the meat and email.

Hormel shipped its two billionth can of SPAM in 1970, and in December of that year, the BBC first aired the twenty-fifth episode of a popular television show called *Monty Python's Flying Circus.* The program, an homage to farce, poked fun at every sacred cow it could find, seemingly taking especial glee in both lampooning and glorifying the British working classes in the same breath. A sketch at the end of episode 25 takes place in (as we learn

[1] Daigneau's connection with the naming of SPAM outshines his legacy as a Broadway actor. The Internet Broadway Database (www.ibdb.com) lists him appearing in only three productions between 1923 and 1937. (Sometimes I wonder if using Google can lead to Attention Deficit Disorder.)

later) the Green Midget Café in Bromley. As the scene opens, most tables are occupied by men dressed in full Viking warrior regalia (logic was often the first casualty of any *Python* sketch). Mr. and Mrs. Bun enter the café—not the usual way, but floating into their seats from overhead wires.

Mrs. Bun and the Waitress are played by Graham Chapman and Terry Jones, respectively, speaking in shrill and forced women's voices that could shatter glass. Mr. Bun (played by Eric Idle) inquires about the menu, and the Waitress replies:

> *Well there's egg and bacon; egg sausage and bacon; egg and spam*[2]*; egg, bacon and spam; egg, bacon, sausage and spam; spam, bacon, sausage and spam; spam, egg, spam, spam, bacon and spam; spam, spam, spam, egg and spam; spam, spam, spam, spam, spam, spam, baked beans, spam, spam, spam and spam.*

Upon hearing that, Mrs. Bun innocently asks if they serve anything without SPAM in it because she doesn't want any SPAM. After more back-and-forth, it becomes clear that everything on the menu has at least some SPAM in it, to which Mrs. Bun shrilly replies:

> *I don't like spam.*

Suddenly the Vikings start singing a song with the words:

> *spam, spam, spam, spam, spam ... spam, spam, spam, spam ... lovely spam, wonderful spam ...*

To quiet the Vikings, the Waitress yells "Shut up! Shut up! Shut up!" This exchange continues for awhile, each time the menu items revealing more and more SPAM, at which point the Vikings start up their song again, and the Waitress ends it all with "Shut up! Shut up!"

The routine goes on for just a bit more, but if I try to describe the Hungarian tourist and ensuing nonsequiturs, you'll think I'm one of the escaped and lobotomized mental patients that frequently appear in the program. The lasting impression most viewers got from this sketch was an ever-increasing presence of SPAM mindlessly overtaking everything.

Although *Monty Python* was originally a BBC program, it soon found a following in the United States with the help of local Public Broadcasting Service (PBS) stations, which were accustomed to importing programming from the United Kingdom to fill their commercial-free broadcast hours. In the 1970s and into the 1980s, there was scarcely a PBS station that didn't run the *Python* episodes year after year. The program developed a genuine cult

---

[2] The published script uses the nontrademarked version of the word "spam," but the meaning is clearly for SPAM. The full script text can be found in *The Complete Monty Python's Flying Circus, All the Words,* Volume 2, Pantheon Books 1989.

CHAPTER 6

How Spammers Get Your Email Address

An email address is a funny thing. Not funny ha-ha. Funny strange.

On the one hand, most of us willingly display our email addresses on Web sites, in public forum messages, and on our business cards. The goal of such exposure is to make ourselves accessible to others—including strangers—who share our interests and wish to engage in one-on-one personal communication about topics dear to our hearts. On the other hand, most of us treat our email addresses as something private. It is a globally unique identifier, yet (thankfully) no global master email address directory exists. Someone who wants to send a message to your address must know that magic combination of letters and numbers.

The trouble with spammers is that they misinterpret the boundaries between the public and private spheres of an email address. Does including your email address on your Web page with a link that says "Email me!" mean that you invite anyone to send you mail about anything? Many spammers would answer a resounding yes! But your original intention was to be courteous on the Web, and perhaps to hear from others who want to contribute to your site. Too bad. You may think of your email address as being private property, but once it's "out there," you can never reel it back in.

There it is: a sequence of several characters with an @ sign and a dot or two that, once exposed, can be traded, rented, and sold for real money (in the spamonomy) without your permission or knowledge; a character sequence that allows strangers to use up your bandwidth, mail server disk space, PC disk space, and time without your permission; a sequence that, no matter how much sanctity you ascribe to it, will be desecrated by spammers who couldn't care less.

CHAPTER 9

How Spam Differs from Junk Mail

One of the spammer's arguments in favor of their type of advertising is that spam is no different from the bulk mail that arrives, sometimes voluminously, in your postal mail box. Spammers using this defense cite statistics about how many trees gave their lives to produce the paper on which the flyers and catalogs were printed; or the hundreds of thousands of dump trucks full of junk mail that head to the land fill each year.[1] Then they cite how environmentally friendly email is, regardless of quantity, frequency, or aggravation.

Certainly not all consumers are fond of advertising mail. It didn't get its "junk" moniker because folks love the stuff unconditionally. In Australia, you can even put a sign on your postal mailbox to reject delivery of junk mail.[2] On the other hand, there is a good chance that you are receiving this material in the mail because somewhere along the line you purchased from a catalog or a store that sends out mailings, subscribed to a magazine, attended a seminar, or in some other venue filled out a form that included your name and address. That makes your mailing address a valuable commodity, not only to the company that sold you some goods, but to other companies that rent the seller's mailing list for complementary or related merchandise. Unless you specifically opt out of receiving future mailings from the original company, you'll stay in the database of mailings for a year or more, receiving additional mailings and catalogs from time to time.

[1] They forget to mention how much of that gets recycled, but I split hairs.

[2] Unlike the United States, Australia allows advertisers to deliver flyers and catalogs to postal mailboxes without going through the post office. This has led to abuse, overstuffed mailboxes, and a litter problem. Advertisers who do this "letterboxing" by and large respect the wishes of the "No Junk Mail" stickers.

If some of this terminology—address, opt-out, list rental—sounds spammish, you're right, to the extent that many companies and organizations with long traditions in direct mail have tried to adapt their industry to the email delivery mechanism. In truth, the "snail mail" order world is far more sophisticated in linking your address to more detailed demographic information that becomes part of the value of your address when other mailers rent lists. Using computerized techniques called *data enhancement* or *data appending,* mail order companies associate your name and address with information such as the types of products you buy, the size of your order, and how often you buy. If you knew the ways your name and address were being compared and blended into myriad demographic segments and census data, you'd probably freak out.

Just as there are stupid spammers, not all conventional mail order companies are on the ball. If they (or the service bureaus that run the mailing list computers) don't do a good job in a process called *merge-purge* (merging multiple lists and purging the duplicates), you may receive three copies of a catalog in one day mailed to slightly different variations of your name and address. Sometimes your name gets into a demographic category that makes no apparent sense to what you think your mail order buying habits are.[3]

Despite numerous similarities on the surface, substantial differences separate the typical spam message in your computer inbox from the direct mail record club, credit card application, magazine subscription, and gadget catalog offer arriving in your postal mailbox. Here are the high points.

Goal of a Mailing

Direct Mail: The cost of acquiring a new customer is so high that a mailing to a list of prospects is aimed at not only converting a prospect into a paying customer, but, ideally, building a relationship with the customer so that he or she will continue to buy from the mailer in the future. It's not uncommon for a direct mail company to expect to lose money on the first order in the hope of keeping that customer long enough to get another, more profitable order going in a subsequent mailing.

Spam: If the advertiser really does deliver a product or service described in the email message, the primary goal of the high-volume spammers is to make one sale. The cost of goods is so small that there is sufficient profit (even after paying the spammer and/or affiliate) in each sale to make a prof-

[3] And yet, when a single, heterosexual male finds a Victoria's Secret catalog in his mailbox, suddenly it's not all junk mail.

CHAPTER 12

Spammer Tricks Part Two: Messages

In this chapter, I continue the parade of spammer tricks, here focusing on the message body. Most of the body tricks are designed to bypass computerized routines that perform spam filtering and reporting, while others are explicitly meant to trick the recipient in a variety of ways. If you simply view or preview messages employing most of these tricks, you won't notice the tricks because they're buried within the HTML coding. In fact, most of these tricks rely on recipients using email programs that render HTML just like a Web page. The "biggies," such as Microsoft Outlook (all flavors), AOL, MSN, and the Web-based email services like Hotmail, all do this.

To uncover whether a suspected spam message is trying to pull the wool over your or your mail software's eyes, you'll need to look at the source code view of the message. Despite the complexity of reaching the source view in some email programs, it is something I strongly recommend that everyone do for every suspicious message.[1] Viewing a message's source code (without first viewing or previewing the message) is the safest way to scan a message to find out if it's something you want to read "for real."

The problem with viewing the source code is that a lot of times it looks like pure gibberish to the nontechnical user. In many cases, you are, in fact, seeing gibberish, as various tricks confirm. But even a legitimate message that has HTML coding in it (as all messages from AOL and MSN, for example, do) can look pretty scary with all those angle brackets and strange words surrounding the message content. That said, the more you see this stuff, the more comfortable you'll be with it, even if you don't understand all of the codes and

[1] I supply instructions for Outlook users in Chapter 17.

CHAPTER 13

Beware Geeks Bearing Gifts

Any marketer on planet Earth will tell you that the word "free" is the most powerful tool in a promoter's vocabulary. What an amazing hold the notion of "gettin' somthin' fer nothin'" has on the human psyche. It's an irresistible attraction.

Precisely what hackers and scammers are counting on.

Thanks to the public's eager adoption of free downloads of music, video, software, screensavers, pornography, and other stuff, millions of PCs around the world are now burdened with add-in programs that run in the background to do things like:

- Change your browser's home page to an advertising site or portal not of your choosing.
- Display pop up windows advertising products that are related to the content on Web pages you visit.
- Replace a Web site's banner ads with ads from other sources.
- Capture every character you type, including Web site addresses, user names, and passwords, and report the content to individuals you don't know.
- Intercept Web searches by taking you to a search engine not of your choosing.
- Turn your PC into a proxy server for mailing spam and/or redirecting spam links to the spamvertised Web sites.

- Install additional software on your machine at the whim of a hacker somewhere else on the Internet.
- Take complete remote control of your PC.

It's not just gullible computer newbies who have their computers overrun by software known as adware, spyware, and malware (as in malicious). The avenues of entry for most of this stuff include the following:

- Installation of free programs (including well-known music-sharing services) and some media players
- Anonymous or forged viral emails containing executable attachments
- Instant messaging (IM) and Internet Relay Chat (IRC)
- "Greeting cards" from anonymous senders and even best friends
- Web pages and emails exploiting numerous unpatched security holes in Microsoft Windows and Internet Explorer for Windows
- Blatant software installations whose long-winded, legalese license agreements tell the user in language as clear as mud that the software does potentially nasty stuff
- An infection spread over a local area network (LAN) initiated from a computer that got infected via email, Web site, IM, or IRC exploit —including the laptop that was connected to a home network last night

Most users whose PCs are infected with spyware (I'll use that term to encompass it all) don't know that somebody else's software is controlling their Web browser or forwarding home banking logins to heaven-knows-where. Inexperienced computer users typically attribute bizarre behavior of their machines to the mysteries of PCs, and shrug their shoulders when the browser starts up today with a different home page hawking cheap vacations or mortgage refinancing. Any home computer used by youngsters is extremely vulnerable because kids tend to put more trust in free software offerings put before them; their friends pass along links to "cool stuff" that is easily downloaded for free, and then infects the new machine.

Despite the risks, there is plenty of good stuff available for free download on the Internet that doesn't carry any of this spyware baggage. Knowing which free software is good and which will open your machine to Bad Guys is very difficult to determine. The Web sites hosting the most vile software could look very slick and professional, while the safest open source package may come from a page that looks like it was thrown together in two minutes.

CHAPTER 15

Technology as a Partial Solution

Ask a typical computer programmer or systems engineer how best to tackle spam, and the suggestions invariably involve technical solutions: software on PCs, software on servers, new email protocols, fee-for-sending systems, and so on. This is only natural, because to many computer folks, spam seems inherently like a technical disease in need of a technical cure.

It turns out, however, that just as there are different types of spammers, email recipients come in all shapes and sizes, and have various likes and dislikes. One technical system—at least of the ones proposed and implemented thus far—does not fit all. Antispam nerds have been pursuing this problem for over a decade, and we're no closer to a universal solution today than we were when spam first appeared. Some technical solutions work great for some email users, but others see those solutions as merely masking the symptoms of a more insidious disease that may need drastic surgery to cure completely.

Now that hundreds of spam-fighting products and services are available to individual users and system administrators, I'll leave it to others with testing facilities to evaluate and recommend some products over others. One Web site you can use as a starting point for your own software investigations is spamotomy.com. Also look into the Web sites and publications that produce independent comparative reviews of competing systems (infoworld.com, pcmag.com, computerworld.com, cnet.com).

Most spam-fighting products, out of necessity, employ a blended approach. One type of filtering or blocking is usually not enough to keep the spew at bay. What I hope to explain in this chapter is not any particular product's prowess at keeping spam out of your hair, but rather the basic types

of antispam technologies being hurled at the tidal wave of unwanted garbage. I choose this way to describe the technical approaches because I hear too many new recruits to the spam-fighting platoons say things like, "Why don't we just…?" as if one technique would solve the world's spam problem. While a particular idea may be a good one, it's important to understand why it might fail in other circumstances or contexts.

In case you're wondering, I use a home-grown variation of a long-available free utility program that I've tailored to the spam and ham (mail I want to get) that arrives at my server. Since I control my own mail server, I have the luxury of pinpoint control that most email users don't. I'm able to keep almost all spam out of my personal computer's inbox—my primary goal of spam control. And I don't offer my system to others because it is a custom fit for the way I run my email server; I wouldn't presume it would work as well for any other server or user.

This chapter presents the top technical solutions that have been proposed and/or implemented so you can see the range of ideas and activities ultimately aimed at eliminating spam from reaching every user's email inbox. The basic categories are:

- Server-side[1] content filtering
- Server-side IP blocking
- Server-side whitelisting
- Server-side authentication
- Upgrading or replacing SMTP
- Challenge-response systems
- Email fee systems
- Disposable email addresses
- Client-side content filtering
- Client-side whitelisting
- Individual spam reporting
- Electronic attacks

[1] "Server-side" means that the operation takes place either on the mail server that initially receives the mail (called a gateway in administration-speak) or on a server hosted by an outside service whose job is to perform the necessary filtering before the mail is passed back to the receiving domain for distribution to users' inboxes. Some commercial spam-fighting products work only on the mail gateway; others require forwarding all mail to the outside service.

CHAPTER 16

The Law as Partial Solution

Just as geeks turn to technology for the ultimate spam solution, politicians head for the legislatures of the world to enact laws that attempt to satisfy the demands of their constituencies. The job of lawmakers might be easier if it weren't for the fact that their constituencies consist of parties on both sides of the issue: those who send spam ("unsolicited email marketers") and those who don't want to receive spam ("solicited email marketees").

It sounds very pure and righteous to label some activity "illegal." The threat of committing an illegal act is not that you're going against the law, but that you might get caught and be punished for your illegal action. Even with those threats, I doubt in recorded history that the imposition of a law has completely prevented everyone from committing the illegal action after the law was enacted. Typically, a law is enacted to *stop* something that has been going on. I mean, look at all the "not" provisions in the Ten Commandments. Even the positively-worded one about honoring thy mother and father probably came to mind because for centuries kids were being kids. What that commandment is saying is: "Thou shalt *not* dis the rents."[1]

Enacting laws against spam activity in many parts of the world has been a tedious process, but started gaining traction in 2003 in places like the United States, the European Union, and Australia. The implementations are uneven (some would say "hollow" about the U.S. law), but there is an inkling that lawmakers in some parts of the industrialized world recognize that spammers who have exploited an unfettered system have gone too far in placing undue burdens on Internet networks, systems, and users.

[1] Translation for adults: "Don't disrespect your parents."

One overriding factor undermines even the most strident lawmaking efforts: Spam and the Internet operate on a global level, but laws so far have been limited in their jurisdictions. The global nature of spam and the local nature of laws seem to be rather difficult concepts for individual users afflicted by spam to comprehend or reconcile. Behavior of the worst of the spammers, who utilize offshore resources for mailing or Web site hosting, and who use multiple layers of redirection, relaying, and hijacking others' systems to disguise the audit trail, make it extremely difficult—at times impossible—to build a legal case that can successfully prosecute the offenders. Just because a prosecutor can look at the source code of a spam message and quickly identify a half-dozen apparent violations of a local law's antispam provisions doesn't mean that there is sufficient incentive or evidence to locate and convict the perpetrator. As you'll see later in this chapter, building a bulletproof case is much tougher work than hiring a bulletproof mailing or Web hosting service.

If I wanted to bore you to tears, I'd provide annotated versions of spam-related laws currently on the books. Instead, I'll simply run down the main issues that various laws have addressed (or ignored, as the case may be). Please note: *I am not a lawyer, nor a professional legislative analyst;* I'm just a regular guy trying to make sense of the laws that have been enacted. Some issues covered by laws are "no-brainers" in that they occupy a common ground in the fight against spam. On several other issues, however, various legislatures seem to be under the same misapprehension as lots of citizens: that making something illegal will inhibit the activity, so there's no need to make the laws very restrictive, lest the laws appear to infringe on other existing legal rights.

I'll be paying particular attention to three recently enacted laws that affect a large segment of the Internet population using Latin alphabets:

Name	Jurisdiction	Passed	Effective Date
The Privacy and Electronic Communications (EC Directive) Regulations 2003	United Kingdom	September 18, 2003	December 11, 2003
Spam Act 200	Australia	December 12, 2003	April 11, 2004
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003	United States	December 16, 2003	January 1, 2004

INDEX

C

D

E

F

G

J

K

L

M

N

O

S

T

U

V

W

X

Z