Final revised text of this interim version was published in August 2005 and is available for free download at

<http://www.freesoftwaremagazine.com/free_issues/issue_06/neednt_eat_spam/>

Note that graphic images therein are separately downloadable by clicking on the token image embedded in the online article itself.

You Needn't Eat Spam (Nor Worms)

by

Jeffrey Race

INTRODUCTION

Spam, also known as UBE or Unsolicited Bulk Email, is a superficially intractable problem in fact easily solved with simple insights known to every parent. The wonder is not why spam is so troublesome, but why it has persisted so long when solutions are so simple.

A pestilence in its own right, spam is also the dead canary sternly warning us that the new communication and control system the world will inevitably come to rely upon for mission-critical tasks is dangerously vulnerable to catastrophe from any seriously talented programmer with a motive for world chaos[1]. (Recall that Goner, one of the world's worst viruses so far, was written by Israeli 14-year-olds using the software equivalent of an Erector Set.) Spam and related threats are set to worsen greatly with the move to high-speed connectivity into the homes of a new generation of point-and-drool users loaded with Microsoft Windows enabling raw socket access by default.

This vulnerability is not inevitable; it results from the negligent operation of the Internet, sacrificing security to profit and all-too-human laziness on what is known elsewhere as the Environmental Polluter business model. ("It's cheaper to dump our waste in the river than to buy pollution-control equipment.")

Internet security is today where America's airport security was on September 10, 2001, and the consequence of this sad state of affairs is likely to be just as devastating in property if not in life, unless corrective measures are taken. The same present-day negligence that brings you spam also increases vulnerability to viruses, worms, Trojan horses and sabotage. As with drunk driving, change will come only when people get mad and decide to do something about this eminently preventable menace.

Individual victims, and many Internet Service Providers (ISPs), now employ filters to stem the incoming flood, but this *sauve qui peut* measure leaves intact the burden on the network. A step up is using utilities like Spamcop,[2] which actually aim to report spam to a responsible party, but this palliative fails to prevent spam at the system level and blunts only the upload but not the return path (more on this in a moment). More importantly it violates fundamental wisdom about large human groups: as William Haddon taught us with traffic safety, any endeavor relying on large numbers of people all to do the right thing is bound to fail. Instead one must place responsibility on the few people who can most easily fix the problem, and rigorously monitor their performance with public oversight or private standards bodies.

WHAT IS SPAM?

Spam is e-mail sent unsolicited in bulk. Content (commercial, political, charitable) matters not at all. Spam has no relationship to free speech, privacy or anonymity, but is all about theft, fraud, and unjust enrichment. Spam burdens ISPs and backbone providers (who link ISPs) in wasted staff time and computer and communication resources. It is a burden on the recipients in opening, sorting, and deleting, and in clogging hard drives and incoming mail channels. And lots of spam

is damaging both to society and to the recipient: child porn, consumer fraud, stock swindles.

WHY SPAM HAPPENS

How can this pestilence continue to worsen, when other serious social problems are stable or declining? (Think Osama bin Laden, drug abuse, drunk driving.)

Simply because the Internet now runs by ignoring basic principles of human behavior known to every parent, and universally applied elsewhere in civilized life:

* Everyone is responsible for his actions.

* Actions are traceable to their authors.

* Actions bring to their authors good or ill, according to their impact on others.

In short, spam exists because action is divorced from consequences. *That* must be fixed.

HOW SPAM HAPPENS

A spammer must upload from his own computer in order to reach victims, and he must create a return path for the few who buy. Upload must go by the Internet, but the return path may be via Internet (e-mail or website), or via fax, phone, or postal mail.

A few years back most spammers used e-mail accounts in their own (or phony) names directly to upload spam, but ISPs soon blocked this path by technical means. In the competition that characterizes most of human life, the spammers then grew cleverer and now employ a variety of advanced upload methods such as open mail relays (currently more than 100,000, mostly abroad), insecure web proxies and malformed CGI scripts on mail servers.

However the spammers still must connect to the Internet, and there is virtually no legal way to upload spam in the USA, due to contractual bans imposed by backbone providers such as UUNet (part of MCI) and PSINet on their ISPs, who in turn impose these bans on their users. Uploading spam always entails one or more offenses like tort, Terms of Service fraud, violation of contract, or criminal activity such as trespass.

Many providers also contractually bar websites or e-mail accounts promoted by spamming, and the sale of spamming software utilities (the Internet equivalent of burglar tools).

Spam continues because many ISPs fail to enforce these simple rules against their customers, and the backbones do not enforce the rules against the ISPs. Spam enters the USA because of a lack of equally simple rules easily adopted and enforced.

Why can't the service providers, and the backbone providers, enforce the contracts?

They can, and many do, choosing to operate ethically. Those who don't are driven by money, opting for the Environmental Polluter business model. Anything you hear to the contrary is the same self-serving propaganda we heard from all the polluting industries of the past.

But don't believe me; hear the words of a successful spammer himself, "Brian", posted to a spam-support group to advise budding Internet fraudsters:

> "ISPs are a dime a dozen and should be grateful for your business. There are also hundreds of hosting services, likewise hungry for business. They all have terms of use that ostensibly oppose 'spam'. But if they really meant business, why do I get hundreds of messages per day? . . . . They're in business to make money."

The sad fact is many Internet providers earn substantial revenue from the spam industry, so are reluctant to turn away paying customers. In the words of one inexplicably honest abuse-desk staffer, recently posted on the Internet:

PROVIDERS CLEAR OF OFFENDER AFTER COMPLAINT	PROVIDERS RETAINING SPAMMER AFTER COMPLAINT	PROVIDERS WELCOMING SPAMMER EXPELLED BY PREVIOUS PROVIDER
ATT-USA	UUNet	UUNet
BellSouth	Global Crossing	Global Crossing
	Sprint	Sprint
	Broadwing	Broadwing
	Verio	Verio
	Level3	Level3
	Exodus	Exodus
	@Home	@Home
	Abovenet	GT Canada
	PacBell	Qwest
	StarLan	Skynetweb
	Cable & Wireless	
	Concentric	

> "I am sad to inform you that we are not about to do anything with this spammer. It's not easy for our sales director to say 'go away' to a customer who pays approximately $2,700 monthly."

This is the first-approximation reality on the Internet. For big-time spam-enabling backbones like UUNet and Sprint and their downstream ISPs, abuse desks with their "thank you for your report" auto-replies aim to strike a balance, keeping the money coming in from their downstream ISPs while placating enraged victims with illusions of action. In fact the only effective action--cutting off polluting ISPs--is seldom imposed.

But there is more. We can see just how subtle is the issue by looking at two poles of the problem, a white-hat provider and a black-hat (in the jargon of the anti-spam community).

First, look at this table, recording the results of ten months of my own complaints about spamming to providers of connectivity for spam-promoted websites. Though the total number of complaints was only about 100 and so subject to a certain degree of error, some conclusions are overwhelmingly clear. How does such a pattern emerge? Let us study incidents with two firms running on differing models: AT&T and UUNet.

One involved a particularly obnoxious spammer connecting via AT&T in the USA. I made routine complaints without effect, and finally became so incensed (when the spammer caused great injury to a victim whose identity he stole) that I contacted the firm's general counsel in Basking Ridge, New Jersey. A senior attorney was assigned to the case, and after a short time that spammer was history, at least on AT&T. The firm behaved ethically, once a victim was able to stir management's attention.

A second case illustrates the problem even for an ethical firm. My complaints about another spammer-for-hire's continued use of AT&T Canada connectivity elicited the following explanation from the technical support supervisor.

> "The spammer in question keeps signing up with us with fake telephone numbers and credit cards. AT&T Canada does not have a system in place that automatically verifies credit cards. This is only noticed at billing. We authorize the user by calling him back at the number he supplies. Most likely the user is using a pay-as-you-use cell phone. I have been informed

that there is not much more that we can do from our end than to keep shutting this individual down each time he signs up."

In other words, the spammer repeatedly defrauded AT&T Canada civilly and repeatedly committed credit card fraud, a serious criminal offense. Management never adopted measures to detect the credit-card fraud as it occurred (not a difficult task, as anyone knows whose card has been rejected at the sales counter for being overlimit!) and never even made a police report. A few minutes of research at the Register of Known Spamming Operations[3] pulls up sufficient information on the spam principal's Internet rap sheet that a criminal prosecution would be trivial to mount. AT&T management did not do the simplest and most obvious things to prevent a repetition of these civil and criminal offenses, and indeed continued to extend service to the perp. Once I got attention of management, they acted. But little attention was paid until an irate victim created an embarassing scene.

Remember, AT&T is among the *best* the Internet has to offer.

At the other end of the spectrum consider my own experience of the most important Internet backbone provider: UUNet. On behalf of this firm and some others including PSINet and AOL, the Virginia legislature in 1999 passed a special law criminalizing spamming, a powerful tool if used since America's principal Internet mail servers are located in that state.

When I began researching this project I dutifully reported spammers using UUNet through channels but found they continued to be connected by UUNet. I finally found a sympathetic manager, John Bradshaw, but he was not empowered to act decisively against violators of his Acceptable Use Policy. Bradshaw referred me to UUNet's attorney Neil Patel, to whom I nominated egregious offenders, in one case even providing essentially a complete case file including legal service address. Patel declined to act, apparently under instructions. When I asked to whom I should speak in management to change the policy, he said "Mr. Ebbers" (then MCI's chairman). Bradshaw and Patel are no longer with UUNet, which obdurately refuses to take effective action against abusers. I retain in my logs to this day many outrageous offenders whom UUNet refuses to force its downstream customers to cut loose. (UUNet's contracts clearly empower it to disconnect downstream providers for malfeasance.)

Reality as seen from inside UUNet is instead one of "great progress". Abuse staffers point to new technical measures such as Port 25 filtering (which has dramatically reduced complaints against UUNet) and stress in their defense that they daily shut down dozens of offending websites. However the victim's reality is that UUNet abuse staff still operate (and fail to see they operate) within the endless loop dictated by management's Environmental Polluter business model. And technical measures like Port 25 filtering work only against the upload path, not the return path to spam-promoted websites hosted by UUNet's refractory downstreams.

Why don't UUNet and those like UUNet who accept customers thrown off other networks enforce the rules which exist on paper against spamming? They claim their abuse desks are overloaded with work. One shameless ISP, Easynet, even sends this brazen auto-reply to complaints:

"Thank you for your message to abuse@easynet.net. Your email has been received and will be processed in due course. Due to the overwhelming amount of email received at this address, you may not receive a human response."

It is hard to imagine a more candid confession of failure to secure one's network against abuse than this Easynet message. But consider these comments offered by one reviewer of a draft of this article, formerly abuse-desk manager for a Westcoast backbone provider:

"Some abuse desks, such as the one I

managed, were terribly understaffed and hampered by high-level refusal to enforce their policies against very large customers. In one case, a VP of [the backbone provider's parent company] decided that [a very large, high-volume, enormously-profitable customer] would not be cut off, despite numerous (thousands to tens of thousands at a minimum) well-documented instances of spamming *and* the recommendations my superior and of *his* superior as well. The managers and the abuse desk personnel were all terribly depressed by this hypo crisy, but we were powerless."

If one probes a bit deeper, more sad truths emerge. Spamperps now open multiple accounts and webpages under false names, spew out their spam, sometimes are shut down, then move to the next already-prepared account or webpage on the same host, and repeat their illegal behavior. Sometimes the accounts are for hire (as with AT&T) and sometimes they are free permanently (supported by advertising) or temporarily (a trial signup period). Abuse-desk staffers cheerfully call this whack-a-mole; engineers call it an endless loop.

Absence of identity checking permits this endless loop. When questioned, some ISP managers reply that they could not possibly earn a profit if they had to secure their networks against abusers. (Of course what they are doing is exactly what someone does when he leaves the keys in the ignition of his unlocked car in a bad neighborhood: allowing strangers onto one's property to injure others.)

What's wrong with this picture? It is precisely the Environmental Polluter business model: design a business to benefit by gathering revenue for the stockholders while imposing on outsiders the economic losses to society arising from one's polluting operations. Offending ISPs allege "no one would sign up for an account" if each had to be verified, which may be true as long as there are race-to-the-bottom providers extending connectivity to any malicious stranger. If no one could offer service allowing strangers to injure others, then the current competitive race to the bottom would cease. (Effective and innocuous measures exist to confirm identity, used by many firms in many sectors of our economy. A technical solution exists even to preserve anonymity by permitting but rate-limiting such accounts.)

Fortunately for our physical health, this business model disappeared years ago from the chemical and plastics industries through a combination of legislation and aggressive trial lawyers.

THE SPAMMER BUSINESS MODEL

Spammers have their own business model, aptly summarized as the Thousand Cuts, which meshes with the Environmental Polluters to victimize the rest of us. The spammers well know the illegality of their businesses but also know the pain is spread in small amounts among large numbers of victims, no one of whom can make an economic case for litigation. Even someone determined to act finds it difficult due to cumbersome legal procedures, the cost of discovering obfuscated identities, and the torpor of the agencies responsible for ensuring accurate databases.

WHAT AMERICA CAN DO

Spam is increasing because no ill conseqences befall the malefactors and their enablers. As every thoughtful parent knows, this method is guaranteed to raise antisocial offspring, and it has sure worked on the Internet.

What to do? Obviously, smash these two business models. Big, immediate improvements require no legislation and little or no litigation, just doing the obvious on the Internet comparable to what every loving parent does in rearing his children. Legal and procedural changes could have some role in terminating any residue after implementing the basics, but they are not essential to a vast and immediate drop in

spam.

Legislative hearings might however usefully spotlight the Environmental Polluter business executives, just as they were essential in smashing this model in the industrial sector.

The following steps can end spam as an issue for American internet users.

First and foremost, ISPs must use blocklists to *bounce* all incoming mail from polluting mail servers, rather than just filtering out incoming spam. This is the only method that works, and it works *immediately* (we're talking hours here).

Blocklists assemble the so-called Internet Protocol addresses of mail servers known to emanate spam. Numerous such lists are available, using various criteria such as whether the manager of the mail server is spammer-friendly, negligent in the operation of his mail relays, running insecure CGI scripts or proxies, disobedient to the ruling documents of the Internet known as RFCs, or complaisant to trafficking over his network in Internet burglar tools.

Some ISPs now use blocklists, bringing devastating consequences to spam-enabling mail relay operators and blissful relief to their own customers.

What happens when an ISP uses blocklists? All mail from polluting ISPs bounces back to the sender with a diagnostic message to the effect:

> "REJECT=550 Your mail is returned since transmitted from a spam-compromised mail relay at IP address xxx.xxx.xxx.xxx. Please contact your system administrator to bring this mail server into compliance with current best practice."

Immediately scores or hundreds of customers complain to the *offending* ISP, which is forced to manage its mail servers properly. This differs from the present state of affairs where the victims complain uselessly to their own (receiving) ISP, which can at best (in the absence of a blocklist) filter the spew from chronic polluters.

Even the best ISPs (including my own, AT&T) occasionally fall afoul of blocklists, but they cure the problem fast. Indeed it is almost comical how fast spamming stops when a blocklist is used, or even just threatened. Consider the case of Connect, one of Australia's largest ISPs, which long harbored a notorious spammer. At 10:00 a.m. on January 3, 2001, a group of concerned system administrators finally tired of politely asking Connect to shape up and instead laid down their new zero-tolerance policy: blocking would ensue that day unless Connect disconnected the spammers on its network. By 1:30 p.m. the spammers were gone, with no interruption in service. Merely the threat of disconnection from the Internet caused management to pull up its socks.

A similar incident occurred in late September, 2001, in Australia when Optus defiantly refused to cut spammers loose. Blocklist adoption by an important group of victims forced Optus to change its policy two days later.

In an equally dramatic incident Earthlink, an American ISP not famous for cracking down on spammers, was forced to sue abusers, stating in its pleading[4] that it finally had to act because blocklists jeopardized its Internet connectivity. Before the blocklists Earthlink was content to let injury accrue to the victims on other networks; after the blocklists began to bite, Earthlink was motivated to put its own house in order due to the magic of "actions have consequences".

Essentially blocklists keep unsafe ISPs from connecting to the Internet just as credit reports exclude defaulting debtors from the credit markets and pre-flight inspections keep unsafe planes out of the sky. Some inconvenience may arise until safety and security are assured but it is small, necessary, brief, and falls upon the offender rather than the victim. (No passenger feels enraged on returning from the runway to the gate when the captain announces the plane is unsafe.)

In fact when blocklists are announced in advance, as to Connect, there need be no service interruption at all.

To continue the air analogy, the rule to adopt is "If you're not flight-ready, you're not flying". You as an ISP fully comply in terms of customer traceability, contractual compliance, and message payload, or you are not going to connect to the Internet. If you are a backbone provider and you don't enforce these requirements on your downstream customers, you are cut off, just as an airline is shut down if not applying proper safety and maintenance procedures, or an airport is closed for lack of security. (This actually happened in Boston in 2001.)

Adoption of blocklists can be encouraged by customer demand, by pressure from public standards bodies, or even by government. Its effect might at first be to split the Internet into zones of purity and islands of pollution. As blockage expands, spammers will be pushed into ever smaller and less connected domains, which grow ever more blocked. This cumulative process would end quickly, with residual polluted areas populated by ISP customers who don't have much need to communicate with zones of purity.

People in today's worst offending areas (China, Korea and Taiwan) could still communicate with the rest of the world by phone or fax until administrators bring their systems into compliance. No one's life or property is threatened, unlike the present desperately unsafe system.

Second, every upstream provider must be required to verify (by testing) that all downstream customers are in compliance with current best practice. Some upstreams now do this; it is easy and would end the present controversy that the Internet must now essentially be policed by volunteers ("open-relay testers"). To end the controversy, this measure could be endorsed by appropriate standards bodies.

Third, two critical guardians of Internet integrity, ICANN and the the Regional Internet Registries[5] (RIRs), must be encouraged to start doing their jobs right. These bodies are charged in different ways with creating the "telephone directory" which allows Internet users to find each other. However the resulting database of identities is corrupted by massive registration fraud on the part of the spammers, precisely to prevent the victims from finding their tormentors. In ICANN's area of authority such a corruption is (again!) in principle impossible because an Internet domain name registrar contract of accreditation strictly requires correct and current contact data in the mandatory WHOIS database (under pain of disaccreditation). However many such registrars cheerfully make a living from spammers with fraudulent registrations and brazenly refuse to act against their outlaw customers despite vigorous and repeated complaints. ICANN is charged with preventing such complicity in fraud and is fully empowered to yank accreditation. However my own unhappy experience with ICANN confirms--to put it charitably--that no one there will be committed for psychiatric care due to obsession with suppressing registration fraud. (I requested but could obtain no information on any history of cracking down on the fraudsters or their registrar protectors. At least one fraud I personally pointed out to ICANN was ignored for many months. And how about the spammer whose legal service address, accepted by the ICANN-accredited registrar Opensrs, is the Mount of Olives . . . ?)[6]

The RIR's charters are less authoritative, itself a serious problem, and the community in which they are involved is aware of defects in the database. Again, personal contact indicates that that their headquarters staffs are not anguished with concern for the inability of victims to identify their tormentors; indeed many actively oppose measures to enhance accuracy ("not our problem").

The failure of both these critical organizations to perform their duties should be righted, if necessary by a critical public spotlight or even legislation. The present corruption of the public database of Inter-

net citizens makes life unnecessarily easy for the spamperps and unnecessarily hard for the victims.

Fourth, the legal profession in cooperation with anti-spam groups should aggressively attack the major spam-enablers, for which numerous legal grounds exist such as public nuisance, attractive nuisance and negligent enablement. It may be possible to recover huge money damages in view of the billions of dollars in annual losses provably resulting from wilful failure to enforce contractual agreements, and from negligent operation despite management's foreknowledge that damages are certain from their failure to adopt preventive measures. A car owner leaving his keys in the ignition must accept the consequences of foreseeable joyrides by neighborhood hoodlums. ISPs and backbone providers well know torts, or worse felonies, are being and will continue to be committed with their property but fail to adopt even the most obvious preventive measures. Why should this ridiculous state of affairs be allowed to continue? This arena is a perfect fit for class action because of the many small victims none of whose losses give rise to an incentive to sue.

Fifth, limited prosecutorial or administrative actions are in order. Many spammers are incorporated and it is not hard to see how their charters could be summarily revoked for violating their corporate charter, since spamming necessarily entails violation of civil and often criminal law. A quick and probably uncontested hearing should usually suffice. A few exemplary prosecutions *pour encourager les autres* could be mounted on a variety of grounds. One promising criminal approach is "fraud in the inducement". Violation of the "click to sign up" Internet account agreement would ordinarily be construed as a civil dispute, but a chronic pattern of contract violations where the spammer intends to violate *ab initio* is probably criminal conduct in many jurisdictions. Using this theory, public prosecutors could sue on behalf of the public, since major spam-enablers like UUNet refuse to use even the law specially crafted for them. The surprise here, of course, is that the Virginia anti-spam statute has remained a nullity due to disinterest by both public and private bodies.

Finally, some modest legislative action may be in order as a residual cleanup measure. Primary would be removal of existing immunities granted to ISPs and backbone providers, which would allow the full force of the law to be brought to bear by class actions for management negligence and for its adoption of the Environmental Polluter business model.

Also, fast-track procedures should be adopted to speed unmasking of spammers, who now hide behind toll-free numbers, maildrops and freefax services. In principle identities can be uncovered by subpoena but its cumbersomeness and the uncooperativeness of small claims courts prevent the emergence of an army of aggrieved private enforcers as has been effective in other public-interest areas like junk faxing and telemarketing. Simple administrative procedures could easily be established to release identities upon presentation of *prima facie* evidence of spamming. This would relieve the burden on public prosecutors, allowing them to save their limited resources for child porn, stock swindles and identity and intellectual property theft.

WHAT CAN AN INDIVIDUAL DO?

Don't just filter, or hit the Delete key, which only leave the burden on others. Be a hero--every person can. The shocking but well-documented fact is that although most spam victims whine and call for new laws, only a tiny fraction of one percent complains to responsible parties, allowing Environmental Polluter executives to live in peace. Whining produces nothing but a lot of hand-wringing press articles. But a polite victim, armed with full documentation, can go straight to the top (as I have done many times) and make it too uncomfortable for the facilitators to carry on serenely. Go after the lawyers, executives and board members of the enablers. If

necessary, phone them at home, or go to see them. Explain politely the Environmental Polluter business model. I have put many spammers out of business and played bit parts in several criminal prosecutions. It is fun, educational and good for your mental health.[7]

CONCLUSION

Don't be fooled by press articles bleating about the irresistibly rising tide of spam and the urgency of legislation. The solutions are clear, have worked for other industries, and orders-of-magnitude improvements can be had without new laws.

Measures to stop spam dead would also reduce security threats including use of the Internet for terrorism, fraud, sabotage and security/network threats like viruses, worms and Trojans.

One needs only to enforce existing contracts and management charters (e.g. ICANN's) and to apply the basic principles of civilization to the Internet. No one would fly an airline run like today's Internet. Why should we tolerate such misoperation of an ever more critical resource in modern life?

For Americans, spam is not inevitable. It is the predictable consequence of management decisions to use the Environmental Polluter business model and of the legal system to permit the Thousand Cuts spammer model. It can be stopped completely, within days, without lasting collateral damage, just like a brief hospital visit to recover from a dangerous illness, which spam certainly signals for the Internet. It takes only understanding, a few acts of will, and doing a few obvious things, just like the airport security measures now finally being adopted.

Recently my beloved daughter Jasmine (then just ten) was given to some misbehavior we thought she'd do better to lose. Talking with her rationally was like talking to Neil Patel at UUNet--she listened, then she went on misbehaving as before, much to the annoyance of her parents. When pressed, she declared she wished to discuss the matter no further, so we shut off her DSL connnection. Two days later the misbehavior disappeared. When the measures described above are adopted, that's how long it will take for spam to disappear from America.

1 <http://www.icir.org/vern/papers/cdc-usenix-sec02/index.html>
2 <http://www.spamcop.net>
3 <http://<www.rokso.org>
4 <http://web.archive.org/web/20011106203918/http://biz.yahoo.com/law/010925/90405-5.htm>
5 Supervision over domain name assignment falls to ICANN, the Internet Corporation for Assigned Names and Numbers. Internet Protocol addresses are allocated to users by four registries worldwide, ARIN (American Registry for Internet Numbers), APNIC (Asia Pacific Network Information Center), RIPE (Reseaux IP Europeen) and LACNIC (Latin American and Caribbean Internet Addresses Registry).
6 There are hints that ICANN's performance may improve; see its threat to Verisign over the latter's toleration of registration fraud, and Verisign's finally agreeing to do its job, at <http://www.icann.org/correspondence/mitchell-letter-to-touton-11sep02.htm>
7 For particulars of my novel approach see <http://www.camblab.com/nugget/nugget.htm>.

Version date March 28, 2003

Jeffrey Race, President of Cambridge Electronics Laboratories, developed an interest in spam when, while coding his firm's website, he discovered he could use neither a <mailto> tag nor a business e-mail contact address due to the foreseeable depredations of the spambots.

A practical proposal to end the spam menace, based on the principles outline above, is available for download at <http://www.camblab.com/misc/univ_std.txt>.

Comments please to <jrace@attglobal.net>