TABLET PC TEST DRIVE
Can a hardcore PC power user be happy with an Intel-powered clipboard?

ROBOT DOG!
Sony's AIBO takes on a living, breathing pup

PALM TUNGSTEN T
Reviewed: Palm's most innovative PDA in years

MAXIMUM PC

JANUARY 2003

MINIMUM.RS

STOP SPAM DEAD

▶ HOW TO CRUSH THE JUNK E-MAIL ONSLAUGHT—

EVERY STEP EXPLAINED

SOFTWARE AWARDS

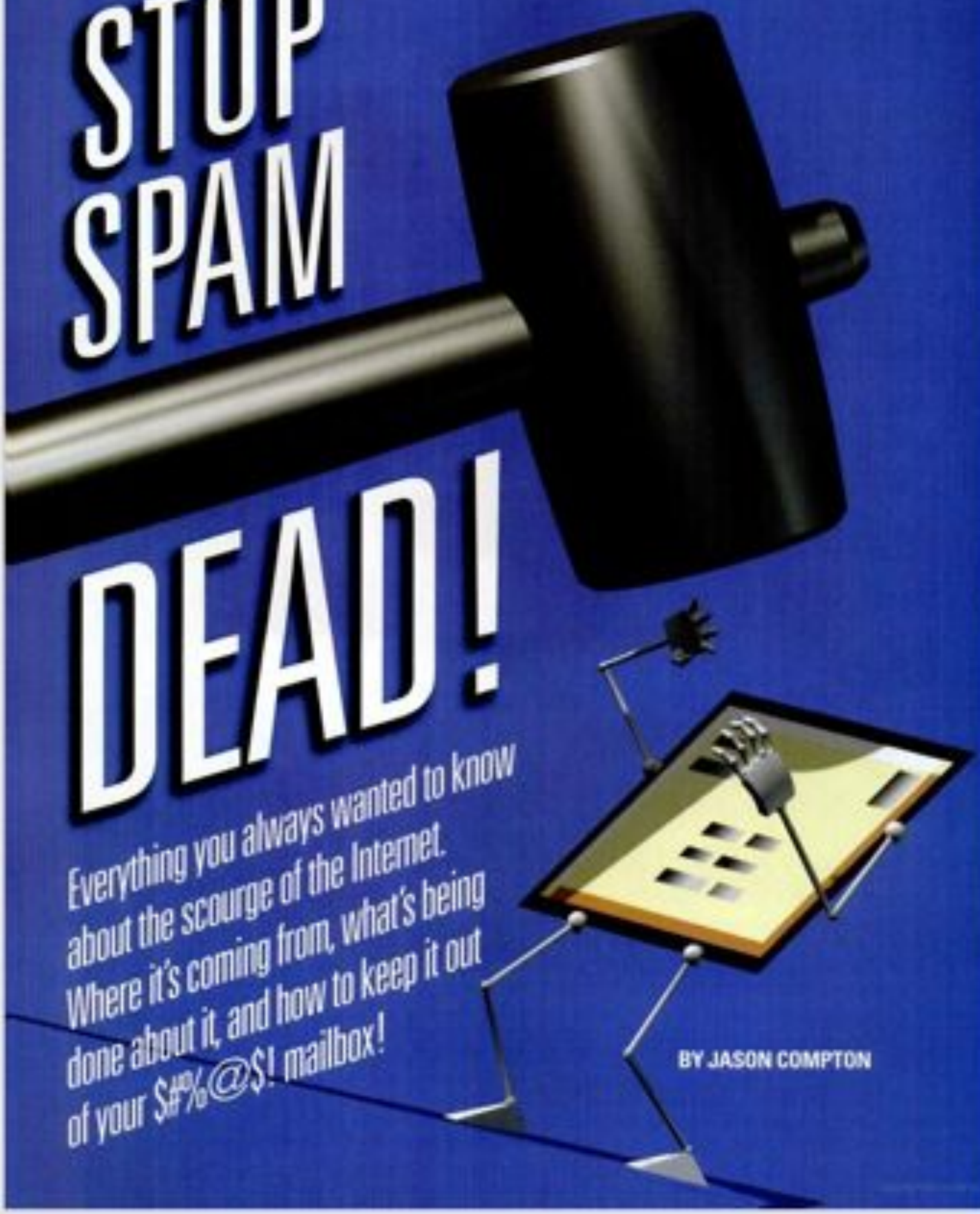
We pick the best apps and utilities of 2002. Our list cannot be disputed!

▶ MONGO CASE ROUND-UP

We rip apart and review 7 radical PC enclosures!

STOP SPAM DEAD!

Everything you always wanted to know about the scourge of the Internet. Where it's coming from, what's being done about it, and how to keep it out of your $#%@$! mailbox!



BY JASON COMPTON

INCREDIBLE INVESTMENT OPPORTUNITY IN NIGERIA!

HOT YOUNG AMATEURS ARE LOOKING FOR YOU!

GUARANTEED METHOD TO INCREASE THE SIZE OF YOUR...

Well, you get the idea.

If you use a computer, you know what spam is—and you hate it. We'd like to say that the government is taking action to prevent spammers from cramming our inboxes with scams that range from the insidious to the ridiculous. We'd like to think that legislation is coming to stop junk e-mail from chewing up bandwidth and mail server resources. But that hasn't happened yet.

In one published report, Microsoft stated that four out of five messages handled by its Hotmail servers are spam—and Hotmail has blocks to ditch far more than that before delivery! Similarly, the spam-filtering service provider Brightmail reported that it tracked more than 5 million "spam attacks" in August alone (one attack being a particular mailing incident, which could lead to hundreds of thousands of e-mails). One in 20 of the spam attacks was a flat-out scam. One in nine contained porn.

Spammers are getting sneakier and sneakier, and they're not going away. The ones with "legitimate" products to sell make their business model work by closing just a few sales to cover their spamming costs. And as for the rest? "Spam e-mail gives people the opportunity to get a fraudulent offer in front of millions of people for low cost," says Bryson Gordon, product line manager at McAfee.com. "The potential criminal payoff is enormous."

If you're *not* interested in increasing your bust size, and if you're *not* interested in checking out Jenna's sorority house web cam, and if you're *not* interested in helping Nigerian expatriates get back on their financial feet, then it's time to go to war. The following anti-spam handbook will show you how to prevent spam, and how to deal with the onslaught once you've been marked. We'll also introduce you to the wretched jerk who's behind a lot of the garbage.

It's time to fight back.

Illustrations by James Dietz

Stopping Spam Before It Starts

An ounce of prevention? How about a pound of prevention? That's what it takes to keep your inbox out of the spammers' crosshairs. In this section, we give you the 10 best methods for throwing off the spammers *before* they find you. If you follow these instructions to the letter, you may never have to worry about the rest of this article.

On these two pages, you'll also see many references to e-mail filtering, which is explained in detail on page 32.

#1: Hide Your True Name

Keep your primary e-mail account (the one you pay for and cherish most) as invisible as possible. That means never using it to post to Usenet or web forums. And if you must use your primary account for communication with strangers, you should obscure your address with garbage characters, or call yourself something like "**jREMOVEMEsmith@REMOVEMEisp.com**" to prevent automatic e-mail scouring programs from catching you.

It also pays to never, ever sign up for anything with your primary e-mail address. Instead, you should use a spare e-mail address from your ISP if it provides one, or sign up for a free web e-mail account at Hotmail or Yahoo. Either way, it pays to have one e-mail address for doing occasional business, and another, more protected address for daily correspondence.

#2: Don't Open It

This is tough advice to follow, but if you see something that's clearly spam, try to avoid even opening it. Why? Because spammers know when you've opened their messages, and once they've identified your address as working and active, they'll spam you again and again. Opening spam can also drop cookies into your PC, and that's trouble as well. We must also note that if your e-mail reader's "message preview" mode shows you images or "HTML graphics," you can get nailed that way, too. So disable anything more elaborate than text previewers to play it safe. Finally, avoid electronic greeting cards. Both senders and receivers open themselves up to spam.

#3: Opt Out Now!

When you get an announcement concerning a company's privacy policy, call the provided 800 number and "opt out." This lets the company know that you don't want to share your personal data—including your e-mail address. Also, when a site with which you've voluntarily registered sends you an e-mail regarding privacy policy changes, pay close attention. It's not uncommon for a site to automatically opt you in to new types of information-sharing. Institutions like banks and insurance companies won't necessarily make opt-out procedures easy to find, so look closely at what may seem like benign mailings announcing new services. These e-mails may include opt-out information (legally mandatory in some states) buried in the fine print.

#4: To Remove or Not to Remove?

Conventional wisdom says you should never, ever send an obvious spammer a "remove request" because he or she will simply add your address to the list of active e-mail accounts ripe for spamming. We stand by this advice, but some spammers swear that they honor remove requests. Federal Trade Commission attorney Brian Huseman says the FTC conducted a test in which it sent out remove requests, and then monitored spam levels to see if they increased.

Surprisingly, the testers did not get additional spam. They hardly got less, though, as 63 percent of the remove addresses were simply invalid!

If you're really eager to pick a fight, you can try busting someone who won't remove you. After its test, the FTC sent out more than 30 warning letters to the companies with bogus removal links. All of which leads us to...

#5: Tell the FTC

The Federal Trade Commission loves to get your spam. Send it to uce@ftc.gov. The Commission collects about 50,000 messages each day, and shares the profiles of spammers (and the spam they send) with other government agencies. The government folk can search the database, compare notes, and, hopefully, get around to shutting down the worst offenders.

#6: Contact the Right ISP

It often pays to contact the ISPs that host spammers—many have policies that prohibit dirty e-mailing deeds. You can typically get a spammer's ISP info by deconstructing a spam's e-mail header (see page 34 for details). When working with the spammer's ISP, remember to simply forward any spam you received. Do not use the "bounce message" or "redirect message" features of your e-mail client to forward the message unless specifically instructed to. You'll look like you're relaying spam. Also, your own ISP admins may want to see the spam as well. It will let them know that their server-side spam filters need updating.

#7: Alert Spoofing Victims

Unfortunately, professional mailing tools have made it easy to spoof (that is, forge) the "From" lines in e-mail messages. As a result, spammers will spoof the names of legitimate businesses to entice you to open up their junk: "Look, I got a letter from Flowers.com—it must be legit!"

However, in a satisfying twist of fate, Flowers.com (among other companies) has successfully sued spammers for fraudulently putting its name in "From" lines. So if you recognize that a message has clearly not come from the person or company noted in the "From" line, let them know about the spoofing ASAP. Make sure you explain that you're not blaming them for the spam, but rather, just trying to alert them to an attack on their name. It also helps to determine if the spoofed company has an Internet abuse e-mail address. If not, you can simply notify the appropriate webmaster.

#8: Don't Feed the Spammers

Even if the e-mail looks legit, and even if it's from a company you know other people have done business with, don't reward a spammer by buying his product. The spammer will probably pass along your valid e-mail address to yet another mailing list or company, and the spam nightmare will continue into perpetuity.

The best strategy is to buy the product from someone who doesn't assault you with spam. And if you truly must have the cheap toner cartridges or herbal Viagra pills, and the spammer is the only "retailer" that carries the product, then at least deny the clickthrough that says you're responding to the spam. Instead, visit the spammer's site the long way—visit the URL by typing its address in your web browser.

#9: Build a Mini-Black Hole

One approach to killing spam is to throw all of the e-mail from a known spammy ISP into a "black hole. You can do this by configuring your e-mail server (if you have your own) to automatically refuse to accept or relay that ISP's traffic. While hardcore "black hole" spam blocking is best left to your ISP, there are some nasty abusers you might want to block at the local level just to be safe. A good, reasonably concise list of chronic baddies is at **www.cluelessmailers.org/Wiacklist**. The blacklist includes details of exactly what the spammers do, so you can make your own judgment about whether they deserve filtering.

#10: Start Building a Whitelist

Another drastic approach is to build a "whitelist"—a list of "safe" domain names and e-mail addresses that are allowed access by your e-mail program. Whitelist members are allowed past your e-mail filters, while all other ISP domain names and e-mail addresses are halted at the gate.

If matters ever get truly desperate, you can also filter e-mail traffic from anyone but your known friends. If you think you might possibly take this course sometime in the future, make sure that you always add "trusted senders" (and no one else) to your address book during the course of regular e-mail reading. This way, in the event that you do adopt a whitelist filter, you won't have to comb through a lifetime of e-mail to build it up.

Spam Filtering: How to Control the Flood

Prevention is all well and good, but the fact remains that unless you resort to the most extreme measures (such as whitelisting), you're still going to get spam. Spammers will stop at nothing to get your address. They'll even use flat-out guesswork, running huge lists of words into an address-generation program to build a list of likely e-mail addresses of a given ISP. Spammers also take common name and initial patterns, and then add numbers to them (joe43, missy0401?9) to hopefully find a heartbeat on the other side. Yes, they go to such lengths.

Luckily, your e-mail client has filters to help you solve the spam problem when basic prevention measures fail. Not all filters are created equal, but the basic idea is the same across the board.

First you define what you're looking for—for example, all e-mails with "Herbal Viagra" in the subject line. Next you tell the filter what to do about a suspicious message—you might delete it outright, or transfer it to a "suspicious" folder. This way, you can periodically review the quarantined messages to see if your filter junked something you actually want to receive. (For some odd reason, Gordon's e-mail filters always dump Katherine's messages into quarantine. Go figure.)

Virtually every e-mail program uses the same language for developing filtering rules. Some programs, such as *Outlook XP*, offer more choices for default rules than others, but there are really only two options you're interested in: filtering based on sender/header information (i.e., filtering out specific e-mail addresses or key words in subject lines), and filtering based on keywords found in a message's body content.

Let's take the first strategy. Some spammers actually play fair, and place the letters "ADV" (for "advertisement") in their subject lines. With your filtering tools, you can create a subject line rule that blocks all e-mail containing the phrase "ADV." Of course, not all spammers use this identifier, and you may even want to receive e-mail from some companies that do.

Some e-mail programs let you delete spam on the server level, rather than pulling it down and stuffing it into a separate mailbox marked "suspicious." This is a drastic strategy, however, and could end up making you feel rather foolish if your filter kills e-mail you actually wanted to read. That's why we recommend the "suspicious" folder approach. Browse it every few days to make sure you haven't missed an announcement about the end of the world, and if you find more than one "false positive" (an e-mail that's been mistakenly tagged as spam), it's time to re-evaluate your filters and find the common thread.

Be sparing in your use of keyword filters. If nothing else, you might miss out on a friend telling you about the hilarious spam he just got for a combination toenail fungus/genital enhancement cream.

The web-based Yahoo and Hotmail e-mail services let you filter according to specific words or senders, but the best use of your time will be to use the "This is Spam" and "This is not Spam" reporting features. By showing Yahoo and Hotmail what they let slip through (or what they accidentally blocked), you only improve their overall spam abatement program.

Finally, don't be disappointed if your filters fail to stop everything—even the words you're looking for. Filters can be defeated by sneaky HTML tricks, such as inserting do-nothing tags in the middle of words.

Spam's Worst Moments

The history of man's inhumanity to man via the parable of junk e-mail

THE VERY FIRST SPAM?
In May 1978, Digital (now a part of HP) sent out an e-mail invitation for a product demo to hundreds of Arpanet users. Most of the intended recipients never got the mail due to a glitch, but community reprisal was still sharp and furious. Arpanet bigwig Major Raymond Czahor even chastised the company in all caps.

IMMIGRATION! EVERYBODY FREEZE!
In 1994, the law firm of Canter & Siegel tried to boost sales with an alarmist spam announcing the impending end of the "Green Card Lottery," and inviting immigrants to turn to them for help. Although this was originally a Usenet spam, it lives on eight years later. While researching this story, we actually got a "US Greean Card For You" spam (note the clever spelling error to defeat simple spam filters).

TRASH TO TREASURE
Jeff Slaton—among the first to sell worthless crap online for real money—broke a lot of ground with his "atomic bomb schematics" spam, which he mercilessly pelted at individuals and mailing lists. The declassified docs from Los Alamos were basically free, but Slaton sold them for $18. Slaton might also have been the first to provide a bogus e-mail address for people who wanted to be removed from the spam list, and the first to proudly proclaim himself the "spam king."

CAPITALIZING ON TRAGEDY
On September 12, 2001, Opt-In Marketing Services blasted out a spam to "ask all our members to immediately give blood or money." The provided links to the Red Cross were legit, but 75 percent of the spam window was actually an ad for life insurance.

.USA IS NOT OK!
Shortly after 9/11, TLD Network Ltd. urged its spam recipients to "Be Patriotic!" and register .usa domain names for $99 a shot. Trouble was, the .usa domain never existed. It was all a scam. When the FTC shut down TLD earlier this year, it estimated that the company and its partners had pocketed over $1 million.

Creating a Spam Filter

Good hygiene for your e-mail client

Virtually all major e-mail clients, including online services such as Yahoo and Hotmail offer some kind of e-mail filtering. Most of the clients call them filters, but Microsoft had to be different, so it calls them "rules."

Because the process of creating e-mail filters is almost identical among all the clients, we're going to zoom in on the process of getting rid of those damn Viagra spams using *Outlook Express*. If you use *Outlook XP*, *Eudora*, or even *Netscape/Mozilla*, you'll still find the filters (or "rules") under the "Tools" menu in each application.

STEP 1
SELECT THE CONDITIONS FOR YOUR RULE

This is where we tell *Outlook* which e-mails to be concerned with. Because we don't want to accidentally filter out frantic e-mails from friends who, um, can't perform the way they used to, we're going to restrict filtering to just the subject line of the e-mail. After we checked the appropriate box ("Where the subject line contains..."), a "contains" hyperlink appeared in the Rule Description box. We then clicked the hyperlink, and typed the word "Viagra" into the target.

STEP 2
SELECT THE ACTIONS FOR YOUR RULE

Here's where we tell *Outlook* what to do with the e-mail it has intercepted. You can actually assign multiple actions to an e-mail. For instance, you could have the suspected spam forwarded to your IT department so they can tweak their filters to catch more spam, and then also have it deleted from your Inbox. Here, we've checked "Move it...," which brought up a hyperlink in the Rule Description box. In this hyperlink's target, we chose our Spam folder. At some point, we'll check this Spam folder to see if *Outlook* deleted valuable e-mail by mistake.

STEP 3
REMEMBER THE WHEREABOUTS OF YOUR RULE

Finally, we name the rule something recognizable, so that we can find, open, and edit it later to hone its accuracy, if need be. That's one spam rule down, and many more to go!

New Mail Rule

Select your Conditions and Actions first, then specify the values in the Description.

1. Select the Conditions for your rule:
   - ☐ Where the From line contains people
   - ☑ Where the Subject line contains specific words
   - ☐ Where the message body contains specific words
   - ☐ Where the To line contains people

2. Select the Actions for your rule:
   - ☑ Move it to the specified folder
   - ☐ Copy it to the specified folder
   - ☐ Delete it
   - ☐ Forward it to people

3. Rule Description (click on an underlined value to edit it):

   Apply this rule after the message arrives
   Where the Subject line contains 'Viagra'
   Move it to the Spam folder

4. Name of the rule:

   I don't need Viagra - yet

MailGuardian: Drastic But Effective

More spam protection than mere filters can provide

There are a number of commercial utilities that promise to excise spam from your life, but MailGuardian (**www.mailguardian.net**) is the best one we've tested. The combined one-two punch of *MailGuardian* and your e-mail client's own filtering system is the most comprehensive yet fault-tolerant approach we know of today.

Instead of scanning your e-mail for keywords or specific headers, MailGuardian checks the originating SMTP server for every e-mail you receive, and compares it with a constantly updated list of servers used by known spammers. A suspected spam message gets flagged as spam on MailGuardian's server before you ever see it, and a keyphrase is placed into the subject line of the e-mail. From that point on, it's easy to banish messages that MailGuardian flags as spam using your mail client's built-in filters. MailGuardian costs $30 a year, but that's a small price to pay to regain control of your Inbox.

Decoding E-mail Headers

Here's how to find—and bust—the people behind your spam

The last thing spammers want to do is make it easy for you to respond directly to them and pelt them with your rage, so they resort to all sorts of wicked chicanery to remain anonymous. But in doing so, they still have to go through a network that wasn't designed to help bulk e-mailers cover their tracks. By looking at your e-mail headers (which are, most of the time, conveniently hidden from view), you can often draw a bead on the offenders, and then report them to their ISPs.

To see the full message headers that accompany every single piece of e-mail, you can select View/Options in *Outlook XP*; Properties/Details in *Outlook Express*; and View/Headers-All in *Mozilla/Netscape*.

Now, let's take a look at a piece of spam to root out the source. Names and IP addresses have been changed to protect the innocent and not-so-innocent. ■

Charting the Spamdemic

The conspiracy is vast, but not invisible

In a single, sweeping 4430x2526 EPS file, Bob West has charted the global spam conspiracy's massive size and complexity, linking one offender to another in the ultimate flowchart of treachery and deceit. West's creation is called the Spamdemic Map (available for download at **www.cluelessmailers.org**), and it shines a bright light on companies and organizations that would probably prefer to operate in the shadows.

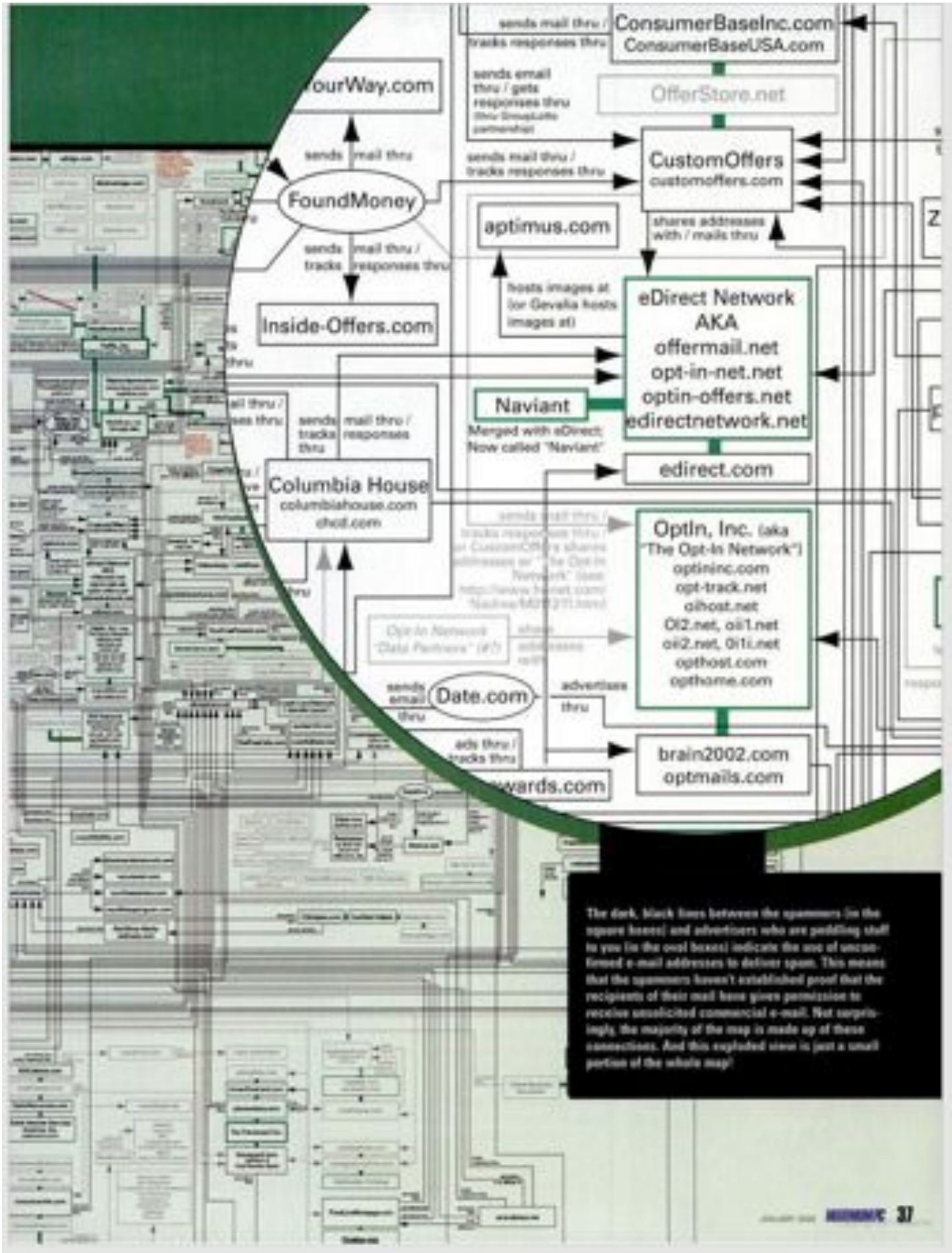
Spam emerges from a vast web of partnerships that includes not just the spammers themselves, but also advertisers desperate to sell goods, marketing agencies determined to make commissions, and ISPs that provide bandwidth to rogue spammers. What all these institutions have in common, however, is a rapacious appetite for e-mail addresses, and many are willing to turn a blind eye to addresses that may have been collected without their owners' permission.

"[The map] is meant to serve as a warning to mailers, marketers, advertisers, and e-mail users as to the potential for abuse when unconfirmed addresses are used in marketing," says West. The cartographer contends that while spammers may trust their address suppliers to provide legitimate e-mail addresses that have been gathered with users' permission, the true source of those names could be quite shady.

"Although lots of spammers try to hide their associations," says West, "others proudly name their 'marketing partners'—in other words, those with whom they buy or sell your personal information, often without your permission." These "marketing partners" could include your bank, your grocery store (did you sign up for that "Super Saver" card?), and anyone else who happens to know where to find you online.

"Adobe Illustrator, a little research, and lots of caffeine" are the map's foundation. West makes liberal use of IP (domain name) owner lookups to draw connections for the map, but a great deal of his information simply comes straight from the spammers themselves.

So before you give your e-mail away to a seemingly legitimate firm, check the Spamdemic Map. You never know who might be slipping it to a clueless mailer.



The dark, black lines between the spammers (in the square boxes) and advertisers who are peddling stuff to you (in the oval boxes) indicate the use of unconfirmed e-mail addresses to deliver spam. This means that the spammers haven't established proof that the recipients of their mail have given permission to receive unsolicited commercial e-mail. Not surprisingly, the majority of the map is made up of these connections. And this exploded view is just a small portion of the whole map!

The Appalling Face of Spam

His name is Ronald "The Spam King" Scelson, and he's getting rich by stuffing your inbox full of crap

He says he won't send you outright porn or promotions from "multilevel" marketers running pyramid schemes. But if you've been pestered to buy life insurance, satellite TV, or a "cell phone booster" lately, chances are pretty good that Ronald Scelson of Slidell, LA sent you the spam.

Since the late 1990s, Scelson has made a very comfortable living blasting your mailbox—again and again and again—with ads for travel, sex toys, and whatever else someone will give him $1,000 a day to push. Scelson says that when he ran a company called (of all things) Opt-in Marketing, he sent more spam than any other person in the country. Unrepentant boasts like these are what have earned him the title of "Spam King," and made him the target of anti-spam activists.

"We told the world who our company was, gave a phone number, and four different ways to be removed, but all this did was give the anti-spam groups like Spamhaus and Spamcop easy ways to track us." Scelson says the anti-spam advocates jumped on the ISPs running his removal servers, and threatened to blacklist their domains if they didn't shut him down. This led to multiple disconnections by major ISPs. And those disconnections added up to months and months of lost revenue for his business, and mounting bills from ISPs that continued to charge him for the pipes he installed—but couldn't use—for spam.

So no more Mr. Nice Guy, Scelson says. He left the day-to-day operations of Opt-in Marketing behind, and now operates under his own banner as an unleashed spammer, pulling every dirty trick in the book to deliver his e-mail.

"I don't frankly care; I'll break every rule there is to break," he says. "I will relay-rape, go through proxy servers and spoof them, I will spoof IP addresses. I will do everything I can for them not to find me to shut me down. I can stay up like this for years, and they'll never totally lock on to me." (Lest there be any questions, online jargon dictionaries define relay-raping as, "The hijacking of a third party's unsecured mail server to deliver spam.")

Scelson says he has yet to be brought to trial for anything, and he even wriggled out of one lawsuit because, under Louisiana state law, he didn't meet the volume requirements of a particular statute, which stipulated that an illegal spammer had to send thousands of e-mails at a time. Although each of his 20 servers can blast out 9MB of spam in a second, they send just one e-mail at a time each over a DS3 pipe. Score one for loopholes.

Scelson claims a database of 130 million e-mail addresses, some of which he buys, and some of which he pulls directly from online directories. Nevertheless, Scelson says he processes remove requests on a weekly basis, and applies opt-outs to all of his advertising clients, and that he spams only "public e-mail accounts," not private domain names or corporate e-mail. "If you're Hotmail, Juno, BellSouth, AOL—those accounts are going to receive bulk e-mail," he says.

The Spam King says he would welcome legislation that sets ground rules for spam, as long as ISPs and filter operators have to play fair as well. "California passed a law that you have to have 'ADV' in the subject line [of spam]. This is great. Individuals can filter 'ADV' and not get junk mail from us," he says.

Nonetheless, Scelson says he thumbs his nose at the statute, because some ISPs simply block all e-mail tagged with "ADV."

"At that point," he says, "how do you expect me to honor that law?"

Thanks to vigilante activists, Scelson says he's on virtually every spam list known to man, but he likes it: "I've gotten some of my best products and clients thanks to that." He says he regularly receives death threats, and industry allies like the Direct Marketing Association and Privacy Consortium don't lend him a hand.

"Is it the right way to mail, using other people's resources? Absolutely not. But [anti-spam advocates] tried to put me out of business because of doing it the right way," Scelson says. The Spam King says he will continue with his underhanded ways until forced to do otherwise. "In five years, I'll be even richer than I am now." ■