Spam-Proof Your E-Mail Address

2nd Edition

By Brian Livingston

US $9.95

Help me make this format viable

Publishing in an electronic format is great for works that are between 10 and 100 pages long. E-documents are ideal for many topics that are too long for an article and too short for a bound, printed book. But publishing information in this way can only continue if you'll help make it an economically viable medium. We need to support electronic publishing so independent journalists such as myself can earn a living through our research and writing.

This PDF file — readable with the free Adobe Reader application — is licensed to you only for your personal use:

- You may download one copy, but you may not make copies for others;
- You may print one copy, but you may not print copies for others; and
- Others who want copies must purchase copies for themselves.

To purchase an additional copy, please visit:

https://www.WindowsSecrets.com/spamproof

If you'll help me by supporting these simple rules, then I'll promise to do my best to uncover and publish the most helpful information I can for you to enjoy in the future.

Thanks,

Brian Livingston
Author, *Spam-Proof Your E-Mail Address*
Co-Author, *Windows 2000 Secrets* and *Windows Me Secrets*
Editor, WindowsSecrets.com

Table of Contents

2nd Edition: Published January 2006
1st Edition: Published July 2004

If revisions are made to this e-book, the new information will be released in my twice-monthly e-mail publication, the *Windows Secrets Newsletter.* For the latest tips, get a free subscription at the following Web page:

http://WindowsSecrets.com/info

Table of Figures

Edition 2 Build 1

Executive Summary

SPAM — UNSOLICITED BULK E-MAIL (UBE) — surpassed legitimate e-mail messages in 2003, according to MessageLabs.com and others. The volume of spam is increasing geometrically. But you can take a series of simple steps to keep an e-mail address from getting onto spam lists.

1. **Spammers get your e-mail address from Web pages.** Studies by the Center for Democracy & Technology and the U.S. Federal Trade Commission show that almost all spam is being sent to addresses that were posted on Web sites.

2. **You may need a new address.** There's no way to get an e-mail address off spammers' lists once it's there. If your address already receives spam, you'll need a new one — but you'll have to change only once, using the tricks in this e-book.

Spam makes up the majority of all e-mail messages.

3. **Use "disposable" addresses.** Addresses at major Internet service providers (ISPs) are high-value targets for spammers. I'll show you free and low-cost alternatives that allow you to make up a different e-mail address every time you give out your contact information. If one of these addresses gets onto a spammer's list, simply shut it off.

4. **Post your new addresses only as images.** I'll show you how to make images that display any e-mail addresses you wish to post on Web pages. Spammers use "harvesting" programs to search the Net for addresses. But they can't afford the time to perform optical character recognition (OCR) on every image on the Web to find addresses.

5. **If you must use "mail me" links, encrypt them.** If an image alone isn't enough, you may wish to post "click here to send me e-mail" links on your Web site. I'll show you free services that make these links easy for you to create but hard for harvesters to collect.

If you know how to take all of the above steps, you're done. Stop reading this e-book and go spam-proof your old or new e-mail addresses.

But if you need help to do any of these steps, read on. There's a wealth of detail in the pages to come.

1. What Research Shows About Spam

In spring 2003, a respected nonprofit, public-interest organization in Washington, D.C. — the Center for Democracy & Technology (CDT, http://www.cdt.org) — released a lengthy study of how spammers acquire the millions of e-mail addresses they mail to. The study consumed almost a full year. CDT researchers first created dozens of fresh, never-used e-mail addresses, such as m45k5e@egovtoolkit.org. Each address was then used on the Internet in different ways:

- **Posted on Web pages.** Some addresses were left online for a full six months. Others were removed from the Web after two weeks to determine whether any difference could be detected in the volume of spam that was subsequently received. Other addresses were posted in obscured ways, such as "m45k5e at egovtoolkit dot org."

Figure 1: The CDT study released several newly-invented e-mail addresses in a variety of ways, such as using them to fill in forms and register online at careerbuilder.com (above).

- **Posted in Usenet messages.** Some addresses were used only in the headers of messages posted to Usenet news groups. Others were typed into the body of the messages. Some of these addresses were obscured, as discussed above.

- **Subscriptions.** The organization used various fresh e-mail addresses to sign up for newsletters from sites such as Amazon and Travelocity.

- **Memberships.** Some addresses were used to sign up at career, auction, or discussion sites such as CareerBuilder, eBay, and WebMD. Again, some addresses were obscured.

- **Domain registration.** Other addresses were provided to companies that register domain names, including netsol.com and npsis.com.

The full report of the CDT study is posted on the Web at:

http://www.cdt.org/speech/spam/030319spamreport.shtml

Spammers get addresses by 'harvesting' web pages

After six months of the e-mail addresses being visible on the Internet, the center had received more than 10,000 messages. About 1,600 were newsletters and other legitimate communications that the researchers had signed up for. The remaining 8,842 messages (85%) were spam.

An astonishing 97% of the spam messages were received by those addresses that had been posted on Web pages. Only 3% were received by the addresses that had been used in all other ways combined.

The evidence is that spam lists are largely acquired by computer programs called *harvesters* that are operated by spammers. These harvesting robots scan millions of Web pages looking for "at" (@) signs surrounded by a name and a valid domain, such as example.com. Spammers have built up lists comprising hundreds of millions of e-mail addresses in this way.

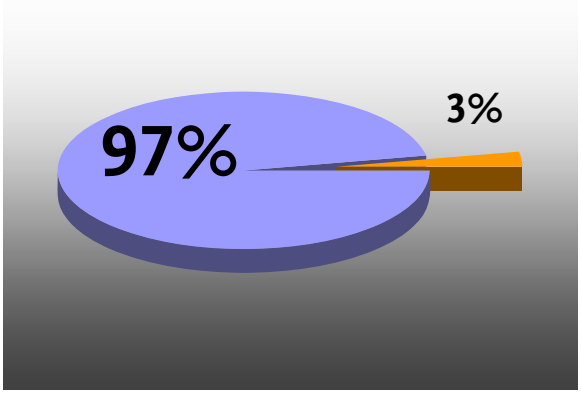

Figure 2: Over 97% of the spam received in the CDT study was generated and sent to addresses that were posted on Web pages. Only 3% was generated from other sources.

A federal agency confirms the harvester problem

The CDT study was a more extensive version of an experiment performed in the fall of 2002 by the U.S. Federal Trade Commission. The FTC used 250 fresh addresses of its own in various ways. Within six weeks, 3,349 spam messages had been received by these addresses.

According to the FTC, 86% of the addresses posted on Web pages and online newsgroups had received spam. Also, half of the addresses posted on free, personal Web page services were spammed. But, the FTC said, "Addresses posted in instant message service user profiles, 'Whois' domain name registries, online résumé services, and online dating services did not receive any spam during the six weeks of the investigation."

A summary of the 2002 FTC report is posted at:

http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm

The FTC repeated this study and released a new report in November 2005. This time, the agency created 150 new e-mail addresses. It posted them on Web pages and in message boards, chat rooms, Usenet groups, and blogs.

Within only five weeks, these addresses were receiving an average of 45 spam messages a week, the FTC says. More than 99% of the spam was received by the addresses that had been posted on Web sites. The other locations generated almost no spam.

In a 2005 FTC study, harvesting generated 99% of new spam.

The fact that spammers use harvesting software to collect addresses from Web sites seems to be even more true now than it was a few years ago.

The FTC's 8-page November 2005 PDF report is posted at:

www.ftc.gov/opa/2005/11/spamharvest.pdf

'Dictionary attacks' are a problem but not the worst problem

A "dictionary attack" occurs when a would-be spammer sends messages to every possible combination of names at a company. The spammer presumes messages that are not rejected (bounced) by the company are valid addresses. This builds the spammer's list.

During the course of the CDT study, the center's mail server was actually subjected to a dictionary attack. A robot tried addresses such as these:

aa@egov.org, ab@egov.org, ac@egov.org... aaa@egov.org...

"Brute force" harvesting such as this is a genuine problem, but is fairly easy to block, as CDT itself did. I'll discuss in the chapter called Creating a New Spam-Proof Address how to defend yourself against such attacks.

'Unsubscribing' from spam lists can lead to more spam

You often hear people say, "You should never unsubscribe from anything. You just get more spam."

My research indicates that it's safe to unsubscribe from legitimate e-mail lists that you voluntarily joined. What's unwise is to try to unsubscribe using the "unsub" links you find in spam messages you didn't ask for.

At one time, spammers used to ignore unsubscribe requests completely. The FTC, in a 2002 study, tested the unsubscribe options that appeared in 200 spam messages that carried opt-out wordings. The agency found that the "vast majority" of spam unsubscribe routines flatly did nothing. A summary of this study is posted at:

http://www.ftc.gov/opa/2002/04/spam.htm

Unfortunately, since that time, a few spammers have started to make use of their unsubscribe pages.

One company that makes its business studying whether or not unsubscribe pages can be trusted is Lashback.com. This firm notes unsubscribe forms that are advertised in e-mail messages. The company then creates new, unique e-mail addresses and enters them into the Web forms.

Figure 3: The FTC showed in two studies that spammers use "harvester" programs to copy e-mail addresses off Web pages.

If one of these "unsubscribed" addresses starts receiving spam, Lashback records the IP address that sent the mail on an "unsubscribe blacklist" (UBL). The sender of the spam is presumed to be abusing e-mail addresses gathered from unsubscribe forms. The deceptive unsubscribe page is also recorded on a list of Web sites to avoid.

As of January 2006, the company was monitoring 170,000 different unsubscribe mechanisms on the Web, according to Lashback president Brandon Phillips. Almost 13,000 (7.6%) show signs of what he calls "suppression list abuse." When I interviewed

this company's executives for an article back in October 2004, the comparable figure was only 1.4%. Spammers seem to be increasing their exploitation of unsubscribe forms to trick innocent e-mail users into handing over their addresses.

You can look up individual Web sites to see if they're listed in Lashback's database of spammy "unsubscribe" forms. Administrators of corporate networks can perform lookups against the database to prevent employees from unwittingly visiting these malicious sites. See:

http://lashback.com/ubl.htm

Another trick spammers use to get your address is phony "do-not-email" services. Spamhaus.org, a respected antispam service, maintains a list of these con games, which have names like "opt out" and "global remove." A few of the services even charge money for the "service," after which they sell the collected e-mail addresses to spammers, Spamhaus says.

No one can get you off spammers' lists, whether you pay for the service or it's free. Check Spamhaus's listings before trusting any such offer. The current description of known scams is at:

http://www.spamhaus.org/removelists.html

Viewing spam images can generate more spam

You don't have to respond to a spam message to verify to the spammer that your e-mail address is valid. Merely viewing images in spam messages — which you can do by viewing them in the "preview pane" of Microsoft Outlook, Outlook Express, and other e-mail programs — can automatically reveal to spammers that you saw a message, at least momentarily.

How does the fact that you opened or previewed a spam message let a spammer know that your e-mail address is working?

One study of this technique was conducted by Masons, a London-based international law firm. Using numerous fresh e-mail addresses, the February 2003 study found that:

- 83% of spam messages contain a small image that, when downloaded for display by your e-mail program, confirms your existence;
- Addresses in the study that received spam messages but didn't view them received a volume of spam that remained roughly steady;
- By contrast, addresses that opened or previewed all the incoming spam messages received approximately *double* the volume of spam two weeks later, compared to the "nonviewing" addresses.

A summary of the Masons study is posted on the firm's Web site, Out-law.com, at:

http://www.out-law.com/php/page.php?page_id=pressrele3360&area=about

To combat the ability of spam to "phone home," newer e-mail programs (such as Microsoft Outlook 2003) are configured by default not to show images in the body of incoming messages. If you use one of these programs, you need to turn images on for each sender that you trust.

Personally, I like to see images — which sometimes contain important content — in my incoming e-mail newsletters. It doesn't hurt to turn on images for those lists that you've chosen to subscribe to. The publisher of the newsletter already knows that your e-mail address is valid, so it doesn't matter if you view the images in the messages.

If you receive a lot of mail that's potentially spam, you can quickly cruise through it — without viewing images or anything else — by simply turning your preview pane off. You can then decide which e-mails to delete by examining the Subject lines. Most spam bears gimmicky Subject lines, such as "Hi!," "You requested this," and "Drugs for less."

In Outlook 2003, you can quickly turn off the preview pane using only four keystrokes: Alt, View, Reading Pane, Off (Alt, V, N, O). After you've deleted any likely spam messages, a similar keystroke sequence turns the preview pane back on. Most other e-mail programs have a similar way to do the same thing.

Unsubscribe from legitimate lists, don't bother with spam

You shouldn't waste time trying to unsubscribe from actual spam. But that doesn't apply to legitimate e-mail newsletters. Responsible publishers provide unsubscribe routines that actually work.

Simply follow these two rules:

- **Don't try to unsubscribe from unsolicited bulk e-mail.** Spam you receive should never be opened, previewed, or responded to in any way. (And you should absolutely *never* buy anything that's advertised in spam! Many such offers are fake. If you order something from a Web page advertised in a spam message, you can easily lose your money or receive an inferior product, if you receive anything at all.)

- **Do unsubscribe from legitimate e-mail lists you no longer want.** Reputable publishers provide a working unsubscribe link at the top or bottom of every message. Don't click "Report As Spam" buttons in your e-mail program to stop receiving legitimate newsletters. Instead, simply use the publisher's own unsubscribe mechanism.

Ultimately, the best way to minimize the hassle of spam messages is to make sure your e-mail address doesn't receive spam in the first place.

That's the subject of the following chapters.

2. How to Spam-Proof Your Address

SPAM-PROOFING YOUR E-MAIL ADDRESS helps you avoid viewing spam messages. After all, the best way to guarantee that you don't open any spam is to stop spam from finding you in the first place.

Spam-proofing means making sure that your address never appears on the Internet in plain text where harvesting programs can see it.

Besides harvesters, spammers do use lesser ways to build their lists. Online signup forms that re-sell your address are a concern. But your Priority One must be to make your e-mail address invisible to harvesters.

I've spent months researching and testing various ways to spam-proof e-mail addresses. The methods I've found break down into the following types, from the simplest to the more advanced:

- **Level 1: Obscure your address (simple, but not 100% effective).** You can spell out the punctuation marks in your e-mail address as the words "at" and "dot" on the Web. As I explain below, however, some harvesters have gained the ability to interpret the words "at" and "dot" and grab your address. I don't recommend that you rely on this method to stay out of spammers' lists.

- **Level 2: Display your address as an image (pretty simple).** Displaying your e-mail address as an image is the simplest form of protection that can't be read by harvester bots. Any graphics program can make your address into an image with a white or colored background that matches the background of the Web page you plan to put it on.

- **Level 3: Make clickable links that are encoded (moderately simple).** I'll show you a free method to form a clickable link, such as "click here to e-mail me," that harvesters can't decode — and probably will *never* be able to decode.

- **Level 4: Use "disposable" addresses and Web forms (advanced).** The best approach to spam-proofing is to create your own "disposable" addresses, using free or low-cost services I recommend below. If you have some technical skills, you can also accept e-mail using Web forms you create.

Removing existing addresses from Web pages can reduce spam

The CDT study found that addresses that were posted on Web pages for two weeks or so, and then removed from the Web, gradually received less spam until the volume approached zero.

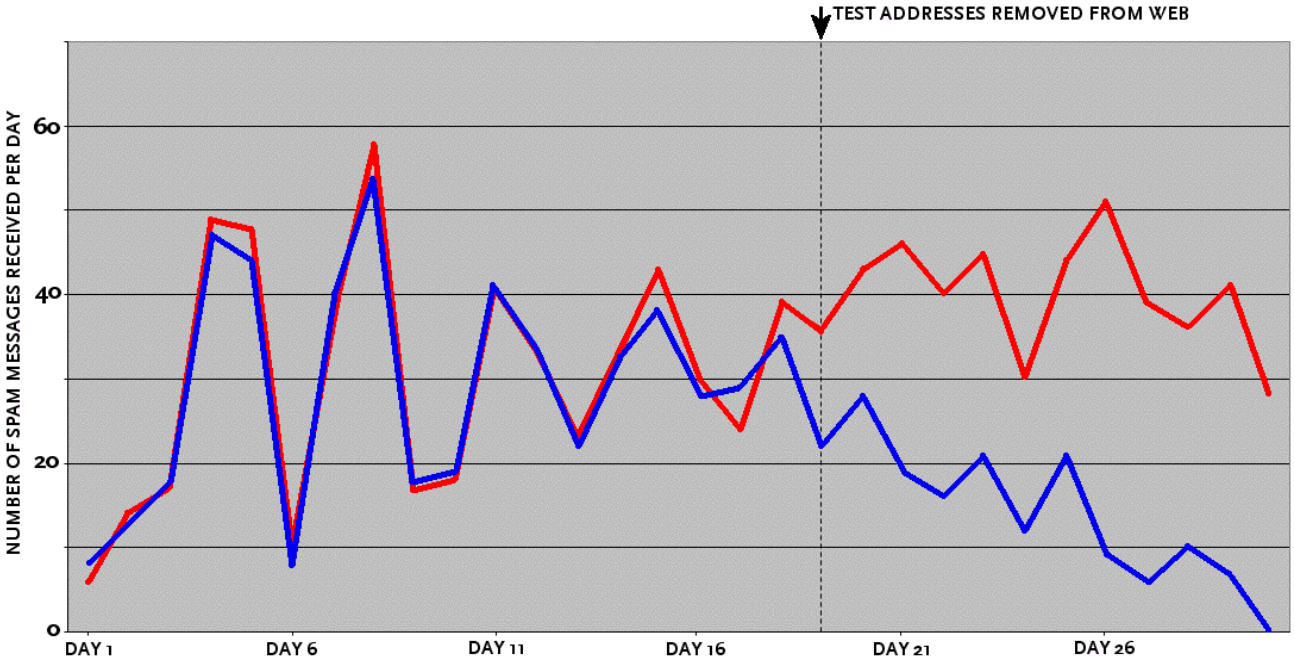

Figure 4: Addresses that were removed from the Web received less spam until it reached zero (lower line). Addresses that remained on the Web continued to receive about the same level of spam (upper line).

What explains this? I believe many beginning spammers use harvester programs to try to quickly build up their e-mail lists. But these perps give up in failure after their first few e-mail blasts don't produce the windfall profits that were promised. E-mail addresses that appeared on the Web for only a few weeks, therefore, may be on lists that were soon discarded.

If your address has been visible on the Web for years, however, it might be on so many spam lists by now that it's too late to make it invisible. In that case, you may have no choice but to change your address. Faced with this situation, some people actually prefer setting up one or more all-new addresses. It definitely starts you over with a clean slate.

Whether you try to reduce the volume of spam to an existing address or create fresh addresses is up to you. What I *can* say is that — using the methods in this e-book — you'll probably need to change your address no more than *once* instead of several times over the next few years.

3. Level One: Use Obscured Text

Obscuring your e-mail address by spelling out its punctuation marks is one simple way to try to hide your address. It's not 100% effective. But if you're somehow forced to state your e-mail in a discussion forum or wherever, you should at least obscure the punctuation marks as follows:

chris at example dot com
chris ("at") example ("dot") com
chris AT example DOT com

I personally tested this approach for two years after I set up a Margie.net Web site for my wife, the painter Margie Livingston, in February 2001. (Building the site was actually a surprise Valentine's Day present for her, which shows you what a geek I am.) Since it was important for people to easily be able to reach her, I placed her e-mail address on her home page in plain text, but obscured as "margie at margie dot net".

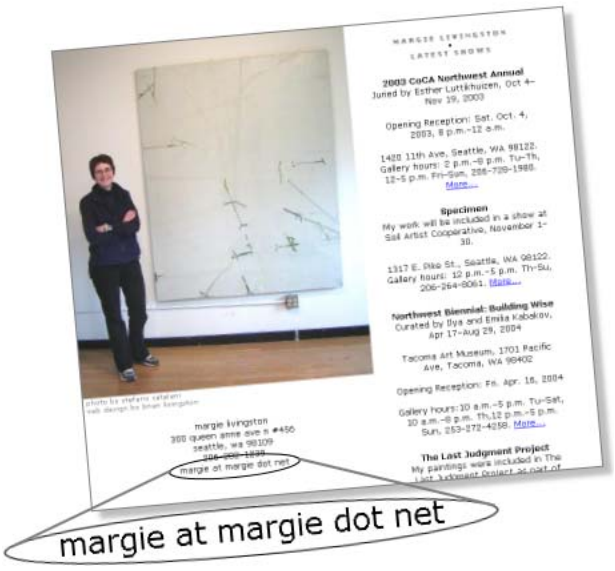

Figure 5: Spelling out your e-mail punctuation no longer keeps all harvesters from recognizing it.

Numerous Web pages link to her site (it's currently Google's No. 2 listing for **german romantic painters**). Despite this fact, her address received no significant amount of spam over a 30-month period. By contrast, her old university e-mail address, was posted in plain text in 1999 as part of her MFA graduating class. That account was crammed with spam before she deactivated it.

Unfortunately, the November 2005 FTC report that I cited above states that at least one harvesting program has gained the ability to translate "at" and "dot" into the punctuation marks of an e-mail address. I recommended in the 2004 edition of this e-book that this method should not be relied on. I've converted Margie's e-mail address on her site into a black-on-white image and added a contact form. I recommend that you do so, too. I'll explain in the next chapter how do to this and why it's better.

4. Level Two: Use Address Images

A fail-safe, spam-proof way to display an e-mail address on a Web page is to use a graphic. Harvesters don't currently perform optical character recognition (OCR) on images to see if they contain e-mail addresses. I don't believe harvesters ever will. That's because harvesting bots are designed to scan billions of Web pages to collect millions of e-mail addresses. Taking the time to analyze every image on the Web would never reap as many addresses as simply searching for "@" signs in text and, when one is found, checking to see if it's part of a valid address.

Figure 6: The contact page for BriansBuzz.com contained an address image (left) and an encrypted, clickable link (right). A fill-in form is also available. All are spam-proofed.

Once again, I've tested this method on my own Web sites. For example, sites I operate such as BrianLivingston.com and WindowsSecrets.com (formerly BriansBuzz.com) bear my e-mail address as both an image *and* as an encrypted, clickable link. None of my personal e-mail addresses that have been obscured in any of these three ways have ever received any noticeable amount of spam.

That contrasts sharply with all of my previous e-mail addresses. They were publicly posted in various pages over the course of several years through April 2003, during which I wrote weekly columns for *InfoWorld* Magazine. These addresses were buried, one after another, by spam. My posted address in my bio on numerous InfoWorld.com Web pages over the years had to be changed from "tips@BrianLivingston.com" to "Brian@BrianLivingston.com" to "Brian@BriansBuzz.com" as I abandoned one for the next. These addresses continue to receive thousands of spam e-mails a week, even though I was long ago forced to admit defeat and stop checking these accounts.

Fortunately, it's easy to save addresses as unharvestable images and links. In this chapter, I'll explain how to make a graphical address. In the following chapter, I'll describe how to make a spam-proof clickable link.

How to save your e-mail address as a spam-proof image

Every graphical operating system has some kind of graphics program that can make images. In Microsoft Windows, it's called MSPaint, Paintbrush, or other names. If you own and know how to use a high-end graphics program — such as Photoshop or Paint Shop Pro — feel free to employ these more-powerful tools. But any simple paint program will do.

Step 1. Start your paint program. In Windows, you can do this by clicking Start, Programs, Accessories, Paint or a similar series of menu items.

Step 2. Fill the drawing area with the background color of the Web page on which you'll post your e-mail address. Your drawing area may already be filled with the color white. To fill the drawing area with a different color, left-click your desired hue in the color bar (try View, Color Bar if you don't see such a bar). Then click the Fill With Color tool (see Figure 7). Finally, click anywhere within the drawing area to flood it with color.

Figure 7: The Fill With Color tool.

Step 3. In the color bar, left-click the color you wish to use for the text of your e-mail address. Then click the Text tool (see Figure 8). Holding down your left mouse button, draw a rectangle large enough for your address. Once you let go of the button, a Fonts selection box should appear. Select the typeface and size for your address. Remember, images don't expand and contract when visitors to your Web page adjust the text-size setting in their browsers. You should therefore pick a medium font size that'll look good no matter how a visitor's browser may be configured.

Figure 8: The Text tool.

Step 4. Use your keyboard to type your e-mail address (see Figure 9). Go ahead and include the "@" sign, dots, and any other punctuation marks. Harvester programs can't understand images, so you don't need to obscure the address text.

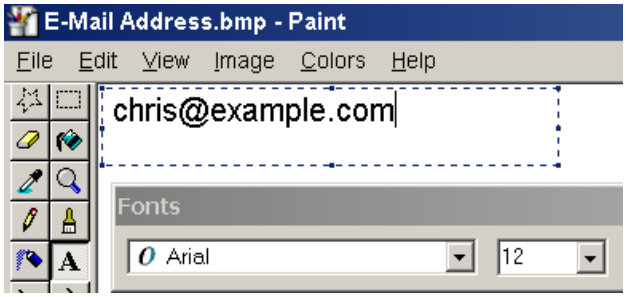

Figure 9: Typing your address into the text box.

Step 5. Click the rectangular selection tool (see Figure 10, next page). Holding

Figure 10: The Rectangular Selection tool.

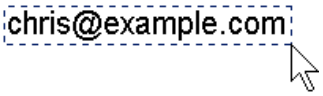

Figure 11: With the Rectangular Selection tool on, hold down the left mouse button while dragging the mouse to define a rectangle just large enough to fit around the address image.

down your left mouse button, draw a rectangle that fits all the pixels of the e-mail address inside the area (see Figure 11).

Step 6. Save the selected area to an image file. In MSPaint, pull down the Edit menu, then click Copy To. If your graphics program gives you a choice of formats to save into, select GIF, JPEG, or BMP, in that order of preference. (GIF is better for images with fewer than 256 colors, whereas JPEG is better for images with many colors. BMP is acceptable if neither of the other formats are available, but it produces larger files.)

'Turing test' images are not needed for spam-proofing

Figure 12: A human can read these fuzzy characters; a bot cannot. But you needn't use any tricks such as this to make yourself invisible to harvesters.

A *Turing test* (named after Alan Turing, who proposed it in 1950) involves questions that a human can answer but a computer cannot. Some Web sites display a kind of Turing test so search-engine robots can't read any of their pages. A picture of a distorted series of letters appears on a login page. Visitors must correctly type the letters into an input box before they are allowed to browse any additional pages. Figure 12 shows one kind of distorted lettering, which is called a *captcha*. This example was produced by a program developed by First Productions Inc.

I don't believe most Web sites need to distort their e-mail address images in this way to keep harvester bots at bay. Harvesters will always try to speed through millions of Web pages as fast as possible to extract the greatest number of addresses from plain text. In my opinion, they'll never slow down to analyze every image on the Web to find addresses.

If you host Web pages with high-value content that's subject to constant assaults by robots, however, you may wish to distort your images to the extent of a Turing test. (Remember that captchas cannot be read by visitors with impaired vision, so you'd need to provide alternate ways for them to respond.) First Productions offers a free captcha program:

http://www.firstproductions.com/cgi/human/

How to place your address image on a Web page

Once you have an image file that contains your e-mail address, you're ready to place it on a Web page. If you have a Webmaster to do this for you, you're done. If not, the following is the HTML code that's used on my Web pages to display my e-mail address image (the code can be all on one line or on multiple lines — in HTML it doesn't matter):

```
<img src="/images/BrianL.gif" border=0 hspace=30 vspace=0
alt="address image" width=172 height=15>
```

Obviously, you should use a SRC tag that refers to the file name you chose for your own address-image file. The tag should also point to the directory where you've stored the file on *your* Web server, not mine.

Notice that the ALT tag used in this example is "address image," not "yourname@example.com". Normally, we'd insert into the ALT tag a bit of text that was as self-explanatory as possible. This text would fully describe the image for vision-impaired people who use automated "screen readers" to read Web pages to them audibly through their PC's speakers. In this case, however, placing the e-mail address into an HTML tag using ASCII text would make it visible to harvesters. This would defeat the spam-proof purpose of the image.

If you feel that the ALT tag absolutely must contain an audibly readable e-mail address, you can use obscured text to provide yourself with some protection against harvesting bots:

```
alt="chris at example dot com"
```

If a graphic has an ALT tag, the text within it is displayed in a small pop-up box called a "tooltip" when you hover your mouse pointer over the graphic in Microsoft's browser, Internet Explorer for Windows. This behavior isn't technically correct, however. Only text in TITLE tags is displayed in tooltips in Internet Explorer for Mac, Mozilla, Firefox, and other standards-compliant browsers.

If it's important to you that a tooltip pops up when a visitor hovers a mouse pointer over your graphic, put your text into a TITLE tag. Internet Explorer for Windows displays tooltips for both TITLE and ALT tags, so this will work for you in all browsers.

5. Level Three: Use Encoded Links

MANY WEB SITES allow you to click a link to start a new e-mail message. The correct "To" line is already filled in. This is convenient for visitors who wish to communicate with people associated with the site.

Unfortunately, harvesters can read the e-mail addresses that are contained in these links. The HTML tag that's used to generate these e-mail links is *mailto*. Here's what an ordinary mailto link looks like in HTML:

```
<a href="mailto:chris@example.com">Send me an e-mail</a>
```

The above snippet of HTML displays the following in a browser window:

Send me an e-mail

Harvesters see the raw HTML of a page, not just the words that appear on screen. Therefore, bots can vacuum up "chris@example.com" into their spam lists just as easily as if the address was visible as plain text.

Fortunately, it's a simple matter to encode your mailto links so they work perfectly in every browser but are ignored by harvesters. After testing several different methods, I recommend a tool that's available free at:

http://automaticlabs.com/products/enkoderform

Figure 13: The Anti-Spam Address Enkoder at AutomaticLabs enables you to create in one or two minutes a clickable "mailto" link that harvesters ignore. This spam-proofs the e-mail address.

(This service, which is now hosted by AutomaticLabs.com, was previously offered at a site called Hiveware.com.)

Using the AutomaticLabs method requires a bit more knowledge of HTML than the previous methods — but not much more. In just a few minutes, you can create your own clickable link that's invisible to harvester bots.

There are two steps in the process. I'll walk you through them on the next page.

How to create encrypted, clickable 'mailto' links

Step 1. Visit http://automaticlabs.com/products/enkoderform. An "Enkoder Form" page appears. Type your specific information into the Basic Form (see Figure 14). Use the "@" sign and "." in the address. These will be safely encoded. Use the following three lines as a guide:

E-Mail Address:	chris@example.com
Link Text:	Launch e-mail
Link Title:	chris at example dot com

Step 2. Click the Encode button. That's all there is to it.

Figure 14: Type just three lines of text into the form. This sets up a clickable "mailto" link that's protected from harvester programs.

How to place your clickable link on a Web page

After you click the form's Enkode button, AutomaticLabs displays a new page called Results (see Figure 15). The main text box on this page contains a JavaScript routine that's encoded. Pasted into the HTML code of a Web page, this launches a new e-mail message with your address in the To line. Simply select the Hiveware text with your mouse, then copy and paste it into your HTML where you want your link to appear.

Your new JavaScript code may be inserted at the top or bottom of a page, into the cell of a table, almost anywhere. Wherever you put the link, people can click it to start a message to you in their own e-mail program.

AutomaticLabs also offers an Advanced Form, into which you can enter sophisticated HTML tags, links, and images.

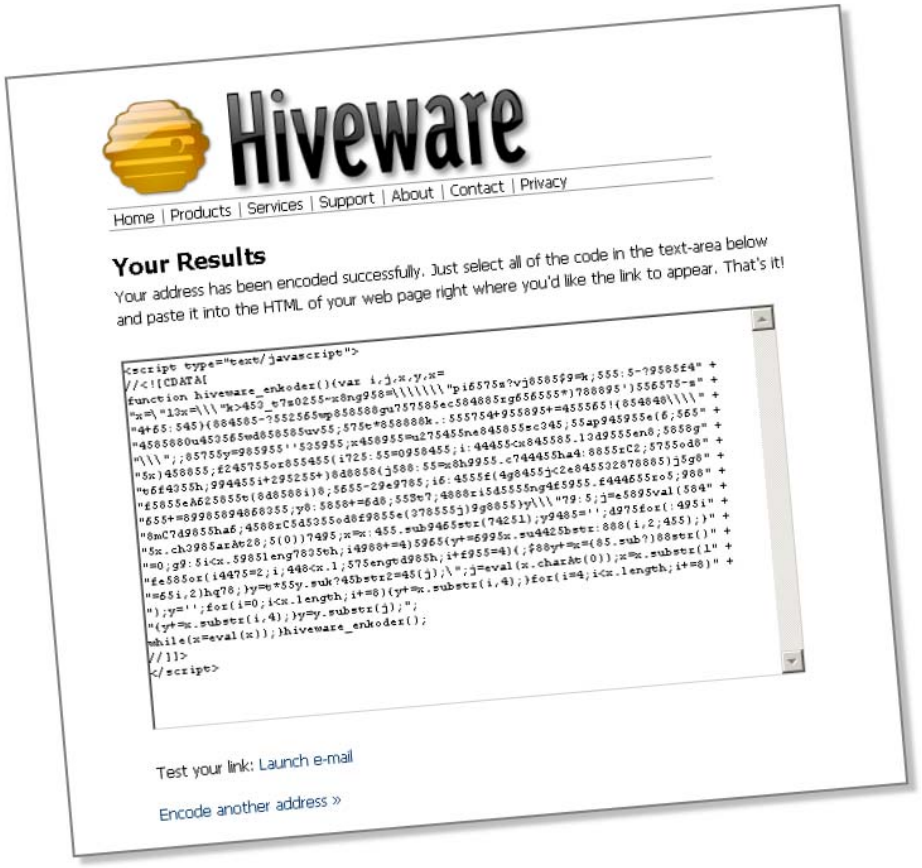

Figure 15: The routine produces a block of JavaScript that you copy and paste into your HTML code. Harvesters ignore the clickable link that results.

How the two different methods work together

Figure 16 is a duplicate of Figure 6 in order to remind us how an address image and an encrypted, clickable e-mail link can work side-by-side.

In Figure 16, the address on the left is an image that is not clickable. The blue underlined words on the right are a JavaScript encoded link that *is* clickable.

The reason to use both styles of the address is that, in some browsers, JavaScript is off. Approximately 1 in 10 browser users have disabled JavaScript, according to statistics from http://www.thecounter.com/stats/.

Figure 16: The e-mail address on the left (inside the ellipse) is an image that is not clickable. The words on the right are an encrypted JavaScript mailto link that *is* clickable.

People who've disabled JavaScript won't see the blue link and can't click "Launch e-mail." But the page is useful anyway, because the e-mail address in the image remains visible in all browsers. (Even people who've turned off images in their browsers can see and use the fields of the comment form farther down — a feature that I'll describe a bit later.)

When you hover your mouse pointer over the JavaScript link you made, you may notice that your browser's status bar says something like this:

```
mailto:chris@example.com
```

The text clearly shows users what to expect if the link is clicked. This is precisely what we want. Because a browser only needs to render one page at a time, it can easily decode the JavaScript almost instantly. But harvester bots can't and won't take this time. Interpreting the millions of lines of JavaScript code on Web pages — on the slim chance that an address might be found — would slow a harvester to a snail's pace.

6. Level Four: Forms and Related Steps

The contact page shown in Figure 16 contains a fill-in comment form. This is provided in case visitors don't have JavaScript enabled in their browsers or don't want to communicate by composing an ordinary e-mail at the moment. (They might be visiting the page while using an Internet café, and they prefer not to use the establishment's mail account.)

Avoid security nightmares with Web forms

If you use a comment form on your site — or you plan to add one — make sure that your Web form is secure. Insecure forms can be hijacked to send millions of spam messages that appear to be coming from your mail server (and *are* coming from your mail server).

For example, old versions of Formmail.pl — one of the Web's most widely used Perl scripts — had a flaw that allows outsiders to take control of your mail server in this way. One security researcher, Anders Brownworth, posts a page of workarounds that eliminate this possibility:

http://www.anders.com/projects/sysadmin/formPostHijacking/

If you know C or Perl, you can use free programs such as Nomailto.c and Nomailto.pl to make safe Web forms. These programs are described at:

http://www.turnstep.com/Spambot/avoidance.html

If you do host a comment form on your site, be certain that it's reviewed by professionals who've mastered the security issues that are involved.

Using contact forms to protect against posting

You might be 100% careful in spam-proofing your address. You've kept it from appearing in plain text in any of your Web pages. But all your care could be spoiled if other people naïvely post your address on the Net.

If a Webmaster doesn't have the time to make address images, ask for a link to your contact page rather than your address itself. The publications I write for must agree to post a link to "WindowsSecrets.com/contact" instead of posting my address. Harvesters have never found my address on these sites. You can ask the same from Webmasters you know.

7. Creating 'Disposable' Addresses

If your long-time e-mail address is deluged with spam, you may decide to start over and spam-proof an all-new address. If that's the decision you've reached, there are several tips that can help make this changeover the last switch you have to make for a very long time.

Using e-mail addresses you can throw away

One of the best ideas to prevent spam from ruining your e-mail account is the concept of "disposable" addresses. You give a different address to each person or company you communicate with. If someone puts one of your addresses on a spam list, you simply "turn off" the compromised address without interfering with your other addresses.

Figure 17: Various firms offer "disposable" addresses.

To test this concept, I signed up with a service named Mailshell.com in 2001. The company offered an unlimited number of disposable addresses. This allowed me to prefix Mailshell.com with my own label — e.g., whatever.mailshell.com. I could then make up fresh addresses that looked like this:

> I told Amazon.com I was "amazon@whatever.mailshell.com".
> I told eBay.com I was "ebay@whatever.mailshell.com", etc.

Since 2001, I've given out more than 300 different disposable addresses. These addresses have almost never received any spam. In three or four cases in which a Web site did allow an address to get into spammers' hands, I simply disabled the affected address by causing it to bounce.

Previous customers such as myself are still supported, but Mailshell no longer accepts new users to its disposable address service. That's OK, because numerous other firms do so, many of which are completely free.

'Basic' and 'advanced' modes of making disposable addresses

One free service that I recommend is called Spam Gourmet. Once you create an account, you make up a regular e-mail address with the service, such as:

user@spamgourmet.com

You never give out this address to anyone. Instead, you make up a different keyword every time you need to hand over an e-mail address to a Web site or whomever. This is followed by a number between dots. The number represents how many messages you're willing to receive from that sender, up to 20.

If you were giving your e-mail address to Amazon.com, for example, the address you make up might look like one of the following:

amazon.20.user@spamgourmet.com (can send 20 messages)
amazon.3.user@spamgourmet.com (can send 3 messages), etc.

You can use Spam Gourmet's "advanced mode," which is also free, to specify trusted senders. These people or companies are allowed to send an unlimited number of messages to you. You can also use the advanced interface to specify "watchwords." These are character strings that must appear in any new e-mail addresses that are created. This prevents someone from making up a new address that would forward mail to you.

To use Spam Gourmet, you must provide a valid e-mail address that you maintain someplace else. The service uses your working e-mail address to forward to you any mail that comes to your disposable addresses.

If Spam Gourmet doesn't suit your needs, a list of the top 10 disposable address services, assembled by About.com guide Heinz Tschabitscher, is posted at:

http://email.about.com/cs/dispaddrrevs/tp/disposable.htm

Using your own domain for disposable addresses

If you own (or your company owns) a domain name, you may be able to use it to create as many multiple addresses as you like. If your username is Brian at MyCompany.com, you could add disposable information after your username. A hyphen or plus sign might separate the info, like this:

brian-amazon@mycompany.com
brian+ebay@mycompany.com, etc.

This approach seems to be very popular with subscribers to the *Windows Secrets Newsletter*. Out of more than 140,000 subscribers, more than 2% of them have "brian," "secrets," or something identifiably disposable in the left half of their addresses. If I ever turn into a spammer — no, I never will, but if I did — these people would immediately nail me.

Avoiding dictionary attacks

Dictionary attacks, in which a spammer sends messages to every possible name at a company to see which ones don't bounce, were discussed in the chapter entitled "What Research Shows About Spam."

Companies can defend against such brute-force attacks by configuring their servers to disconnect from any party who sends messages in rapid sequence to hundreds of addresses that don't exist. The technical steps required to do this are beyond the scope of this e-book, but suffice it to say that you should call in security experts when planning such defenses.

If you've decided to switch to a fresh, new address — and you intend to keep it spam-free — your risk of dictionary attacks is greatest if you have an account with a major Internet service provider, such as AOL. Large ISPs often assign user names that are a first name followed by a series of digits — for instance, bob123@aol.com. To avoid having your new address randomly guessed by spammers, consider using a punctuation mark (a period, hyphen, or underscore) in your user name:

bri.liv@example.com, bri-liv@example.com, bri_liv@example.com

Adding just these three marks into a brute-force attack would quadruple the number of addresses that a spammer would have to test. They're more likely to limit their routines to easier names, leaving yours untried.

8. What About Spam Filters?

YOU MAY HAVE NOTICED that I haven't talked much about spam filters in this e-book. That's because I chose in this book to focus on ways you can *reduce* — not just *manage* — the spam you receive. Spam filters today are important for many companies, but they vary widely, including:

- **Block lists.** Programs that discriminate against IP addresses from which spam has come in the past;
- **Safe-sender lists.** Programs that give priority to mail from "approved senders";
- **Content filtering.** Programs that rate suspicious *vs.* legitimate words in messages to guess the probability that they're spam;

and many other variations.

The major weakness of these approaches is that they do nothing to stop spammers from sending out exponentially more spam year after year.

- **Spamhaus.org,** an anti-spam service, maintains data on unsolicited bulk e-mail (UBE). It shows that fewer than 200 spammers are responsible for 80% to 90% of all spam worldwide.
- **Brightmail.com,** a filtering technology company, estimates that — despite the small number of hardcore spammers — spam's rapid growth puts it in the majority, surpassing legitimate e-mail in 2003.
- **ePrivacyGroup.com** has stated that spam is exploding at a rate of 450% per year, based on 2002 figures provided by Declude.com.

Let's say spam is "only" doubling annually. In 24 months, will your mail server be able to scan and filter 4 times the spam volume it processes today? If so, look ahead just 36 months. Will you want your server to process 8 times the gigabytes of spam that it already receives?

The answer is no. That's why I decided to focus on steps you can take to make your e-mail addresses invisible to spammers and reduce the flow. That won't make spam a thing of the past, but it's a start.

9. Should Spam Be Illegal?

THAT BRINGS US TO THE FINAL QUESTION before us. If trends continue (and they may actually get worse), every e-mail server will soon have to face 8 times the bandwidth of spam that it's already receiving. Will there be a technical or a legal solution before the infrastructure we rely upon has a heart attack from the congestion?

The computer industry is notorious for its suspicion of government regulation. But in the case of spam, there will be no technical solution without the U.S. and other countries actually banning the sending of UBE and enforcing the prohibition. Spammers are raking in millions — and it's awfully hard to make people stop doing something that's not illegal.

Let me be clear that we should never support government censorship of content. We should oppose letting any government say, "The content of *this* message is OK, but the content of *that* message is not OK."

Fortunately, calling for a ban on spam is in no way advocating for censorship. The principle is clear and simple. Like fax machines, e-mail is a *receiver-pays* system. Did Recipient A request bulk e-mail from Sender B? If not, the bulk e-mail should be illegal, because spam is just plain theft:

- **You pay for the bandwidth and storage of spam,** whether through your company's servers or your Internet service provider, or both;
- **People who must pay by the minute to download e-mail** — which includes travelers and many residents of countries outside North America — bear direct costs worth billions of dollars (and no sense);
- **Users of services such as Hotmail.com must pay** annual fees if their storage exceeds a few megabytes — which can be *one day's* spam.

Unsolicited commercial *faxes* are already against U.S. federal law. Adding UBE to that ban would be a big help. The European Union and Australia have already passed total bans. America must do so, too. Yes, I know criminals ignore spam laws. But criminals ignore *all* laws. That's not a good argument against having laws. A total spam ban would energize the technical solutions that can attempt today to detect spammers.

Let's work to pass such laws — or give up on e-mail and go back to faxes!

About the Author

Brian Livingston is the author or co-author of 10 books, including *Windows Me Secrets* and *Windows 98 Secrets* (with Davis Straub) and *Windows 2000 Secrets* (with Bruce Brown and Bruce Kratofil), published by Wiley Publishing Inc. (which acquired the former IDG Books Worldwide). His books have sold 2.3 million copies and have been translated into more than 30 languages. At one time or another, his books have been the No. 1 best-selling computer book in the U.S., Canada, U.K., Brazil, Australia, and New Zealand.

As a follow-up to his books, he is the editor of a twice-monthly e-mail publication, the *Windows Secrets Newsletter.* Free subscriptions are available at WindowsSecrets.com.

He is currently a contributing editor of *Datamation.* He has also served as a contributing editor of CNET News.com, *PC/Computing, PC World, eWeek,* and *Windows Magazine.* As a contributing editor of *InfoWorld* from 1991 to 2003, he published over 600 columns that were syndicated to 75 countries, appearing in CNN.com and several other sites.

Livingston has 35 years' experience as a computer manager and technology writer. In 1991, he received the Technical Excellence Award from the National Microcomputer Managers Association for his advocacy of standards in the computer industry.

Technical Support

It is unfortunately not possible for the author to answer e-mailed questions regarding the topics in this $9.95 e-book. If your company has significant information-technology needs, a per-day consultation may be arranged. To start the process, contact Brian Livingston's research director, Vickie Stevens, at:

research@BrianLivingston.com

This page was included but left blank to provide a multiple of 4 pages for booklet-style printing.

NOTES

For book shelving:
Print the cover page and this page. Insert them into the clear overlays of a binder.

Spam-Proof Your E-Mail Address

2nd Edition