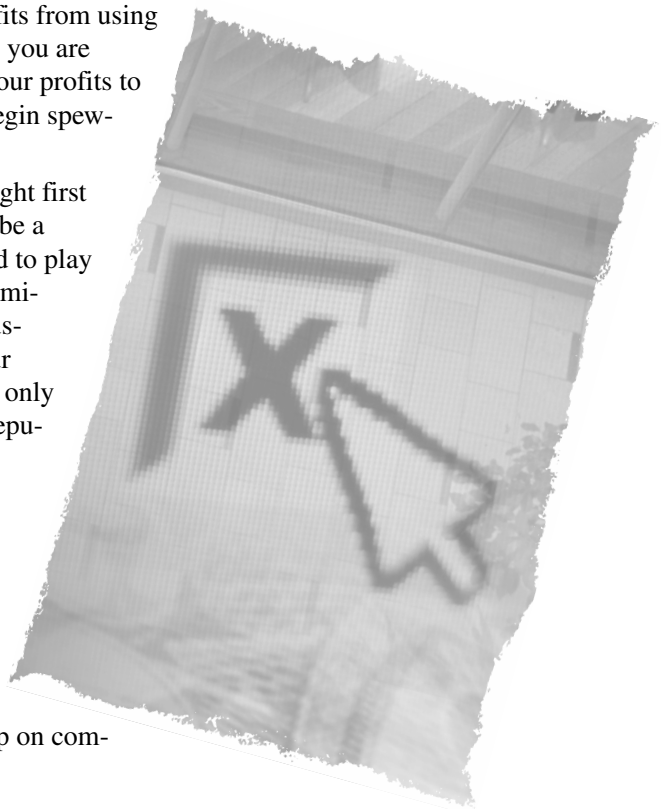
Part 1

Getting Started in E-Business

You do not have to launch a new "dot-com" or move your existing business online to realize tremendous profits from using the Internet in your business. On the other hand, you are going to be greatly disappointed if you expect your profits to explode just because you put up a Web site or begin spewing great gobs of promotional email.



Establishing a business Web site can be the right first step, but your brand new business Web site will be a waste of money unless it is consciously designed to play a strategic role in an integrated business plan. Similarly, using email to reach out and touch your customers can produce tremendous benefits for your bottom line, but improperly used, email will not only waste your time and money, it can wreck your reputation and wreak havoc with your business.

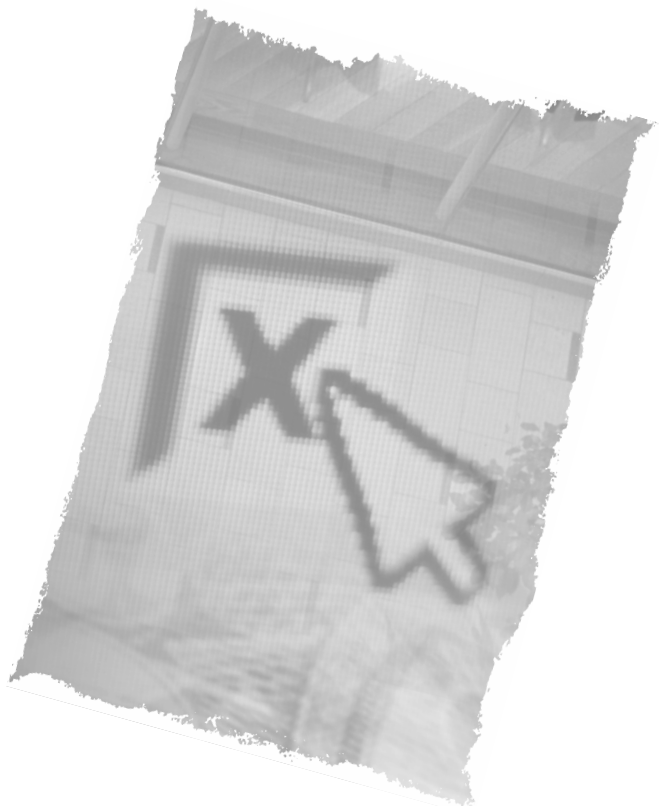
One day in the not-so-distant future, all businesses, large and small, will have Web sites and routinely use email, just as businesses today have universally adopted the fax and phone. Once fully integrated into the business community, Web sites and email will become just two more "traditional" business tools. Business owners and managers today can get a leg up on com-

petitors by immediately and aggressively embracing the Internet and the new strategies it makes possible. To get the most out of this powerful new medium without risking the farm in the process, keep doing what you already know works, and carefully evaluate each new tactic you decide to test, adopting and expanding those that prove their worth by making your business more profitable.

The chapters in Part 1 offer a discussion of the relevant issues and suggest lots of specific ways to use email and a business Web site to improve your profits. We will get to your Web site soon enough, but let's begin where the real power of the Internet can best be captured for big profits: in email.

1 Responsible Email Targeting

In this chapter . . .



As you consider employing the powerful new capabilities of email in your business, you need to become comfortable with the medium yourself. If you have not already done so, get with the program! Get into the habit of using email first wherever possible. You will find it saves you time and improves your communications effectiveness—and, as a bonus, it will help you gain expertise in using the medium as a promotional tool.

It is important that you leap over the novice stage in the use of email, because novice mistakes in email will make you look amateurish and stupid. Essentially, avoiding these mistakes requires that you adopt a conservative writing style and that you always edit your own messages before sending them. Be sure to keep your spell checker turned on as well! See the box for more advice about proper form in the use of email.

Common Mistakes in Email

Be sure you do not make these mistakes in your business email correspondence:

- ***Improper use of capitalization***
- ***Failure to capitalize the personal pronoun, "i"***
- ***Failure to capitalize the first words of sentences***
- ***Capitalizing EVERYTHING IN THE MESSAGE***

In email, using all-caps is the equivalent of SHOUTING! So do not do it—unless you mean to SHOUT!

- ***Improper use of, or omission of, punctuation***

Periods, commas, and other common punctuation should never be omitted. These elements are just as important in an email message as in any other written communication. They are there to help the reader understand your meaning. Make sure they are there in your messages.

- ***Typos***

ALWAYS (see, I am SHOUTING) edit your message before sending. Nothing less than perfect spelling, grammar, and punctuation is the standard in business communications, and that same standard applies in email as well as in conventional written correspondence.

- ***Overuse of "smilies"***

The cute little "emoticons" used commonly to convey attitude ought to be used sparingly, if at all, in your business communications.

These symbols are read by turning your head to the left and viewing the smilie as if it were vertical.

The Unofficial Smilie Dictionary (original source unknown; found lots of places on the Internet)

:-) Your basic smilie. This smilie is used to inflect a sarcastic or joking statement, since we can't hear voice inflection over email.

;-) Winky smilie. User just made a flirtatious and/or sarcastic remark. More of a "don't hit me for what I just said" smilie.

:-(Frowning smilie. User did not like that last statement or is upset or depressed about something.

:-I Indifferent smilie. Better than a frowning smilie but not quite as good as a happy smilie.

:-> User just made a really biting sarcastic remark.. Worse than a :-)

- **Use of chat room abbreviations**

Youngsters who have taken to email like ducks to water have developed a shorthand for communication in a chat room setting that has spilled over into email. Such abbreviations as *ttfn* (ta-ta for now) *brb* (be right back), and *lol* (laughing out loud), among many others, are convenient communication tools in a fast-paced medium such as online live chat, where all the players understand the abbreviations. In business communication, however, you need to consider that many of your readers will not understand them, so you must retreat to the conservative position and spell out expressions in order not to leave anyone out.

- **Failure to respond quickly**

All email users expect a fast reply. After all, they know you received their message almost immediately following their sending it. Many will sit impatiently, waiting for a response. You will reap tremendous advantages by simply responding quickly to email messages. Just set up your email to sound a chime when a message comes in, stop what you are doing, and look at it. If possible, reply immediately. Even a simple reply, such as "I just got your message and will be back with an answer by 10:00," will be greatly appreciated.

Used in a responsible manner, email is emerging as the most valuable new capability offered by the Internet, but what exactly constitutes "responsible" business use of email?

OPT-IN OR OPT-OUT?

What some people consider a responsible use of email, others consider an unacceptable abuse of the free Internet. Although the issue is not yet settled, we are rapidly moving toward a workable set of standards for responsible business use of email. Everyone agrees that email with commercial content can ethically be sent to people who were first asked and who then agreed to receive the commercial messages. This system, referred to as "opt-in," or "permission marketing," represents the most conservative position on responsible business use of email. The essence of this position is expressed in the guidelines for the commercial use of email issued by Mail Abuse Prevention System LLC (see box).

MAIL ABUSE PREVENTION SYSTEM LLC, GUIDELINES FOR RESPONSIBLE USE OF COMMERCIAL EMAIL (HTTP://MAPS.VIX.COM/MANAGE.HTML#GUIDELINES)

Principles:

All communications must be consensual.

No persons should ever have to unsubscribe from a list they did not intentionally subscribe to.

Guidelines:

Permission of new subscribers must be fully verified before mailings commence. This is usually accomplished by means of an email message sent to the subscriber to which s/he must reply, or containing a *URL* [URL stands for uniform resource locator, also commonly called the domain name] which s/he must visit, in order to complete the subscription. However it is implemented, a fundamental requirement of all lists is for *verification* of all new subscriptions.

There must be a simple method to terminate a subscription. Mailing list administrators must provide a simple method for subscribers to terminate their subscriptions, and administrators should provide clear and effective instructions for unsubscribing from a mailing list. Mailings from a list must cease promptly once a subscription is terminated.

There should be alternative methods for terminating a subscription. Mailing list administrators should make an "out of band" proce-

dure (e.g., an email address to which messages may be sent for further contact via email or telephone) available for those who wish to terminate their mailing list subscriptions but are unable or unwilling to follow standard automated procedures.

Undeliverable addresses must be removed from future mailings. Mailing list administrators must ensure that the impact of their mailings on the networks and hosts of others is minimized. One of the ways this is accomplished is through pruning invalid or undeliverable addresses.

Mail volume must take recipient systems into account. List administrators must take steps to ensure that mailings do not overwhelm less robust hosts or networks. For example, if the mailing list has a great number of addresses within a particular *domain,* the list administrator should contact the administrator for that domain to discuss mail volume issues.

Steps must be taken to prevent use of a mailing list for abusive purposes. The sad fact is that mailing lists are used by third parties as tools of revenge and malice. Mailing list administrators must take adequate steps to ensure that their lists cannot be used for these purposes. For example, administrators can maintain a "suppression list" of email addresses from which all subscription requests are rejected. Addresses would be added to the suppression list upon request by the parties entitled to use the addresses at issue. The purpose of the suppression list would be to prevent subscription of forged addresses by unauthorized third parties. Such suppression lists should also give properly authorized domain administrators the option to suppress all mailings to the domains for which they are responsible.

Terms and conditions of address use must be fully disclosed. Mailing list administrators must make adequate disclosures of how subscriber addresses will be used, including whether or not addresses are subject to sale or trade with other parties. Also, conditions of use should be visible and obvious to the potential subscriber. For example, two lines buried deep within a license agreement do not constitute adequate disclosure.

Acquired lists must be used for their original purpose. Those who are acquiring fully verified opt-in lists must examine the terms and conditions under which the addresses were originally compiled and determine that all recipients have in fact opted-in to the type of mailing list the buyer intends to operate.

The nature and frequency of mailings should be fully disclosed. List administrators should make adequate disclosures about the nature

of their mailing lists, including the subject matter of the mailings and the anticipated frequency of messages. A substantive change in the frequency of mailings, or in the size of each message, may constitute a new and separate mailing list requiring a separate subscription.

One subscription, one list. Addresses should not be added to other lists without fully verified consent of the address owner. It should never be assumed that subscribers to a list about foo want to be added to another foo list, let alone a list about goo. A notification about the new mailing list may be appropriate on the existing mailing list, but existing subscribers should never be subscribed automatically to the new list.

Source: Mail Abuse Prevention System, LLC http://maps.vix.com/manage.html#MAPS_Principles, accessed 4-13-2001.

An important advantage of permission marketing is that you can learn a great deal more about your recipients than just their email addresses. While you are asking their permission to send them your commercial messages, you can also learn their names, zip codes, what categories of product they like, and more. With each piece of information you gain about your customers and prospects, you can better target their specific needs and desires, allowing you to make their lives better while improving your profits as well.

Opt-in—permission marketing—offers the very best opportunities for effective use of email, no matter what your business. You should use opt-in systems whenever and wherever you can find the means. Detailed instructions for setting up an opt-in system are provided in Part 2.

OPT-IN IN PRACTICE

A good example of opt-in, or permission marketing, can be found on the Web site of Trend Micro (http://www.antivirus.com). This company, which markets antivirus software, makes itself a welcome presence by offering free "house calls" during which, after you download a small program, they will scan all your hard drives for viruses at no charge. Once you have installed their antivirus program, the company offers regular email updates on any new viruses going around. The email updates, which the recipients can cancel at any time, then become a vehicle for keeping Trend Micro and its products high in the minds of the company's customers.

In "opt-out" systems the business owner assumes he has permission to send commercial messages until told otherwise by the recipient. To use an "opt-out" system responsibly requires that the recipients be carefully targeted. Sending commercial email to people about whom you know nothing but their email address is irresponsible use of email, also known as spam.

SPAM: CANNED MEAT PRODUCT OR JUNK EMAIL?

Spam is not an abbreviation for anything. This derogatory nickname for junk email is just an adolescent attempt to be humorous. The youngsters who populated the Internet when it was first opened to the public applied the nickname to the junk email that was beginning to proliferate, and it stuck, much to the dismay of the brand owner. Here is the quote from a Monty Python skit that inspired the name spam to describe junk email. A waiter is explaining what they have on their menu:

> "Well there's egg and bacon; egg, sausage and bacon; egg and spam; bacon and spam; egg, bacon, sausage and spam; spam, bacon, sausage and spam; spam, egg, spam, spam, bacon and spam; spam, spam, spam, egg and spam; spam, spam, spam, spam, spam, spam, baked beans, spam, spam, spam and spam; or lobster thermidor aux crevettes with a mornay sauce garnished with truffle paté, brandy and a fried egg on top of spam."

Source: The Complete Monty Python's Flying Circus : All the Words, Volume 2 by Graham Chapman, Monty Python, Pantheon Press, Publisher.

Let me be clear. I do advocate the use of an opt-out email system provided you meet the following conditions:

- You know enough about the recipients, before sending any email, to be reasonably sure they are potential customers for what you offer.
- You do not attempt to hide your identity as the source of the email you are sending.
- You provide a working "from" or "reply to" address in the messages you send so that recipients can contact you if they wish.
- You remove permanently from your mailing list the address of anyone who requests that you do so.
- You do not violate the Acceptable Use Policy of your ISP (Internet Service Provider) or your mail service provider.

If you carefully follow these guidelines, very few will object to receiving your mailings, and you will violate no laws that are currently in force or likely to be passed any time soon.

RESPONSIBLE OPT-OUT IN PRACTICE

An accounting software company collected approximately 6,000 email addresses of CPAs located in the five-state area by searching the online professional directories. The company planned to send periodic mailings to these professional accountants promoting the software product as a good solution for the CPAs' clients.

An irrigation pump manufacturer collected over 3,000 email addresses of landscape architects from a variety of on- and offline directories. The manufacturer sends periodic promotions inviting the architects to visit the manufacturer's Web site to learn more about the advantages of the pumps offered.

A local restaurateur who collected 400 email addresses of downtown workers by offering a drawing for a free lunch now sends weekly announcements of the lunch specials to these addresses.

A local Economic Development Authority began mailing all the members of the local area Chamber of Commerce and others in the professional community a monthly "economic update" without obtaining the permission of any recipient.

A university student collects the email addresses of other students wherever he can and sends an email to all, advertising his willingness to buy used textbooks near the end of the term.

Only the most conservative anti-spam advocates would consider the examples just cited to be spam, and neither the bills pending in the U.S. Congress nor any of the 17 state laws currently regulating commercial email would classify these applications as illegal spam.

SPAM AND THE LAW

U.S. Federal Law: As of January 2001, no anti-spam laws have yet been enacted at the federal level, but no fewer than ten are under consideration, with one having already passed the House and now being

considered by the Senate. Most likely to be first signed into law sometime in 2001 is a regulation modeled after the California law discussed below.

California: This law permits ISPs to sue those whose send spam if it is a violation of an ISP's policy, and imposes criminal penalties upon those who hide the address from which the message is sent. A related California law requires spam to include opt-out instructions with a toll-free telephone number or a valid return address. This law also requires senders to honor opt-out requests and requires email advertisements to contain "ADV:" or "ADV:ADLT" at the beginning of the subject line so that recipients can filter out the advertisements if they wish. Damages in the amount of $50 per message sent, up to $25,000 per day, are permitted.

Washington: While Nevada enacted an early anti-spam law making spam illegal under certain conditions but providing no penalties for violations, Washington state had the first anti-spam law with teeth. The Washington law prohibits sending spam from any computer in the state of Washington or to any address in Washington. In defining spam, the law prohibits hiding the address from which the message is sent and using a misleading subject line. Damages are specified at $500 per message sent (!) and $1,000 per server affected.

Virginia: Several spam laws in Virginia make it a crime to hide the address from which the message is sent or to sell software that is designed to make that possible. Damages of $10 per message, up to $25,000 per day, are permitted.

Since the establishment of these laws in Washington, Colorado, and Virginia, the states listed below have also enacted anti-spam laws, which contain a wide range of provisions.

Colorado	Missouri
Connecticut	North Carolina
Delaware	Oklahoma
Idaho	Pennsylvania
Illinois	Rhode Island
Iowa	Tennessee
Louisiana	West Virginia

Even though the methods by which you decide to whom you will send your commercial email are well within the law, you should use opt-out sparingly and carefully. Some recipients will strongly object even to responsible opt-out approaches,

such as the examples listed earlier, and these people can cause you lots of problems if they happen to object to receiving one of your messages.

The ethics and values of our customers and prospects are quite different on- and offline. It is vital to remember that people are far more sensitive *online* than they are *offline* and that they have the means to inflict a great deal of pain on anybody they see as an online offender. Be aggressive in your email usage, *but be careful*. Whether you use opt-in or opt-out, test every email tactic you plan to use on a small group of typical recipients, then on a moderate-sized group, before launching into the full campaign.

Unpleasant fallout from these early tests can often be contained, whereas the repercussions from just charging ahead may be disastrous. Besides, you can run multiple tests in just a few hours. Why take unnecessary risks?

In the sections of this book that follow, you will learn about several powerful email strategies you can use in your business. Before I go on, let me address the most tempting tactic of all: blatant spam.

WHY NOT SPAM?

Right up front, let me repeat: sending spam is not a responsible use of the power of the Internet and you ought not to do it. If you buy that statement straight up, you can skip this section. If, like a lot of my clients, you are curious to know what is so wrong with spam, read on.

What can you do with email? The first obvious response from early Internet business people was to get lists of email addresses for all potential customers and send them promotional messages. After all, email is free, right?

As it turns out, email is anything but free. Unlike junk mail, for which the sender pays the cost of the postage and the mail piece and therefore the full cost of its delivery, the cost of email is borne mostly by the recipient, or more accurately, by the person who operates the recipient's email server. If you buy Internet access from AOL, for example, along with your Web access, you also get email from AOL. When anyone sends junk email to you, AOL bears the cost. Of course, that cost is ultimately passed on to you and the other AOL subscribers in the form of higher costs than there would be if there were no spam.

When the post office receives complaints about junk mail, they are not especially sympathetic. After all, they make good money from all that junk mail because postal rates are set so that each class of mail pays its own way. However, when a recipient of spam (junk email) complains to her Internet Service Provider (ISP) who also usually operates her email server, she gets a very sympathetic hearing. Outfits

like AOL and MSN don't want to handle such mail because it arrives in great quantities, tying up the server and forcing them to invest in more computers and in greater bandwidth to handle it all. The ISP responds to all this unwanted traffic in a variety of ways. First they set up email "filters" to automatically reject mail coming from Internet addresses and domains that are suspected of sending spam. When some spam does get through the filters, the email system operator or SYSOP (short for system operator) traces the email back to its origins and complains (loudly!) to the person operating the sending email server, and to the host of any Web sites referred to in the message, and to all their respective upstream connection services. The result? A minute or two after the first batch of spam is noticed by an activist recipient or an alert SYSOP, the sender's email account and Web site are closed.

SPAM AND THE INTERNET

The Hormel company does not think that disparaging their canned meat product in this way is funny at all, but they have pretty well accepted the reality that spam now refers both to a tasty canned meat product and the junk email we all love to hate. Below is an official statement excerpted from the Hormel website (http://hormel.com) on January 8, 2001.

"You've probably seen, heard or even used the term 'spamming' to refer to the act of sending unsolicited commercial email (UCE), or 'SPAM' to refer to the UCE itself. Following is our position on the relationship between UCE and our trademark SPAM.

"Use of the term 'SPAM' was adopted as a result of the Monty Python skit in which a group of Vikings sang a chorus of 'SPAM, SPAM, SPAM . . .' in an increasing crescendo, drowning out other conversation. Hence, the analogy applied because UCE was drowning out normal discourse on the Internet.

"We do not object to use of this slang term to describe UCE, although we do object to the use of our product image in association with that term. Also, if the term is to be used, it should be used in all lower-case letters to distinguish it from our trademark SPAM, which should be used with all uppercase letters.

"This slang term does not affect the strength of our trademark SPAM. In a Federal District Court case involving the famous trademark STAR WARS owned by LucasFilms, the Court ruled that the slang term used to refer to the Strategic Defense Initiative did not weaken the

trademark and the Court refused to stop its use as a slang term. Other examples of famous trademarks having a different slang meaning include MICKEY MOUSE, to describe something as unsophisticated; TEFLON, used to describe President Reagan; and CADILLAC, used to denote something as being high quality."

Position Statement on "Spamming"

"We oppose the act of 'spamming' or sending unsolicited commercial e-mail (UCE). We have never engaged in this practice, although we have been victimized by it. If you have been one of those who has received UCE with a return address using our website address of SPAM.com, it wasn't us. It's easy and commonplace for somebody sending UCE to simply adopt a fake header ID, which disguises the true source of the UCE and makes it appear that it is coming from someone else. If you have or do receive UCE with this header ID, please understand that it didn't come from us."

Source: Hormel Web site: http://www.spam.com/ci/ci_in.htm, accessed 4-13-2001. With permission.

A rather large group of self-appointed anti-spam vigilantes have arisen to fight the "evil spammers." These folks have developed sophisticated and aggressive methods for thwarting spam. They take tremendous delight in mounting campaigns to have targeted domains which they suspect of harboring spammers banned from important areas of the Internet such as AOL and MSN. Obviously, if a domain is blocked from sending mail to AOL's 22-plus million subscribers, the spammers using that domain are greatly disadvantaged in their promotional efforts.

The primary weapon anti-spam activists use is the email filter. The domain names of ISPs and other email server operators who are found to be allowing spammers to send their mail, are relegated to the dreaded "Realtime Blackhole List" (RBL). Here is how it works. Think of the domain name as the "city" part of the Internet address. Once an operator's domain name has been placed in the RBL, all the other Internet operators who subscribe to the free RBL service, and a large majority of ISPs do subscribe, will automatically block all of the email originating from the offending operator's server. That is analogous to all the post offices in the country automatically rejecting any mail from Cincinnati! The businesses and people who live in Cincinnati may soon choose to live elsewhere if they cannot get their mail out! The same is true for the Internet, only faster. Once a user realizes that her email cannot get through to her friends, she does not care why. She is gone in less than a week. If you want to get the attention of an ISP, just threaten to put their domain name into the RBL and watch them fall all over themselves to correct the problem.

Organized Anti-Spam Efforts
The Realtime Black Hole List (RBL)
(http://maps.vix.com/rbl/)

This project, run by Mail Abuse Prevention System LLC (MAPS) began in 1997. MAPS maintains a list of all the sources they can identify from which spam appears to originate. The Internet address of each of these sources, once identified as a source of spam, is added to the RBL. Thousands of cooperating ISPs routinely block these blacklisted sources, rendering them inaccessible to all the subscribers of the cooperating ISPs. Those in the RBL cannot then send or receive email. Any Web pages that reside on these blacklisted sites cannot be seen by the cooperating ISPs' subscribers.

The stated purpose of the MAPS RBL is to punish the ISPs who harbor spammers, and so encourage them to police their subscribers' activities, canceling accounts as needed to prevent spamming.

Open Relay Behavior-Modification System (ORBS)
(http://www.orbs.org/)

ORBS is a system that looks for email servers worldwide that permit so-called third party relaying of email. Such servers are added to the ORBS list, and that list is then used by thousands of legitimate ISPs to block traffic from the listed sites. Spammers routinely search for such relay servers because by routing their spam through an offshore server, say somewhere in Yugoslavia or Brunei, they can more effectively hide their identity and location from those who would like to use their "smite thee" button (if they had one, that is). Another reason spammers are likely to hijack these accessible servers is that they are frequently run by novices to the Internet world who are unaware of the penalties for permitting spam.

It is testament to the economic power of email that we still, in spite of these significant and powerful disincentives, find our email boxes brimming with spam every day. Email works!

Two kinds of businesses that routinely use spam are get-rich-quick and porn vendors. Since these fringe businesses have a difficult time keeping a Web site up

even when they use more legitimate promotional methods, they must figure they have little to lose by employing spam. Their markets tend to be very general, with almost any email recipient a potential customer for these "products."

WHO ARE THESE SPAMMERS?

Jason Heckel has the dubious distinction of being the first spammer to be sued under the Washington state anti-spam law. Jason was a 24-year-old man living in Oregon when he decided to use spam to sell a 47-page booklet he wrote, titled *How to Profit from the Internet*. According to newspaper reports, he used a bulk email program called *Extractor Pro* to harvest email addresses from the Web and then to send from 100,000 to 1,000,000 messages a week advertising his $39.95 booklet. His sales were reported to be around 40 books, or approximately $1,600 a month. Fortunately for Mr. Heckel, the suit was thrown out as being unconstitutional. Following the ordeal of the lawsuit, however, Mr. Heckel has reportedly stopped spamming.

Sam Khuri, owner of the Benchmark Print Supply Company of Atlanta, Georgia, was sued for spamming by BiblioTech, his ISP located in London, England. Khuri was selling toner cartridges using an email promotion. The problem for the ISP was that a large volume of email messages Khuri attempted to send had incorrect email addresses. As a result, the BiblioTech mail server was overloaded by all the "bounced" mail and was actually down for three days.

Adrian Paris, operating under the business name ProPhoto UK back in 1998, sent more than a quarter of a million email messages using the ISP Virgin Net. When the ISP began receiving complaints and demanded that Paris stop sending his spam, he apologized, claiming the emails were sent out by mistake and promised to stop. He then set up another Virgin Net account and recommenced spamming. This time, though, his efforts caused Virgin Net to be added to the Real-Time Black Hole List (RBL), the ultimate weapon of the anti-spam vigilantes, which greatly impedes the ability of legitimate email to move through the ISP and can even mean the demise of the ISP as a viable business. Virgin Net then sued Paris following his repeated spamming efforts. The lawsuit was settled before reaching court, with Paris agreeing to pay about $8,000 in damages and to cease spamming through the Virgin Net system. Paris was selling bulk email lists of 1 to 10 million addresses, for about $40 to $250.

Let me say to any of you still thinking about having a go at spamming, just realize that using pure spam will relegate you to the lower reaches of the on- and offline communities. You may find it embarrassing to admit to your friends and business associates that you are a spammer. Your spouse will probably give you flack for doing it. Hostesses at restaurants will make you sit near the kitchen door, and drivers will yell obscenities at you. Dealing with the people who offer such spam support services as bulk email lists, bulk mail software, bulk-safe Web sites, and bulk-safe email accounts may make you feel like showering more often. The odds are very good that you will get taken lots of times before you find anybody reliable in that support community. You can expect to buy host space and email accounts that promptly get closed down, despite your having paid hundreds of dollars extra for these services because some smiling con artist has assured you that his email account service is bulk friendly. In this community the terms are always cash in advance and no refunds. This is the floating crap game of the Internet world, and the dice are most definitely loaded. Play this game at your own risk, and don't say you weren't warned.

EMAIL LIST DEVELOPMENT . . . . . .

There is an easy way and a hard way to obtain your email list. I am sorry to have to tell you that the hard way is generally going to produce the best long-term results for your business. First, though, let's consider the easy way: renting or buying lists.

Buying Lists

"1,000,000 email addresses. Clean and all brand new! Just $299!"

"35,000,000 email addresses on CD-ROM! Free with the purchase of our $299 bulk email program!"

"25 Million Free Email Addresses With Purchase [of bulk email software]!"

"1,000's of email lists where you can advertise without spamming!"

Should you start shopping for address lists to use in your direct email marketing efforts, and there are certainly plenty to choose from on the Web; in the spam you receive, you will find a stunning range in prices—from $.0000085 or even less to $.30 or more an address! The top price is over 35,000 times the bottom price! What is the deal?

There are actually several factors at work. First, as I've already said, those offering to sell bulk email lists are almost universally despised, so you are not dealing with mainstream business people. These folks are not above "generating" email addresses by using a software program. Historically, this has been done with CompuServe ad-

dresses, which not long ago used to contain a ten-digit numerical account "name," followed by "@compuserve.com." With a setup like that, it is easy to see how a computer could generate several million such addresses in just a few minutes by repeatedly scrambling the digits. How many such randomly generated addresses are likely to be good? In one study, less than 4% were good addresses. That means more than 960 out of a thousand messages sent were bounced back for a bad address!

Most of the customers for bulk email lists are business novices trying to capitalize on the Internet gold rush. Like most novices, they are easy to bamboozle. After all, what is a mere $1,000 minimum when the budding capitalist expects to make $50,000 in Internet sales by tomorrow afternoon! The hype in the realm of bulk email will take your breath away.

Renting Lists

When you rent a mailing list for ordinary "snail mail" (regular postal mail), the list is delivered pre-printed on mailing labels. You use the list one time and then rent it again if you wish to send a second mailing to the same folks.

In email, when you rent a list, you never even see the addresses. If the list owner showed you the email addresses, you could just copy them for reuse as often as you liked. Obviously, the list owner would not like that. Customers would quickly get tired of getting too much email and would opt out or start doing hostile things.

If you never see the addresses you are renting, you must be careful. As in most projects having to do with Internet marketing, you need to move one step at a time. Start with a little test, then increase to a larger test, then a little larger, and so on, until you get where you want to be. A reputable company will assist you in such an approach. Beware the guy who insists on a great big program out of the starting gate. Such an approach is dangerous. On the happy side, you might get such a great response that you become overwhelmed with orders or inquiries, with the result that many of the leads you spent money to generate end up going to waste before you can get back to them. On the darker side, if your vendor is not on the up-and-up, and you pay for a big mailing, the negative reaction it triggers can sink your ship before you know what hit you.

Building Lists

When you think about developing an emailing list for your business, you might consider using one of the harvesting software programs. Here is how they work: The harvesting program sends instructions for a search to each of the search engines on the Web, just as if you were visiting the search engine site and had entered your chosen

search term at that site. When the search engine sends the search results back to your computer, the program intercepts them, and instead of displaying the page in your browser, it searches through the page looking for "@" symbols. Each time it finds one, it assumes it is in the middle of an email address. All it has to do then is find the front and back ends of the address and put the whole thing into a text file, then go on with its search. A modern harvesting program running on a typical powerful desktop PC can search through thousands of pages an hour, collected from dozens of search engines. Sounds great, right?

In theory, harvesting addresses will produce a high-quality list if you choose search terms related to what you sell. The claim of the harvesting software vendors is that the address owners are likely to be interested in what you have to offer and the addresses harvested will be current and active. By targeting the harvesting program on special interest sites, the claim is, you will be able to collect addresses of individuals as well as companies.

In practice, harvesting addresses is a waste of time. Consider first the quality issue. Try this: visit AltaVista (http://www.altavista.com), one of the best search engines on the Web. Enter a search term and view the results. The first several listings are almost certainly relevant, but go down a few pages. What you will find is that, after the first two or three pages, the remaining thousands of pages that were returned are not the least bit relevant to the search terms you entered. In fact, it requires a very technical analysis even to see why the search engine chose to return most of the pages.

Another thing you will find is that a harvesting session will return a very high percentage of SYSOP addresses. Web developers and systems operators frequently put their addresses in a "footer" at the bottom of each Web page for the benefit of those who need technical assistance related to the page. (A footer is a few lines of text set up to appear automatically on each page.) These technical people are exactly the people a spammer does *not* want in his list. These folks have the means and the attitude to do you the most harm in the shortest time possible. If you want to see a rapid and hostile response, just send a spam message to a bunch of SYSOPs!

How about freshness of addresses? Netizens (net denizens) are nothing if not adaptable. Today we have all learned that the more often we put our email address out there, the more spam we receive. Many folks use free "throwaway" addresses at Hotmail or Yahoo, which they change frequently when they start getting too much spam. Web page owners, especially those whose pages contain directories of email addresses, also use a number of tactics to make harvesting more difficult, such as replacing the "@" symbol with some other character.

As has often been observed, there's no such thing as a free lunch.

Okay, here is the hard way to build and maintain your own prospect lists. Forget automatic harvesting. Forget the mailing list vendors. You do not need them, and if you try to use these tactics, you will probably suffer more than you prosper.

What does that leave? Simply put, collect your existing customers' addresses and dig for prospects' addresses using conventional methods, the Internet, your Web site, and any other tactics you can think of. Using these tactics you will not generate a list with millions of addresses on it. Your list will not even have hundreds of thousands of addresses. Your list will probably begin with just a few dozen or a few hundred email addresses and/or names. As you work on it, your list will grow to thousands, but they will be thousands of interested potential or existing customers, and if properly managed, this list can easily become your most valuable business asset.

Collect your customers' addresses at every opportunity, one at a time. Set up systems to collect each customer's email address automatically during the sales process or during any customer contact event. Pay bonuses to employees for meeting a quota of addresses—but be careful that you do not reward employees for unethical collection practices.

Collect your prospects' addresses wherever you can legitimately find them. If you exhibit at trade shows, make sure all the cards you collect in your fishbowl have an email address on them. If your customers have a common interest—quilting, auto mechanics, antiques, or whatever—find their special interest groups on the Web and mine their email address directories. Sending a promotion for quilting classes to a list of quilting club members is fair practice in most peoples' minds. Just be sure that you honor any remove requests when you get them.

Collecting the addresses of prospects when they are individuals with no organizing behaviors to help identify them is a lot more difficult, but savvy business promoters can still manage to do it. Two tried and true methods are customer referrals and contests. Ask customers for the names and addresses of friends who could be interested in what you have to offer. If they do not have their friends' addresses, look them up on the Web. Several great personal address directories let you do this for free. For a tutorial on finding addresses, take a look at the CD included with this book.

How to Find Email Addresses Online

If you run contests as part of your existing promotional efforts, make sure all entrants provide their email addresses.

Sometimes it is also a good idea to join forces with your competitors or with complementary business associates to create a joint address list for prospecting use by all. In a mall setting, for example, the mall operator or a cooperative of all the tenants could effectively work to collect customer addresses to be shared with other tenant businesses as a reciprocal service. Probably the best way to do this would be to have a joint mailing once a month or so, in which short, separate messages are carried for all

the participating tenants. Once prospects become customers of yours, of course, you should put them on your customer list and handle them differently.

If your customers are businesses or organizations rather than individuals, and you have a well-defined market with just a few hundred potential customers you have already identified, call them and have a chat with their receptionists in which you ask for their email addresses. You can also request their fax numbers, as well as their street and Web addresses. Try also to get the name of the proper contact in their organization. Most will provide the information without question. If asked, just be honest. Tell them what you sell and ask for permission to put them on your mailing list. If what you provide is of interest to them, they will rarely say no. If what you provide is not, they will rarely say yes. All in all, this is a good thing. Why would you want to waste your time and money sending promotional messages to those who will never buy?

Make email your default contact method. It is so much cheaper than any other method that you would be foolish to use anything else when you have a choice. Note: By a large majority, most folks still do not have email addresses, so you need to continue to use your other methods. Just make it a point to get the email address and use this method when you get the opportunity. It will pay tremendous dividends.