The New York Times
nytimes.com

April 22, 2003

Internet Is Losing Ground in Battle Against Spam

By SAUL HANSELL

Alyx Sachs is no longer sending people e-mail offering to "fix your credit risk free."

Confronted by an increasing number of individuals, businesses and Internet service providers using software meant to identify and discard unwanted junk e-mail — commonly known as spam — Ms. Sachs has been forced to become more creative in her marketing pitches. The subject line on her credit e-mail, for example, now reads "get a fresh start."

From a small office on Sunset Boulevard in Los Angeles, millions of messages prepared on behalf of others by Ms. Sachs and her partner are still going out to e-mail in-boxes every day, promising not just to restore a poor credit rating but also to sell printer ink, 3-D glasses and, lately, even playing cards with pictures of wanted Iraqi leaders.

In the cat-and-mouse game of e-mail marketers and those trying to stop them, the spammers are still winning.

So far, nothing that has been tried to block spam has done much more than inconvenience mass e-mailers. Just as Ms. Sachs's company, NetGlobalMarketing, has been able to reword its e-mail to evade spam filters, others use even more aggressive tricks to disguise the content of their messages and to send them via circuitous paths so their true origin cannot be determined.

"There is no silver bullet," said Lisa Pollock, the senior director of messaging at Yahoo, the popular Web portal. "There will always be people who can find a way to get around whatever you have in place."

No doubt making a living selling things by e-mail is becoming harder. Not only are more messages being blocked by automated antispam systems, more senders of e-mail are also facing legal action. Last week, America Online and the Federal Trade Commission each filed suit against e-mailers that they say are illict spammers. Congress is seriously considering legislation to crack down on spam.

But the infestation is growing faster than the antispammers can keep up. Brightmail, which makes spam-filtering software for corporate networks and big Internet providers, says that 45 percent of the e-mail it now sees is junk, up from 16 percent in January 2002. America Online says the amount of spam aimed at its 35 million customers has doubled since the beginning of this year and now approaches two billion messages a day, more than 70 percent of the total its users receive.

Indeed, the spam problem defies ready solution. The Internet e-mail system, designed to be flexible and open, is fundamentally so trusting of participants that it is easy to hide where an e-mail message is coming from and even what it is about.

Another reason there is so much spam is that, with a simple computer hookup and a mailing list, it is remarkably easy and inexpensive to start a career in e-mail marketing. Companies that offer products like vitamins and home mortgages as well as those selling items like penis and breast enlargement kits will allow nearly any e-mail marketer to pitch their wares, paying a commission for any completed transaction.

The microscopic cost of sending e-mail, compared with the price of postal mailings, allows senders to make money on products bought by as little as one recipient for every 100,000 e-mail messages. Internet marketing companies typically charge $500 to $2,000 to send a solicitation to a million in-boxes, but the cost goes up if the list is from a reputable source or is focused on people in certain favored demographic groups. Sending the same offer to a million people by mail costs at least $40,000 for a list, $190,000 for bulk-rate postage and more for paper and printing.

Albert Ahdoot, for example, started a part-time business using e-mail to sell printer-ink refill systems while he was in college. When he dropped out of medical school, he hooked up with Ms. Sachs, a former producer with Geraldo Rivera who later worked in marketing at several Internet companies. With her client contacts, his technology and some e-mail lists they acquired, they started their business about a year ago.

Like many in the e-mail marketing business, Ms. Sachs says her e-mail blitzes are not spam because she sends them only to lists of people who have agreed to receive marketing offers over the Internet. These opt-in lists, as they are called, are generated when Internet users enter a contest on the Web or sign up for an e-mail list in which the fine print says the user agrees to receive "occasional offers of products you might find valuable from our marketing partners."

Arguing that no one is forced to sign up for e-mail pitches, Internet marketers say that the attack on spam has already gone too far, interfering with legitimate business.

"We have allowed these spam cops to rise out of nowhere to be self-appointed police and block whole swaths of the industry," said Bob Dallas, an executive of Empire Towers, an e-mail firm in Toledo, Ohio, widely cited on antispam lists used by many Internet companies.

"This is against everything that America stands for," Mr. Dallas added. "The consumer should be the one in control of this."

But activists who oppose spam say that some e-mailers who argue that they have permission to send e-mail to a certain address often do not. Earlier this year, a New York court ruled that a Niagara Falls, N.Y., company, MonsterHut, had violated antifraud laws for misrepresenting opt-in permissions.

Lower on the marketing totem pole than opt-in mailing is what the industry calls bulk e-mailing: blasting a message out to any e-mail address that can be found. CD-ROM's with tens of millions of e-mail addresses are widely available — advertised by e-mail, of course. These addresses have been harvested by software robots that read message boards, chat rooms and Web sites.

Others use what are called dictionary attacks, sending mail to every conceivable address at major e-mail providers — first, say, JohnA @example.com, then JohnB @example.com, and so on — to find the legitimate names.

Such distinctions, however, are usually lost on users who, in recent years, have found unwanted marketing pitches are overwhelming their legitimate e-mail.

As dissatisfaction has risen, the big Internet service providers, like AOL, and purveyors of free e-mail accounts, including Yahoo and Microsoft's Hotmail, have all greatly accelerated efforts to identify and block spam. Among other things, they have created prominent buttons for users to report offending e-mail as spam.

There is little that Internet services can do to keep spammers from gathering e-mail addresses directly from users. Many people still will type virtually their life history into an unknown Web site that claims to be offering a chance to win a Lexus.

But some Internet providers have built systems to identify when they are being subject to dictionary attacks and cut them off quickly before valid e-mail addresses are deduced.

To identify phrases and other patterns that occur in spam, the Internet service providers look at what is received in thousands of so-called honeypot e-mail accounts — those that have no legitimate reason to receive e-mail messages.

The spammers quickly caught on to this technique, however. So they have varied their messages — morphing, they call it — often by simply appending random words or characters, so the filtering systems no longer see millions of identical solicitations.

At the same time, e-mail users now receive spam that is not only unwanted but cryptic, too. In an attempt to avoid automatic filters that search for certain phrases, marketers offer, for example, "Her bal V1agra" and ways to make "F*A*S*T C*A*S*H."

So the Internet companies now look for unusual spelling as well. "Some people have jobs that change day to day," said Charles Stiles, the technical manager of AOL's postmaster team, which looks after spam blocking. "Ours changes from minute to minute. A filter that works one day will likely not work the next."

Another way spammers avoid detection is to send mail using the HTML format, the language mainly used to display Web pages. Spammers and major advertisers alike think that e-mail with varied type and inserted graphic images is more persuasive than ordinary text. But the spammers also find that this format makes it easier to evade the filtering programs.

A lot of spam now puts the actual sales pitch in an image that is only displayed when the user reads her e-mail. The filter reads merely some random text and the Web address of the image to be displayed.

Spam filters are now being adjusted to be suspicious of e-mails that only have links to Web images. But it is still hard for any program to distinguish, say, a pornographic come-on from a baby picture, especially when processing hundreds of millions of messages a day.

At the same time, the argument is intensifying over what represents legitimate e-mail, particularly when it ends up being blocked by an antispam filter. Last November, AOL threatened to block e-mail from Gap. Even though Gap said it only sent e-mail to people who explicitly signed up for its mailing list, AOL said that many of its members reported Gap mailings as spam. When it investigated, AOL found that Gap had been offering people a 10 percent discount for providing their e-mail address. Nearly a third of the addresses collected were fake, but they often belonged to other people who did not want the Gap e-mail.

"You can't underestimate the power of people to make up an e-mail address to get a 10 percent

discount," said Matt Korn, AOL's executive vice president for network operations.

The other major approach to preventing spam is to block any messages sent from computers and e-mail addresses known to be used by spammers. This is harder than it seems because the spammers are constantly changing their accounts and are adept at methods to make up fake return addresses and hide behind private accounts. That does not prevent the big service providers, and an army of spam vigilantes, from creating blacklists of offenders.

These blacklists, however, often also block legitimate companies and individuals from sending e-mail. That is because the spammers find ways to hijack unprotected computers to relay their messages, thus hiding their true origins.

In the earlier, more innocent days of the Internet, many computers were set up to relay e-mail sent by any other user, anonymously, just to give a helping hand to those with connection problems. Now there still are computers set up to be what is known as an open relay, even though such machines are largely used by spammers.

Another approach to limiting spam, which is favored by big marketers, is to create a "white list" of approved senders, but this raises the question of who will compile such a list. A group of the companies that send e-mail on behalf of major corporations will put forward another proposal tomorrow that would allow senders to certify their identities in every e-mail message they send and report a rating of how much they comply with good mailing standards. Users and Internet service providers would then decide what sort of mail they choose to accept.

"We wanted to come up with a way of shining a big bright light on all those that want to stand in the light and say, `This is who I am, and I was that person yesterday, and I'll be that person tomorrow,' " said Hans Peter Brondmo, a senior vice president at Digital Impact, a major e-mail company and one of the developers of the proposal, known as project Lumos.

Rather than such a self-regulatory approach, the antispam legislation in the Senate would try to make many deceptive e-mail practices illegal. It would force commercial e-mail messages to identify the true sender, have an accurate subject line and offer recipients an easy way to remove their names from marketing lists. And it would impose fines for violators.

For her part, Ms. Sachs, the e-mail marketer, says that any such move would only end up making it harder to run a legitimate business.

"These antispammers should get a life," she said. "Do their fingers hurt too much from pressing the delete key? How much time does that really take from their day?"

By contrast, she said, "70 million people have bad credit. Guess what? Now I can't get mail through to them to help them."