

When They Say You Are a Spammer



When Scott Madlener, a marketing executive at the Performance Communications Group of Chicago, learned that his company had been mistakenly blacklisted for sending e-mail spam, he knew it was bad news.
Joe Tabacca for The New York Times

By Karen J. Bannan

May 24, 2007

About a year ago, Scott Madlener, a marketing executive, e-mailed a client several times but his messages were not getting through.

"It raised a red flag immediately," said Mr. Madlener, executive vice president for interactive strategies at the Performance Communications Group of Chicago. "We asked our system administrator to look at what was happening, and he came back to me with some bad news: we had been blacklisted."

Blacklisting is an annoyance for big companies, but one that a dedicated technology staff can eventually remedy. For many smaller businesses, on the other hand, having messages blocked or shuttled into a spam folder by an Internet service provider or e-mail administrator can mean lost revenue.

E-mail blacklisting was created as a way to help reduce spam. The Internet protocol addresses of suspected or known spammers are compiled into a list, which is often shared and eventually posted on industry sites like Spamhaus.org and SpamCop.net.

But innocent companies like Mr. Madlener's are finding that even people who follow the rules and do not send unwanted e-mail can find themselves in a jam. In Mr. Madlener's case, the company shared its server with some of its clients, and one of them sent out e-mail that was flagged as spam. Mr. Madlener's company was guilty by association, as are many companies that use outside e-mail service providers that offer shared servers.

"It happens a lot," said Shar VanBoskirk, senior analyst with Forrester Research. "There's so much spam out there and it's so expensive to manage that even big I.S.P.'s simply can't handle the volume."

Several years ago, Gary Bevers, the current group publisher for National Petroleum News Magazine, created an e-mail newsletter for his previous employer and sent it out to a list of names he had bought from a reputable marketing company. Unfortunately, the list was old, and only 600 messages out of 10,000 made it through to the intended recipients. The rest were returned as invalid. Because so many e-mails bounced back as addressee unknown, his company's I.P. address was branded a spammer. It looked as though he had sent messages to random names and addresses even though he had bought what he thought was a solid permission-based list.

"It was a simple weekly newsletter with advertising, and we had advertisers complaining that they weren't even getting the newsletter," Mr. Bevers said.

As Mr. Bevers and Mr. Madlener can attest, getting on a blacklist was easy but getting off was another matter. It can take time and perseverance to be unblocked, said Stefan Pollard, director for consulting services at the e-mail service provider EmailLabs, based in Menlo Park, Calif.

"You have to be constantly reviewing and monitoring your bounce logs and looking for the messages that say you've been blocked. The messages will provide the name of the list that's blocked you and why," Mr. Pollard said. "Then you have to go to that list that's blocking you and follow their directions about how to get off. It's going to take diligence and hard work."

For example, if a company is using a purchased list or an affiliate list, or a mail list provided by a third party, and it is found to be on a blacklist, (Duplicate first page for exhibit labeling, per 37 C.F.R. § 42.63(d)(2)(ii).) it will have to provide proof of what is known as legitimate opt-ins, a record of how, when and where each

MICROSOFT CORP.
EXHIBIT 1024

When They Say You Are a Spammer



When Scott Madlener, a marketing executive at the Performance Communications Group of Chicago, learned that his company had been mistakenly blacklisted for sending e-mail spam, he knew it was bad news.
Joe Tabacca for The New York Times

By Karen J. Bannan

May 24, 2007

About a year ago, Scott Madlener, a marketing executive, e-mailed a client several times but his messages were not getting through.

“It raised a red flag immediately,” said Mr. Madlener, executive vice president for interactive strategies at the Performance Communications Group of Chicago. “We asked our system administrator to look at what was happening, and he came back to me with some bad news: we had been blacklisted.”

Blacklisting is an annoyance for big companies, but one that a dedicated technology staff can eventually remedy. For many smaller businesses, on the other hand, having messages blocked or shuttled into a spam folder by an Internet service provider or e-mail administrator can mean lost revenue.

E-mail blacklisting was created as a way to help reduce spam. The Internet protocol addresses of suspected or known spammers are compiled into a list, which is often shared and eventually posted on industry sites like Spamhaus.org and SpamCop.net.

But innocent companies like Mr. Madlener’s are finding that even people who follow the rules and do not send unwanted e-mail can find themselves in a jam. In Mr. Madlener’s case, the company shared its server with some of its clients, and one of them sent out e-mail that was flagged as spam. Mr. Madlener’s company was guilty by association, as are many companies that use outside e-mail service providers that offer shared servers.

“It happens a lot,” said Shar VanBoskirk, senior analyst with Forrester Research. “There’s so much spam out there and it’s so expensive to manage that even big I.S.P.’s simply can’t handle the volume.”

Several years ago, Gary Bevers, the current group publisher for National Petroleum News Magazine, created an e-mail newsletter for his previous employer and sent it out to a list of names he had bought from a reputable marketing company. Unfortunately, the list was old, and only 600 messages out of 10,000 made it through to the intended recipients. The rest were returned as invalid. Because so many e-mails bounced back as addressee unknown, his company’s I.P. address was branded a spammer. It looked as though he had sent messages to random names and addresses even though he had bought what he thought was a solid permission-based list.

“It was a simple weekly newsletter with advertising, and we had advertisers complaining that they weren’t even getting the newsletter,” Mr. Bevers said.

As Mr. Bevers and Mr. Madlener can attest, getting on a blacklist was easy but getting off was another matter. It can take time and perseverance to be unblocked, said Stefan Pollard, director for consulting services at the e-mail service provider EmailLabs, based in Menlo Park, Calif.

“You have to be constantly reviewing and monitoring your bounce logs and looking for the messages that say you’ve been blocked. The messages will provide the name of the list that’s blocked you and why,” Mr. Pollard said. “Then you have to go to that list that’s blocking you and follow their directions about how to get off. It’s going to take diligence and hard work.”

For example, if a company is using a purchased list or an affiliate list — an e-mail list provided by a marketer — it will have to, at minimum, sever ties with the affiliate or provide the name and contact information for the list owner. If a company is working with its own list, it will have to provide proof of what is known as legitimate opt-ins, a record of how, when and where each

person on the list signed up to receive e-mail messages from you.

Sometimes, a company is blocked because its e-mail server is set up incorrectly, leaving it vulnerable to hackers. In that case, the company will have to fix the problem before the Internet service provider or blacklist administrator will even listen to an appeal.

If a company is hacked and a spammer uses the company's e-mail server to send spam, the company will have to prove its server was hacked and show how the problem was repaired. All in all, technology specialists said, it can take several days to two or three weeks to get off a blacklist.

What can small businesses do to avoid blacklists altogether? That answer is not a simple one, either, Ms. VanBoskirk said.

"There's no quick panacea, no check list of, 'Do these three things and you'll be set.' Even if there was, those three things would change as spammers get more aggressive," she said.

But she said a few precautions can reduce the chances of having a problem. First, when hiring an e-mail service provider or I.S.P., make sure it is a reputable one that is committed to eliminating spam. The company should use outbound spam filters, have stringent antispam policies in place and be willing to enforce them. The company should also have some sort of deliverability reporting in place so it can tell you how many of your messages get through and are opened by end users. Finally, if you can afford it, try to send e-mail from your own server. Using a shared e-mail server, as Mr. Madlener found out, can be risky.

You can also avoid problems by including a prominent opt-out link in every message you send so recipients do not feel that they must report your messages as spam to get off your list.

For a more active approach, you can try signing up with reputation services providers like LashBack (www.lashback.com) and Habeas (www.habeas.com). These services assign a reputation score to e-mail senders, so that I.S.P.'s feel comfortable letting in e-mail messages from those with high scores. E-mail certification and accreditation services like Goodmail Systems (www.goodmailsystems.com) and Return Path's Sender Score Certified product (www.senderscorecertified.com) provide similar services.

But all of these strategies may just be stop-gap measures for many companies, Ms. VanBoskirk said. Mr. Madlener agreed.

"There's not a lot anyone can do because people have the right to complain about e-mail at any time. It's sort of like getting a ticket in the city," he said. "It's a nuisance and a problem, but it's very difficult to avoid."