Q: I am the co-owner of a small advertising firm. The other day, my colleague noticed that many of our clients weren't getting his e-mails. The strange thing was that it wasn't all of our clients. Eventually, he figured out that our domain name has been "blacklisted" by the recipients' spam service, not because we spam people, but because spammers have spoofed our IP address to make it look like spam is coming from us. So this ends up being quite a big issue. How can a small business fix this problem?

Tessa Tinney
Partner, Monaco Lange
New York, New York

A: SPAM IS A MAJOR problem for all of us, but it's an even bigger problem for Internet service providers (ISPs), as one ISP might host thousands and thousands of e-mail addresses, all of which could receive hundreds of spam messages per day. ISPs try to prevent spam from happening on two fronts. They want to block as much spam as possible from reaching their users (to reduce fraud and avoid wasting bandwidth) and they want to ensure that their mail servers are not being used to send spam. One of the tools they use to block incoming spam is "blacklists." These blacklists, often maintained by a consortium of nonprofit and for-profit organizations in coordination with ISPs, monitor which e-mail servers are being used for spam. Servers that are repeatedly used for spam are placed on one or more of these blacklists so ISPs (or corporations, for that matter) can block all e-mail coming from them. Another thing to keep in mind is IP spoofing, in which one computer appropriates the IP address of another computer on a network when sending messages. The "spoofed" message is made to look like it's coming from a trusted computer when it's really not. To protect your network from this type of attack you must ensure that your router is filtering IP addresses as they come in and as they leave your network. Implementing an encryption and authentication program can also help.

How else can you protect yourself? If you host your e-mail on your own e-mail server you can look to see if the IP address of your mail server has been added to a blacklist. A list of blacklists is available at email-policy.com/Spam-black-lists.htm and also emailtools.co.uk/tools/blacklist-check.htm. Both websites give you a form you can use to input the IP address of your e-mail server and check if it is on a blacklist. If you host your own e-mail, make sure your server is not configured so that just anyone can use it. If so, hackers or spammers will use it to send spam and you will be blacklisted. Your e-mail server should be configured to allow only authorized users. Another reason your e-mail could be blocked involves how it is configured: A few weeks ago a business colleague of mine said that she was not receiving my e-mail. After some investigating I realized that on the account I was using to send her e-mail (my gmail account), my "from e-mail" had one address but the "reply to" had another. When I changed the "from" and "reply to" to my gmail address, she received my e-mail just fine. My guess is that her ISP blocked e-mail when the "to" and "from" addresses were not the same, in order to reduce spam and/or phished e-mail. If you have taken the above precautions and your e-mails are still not being received, check with your e-mail provider as well as the intended recipients of your messages. If your e-mail is being received by most people, but not all, the problem could be the ISP of the recipients. It could also be that their spam filters are filtering out your messages. If most people are not receiving your e-mail, then call your ISP or local IT consultant and ask for their help. Taking these few simple steps can help ensure that your e-mail gets where it needs to get to, and in a timely manner. □