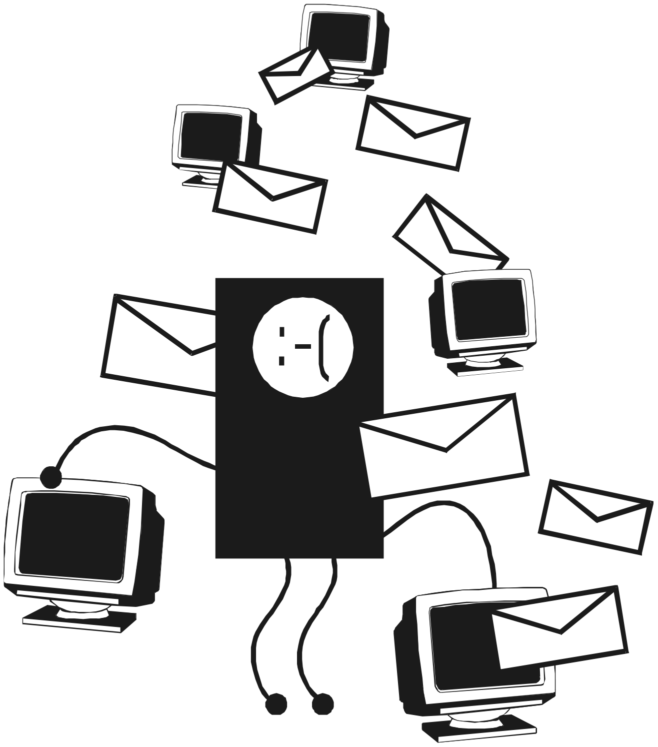
BUSINESS

Federal Trade Commission | For The Consumer

1-877-FTC-HELP | www.ftc.gov

Securing Your Server: Shut the Door on Spam



Your organization probably handles lots of Internet traffic every day — both to and from your clients and customers. The settings of your network servers may open your system to misuse.

If your mail server maintains an open door to the Internet, known as an “open relay,” someone could access it and pass unsolicited commercial email (spam) through it. And if your proxy server is “open,” a spammer could use it to connect to your mail server and send bulk email anonymously. Not only can these abuses overload your server, they also could damage your reputation. That’s because it will appear that you sent the spam.

Now an international group of government agencies says a few quick, easy, and no- or low-cost steps can protect your computer systems from misuse.

How Email Works

To send or receive email, your computer must be connected to a mail server, a machine connected to the Internet that runs software allowing it to process email. When you send an email message from a secure server, software in one part of the mail server checks that you're listed as a user within your organization. If you are, it sends out your mail. When someone sends you an email, software in another part of the server confirms that you're an authorized user and then accepts and delivers the email to you.

But if the server is not secure, and some of its settings allow it to stay "open," it will forward email to addressees who are not listed as users in your organization. Often called *open relays*, *insecure relays*, or *third-party relays*, these open mail servers are configured to accept and deliver email on behalf of any user anywhere, including third parties with no relation to you or your organization. You don't benefit from allowing this email to slip through your server; no one in your organization is receiving it or sending it.

Open relays are a vestige of the early days of the Internet, when many mail servers were kept open to allow email to travel among different networks. Although they helped the Internet grow, they were abused by spammers, who have used them to disguise the origin of their messages.

The Current Problem — Open Proxies

Today, spammers are more likely to use an *open proxy* server to send their spam. A proxy is usually installed to be the only machine on your network that directly interacts with the Web, providing more efficient Web browsing for your users. But if your proxy is not configured properly — that is, if your server is open — it also may allow unauthorized Internet users to connect through it to other hosts on the Internet. For example, a spammer can use your open proxy to connect anonymously to another mail server. Then, any mail that the spammer sends appears to have come from you. In addition, an improperly configured proxy server can allow other types of unauthorized — and potentially damaging — network connections, including instant messaging, computer attacks, or file transfers.

Consequences for Your Business

When spam appears to come from your system, your server can be flooded with complaints from frustrated recipients. That could overwhelm your system and cause your server to crash. Repairing it could be time-consuming and costly, both in financial terms and the potential loss of goodwill from those who think you've sent the spam. The bottom line: An open proxy or open relay is an open door to the theft of your computer services and the impression that you're sending unwanted junk mail.

Securing Your Servers

To prevent these abuses, and the negative consequences for your business, check — and if necessary, secure — your servers. It usually takes just a couple of commands. To find out whether you have an open relay on your system, evaluate the mail transfer agent software (MTA) your company uses to manage its email.

To determine if your proxy server is vulnerable, consider these questions.

- Does your proxy allow connections from untrusted networks such as the Internet?

- Are you using the most current version of your proxy server software and hardware?

- Have you applied the latest patches or upgrades available?

- Are you using proper access controls for your server?

- Is someone regularly checking for unauthorized uses of your proxy server?

- Do you have and monitor an "abuse@[YourDomainName]" email account where people can report abuses of your proxy server?

For More Information

For up-to-date links to information on securing your server, visit www.ftc.gov/secureyourserver. You also can find resources through your favorite Internet search engine by entering a phrase like "open relay" or "open proxy." Keep in mind that there's no "one-size-fits-all" way to secure your server. The solution is specific to the software and hardware that you use.

FEDERAL TRADE COMMISSION | FOR THE CONSUMER
1-877-FTC-HELP | www.ftc.gov

January 2004