FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

Who's Spamming Who? Could it be You?

Spammers may be using your computer to send unsolicited — and possibly offensive — email offers for products and services. Spammers are using home computers to send bulk emails by the millions. Indeed, computer security experts estimate that as much as 30 percent of all spam is relayed by compromised computers located in home offices and living rooms, but controlled from afar.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, spammers can compromise your computer in several ways, depending on what kind of Internet connection you have. All computers connected to the Internet are potential targets, but those with broadband connections are especially attractive to spammers because they are "always on." Spammers scan the Internet, searching for points of entry and then install hidden software that allows remote access to your data and programs. That, in turn, allows the spammer to send messages from your computer. Remote access software also can be installed by a virus: A spammer sends email with a virus in the attachment. If you open the infected attachment, a virus is released that installs the hidden software. The person who sent the virus now can access the data and programs on your computer, or take over many computers and use them to send spam.

It can be very difficult to tell if a spammer has installed hidden software on your computer, but there are some warning signs. For example, you may receive emails accusing you of sending spam; you may find email messages in your "outbox" that you didn't send; or your computer is using more power than it has in the past to run the programs you use.

If your computer has been taken over by a spammer, you could face serious problems. Your Internet Service Provider (ISP) may prevent you from sending any email at all until the virus is treated, and treatment could be a complicated, time-consuming process.

To avoid becoming an unwitting culprit, the FTC encourages you to:

- **Use anti-virus software** and keep it up to date. You can download anti-virus software from the Web sites of software companies or buy it in retail stores. Look for anti-virus software that recognizes current viruses, as well as older ones; that can effectively reverse the damage; and that updates automatically.
- **Be cautious about opening any attachment** or downloading any files from emails you receive. Don't open an email attachment — even if it looks like it's from a friend or coworker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.
- **Use a firewall** to protect your computer from hacking attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files. A firewall is different from anti-virus protection: Anti-virus software scans

incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection.

Some recently released operating system software (including Windows XP) comes with a built-in firewall. Because it may be shipped in the "off" mode, check your online "Help" feature for specifics on turning it on and setting it up properly. If your operating system doesn't include a firewall, you can install separate firewall software that runs in the background while you use your computer and surf the Internet. Several free firewall software programs are available on the Internet. (You can find one by typing "free firewall" into your favorite search engine.) Or you can buy a hardware firewall — an external device that includes firewall software. Like anti-virus software, a firewall needs to be updated regularly to stay effective.

- **Check your "sent items" file** or "outgoing" mailbox to see if there are messages that you did not intend to send. Many spammers have learned to hide their unauthorized access, so even if there are no illegitimate messages in your outbox, you can't be sure that your computer hasn't been used to send spam.
- **If your computer is infected, take action immediately.** If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with fully updated anti-virus software. Report unauthorized accesses to your ISP. Also, if you suspect that any of your passwords have been compromised, call that site's company immediately and change your password.
- **Learn more** about securing your computer at www.ftc.gov/infosecurity.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

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

January 2004