
ftc consumer feature

Bureau of Consumer Protection

July 2002

Federal Trade Commission

Contact: Eric Wenger (202-326-2310)
Paula Kurtzweil Walter (202-326-2583)

Putting a Lid on Deceptive Spam

When Joe Mastruserio of Cincinnati got fed up with “spam” email containing unsavory offers he did not want – like adult entertainment and pyramid schemes – he clicked on the “remove me” or “unsubscribe” links in the text of the email messages. Much to his dismay, those links often led nowhere. So Mastruserio did what more than 200,000 consumers did last year: He complained to the Federal Trade Commission (FTC).

In response to complaints like Mastruserio’s, the FTC investigated and found that the allegations were true. In April, the FTC warned 77 online marketers to discontinue their bogus “unsubscribe” links or face possible legal action.

The warnings represent the FTC’s latest effort to crack down on deceptive spam. In the past four years, the FTC has brought more than 30 law enforcement actions against marketers who used spam to promote get-rich-quick scams and other misleading schemes.

For many consumers, any kind of spam is annoying and time-consuming. But deceptive spam is especially troublesome because it can cheat consumers out of their money, undermine consumer confidence in online commerce and harm legitimate Internet marketers.

There are steps consumers can take to help reduce the amount of spam they get – from keeping their email address more private to reporting spam problems to the FTC.

“Con artists have seized on email’s capacity to reach millions of consumers quickly and cheaply,” says Eileen Harrington, Associate Director for the FTC’s Division of Marketing Practices. “It’s time to wrest this tool from rip-off artists.”

A Study of Spam

The technical term for spam is “unsolicited commercial email” (UCE) – that is, email messages sent in bulk without prior request or consent.

Not all spam is fraudulent. However, spam is frequently used by scam artists because it is low cost and allows them to hide their identities, says Eric Wenger, an attorney in the FTC’s Division of Marketing Practices. “Fighting deception is often an effective way to fight spam,” he says.

Spammers obtain email addresses by buying lists from brokers who have “harvested” addresses from Internet newsgroup postings, chat rooms, websites, and online services’ membership directories. The spammers then use special software to send hundreds of thousands – even millions – of email messages with just one click of the mouse.

Exactly how much spam they send is unknown. But it is increasing. The FTC receives about 40,000 pieces a day in a special mailbox it set up in 1998. Three years ago, the mailbox received about 4,000 a day.

“Spam is a big problem, whether it’s deceptive or not,” Harrington says. “Consumers complain about it, and Internet Service Providers say it burdens them. To many, it’s the bane of cyberspace.”

Enforcement Action

The FTC has taken several steps to curb deceptive spam. It maintains and monitors its spam database to identify emerging trends and developments. The database already has served as the basis for FTC cases involving pyramid schemes, money-making chain letters, credit card scams, credit repair scams, bogus weight-loss plans, and fraudulent business opportunities that were promoted via email.

The FTC also has helped train 1,700 law enforcement agents throughout the U.S. and Canada on investigating deceptive spam and other Internet fraud. As an outgrowth of that training, the FTC is helping create regional “netforces” – groups of local, state and federal agencies that work together to fight deceptive spam and other Internet fraud. One group – the Northwest Netforce, comprised of eight state law enforcement agencies, four Canadian agencies and the FTC – announced in April the results of 63 Internet-related law enforcement actions and the issuing of more than 500 warning letters to spammers for promoting illegal chain letter schemes.

In addition, the FTC, along with other U.S. and Canadian law enforcement agencies, investigated complaints from consumers about spammers who failed to honor their offers to remove consumers’ names from future email solicitations. Consumers indicated that they were unable to follow through on messages that said “click here to unsubscribe” or “reply for removal.”

When investigators tested several of the questionable links, they found that the removal hyperlinks often did not function.

As a result, the FTC sent warning letters to 77 marketers and will continue to monitor “remove me” offers to ensure that they do what they say they will.

Consumer Action

The FTC’s advice to consumers who want to reduce the amount of spam they get is:

- Avoid displaying your email address in public spaces, including newsgroup postings or chat rooms, on websites, or in an online service’s membership directory.
- Check a website’s privacy policy before submitting your email address. Make sure the website doesn’t plan to sell your address. If possible, “opt out” of any such plans.
- Read and understand website forms before you transmit personal information. If possible, select the “opt-out” choice if the website plans to share your information.

- Create two email addresses – one for personal messages and the other for public use, such as in newsgroups or chat rooms. Or, consider a disposable email address service; it creates a separate email address that forwards your email to your permanent address. If the disposable address begins to receive spam, you can shut it off without affecting the permanent address.
- Create a unique email address. Spammers often use “dictionary attacks” to sort through possible name combinations at large Internet Service Providers (ISPs) or email services to find valid addresses. So a common name, like “jdoe,” may get more spam than a unique name, like “jd51x02oe.”
- Use an email filter. Some email accounts provide a tool to filter out potential spam or channel it to a bulk email folder. You may want to ask whether this option is available when choosing an ISP.
- Report the spam to the ISP – yours and the sender’s. Often the email address is “abuse@[your ISP’s name].com” or postmaster@[your ISP’s name].com. The ISP may be able to stop further spam.
- Report the problem to the FTC. Send the actual spam item to spam@uce.gov. Be sure to include the full email header so that your complaint can be followed up. If your complaint has to do with “remove me” or “unsubscribe” offers not working, complete and submit the FTC’s complaint form at www.ftc.gov.

For more on spam and how to avoid it, visit www.ftc.gov/spam.

Says the FTC’s Harrington, “If each of us takes steps to can unwanted spam, collectively, we can do it.”

###

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). 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.
