

# FTC Consumer Alert

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

## Email Address Harvesting: How Spammers Reap What You Sow

Is your in-box clogged with junk email messages from people you don't know? Are you overwhelmed by unsolicited email offering products or services you don't want?

It's no wonder. According to research by the Federal Trade Commission (FTC) and several law enforcement partners, it's harvest time for spammers. But, the consumer protection agency says, the good news for computer users is that they can minimize the amount of spam they receive.

According to the investigators, spammers typically use computer programs that search public areas on the Internet to compile, capture, or otherwise "harvest" lists of email addresses from web pages, newsgroups, chat rooms, and other online destinations.

To find out which fields spammers consider most fertile for harvesting, investigators "seeded" 175 different locations on the Internet with 250 new, undercover email addresses. The locations included web pages, newsgroups, chat rooms, message boards, and online directories for web pages, instant message users, domain names, resumes, and dating services. During the six weeks after the postings, the accounts received 3,349 spam emails. The investigators found that:

- 86 percent of the addresses posted to web pages received spam. It didn't matter where the addresses were posted on the page: if the address had the "@" sign in it, it drew spam.
- 86 percent of the addresses posted to newsgroups received spam.
- Chat rooms are virtual magnets for harvesting software. One address posted in a chat room received spam nine minutes after it first was used.

Addresses posted in other areas on the Internet received less spam, the investigators found. Half the addresses posted on free personal web page services received spam, as did 27 percent of addresses posted to message boards and nine percent of addresses listed in email service directories. Addresses posted in instant message service user profiles, "Whois" domain name registries, online resume services, and online dating services did not receive any spam during the six weeks of the investigation.

In almost all instances, the investigators found, the spam received was not related to the address used. As a result, consumers who use email are exposed to a variety of spam — including objectionable messages — no matter the source of the address. Some email addresses posted to children's newsgroups received a large amount of spam promoting adult web sites, pitching work-at-home schemes, and even advertising hallucinogenic drugs.

### Slowing the Email Harvest

The investigators indicate that email address harvesting usually is automated, because spam can hit the addresses soon after they are used publicly the first time; the spam was not targeted; and some

addresses were picked up off web pages even when they weren't visible to the eye. Still, they say, consumers can protect their email addresses from harvesting programs. Here's how:

- 1. Consider "masking" your email address.** Masking involves putting a word or phrase in your email address so that it will trick a harvesting computer program, but not a person. For example, if your email address is "johndoe@myisp.com," you could mask it as "johndoe@spamaway.myisp.com." Be aware that some newsgroup services or message boards won't allow you to mask your email address and some harvesting programs may be able to pick out common masks.
- 2. Use a separate screen name for chatting.** If you use chat rooms, use a screen name that's not associated with your email address. Consider using the screen name only for online chat.
- 3. Set up disposable addresses.** Decide if you want to use two email addresses — one for personal messages and one for posting in public. Consider using a disposable email address service that creates separate email addresses that forwards to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without affecting your permanent address.
- 4. Use two email accounts.** If you work for a business or organization that wants to receive email from the public, consider creating separate accounts or disposable email addresses for that purpose, rather than having an employee's address posted in public.
- 5. Use a unique email address,** containing both letters and numbers. Your choice of email address may affect the amount of spam you receive because some spammers use "dictionary attacks" to email many possible name combinations at large ISPs or email services, hoping to find a valid address.

Meantime, what can you do with the spam in your in-box? Report it, making sure that you include the full email header. The information in the header makes it possible to follow up on your complaint. Send your spam to:

- **The Federal Trade Commission**, at [uce@ftc.gov](mailto:uce@ftc.gov). The FTC uses the emails in this database to pursue law enforcement actions against people who send deceptive spam.
- **Your ISP's abuse desk.** Often the email address is [abuse@yourispname.com](mailto:abuse@yourispname.com) or [postmaster@yourispname.com](mailto:postmaster@yourispname.com). Forwarding your spam to your ISP lets them know about the spam problem on their system and helps them to stop it. Include a copy of the spam, along with the full email header, and at the top of the message, state that you're complaining about being spammed.
- **The sender's ISP.** Most ISPs want to cut off spammers who abuse their system. Include a copy of the message and header information and state that you're complaining about spam.

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](http://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**  
Bureau of Consumer Protection  
Office of Consumer and Business Education