Block spammers and scammers

Nearly everyone who uses the Internet lists e-mail as a primary reason for getting online, but when it comes to junk mail, electronic spam is more intrusive than the flyers that come rubber-banded to your doorknobs. That's because you, the Internet user, must pay for the bandwidth and disk space that spam takes up. Gobs of spam can also slow down your mail downloads. Even worse: once spammers know your e-mail address, they can sell it to dozens more spammers. One of the most irritating spam letters we've ever seen is the message offering to sell us the names and e-mail addresses of 5 million of our fellow spam victims for only $40.

The spam scam

How do the spammers get your address in the first place? Most of them acquire their stock of addresses through harvesting, a process that uses software to scan Web sites for any text with an @ symbol, recording the addresses in databases. Then they send their own spam to these addresses and/or sell or trade the addresses to other spammers.

What's one of the best ways to keep spammers from tracking you down? Avoid using your primary address; instead, sign up for a free e-mail account at a site such as Hotmail or Yahoo, then use these alternate addresses every time you post messages publicly or order products from Web stores. (For more antispam tips, check out our "Take back the Net" and "The great CNET spam-off" features.)

Spammers also harvest e-mail addresses from posts you make to Usenet newsgroups (for instance, news://rec.travel.europe) and online archives of mailing lists you might subscribe to. Never enter your e-mail address into your newsreader program's settings. It's easy for spammers to skim message boards for e-mail addresses, so use a free e-mail account to sign up for and reply to these. On those rare occasions when viruses send the contents of your address book to spammers, there's nothing you can do, so it's best to have antivirus software running all the time.

Keep a low profile

Of course, the easiest way to keep spam out of your in-box is to keep your e-mail address private in the first place. Give it only to trusted friends, family, and colleagues. Don't enter your primary address into Web forms or shopping order pages, and don't enter your address into your Web or Usenet browser's preferences; some sites can read your e-mail address or real name straight from the preferences. In general, when a Web browser or a Usenet newsreader asks you to enter your real name and/or e-mail address in a settings dialog, just leave the fields blank and move on.

Once spammers get ahold of your e-mail address, they can use HTML e-mail messages to acquire additional addresses from you. HTML e-mail looks different from plain-text e-mail in that it can be formatted with different type sizes and live Web links right in the body of the message. Unfortunately, these messages not only take a long time to load, they can also contain hidden scripts that send the list of addresses in your address book to the composers of the messages. It's fairly easy to disable HTML e-mail messages: simply go into your e-mail program's preferences dialog and deselect the preference to view mail as HTML. (In later versions of Eudora, for example, you click Tools > Options, then select Viewing Mail in the left pane and uncheck the box labeled Use Microsoft's Viewer.)

Other tools, including AnalogX's free Script Defender can stop malicious code in your e-mail before it activates. Script Defender, like CookieWall, runs in the background, waiting until it detects a malicious script. Then it stops the script from activating and lets you know what happened.

Encryption protection

Of course, even if you stick to all of these rules, e-mail messages themselves aren't safe from prying eyes; anyone who intercepts messages between your PC and their destination can read them. Unless, that is, you *encrypt,* or scramble, the contents of the messages so that only you and the intended recipient can read them. You can use a free programs such as PGPfreeware to encrypt your mail, but both you and the recipient have to install and configure it ahead of time. Some e-mail clients offer encryption options, but they require that

you acquire a digital ID from a third party. To encrypt messages within Outlook, for example, you must first subscribe to a company such as VeriSign for a yearly fee for an ID.