

IN THIS CHAPTER

- » Knowing what spam is and why you should worry about it
- » Setting up software to catch spam
- » Tweaking your spam filters
- » Reducing the amount of spam you get

Chapter 21

Securing Your Email

Spam, spam, spam, spam, spam, spam, and spam.

So goes the famous *Monty Python* sketch, in which a woman at a restaurant just wants to order something that doesn't have spam in it.

That pretty much sums up the situations with most people's inboxes these days. The legitimate emails get lost among the spam emails. Wouldn't you like to look at an inbox that wasn't filled with spam?

Nobody likes spam. You don't like it, and your users don't like it either. And believe me, they'll let you know if they're getting too much spam in their inboxes. They'll hold you personally responsible for every email with an offensive subject line, every email that tries to sell them stuff they aren't interested in, and every email that attempts to get them to provide their bank account password or credit card number.

As a network administrator, part of your job is protecting your users from spam. The holy grail of antispam is a solution that never allows a single piece of spam into anyone's inbox, but at the same time never mistakenly identifies a single legitimate piece of email as spam.

Good luck. This level of perfection doesn't exist. The best thing you can hope for is to find the right balance: a happy medium that lets only a small amount of actual spam through to users' inboxes and only occasionally misidentifies legitimate email as spam.