



TIP

Microsoft Exchange mailboxes include a Junk folder that is often the ultimate destination of email identified as spam. You should always check your Junk folder whenever you can't find an email you're expecting.

Not all antispam programs use the Junk folder. Some programs store spam email outside of the user's mailbox, in a separate location on the network or perhaps on the cloud. These programs usually deliver a daily email (often called a *digest*) that lists the emails that were identified as spam. You should review this email whenever you can't find an email you're expecting.

Determining whether an email is spam is not an exact science. As a result, *false positives* (in which a legitimate piece of email is mistakenly identified as spam) and *false negatives* (in which a spam email is not detected as spam and makes it into the user's inbox) are not uncommon. False positives can result in your users not receiving emails they're expecting. False negatives can leave users scratching their heads wondering how in the world the spam filter didn't catch the spam. Sometimes email that to a human is obviously spam slips right by the antispam software.

The challenge of any antispam tool is finding the right balance of not too many false positives and not too many false negatives. Most antispam tools let you tune the filters to some degree, setting them to be more or less permissive — that is, erring on the side of more false negatives or more false positives. The stricter the filters are set, the more false positives you'll have. Loosening the filters will result in more false negatives.



TIP

The possibility of false negatives is one of the main reasons that it's rarely a good idea to configure an antispam program to simply delete spam. Most programs can be configured to delete only the most obvious spam emails — the ones that can be identified as spam with 100 percent certainty. Email that is probably spam but with less than 100 percent certainty should be marked as spam but not deleted.

Understanding Spam Filters

Antispam programs use a variety of different techniques to determine the probability of a given piece of email being spam. These techniques are employed by *filters*, which examine each piece of email; each filter uses a specific technique.

Here are some of the most commonly used filter types:

- » **Keyword checking:** The most obvious way to identify spam is to look for certain words that appear either in the email's subject line or in the email body. For example, a keyword checking filter might look for profanity, sexual terms, and other words or phrases such as "Get rich quick!"