Note that simply blacklisting a sender email address isn't much help. That's because the sender email address is easy to forge. Instead, blacklists track individual email servers that are known to be sources of spam.


WARNING

Unfortunately, spammers don't usually set up their own servers to send out their spam. Instead, they hijack other servers to do their dirty work. Legitimate email servers can be hijacked by spammers and, thus, become spam sources, often without the knowledge of their owners. This raises the unfortunate possibility that your own email server might be taken over by a spammer, and you might find your email server listed on a public blacklist. If that happens, you won't be able to send email to anyone who uses that blacklist until you've corrected the problem that allowed your server to be hijacked and petitioned the blacklist owners to have your server removed.

- **Whitelisting:** One of the most important elements of any antispam solution is a *whitelist,* which ensures that email from known senders will never be blocked. Typically, the whitelist consists of a list of email addresses that you trust. When the antispam tool has confirmed that the From address in the email has not been forged (perhaps by use of an SPF filter), the whitelist filters looks up the address in the whitelist database. If the address is found, the email is immediately marked as legitimate email, and no other filters are applied. So, if the email is marked as legitimate by the whitelist filter, the other filters are not used.


TIP

Most whitelist filters will let you whitelist entire domains, as well as individual email addresses. You most certainly do *not* want to whitelist domains of large email providers such as `gmail.com` or `comcast.net`. But you should whitelist the domains of all your business partners and clients to ensure that emails from new employees at these key companies are never marked as spam.

Some antispam programs automatically add the recipient addresses of all outgoing emails to the whitelist. In other words, anyone that you send an email to is automatically added to the whitelist. Over time, this feature can drastically reduce the occurrence of false positives.


TIP

Use the whitelist to preemptively allow important email that you're expecting from new customers, vendors, or service providers. For example, if you switch payroll providers, find out in advance what email addresses the new provider will be using so that your payroll staff doesn't miss important emails.

- **Graylisting:** Graylisting is an effective antispam technique that exploits the fact that if a legitimate email server can't successfully deliver an email on its first attempt, the server will try again later, typically in 30 minutes. A graylist filter automatically rejects the first attempt to deliver a message but keeps track of the details of the message it rejected. Then, when the same message is received a second time, the graylist filter accepts the message and makes note of the sender so that future messages from the sender are accepted on the first attempt.