Spam Protection

- **Top Questions**
  - What should I do if I get spam mail?
  - What if I believe I did not receive a legitimate piece of mail?
  - Does the Berkeley Lab anti-spam solution delete any spam? / What happens to messages that are identified by the Lab anti-spam solution as spam?
- **General Questions**
  - What is the Berkeley Lab anti-spam solution?
  - Does the Berkeley Lab anti-spam solution block outgoing spam?
  - What is spam?
  - Is the Berkeley Lab anti-spam solution seeing/reading email sent to my Lab address?
  - How well does the service work?
  - How Can I Reduce the amount of spam I receive?
  - Unsubscribe links
  - What if I have more questions about the Berkeley Lab anti-spam solution, which is supplied by IronPort?
  - What other information on spam protection is available?
- **Technical Questions**
  - How often do the Lab's servers get spam ID database updates?
  - sendmail anti-spam rules

**Top Questions**

**What should I do if I get spam mail?**

- **Gmail anti-spam reporting is very easy – click here to see how**
  - **Non-Gmail users:** Report spam to spam@lbl.gov
    Make sure to forward the message as an attachment -- see How to forward a message as an attachment (If you do not send your message to spam@lbl.gov as an attachment, our anti-spam/anti-phishing system cannot use your report.)

  • In either case, Gmail or non-Gmail, all such reports that are sent to spam@lbl.gov now go directly to the anti-spam/anti-phishing support vendor for analysis and inclusion into their spam identification database, which helps improve the service for everyone. If you need to escalate a spam issue, please contact the Help Desk, http://help.lbl.gov, 510-486-4357

**What if I believe I did not receive a legitimate piece of mail?**

If you believe a legitimate piece of email was not delivered and may have been mistakenly identified as spam, contact the help desk at xHELP or help@lbl.gov.

**Does the Berkeley Lab anti-spam solution delete any spam? / What happens to messages that are identified by the Lab anti-spam solution as spam?**

The Berkeley Lab anti-spam solution does not deliver email it identifies as spam.

**General Questions**

**What is the Berkeley Lab anti-spam solution?**

The Berkeley Lab anti-spam solution uses a Cisco's IronPort service that uses a combination of advanced technologies and human analysis to identify spam and prevent the delivery of viruses and other malware.

Gmail users also get the benefits of Gmail's anti-spam and anti-virus solution

**Does the Berkeley Lab anti-spam solution block outgoing spam?**

The Berkeley Lab anti-spam solution blocks both incoming and outgoing spam. This means if you try to forward an email identified as spam, your
email will not be delivered.

What is spam?

Spam is unsolicited e-mail usually sent to a large number of people that usually tries to sell something or get people involved in some sort of scam. As the Internet grows, so does the problem of spam. More and more people are getting more of these spam e-mailings. For this reason, the Lab is taking steps to reduce the amount of spam we receive.

Is the Berkeley Lab anti-spam solution seeing/reading email sent to my Lab address?

No, the Berkeley Lab anti-spam solution is not seeing any email sent to your Lab address except mail you report to spam@lbl.gov

The Lab is using the anti-spam software on our central email servers. The only communication our servers have with the anti-spam vendor is to receive spam ID database updates (new "rulesets"), and to report aggregate statistics about how many messages were identified by Lab servers as spam.

How well does the service work?

The Berkeley Lab anti-spam solution is doing an excellent job of correctly identify the majority of incoming junk mail. Of course, no system is perfect, so it will certainly miss some spam, and incorrectly identify as spam some legitimate mail as spam. Our anti-spam service has a very low false positive rate -- the number of messages it incorrectly identifies as spam -- may be in the range of 1/100,000.

Please refer to the questions above for how to report junk and false positives. Your feedback will help improve the service!

How Can I Reduce the amount of spam I receive?

- **Protect your e-mail address.**
  To reduce or prevent spam to your email address, try not to give out your email address (via news postings for example) to anyone you don’t know.
- **Don’t Comply with Instructions in Spam Messages**
  Some spam messages include instructions for supposedly removing your address from mailing lists, thus by all appearances stopping spam from that spam source. However, if you follow the instructions, chances are you are only making matters worse. Many if not most spammers use the replies to confirm addresses and identities of people who will afterwards receive even more spam. If you get spam, your best bet is to follow the procedures described in this page.
- **Note that spammers often send spam using blind-carbon-copies (bcc), a method to conceal the addressees by hiding the “To:” address.**
- **For LBNL users ONLY: Use your lab-standard email address EPO@lbl.gov**
  Since LBNL lab-standard email addresses of the form \!EPO@lbl.gov\! are protected by the lab’s spam-protection and virus-protection software, we recommend that you set your From: and Reply-To: addresses in your email client and any web pages to \!EPO@lbl.gov\! address if you have not already done so. LBNL employees are urged to request a lab-standard email address (EPO) via see New Email Accounts, IMAP4 Mail, Directory, etc.
- **Unsolicited Commercial E-mail Research Six Month Report (good tips for reducing influx of spam)**

Unsubscribe links

Legitimate companies in fact do unsubscribe as promised and we have often used such unsubscribe links with legitimate companies with good results.

These are companies whose emails to the user “make sense” because the user did business with them, e.g., bought something from them or corresponded with them.

Illegitimate companies use the unsubscribe information to confirm your address is valid. Since it is hard to know who is a criminal, if in doubt, not unsubscribe.

What if I have more questions about the Berkeley Lab anti-spam solution, which is supplied by IronPort?

You can visit IronPort ’s website, [http://www.ironport.com/](http://www.ironport.com/). If your question is related to how the service works at the Lab, please contact the Help Desk at: help@lbl.gov, 510-486-HELP, or [http://help.lbl.gov/](http://help.lbl.gov/).

What other information on spam protection is available?

- Resources for fighting spam
- Information about worms that forge email
- “4-1-9” or “Advance Fee Fraud” schemes
Technical Questions

How often do the Lab’s servers get spam ID database updates?

The Lab’s central email servers get spam ID database updates several times an hour.

sendmail anti-spam rules

<table>
<thead>
<tr>
<th>Selective Blocking</th>
<th>The lab maintains a small set of server-side filters to block long-term, high volume abusers of our system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Relay Blocking</td>
<td>A major contributing factor to the spam problem is the ability for spammers to relay their e-mail through third party servers, making it difficult to track it back to the originator. This is called &quot;third-party relay.&quot;</td>
</tr>
</tbody>
</table>

For more information on why we need to block this kind of relaying, see this webpage entitled "What is Third-Party Mail Relay?"

Therefore, the Lab does not permit "third-party relay." Mail that comes into our server from outside the Lab that is also addressed only to addresses outside the Lab is rejected.

| Sender Address Checking | A hallmark of spam is that the sender address (the "From:" address) is often not valid, since spammers generally don’t want you to be able to respond to the message. So, the sender address on all messages is now checked to make sure it at least refers to a real computer on the Internet. |