Email Safety Tips

Learn some basic ways to protect you and your computer from email viruses and scams.

1. **Don't Open Unexpected Attachments**
   Viruses are often sent via email attachments. UCI scans incoming email (sent to "@uci.edu" addresses) and cleans known viruses. However, new viruses may get through before our anti-virus software has been updated.

2. **Use Spam Filters**
   UCI has many safeguards in place to rid you of unsolicited email or spam. If you use UCI's email services you can set up spam filters using [My Email Options](http://www.security.uci.edu/email/).

3. **Beware of Spoof Emails or Phishing**
   Phishing emails are an attempt by thieves to lure you into divulging personal information for their profit. Learn to recognize the telltale signs of Phishing.

4. **Don't Send Sensitive Data in Email**
   When you send a message, you no longer have control over what is done with it or to whom it is forwarded.

5. **Avoid clicking on links in the body of an email message.**
   While these links may not be a phishing attempt, they may not go to the site you intend. Unless you are completely comfortable that the email is legitimate, it is best to copy and paste the link or type it in directly in your browser.

Safe Computing information taken from office of Information Technology
OIT Help Desk — (949) 824-2222
http://www.security.uci.edu/email/