How do I make sure mass email messages from 3rd party vendors will not be blocked or flagged as SPAM?

Tell Me

If you are using a 3rd party vendor not supported by the University (iContact, Constant Contact and Mailchimp):

1. Email gets flagged as SPAM or blocked for many reasons including:
   a. Subjects
   b. Embedded images
   c. Mixture of upper case and lower case text
   d. Word choice
2. We recommend you always send a test message.
3. If you are using a 3rd party vendor e.g. MailChimp, Constant Contact, iContact, you need to be aware of the DMARC and DKIM requirements.
   a. See this FAQ for more details
   b. To make sure the software is configured correctly, submit a request to ITS and, if possible, include this vendor information:
      i. a list of the vendor's email servers so that they can be added to the University SPF record (a Sender Policy Framework record used to indicate who is authorized to send from an email domain)
      ii. the vendor's DKIM key (DomainKeys Identified Mail) which allows senders to associate a domain name (e.g. @uncc.edu) with an email message.
      iii. The vendor should be able to provide this information
   c. The ITS Security team will work with you to get the necessary changes implemented and to review test messages

See this SPAM infographic describing step 3 above.

Related FAQs

- How do I make sure mass email messages from 3rd party vendors will not be blocked or flagged as SPAM?
- Why is DMARC important?
- What is DMARC (Domain-based Message Authentication, Reporting and Conformance)?
- What is DKIM (Domain Key Identified Mail)
- How do I test for DMARC compliance when I am working with a third party vendor to send mass emails from an @uncc.edu account?