Carnegie Mellon

Guidelines for Bulk Email Distribution

Document Information	
Identifier	
Status	Published
Published	10/01/2007
Last Reviewed	10/01/2007
Last Updated	10/01/2007
Version	1.0

Carnegie Mellon

Revision History

Version	Published	Author	Description
1.0	10/01/2007	John Lerchey Doug Markiewicz	Original publication

Carnegie Mellon

Purpose

The purpose of this Guideline is to instruct users on appropriate use of Bulk Email and to provide recommendations on how to properly send Bulk Email messages in order to reduce recipient complaints and confusion, reinforce security best practice and effectively and efficiently utilize campus resources.

Applies To

This Guideline applies to all University personnel who send, or arrange for a third-party to send, bulk email to University students, faculty or staff.

Definitions

Bulk Email is defined as an email sent to a group of recipients with or without their expressed willingness to be a recipient. Bulk Email is often thought of as email sent to a large number of recipients; however, these Guidelines should be evaluated for appropriateness even in situations that involve a small number of recipients. In general, Bulk Email excludes the following:

- Interdepartmental emails sent during the standard course of business
- Messages sent to a single distribution list, such as an Andrew Mailman Mailing List, following the guidelines set forth by the list moderator

Guidelines

Generally speaking, Bulk Email is appropriate for:

- Messages that directly relate to the continuance of University business
- Messages that alert the campus community of health and safety issues
- Messages that relate to changes in University policy or time sensitive procedures
- Messages that inform a select group of people (e.g. students in a specific class, members of a business organization, all financial administrators, etc.) of an event related to their specific role within the University.

Inappropriate use of Bulk Email includes, but is not limited to:

- Messages that are counter to the University's mission and core values
- Messages that are personal in nature
- Messages that are commercial in nature with the exception of those messages that are in support of University business and are approved by an officer of the University (e.g. email to alumni)

The following recommendations are strongly encouraged when sending Bulk Email:

- *Bulk Email should be sent in plain-text format*

  HTML format emails are often used for malicious intent. For example, hyperlinks can be disguised to trick a user into browsing to a malicious website. HTML format emails can also be designed to exploit vulnerabilities in software. Because of this, some users configure their email clients to block certain aspects of HTML format emails (e.g. blocking images).

- *Bulk Email should be sent from a verifiable University email account*

  Bulk Email should not be sent from third-party email accounts such as Hotmail and Gmail. These types of accounts provide no measure of authenticity. It is recommended that all Bulk Emails be sent from an

@andrew.cmu.edu email accounts. Registration of these email accounts is controlled by Computing Services and email recipients can verify the owner of the email address through the Carnegie Mellon Directory. It may also be appropriate to send Bulk Email using a departmental email accounts (e.g. @scs.cmu.edu) if the audience is internal to that department and recipients are able to verify the owner of the email address. Use of @cmu.edu email addresses should be avoided. There are limited controls around the registration of @cmu.edu email addresses and, as a result, they can be misleading in terms of who the actual sender is. It is important to note that any email address can be impersonated by someone with malicious intent. If an email appears suspicious, the sender should be contacted to validate authenticity.

- *Bulk Email should be sent using Blind Carbon Copy (Bcc) functionality*

  When replying to a Bulk Email, a user may intentionally or unintentionally use the Reply to All option which would result in a second Bulk Email. This type of scenario has a tendency to lead to additional replies. Multiple replies to a Bulk Email can overwhelm an email system and be a nuisance to users. Leveraging Blind Carbon Copy functionality eliminates this risk and helps protect the privacy of recipients. In situations where a separate email is generated for each recipient, use of Blind Carbon Copy functionality is not necessary.

- *Bulk Email should have a Subject that clearly defines the purpose of the email*

  Ambiguous subject lines make it difficult to differentiate between legitimate emails and spam or phishing emails. As a result, an email may be inadvertently ignored or deleted. Unnecessary tags, such as RE and FWD, should also be avoided.

The following are several additional points to consider when sending Bulk Email:

- *Avoid sending attachments in Bulk Email*

  Email attachments are a common tool for propagating computer viruses. As a result, some users are hesitant to open unexpected attachments. Senders of Bulk Email should consider posting files to a University hosted website and then providing instructions in the email on how to download the file. This provides some measure of authenticity. Sending large attachments to multiple recipients can also create unnecessary load on email servers.

- *Avoid hyperlinks to third-party websites*

  Spam and phishing emails often include hyperlinks to malicious websites. As a result, recipients may be hesitant to click on a hyperlink even in an email that appears legitimate. Similar to attachments, posting third-party hyperlinks to a University hosted website provides some measure of authenticity.

- *Consider sending Bulk Email to a public distribution list(s) when available*

  Distribution lists, such as Andrew Mailman Mailing Lists, allow a user to create filters to better sort and manage their emails. In some cases, distribution lists also allow a user to customize how they receive emails.

- *Consider posting a copy of Bulk Emails on a University hosted website*

  It is trivial to make an email appear to be an official announcement when in fact it is not. Posting a copy of the email to a University hosted website and including a hyperlink to this website adds an additional measure of authenticity.

Carnegie Mellon

Additional Information

If you have any questions or comments related to this Guideline, please send email to the University Information Security Office at iso@andrew.cmu.edu.