Guideline for Sending Mass Email to Students

The following guidelines are intended to outline best practices and procedures in the appropriate sending of electronic mail to students of the University of Manitoba in a bulk fashion (mass email).

Recommendations

The following recommendations are strongly encouraged when sending electronic mail in a bulk fashion. Mass email should:

- Be sent in plain-text format.
- Be sent from a verifiable University of Manitoba email account.
- Be sent using "Blind Carbon Copy" (bcc) functionality (see details).
- Have a subject that clearly defines the purpose of the email (see details).
- Not include personal information or personal health information.

Blind Carbon Copy (bcc) Function

When replying to a mass email, a user may intentionally or unintentionally use the "Reply to All" option, which would result in a second mass email. Multiple replies to a mass email can overwhelm an email system and be a nuisance to users. Using the "Blind Carbon Copy" function eliminates this risk and helps protect the privacy of recipients.

Subject Line

Make sure the subject heading clearly defines the purpose of the mass email. Ambiguous subject lines make it difficult to differentiate between legitimate emails and spam or phishing emails.

Additional Points to Consider

Avoid Sending Mass Emails Too Frequently

Students receive many emails from many sources, often making it difficult to navigate information. Senders of mass email should consider the frequency in which mass email is being used. Refrain from sending mass emails for individual notifications and consider sending regular unit emails that contain multiple notifications.

Avoid Sending Attachments in Mass Emails

Email attachments are a common tool for propagating computer viruses. Senders of mass email should consider posting the attachments as a file to a University hosted website and then reference the University website link in the email instead of including an attachment. This practice not only prevents an unnecessary load on email servers, but it also provides some measure of authenticity.

Avoid Hyperlinks to Third-Party Websites

Spam and phishing emails often include hyperlinks to malicious websites. Follow the same practice as attachments by posting the third-party website hyperlinks on a University hosted website and reference the University website link in the mass email instead. This is more secure and provides some measure of authenticity.

Post a Copy of Mass Emails on a University Hosted Website

Posting a copy of the mass email to a University hosted website and including a hyperlink to this website within the email body adds an additional measure of authenticity.

For Further Information:

- Electronic Communications with Students (University of Manitoba Policy)
- Managing Email as a Record
- Contact the Access and Privacy Office, 233 Elizabeth Dafoe Library, 204.474.9462, fippa@umanitoba.ca

Produced by the Registrar's Office and the Access and Privacy Office – Issued May 2013