Policy & Procedures

Email Security Guidelines

Issued by: Technology Steering Committee
Applies to: University Employees and Students
Effective date: March 23, 2003

Introduction

These guidelines are a supplement to NJCU's Email Security Policy and Procedures document.

Scanning messages and files at the server level is extremely processor intensive. This issue is further exacerbated by the total number of users and the use of Email Listserv lists. For example, a message to the University staff list generates 900+ Emails. If the message has an attachment, the list also generates 900+ copies of it! The University hosts 5,000 Email accounts and many lists. Needless to say, the University Email system is very busy 24/7.

Guidelines

To ease Email processing and delivery delays, please follow these guidelines:

- *Be Brief and to the point.* If your message runs more that a half printed page, consider referencing a document posted to a website instead. All departments, programs, and organizations should have a website for providing such documents. If you need a website, please send mailto:websvcs@njcu.edu.
- *Limit the use of Signatures*. A full, contact-me signature is not required on every message – especially when those signatures run several lines of text. Be discriminate. Do not set auto signature on. Instead, insert your signature file manually the first couple of times you send Email to a new contact. There after, forgo the signature entirely. This gives you the opportunity to create/select from a variety of signatures tailored for specific functions. For example, a short contact-me (Name, Title, Dept.), a long version contact-me (includes telephone numbers and alternate Email addresses), Committee signature, Adjunct signature, etc.
- *Trim Replies*. Outlook, by default, is set up to include a copy of the original message when you reply. If the original message is lengthy, leave in the header and trim out text that is unimportant to your reply. Use ellipses (…) between fragments of text to indicate where the text was removed.
- *Choose plain text over HTML-based messages.* Plain text messages pass through the system without checking. HTML-based messages are checked. This option can be switched in Outlook by selecting Outlook as the Email editor instead of Word Mail and "Plain text" as the default format.
- *Choose simple stationary - or none at all!* Messages using stationary are HTML-based with back-ground images and other graphic elements. The more complex the stationary the longer the check takes.

- *Use URLs in Email*. Point to a web page with documents, or to a specific document or file on a website. Files with no attachments pass through the system faster that those with attachments. Depending on the Email client, these URLs are linked automatically enabling the recipient to click through to the site/document immediately. Worse case, the recipient will have to copy and paste the Internet address into a web browser address bar.
- *Limit attachments and attachment size*. In the rare case you need to include an attachment, send it in a form that will have little or no impact on virus scanning. For example, convert Office documents to PDF. Or, compress the file or several files into a single container using WinZip or other compression utility. Image and multimedia file sizes should not exceed 1 MB, raw. Compress anything over 600 KB. The smaller the attachment the faster it passes through the system.