NEW JERSEY
CITY
UNIVERSITY

Policy & Procedures

Email Security Policy

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

Policy Rationale

The University recognizes the necessity of providing Email that is free from computer viruses and harmful attachments. In addition, the University views advertisements via Email, commonly known as Spam, as a waste of resources and will make every effort to prevent NJCU systems from promoting or passing these type of messages.

Policy

The University accepts Microsoft's definition of Level 1 & 2 attachments that present a security risk and will follow Microsoft's recommendation that all Level 1 attachments will not be allowed to pass through the University's Email system. Level 2 attachments will be allowed to pass through but will be rigorously tested for viruses and other harmful programs. As an additional security measure, anti-virus software will be installed on all University computers. To prevent the proliferation of Spam, NJCU uses several methods, from relay blocking to the direct blocking of problematic domains listed with the following Spam tracking services:

- http://www.monkeys.com/anti-spam
- http://www.spamhaus.org
- http://www.orb.org
- http://www.spamcop.net
- http://www.spam-abuse.org

Procedure

For your safety and the safety of the University network, Email that passes through the University Email system (both in-coming and out-going messages) is automatically scanned for viruses, including the attachment, using Sophos Anti-Virus for VMS. Level 1 attachments, deemed too dangerous for transfer, such as URL shortcuts (.url), programs (.exe), et-cetera, are removed in transit. Level 2 attachments, equally dangerous but allowed to pass through, are rigorously checked for viruses using the latest virus identifiers available. Attachments not on the Level 1 or Level 2 list (a.k.a. Level 3 attachments) are passed with minimal or no scanning[1].

All Email will be scanned for viruses at two levels: Server and Client.

---

[1] A list of Level 1, Level 2 and Level 3 files is provided in the document, titled "Dangerous Attachments," which can be found in the ITS Website Support page, http://www.njcu.edu/dept/support.html

Server Processes

Sophos will reject any Level 1 attachment. The sender will get an error message stating why the file has been removed. The recipient will receive the message, but without the attachment. Level 2 attachments will be scanned for viruses by Sophos. Files found to contain a virus will be quarantined and the sender will be notified that attachment contained a virus and was stopped from being delivered. The recipient will not receive any notice. As part of VMS Email services, messages from domains that have been identified as sources of Spam are automatically deleted.

Client Security Process

New and updated versions of Outlook will not allow Level 1 attachments from being accessed or sent. The file remains in the Outlook message store forever. Level 2 files will be allowed to pass. However, the client anti-virus program will scan these files for viruses. If a virus is found the software will attempt to clean the file. If the software can not clean the file, it is deleted or quarantined. If Outlook is set up to filter Spam, advertisement messages will be moved to the spam folder.

Guidelines

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.

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 background 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 <u>rare</u> 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.