Policy & Procedures

Email Security Policy

Issued by: Technology Steering Committee

Applies to: University Employees and Students

Policy Rationale

Effective date: April 5th, 2019

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 is 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:

- Barracuda Spam Firewall.
- Barracuda block list.
- Spamhaus block list.
- SpamCop block list.

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.
Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every six months.

Employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, its amazing.", "Are you available", "Gift Cards".)
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks, mis-spelled words.)

If an employee is not sure that an email they received is safe, they can ask our Helpdesk.
We remind our employees to keep their anti-malware and virus programs updated.

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 the Barracuda Spam Firewall.
Level 1 attachments, deemed too dangerous for transfer, such as URL shortcuts (.url), programs (.exe), et-cetera, are blocked.
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), will be scanned and usually pass through with no issues. All email, sent or received, will be scanned for viruses at two levels: Barracuda and Client.

Server Processes

The Barracuda Firewall will block any Level 1 attachment. The sender will get an error message stating why the file was been blocked. Files found to contain a virus are blocked and the sender will be notified that the email was not delivered. The recipient will not receive any notice. As part of Exchange Email services, messages from domains that appear on the block list are automatically blocked.

Client Security Process

In the event a virus gets through, new and updated versions of Outlook will not allow the client to access Level 1 attachments. The client anti-virus program will scan these files for viruses. The software will attempt to clean the file anytime a virus in an email is detected. If the software cannot clean the file, it is deleted or quarantined. If Outlook is set up to filter Spam, advertisement messages will be moved to the Junk E-Mail folder.

Guidelines

Scanning messages and files at the server level is extremely processor intensive. The total number of users and the use of Email Listserv lists further exacerbate this issue. 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 40,000+ Email accounts and many lists. The University Email system is very busy 24/7. To ease Email processing and delivery delays, please follow these guidelines:

- *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 Format Text tab and Plain Text.
    - *Limit attachments size:* If you need to include an attachment, send it in a form that will not exceed 15mb for the total size of the email.