Spam/Anti-spam Email Preventative Measures Document type:
Advisory The City University of New York
University Information Security Office, security.cuny.edu
Status: Published, 4 December 2006, version 1.0

Continuing increases in the volume and sophistication of spam email have, in some cases, impacted the performance of our email systems causing non-delivery or delayed delivery of email.

Some Internet Service Providers such as AOL and Yahoo have prevented/blocked delivery of CUNY email through a process called blacklisting and labeling email from the CUNY.EDU domain as spam. Blacklisting can also prevent delivery of CUNY.EDU email to many private and public sector organizations.

We are requesting all CUNY faculty, students and staff read, understand and/or be knowledgeable of the material contained within all parts of this advisory. If you are a technical engineer responsible for maintaining a CUNY email system, adopt the practices in Part B, Technical Standards. If you advertise and promote CUNY events, services or products, adopt the practices in Part C, Compliance with Federal CAN-SPAM Law.

Questions or a need for further clarification should be directed to your College or department email administrator.

PART A – PRACTICES FOR ALL USERS

CUNY constituents will generate legitimate business email to students, faculty and staff. Please do not report this type of email as spam email to your Internet Service Provider (ISP) (e.g., AOL, Yahoo).

Avoid enabling automatic forwarding of CUNY email to a public email service such as AOL or Yahoo. If your CUNY email account receives spam email and it is automatically forwarded, the forwarded message could be reported as spam by the ISP.

CUNY can guarantee delivery of email within the CUNY email system, but there is no guarantee of email delivery after it leaves the CUNY email system.

Maintain email distribution lists and Listserv lists up-to-date at all times. Honor requests, on a timely basis, for removal from a list.

If you receive email that appears to be spam email, notify your College or department email administrator for further instructions.

E-mail content should not contain hex-encoded URLs. (e.g., http://%6d%6f%3a%6d%/). Instead, where possible, use clear text URLs, such as www.cuny.edu.

Avoid sending executable code as email attachments (e.g., EXE, PIF, VBS, SCR) particularly to public email services such as AOL and Yahoo. Consider compressing executable attachments with 7ZIP which is a free compression (www.7-zip.org) utility or WinZip before sending.

PART B - TECHNICAL STANDARDS

All CUNY email systems and components, regardless of function and department, must be protected by anti-spam email technology for inbound email. All email servers not protected must be removed from the CUNY.EDU email domain no later than 12/31/2006 and confirmed with the University Chief Information Officer and University Information Security Officer.

It is recommended implementing anti-spam email technology for outbound email (from CUNY.EDU to the public) where possible.

Configure your firewalls to ONLY allow SMTP email to exit your College or department from approved email servers.

All open mail relays (which allow a CUNY.EDU email system to "relay" mail onward to a public destination from a non-CUNY location on the Internet) must be turned off.

The DNS for your email servers should reverse-resolve to the host name and that host name should resolve to the host IP. This is the normal setup but it is often not properly configured in the DNS. Spammers masquerade as others and their true IP address does not usually match the name they are pretending to be. Most well-maintained email gateways will reject outright mail from a sender whose "origins" don't match up.

Set up Sender Policy Framework in your DNS. This is a system whereby you configure the DNS system with information about what relays your College or department uses to send its email. If someone tries to send email pretending to be you (i.e. most spam), the ISP could verify that it must be fake from the DNS databases and reject that email.

Regularly check the major blacklists for any indication that your CUNY email system has been flagged. Move to find the cause and request delisting as quickly as possible.

Set-up a feedback loop with AOL to allow the email administrator to take corrective actions when CUNY.EDU email is reported as spam email.

Whitelist your CUNY.EDU email domains with AOL and Yahoo.

Make sure your campus computers and servers are protected by continuously-updated, high-quality, anti-virus and anti-spyware protection.

Use an enterprise level spyware blocker, which can not only protect users from accessing dangerous sites and getting infected, but can also prevent computers already infected with spyware from communicating with their outside hosts.

PART C - COMPLIANCE WITH FEDERAL CAN-SPAM LAW

In 2003 Congress enacted federal legislation (the "CAN-SPAM Act") establishing requirements for those who send "commercial" email. The Act applies to email whose primary purpose is commercial advertisement or promotion of a commercial product or service. The Act does not define "commercial", but the FTC (in charge of enforcing the

Act) has made clear that the Act applies to educational institutions and other non-profit entities. The Act is not limited to bulk email.

WHAT DOES THE ACT MEAN FOR CUNY?

Commercial Email. Email correspondence sent by or on behalf of CUNY or its related entities for the primary purpose of advertising or promoting commercial products or services must meet the requirements of the Act. Examples of commercial email include:

- email promoting non-educational products of CUNY (e.g., credit cards, clothing, rings, chairs, etc.)
- email promoting concerts, sporting events, and similar events for which a fee greater than that needed to cover costs is charged
- email soliciting fee-based museum or sport center memberships
- newsletters to alumni and friends of CUNY that primarily promote products or services

Non-commercial or Exempt Email. Other CUNY or related entity email is not commercial or is otherwise exempt from most requirements of the Act. Examples include:

- email sent to conduct normal CUNY business, such as email regarding grades, course work, tuition payments, financial aid, employee benefits, policy announcements, or meeting notices
- electronic publications that consist primarily of news or educational material, rather than advertisements or solicitations
- surveys
- transactional email to notify the recipient about changes in an existing subscription, membership, account or comparable commercial relationship
- charitable solicitations

Email to Prospective Students. The applicability of the Act to email sent to prospective students is unclear. It is CUNY's view that email sent to provide information about CUNY's undergraduate, graduate, or professional degree-granting programs is not commercial email subject to the Act because it serves the institution's primary non-profit purpose of advancing education. However, senders should consider including an "opt-out" method, as described below, in unsolicited emails of this type.

Hybrid Email. Messages that contain both commercial content and transactional or non-commercial content are deemed to be commercial if the subject line or body of the message would lead the recipient to conclude that message is commercial or the transactional content does not appear at the beginning of the message.

WHAT THE ACT REQUIRES:

CAN-SPAM requires all commercial emails to include the following:

- **A subject line or heading that is not materially misleading.** The "From," "To," and routing information--including the originating domain name and email address--must be accurate and identify the person who initiated the email. The subject line cannot mislead the recipient about the contents or subject matter of the message.

- **A conspicuous notice identifying the message as an advertisement or solicitation,** unless the recipient has previously agreed to receive the email. The Act allows mailers to determine the form and location of this notice.

- **A valid physical postal address.**

- **A functioning return email address, domain name, or IP address**.

- **A method for email recipients to "opt-out".** Senders must provide a return email address or another Internet-based response mechanism that allows a recipient to ask the sender not to send future email messages to that email address, and must honor the requests. This mechanism must remain functional for at least 30 days after the email is sent. The opt-out notice should be clear about the scope of the opt-out. For example, the opt-out should make clear if it is limited to communications from a particular program, rather than an entire department or college.

CAN-SPAM also requires senders of commercial emails to:

- **Honor opt-out requests within 10 business days of their receipt.**

- **Refrain from selling or transferring the email addresses of people who made an "opt-out" request, unless the purpose of the transfer is so another entity can comply with the Act.**

NOTE: Even if an individual has given prior consent to receipt of a commercial email, all requirements of the Act must be met except the requirement that the email be identified as an advertisement or solicitation.