Anti-Spam Policy[1]

Harrisburg University of Science and Technology
Office of Information Services

I. Introduction

Spam is commonly defined as the sending of unsolicited bulk e-mail of either commercial or non-commercial intent. Spam includes, but is not limited to: advertisements, pyramid schemes, chain letters, propaganda, unwanted questionable subject matter, and/or email that contains a false or misleading header, subject line, identification of the sender, return address, routing or transmission path or other indication of origin, or that uses a third party domain name without permission. In addition, spam includes email that aims to market goods or services sent without the consent/solicitation of the recipient, or without a preexisting relationship between the sender and recipient. Presently, there is no universal method of definitively identifying and preventing email spam. This is a global problem, not confined to Harrisburg University.

II. Purpose

This policy:

a. Outlines Harrisburg University's responsibilities to actively defend against **incoming spam**.

b. Defines the responsibilities for Harrisburg University, its faculty, administrators, staff, students, and other authorized users with regard to **outgoing spam** or the sending bulk e-mail considered by unsuspecting email recipients as spam.

c. Explains the appropriate procedures for enforcing this policy.

d. Offers guidance for reducing the amount of spam one receives.

[1] This policy should read in the context of other applicable Harrisburg University of Science and Technology policies especially the Acceptable Use Policy and the Email Policy.

III. Responsibilities

a. It is the responsibility of the university faculty, administrators, staff, or student workers to communicate this policy and its contents to any and all email users at, or in affiliation with, Harrisburg University. Not being aware of any part of this policy does not excuse one from being responsible for its contents.

b. Given the global pervasiveness of the spam problem, Harrisburg University minimizes the impact of spam by implementing appropriate policies and technologies outlined in the compliance section of this document.

c. HU reserves the right to refuse email or other connections from outside hosts that send unsolicited, mass or commercial messages, prurient or offensive messages, or messages that contain viruses.

d. Users and third parties are prohibited from using HU's network to send spam, or to send any electronic correspondence in violation of any applicable law, rule or regulation pertaining to unsolicited or bulk messages.

e. Selling or purchasing email lists is prohibited.

f. HU is consistent in advertising email addresses on its web site. As much as possible, email aliases (such as admissions@harrisburgu.net) are used to reduce the times a person email is listed.

IV. Compliance

a. To comply with this policy, Harrisburg University defends against spam by employing hardware/software preventions, policy statements, and via educational outreach:

   i. **First line of defense.** *Spam firewall server* – The HU spam firewall server is an integrated hardware and software solution for protecting and reducing the load placed on HU's email server by off-loading spam and filtering viruses and spyware. The firewall server constantly monitors known spammer lists and compares HU incoming mail to these lists. The firewall will refuse the confirmed spam. This layer of protection has had a significant effect on incoming spam. Approximately 70% of the mail that arrives at HU is known spam; this service significantly reduces junk mail. Moreover, essential outbound filtering techniques such as attachment scanning, virus filtering, rate controls and encryption

helps ensure that outgoing HU email is legitimate and virus-free.

ii. **Second line of defense.** *Email server* **–** If an unsolicited email reaches HU's email server, it goes through another thorough line of defense. Sybari Antigen for Microsoft Exchange delivers server-level antivirus protection with multiple scan engine management and advanced content-filtering capabilities. Its layered protection offers a comprehensive defense against undesirable and malicious message traffic.

iii. **Third line of defense.** *Client applications* – While there is no such thing as a perfect filter, software is loaded on each user's computer to combat viruses and malware. This further helps to keep spam at manageable level.

b. To comply with this policy, and in order to further combat spam, all Harrisburg IT Users are responsible for the following defenses:

i. **Fourth line of defense.** *Configure local junk mail controls* **–** Each individual can further defend against spam by configuring Microsoft Outlook's built-in preferences to control mail. These preferences, if properly enabled, can be effective in fine-tuning client-based spam controls for messages that might escape the firewall or email server filtering mechanisms.

ii. **Fifth line of defense.** *General awareness* **–** Users can prevent spam by following generally accepted hints for reducing spam outlined in this document's appendix.

V. Enforcement and Disciplinary Procedures

a. Any user who violates any part of this policy is bound by the enforcement and disciplinary procedures in the Harrisburg University of Science and Technology's Acceptable Use Policy.

VI. Procedure to Update and/or Amend

a. Harrisburg University reserves the right to update and/or amend this document to reflect university policy changes and/or state or federal law.

VII. Appendix: Hints on Reducing Spam[2]

a. Though, at present, there is nothing HU can do **legally** to prevent all electronic junk mail from arriving at HU e-mail addresses. Please be aware of these generally accepted user-driven hints to reduce spam:

i. Delete spam: The most helpful method of dealing with unwanted junk mail of all kinds is to try to recognize it without opening it, and discard it unopened.

ii. Never respond to spam: Responding to spam exacerbates the problem; your response confirms that your address is "live" and open to attack. If you respond, your address will probably be sold to other spammers resulting in even more spam. Moreover, do not write to e-mail addresses asking you to "remove your name from the list" nor visit any web page asking you to remove your name.

iii. Avoid posting your email address: As much as possible, avoid posting your email address on personal or professional web sites or volunteering your email address without knowing how it will be used. Spammers deploy software that "harvests" email addresses from the web. This software crawls the Internet seeking text strings that are user@something.something. When it finds one, it stores it to a spam database.

iv. Use an alternative email address in newsgroups: Newsgroups are a common target for spammers. If you post to a group, you're going to get spam. To participate, try to use a different email address than one you regularly use.

v. Never buy anything advertised in spam. The reason that people spam is because they can make money. They make money, like all advertisers, by convincing people to buy a product. If no one buys the things advertised in spam, companies will quit paying spammers to advertise their products.

---

[2] Adapted from: Spam Recycling Center http://www.spamrecycle.com/antispamthings.htm