Summary of Security Bulletin

In early/mid September 2010, the general media and technical forums have widely reported the spread of a mass-mailing email that contains a link to malicious code that will infect your computer and may result in the exposure of the information you have stored on your computer. To keep you informed, there is a mass-mailing worm often labeled "Here you have" spreading through emails and this phrase is either embedded in the body of emails as a uniform resource locator (URL) link or as a subject heading.

As a general precaution and preventive measures from CUNY/CIS IT Security team:

**Keep your endpoint security (e.g., anti-virus, software security patches) updated at all times.**

**Delete the email, do not click on any of the links or reply to the message. Refer to the CUNY Phishing Advisory posted at security.cuny.edu under CUNY Issued Security Advisories. Never reply to any email that asks you for your personal information regardless of how official it appears.**

**If you disclosed your password in response to an email you must change your password immediately, read the user to the CUNY Phishing Advisory posted at security.cuny.edu under CUNY Issued Security Advisories, and complete the 30 minute information security awareness program also located at security.cuny.edu on the home page. Click on the padlock.**

In addition, please adhere to the following security practices when using the Internet:

1. Avoid clicking on any web links from within an email. These embedded links may direct your Internet browser session to illegitimate web sites asking for personal information and could also download malicious code, such as viruses or spyware, onto your machine. Instead, start a new Internet browser session and enter the legitimate web site address into the address bar of the browser.

2. The content of many phishing e-mails can be very threatening (e.g., account closure, account verification, account updates, account is limited) and can be convincing to entice the user to follow through with the provided instructions. By far, most institutions will use non-Internet methods, such as the U.S. Postal Service, to send these types of notices and then will only send them to your official address of record. If in doubt about the legitimacy of these threatening e-mails, call the institution using the phone number on your last statement or on the back of your credit card.

3. Similarly financial institutions generally require some form of an initial setup to be completed prior to allowing electronic banking services. An online relationship is usually not established automatically or only through an exchange of e-mails. Become familiar with your financial institutions online registration process and how the electronic relationship may change from time to time. If in doubt, call the institution using the phone number on your last statement or on the back of your credit card.

4. Update your computer's operating and Internet browser software on a regular basis. These updates routinely include security enhancements.

5. Maintain anti-virus programs to the current level of protection.

6. Select and maintain passwords that are difficult to guess and change them regularly.