CUNY Phishing Advisory

The following advisory is being distributed to the CUNY community to raise the awareness of specific computer security risks and issues. Please distribute as appropriate throughout your organization.

Increasingly, CUNY students, faculty and staff receive e-mails appearing to be from legitimate sources which are actually fraudulent and clever methods to trick you into disclosing personal information for criminal intent. These techniques are commonly referred to as Phishing. Frequently these e-mails come from familiar sounding names of banks and financial institutions. To minimize the risk of you becoming a victim of identity theft follow these basic 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, 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 through exchange of e-mails. Become familiar with your financial institution’s online registration process. 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.

Carl Cammarata
CUNY Information Security Officer