CUNY Graduate Center
Information Technology

PROTECT YOURSELF AGAINST PHISHING ATTACKS

Phishing is a cunning attempt by hackers to solicit, steal and mishandle users' personal information (e.g. username and password, credit/debit card information, home address, social security number, date of birth, etc.) for criminal activities. Typically, phishing is achieved through emails disguised as legitimate messages from people you're familiar with, reputable banks/financial institutions and well established companies with official-looking logos. Links are included in these bogus types of emails that direct users to a webpage to enter personal data. After users willingly supply the requested data, hackers gain access to their accounts and then engage in malicious and criminal activities.

IT Staff and legitimate organizations will never ask users to supply a password or any other personal information via an email message. **Whenever you're in doubt about the legitimacy of an email message, contact IT Services for assistance at ITServices@gc.cuny.edu.**

General Guidance

Read the CUNY Phishing Advisory as well as related resources posted on the CUNY CIS website at security.cuny.edu. In addition, we suggest you complete the 30 minute information security awareness program also located at security.cuny.edu on the home page. Click on the padlock.

Adhere to the following security practices when using the Internet:

- Never reply to any email that asks you for your personal information regardless of how official it appears. CUNY will not and should not be asking for personal information via email. If you disclosed your user ID and password then you must change your password immediately on any and all systems where the password is used.
- 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 spy ware, onto your machine. Instead, start a new Internet browser session and enter the legitimate web site address into the address bar of the browser.
- 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.

- 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 institution's 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.
- Update your computer's operating and Internet browser software on a regular basis. These updates routinely include security enhancements.
- Maintain anti-virus programs to the current level of protection.
- Select and maintain passwords that are difficult to guess and change them regularly.