Dear CCNY Faculty and Staff:

How to recognize and avoid a phishing attack

If you receive an e-mail that has the same or similar information as the message below DO NOT CLICK on any links!
See details below for how to recognize, avoid and respond to phishing attacks.

1. The sender's email address seems legitimate but if you mouse over it you will reveal an e-mail address that should arouse your suspicion. In this case the actual e-mail address has no affiliation to CCNY or CUNY. However, phishing e-mails may originate from CCNY/CUNY e-mail address, so don't lower your guard.

2. The sender, subject and recipient are designed to convey an authentic and urgent emergency to override your sense of caution. Stay calm and rational.

3. The body of this message is very generic— but they can be very graphically sophisticated. Ask yourself: what account is this e-mail referencing? Why is it not branded with official college letterhead? The lack of specific detail is a strong indication that it's a threat. If you mouse over the link (be careful not to click it) and look carefully it will reveal
Clicking on the link in this phishing e-mail will infect your computer with malware. The malware will attempt to infect other devices – computers, smart phones, and tablets. It will attempt to harvest sensitive information (including passwords, files, SSNs, credit cards) and compromise accounts (e.g. email, Facebook, bank accounts, etc.). These attacks can lead to identify theft.

Instead of clicking on the link, forward suspicious e-mails to itsecurity@ccny.cuny.edu and then delete and purge the original email.

If you are concerned about your account, use the login portal on the CCNY website to navigate to your account (e-mail, CUNYfirst, CUNYPortal, Degreeworks). You can also contact your local computer administrator or the CCNY Service Desk.

We regret any inconvenience experienced due to this issue and appreciate your patience as we address it.

Please contact OIT service desk at X7878 or via e-mail servicedesk@ccny.cuny.edu for further information.