This is a reminder that you need to be alert for fake emails that look like they come from your local police or State Dept. of Motor Vehicles (DMV) claiming you have a traffic violation. At the moment, there is a local scam in New York that falsely states you have outstanding violations you need to either pay for or refute, and if you don't your license will be revoked. This scam may spread to the rest of America soon. Remember that citations are never emailed with links in them, or sent out with an email attachment, and report scams like this to your local police department. Here is how the phishing email reads:

Dear Driver:

We are writing to inform you that the state police department has notified us that you have several outstanding traffic violations. If you do not make restitution for these infractions within 48 hours, we will be forced to revoke your drivers license.

To make payment arrangements online, click here.

To refute these tickets, click here.

Sincerely,

The NY DMV

Phishing emails often direct you to submit sensitive information, threaten to deactivate an account, advise you to change your password or activate or upgrade an account by clicking a link. These schemes also use less alarming ruses, including attaching invoices, taxes, or financial aid forms that contain viruses. Their goal is to compromise the security of your personal computer or smartphone, to harvest your valuable information, and, ultimately, to defraud you and your colleagues, friends and family.

How to Protect Yourself
Always remember, an official entity, including CCNY and CUNY, will never use email to request your userid, password, or social security number or ask for detailed personal and financial information such as PIN numbers, or secret access information for credit card, bank or other financial accounts. Be suspicious if you receive emails or visit websites requesting any of this information, also:

DO NOT click on the links.

DO NOT download the attachments.
DO NOT enter your credentials.
DO NOT reply to the original email.
DO NOT forward it to acquaintances.

If a suspicious message seems legitimate, contact the originating office by phone (using the phone number on the CCNY directory listing) before responding. Or try opening a new browser window and typing the address directly. Please also notify ITSecurity@ccny.cuny.edu.

If you inadvertently disclose your user ID and password change your password immediately on any and all systems where that password is used. Using your account credentials from one hacked system cyber-criminals may be able to determine your username on other systems. If you use the same password on those systems they too could be compromised.

For more information please read the CUNY Phishing Advisory posted at security.cuny.edu under the CUNY Issued Security Advisories.

In addition, we suggest you complete the 30-minute Security Awareness Course viewable here: http://security.cuny.edu/

The following links provide useful resources to help you better understand, identify and avoid phishing scams and how to protect yourself from cyber fraud:

**Screenshots of Convincing Phishing Emails**

**Ouch! security newsletter on the topic**
https://www.ccny.cuny.edu/sites/default/files/it/upload/2013-02_OUCH_Email-Phishing-Attacks.pdf

**CCNY Information Security website, including CCNY/ CUNY policies**
https://www.ccny.cuny.edu/it/security

**United States Computer Emergency Readiness: Team Report Phishing**
http://www.us-cert.gov/nav/report_phishing.html

**Federal Trade Commission: Identity Theft**
http://www.ftc.gov/bcp/edu/microsites/idtheft