

What is required of me as an employee of CUNY?

- Take the CUNY Awareness Course Online at:
<http://www.cuny.edu/about/administration/offices/CIS/security/training.html>
- Visit York IT website on Security Awareness at:
<https://www.york.cuny.edu/it/service-delivery-unit/service-desk/security-awareness>
- Review the insert within this brochure for Cyber Dos and Don'ts also located at:
<https://www.york.cuny.edu/it/service-delivery-unit/service-desk/security-awareness>
- Maintain compliance with the Policy on Acceptable Use of Computer Resources and the CUNY Security Procedures at all times located at:
<http://www.cuny.edu/about/administration/offices/CIS/security/pnp.html>

If you discover or suspect a security breach, you should report the incident to your supervisor, the College CUNY Security Manager (click on Contact Us at security.cuny.edu) and the CUNY Central CUNY Security Office (security@mail.cuny.edu) immediately.



CYBER SECURITY IS OUR SHARED RESPONSIBILITY

PROTECT DATA ON PORTABLE DEVICES

<http://security.cuny.edu>

 **YORK** College

94-20 GUY R. BREWER BOULEVARD
JAMAICA, NEW YORK 11451

Phone: 718-262-5311
E-mail: helpdesk@york.cuny.edu

Cyber Security Awareness

CUNY Security Policies and Safety Practices for securing University personal & professional information



Why is Cyber Security important at York?

We must ensure our academic and administrative systems continue to be available to run the business of the University and to serve our faculty, students, and staff.

We must maintain accurate University data and prevent unauthorized changes (e.g., grades, financial aid information).

We must be reputable custodians and are required by law to protect the privacy of personal data belonging to our faculty, students, and staff.

What are the Cyber Security risks to CUNY?

- Don't be phished. Phishing is a scam in which an email message directs you to click on a link that takes you to a web site where you are prompted for personal information such as passwords, social security number, bank account number or credit card number. Both the link and web site may closely resemble an authentic web site, but they are not legitimate.
- Don't disclose personal information to someone you don't know. Social engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without their realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person, and through e-mail.
- Don't disclose personal information within CUNY unless it is absolutely necessary. The need for disclosing your social security number outside of the Human Resource (HR) department would be unusual. When in doubt, contact the HR department directly to verify the legitimacy of the request.

- Protect your user ID and password and never share them. Your user ID is your identification, and it is what links you to your actions on CUNY's computer systems. Your password authenticates your user ID. Use passwords that are difficult to guess and change them regularly.
- You are responsible for actions taken with your ID and password. Log off or lock your computer when you are away from your workstation. In most cases, hitting the "Control-Alt-Delete" keys and then selecting "Lock Computer" will keep others out. You will need your password to sign back in, but doing this several times a day will help you to remember your password.
- E-mail and portable devices are not secure. Do not ship personal information belonging to you or CUNY faculty, students, and staff to portable devices (e.g., portable hard drives, memory) or send or request to be sent such personal information in an e-mail text or as an email attachment without encryption.
- Be careful when using the Internet. Malicious code can take forms such as a virus, worm or Trojan and can be hidden behind an infected web page or a downloaded program. Keep anti-virus and anti-malware programs and the software on your workstation up-to-date at all times. Only install software authorized by your department, and never disable or change security programs and their configuration.

Where are the CUNY Cyber Security information resources?

[Security.cuny.edu](http://security.cuny.edu) is available 24 hours a day from any Internet accessible location without a user ID and password. All relevant policies, procedures, and advisories, the CUNY Security awareness program and materials, and links to external CUNY Security information resources are located here.

Find the Policy on Acceptable Use of Computer Resources under Info Security Policies.

Find the CUNY Security Procedures – General under Info Security Policies.

To take the CUNY Security Awareness tutorial, approximately 30 minutes, go to the following link: <http://www.cuny.edu/about/administration/offices/CIS/security/training.html>

Who to contact for help with CUNY Cyber Security at YORK COLLEGE?

- Your supervisor.
- Your College web-site.
- Your College Service Desk ext. 5311

security.cuny.edu

The College CUNY Security Manager (click on Campus Security Managers Contact Information at security.cuny.edu under Contact Us).

The College Chief Information Officer or equivalent in the Central Office department.

The CUNY Central CUNY Security Office at security@mail.cuny.edu; or the Contact Us page at security.cuny.edu; or the Who to Contact for Help page at security.cuny.edu.

Where are some external resources for help with CUNY Security located?

1. New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) at www.cscic.state.ny.us
2. Federal Trade Commission at www.ftc.gov
3. Privacy Rights Clearinghouse - Nonprofit Consumer Information and Advocacy Organization at www.privacyrights.org
4. Anti-Phishing Working Group – Committed to wiping out Internet scams and fraud at www.antiphishing.org
5. Microsoft Malware Protection Center, Threat Research and Response at