Hostos Community College

A message from
THE PRESIDENT

Recent CUNY CyberSecurity Incidents

Earlier this week, I met with members of my Extended Cabinet to discuss recent cybersecurity incidents at fellow CUNY campuses. At this time, there has been no related impact to Hostos Community College. However, our campus is not immune to the ever-increasing volume and complexity of cyber threats spreading across the Internet and targeting us through a variety of means such as credential-stealing phishing e-mails, malicious attachments, compromised/impersonating websites, and more.

It is imperative that we remain vigilant of such threats in both our personal and professional lives when using technology. Publicly available professional and personal content on websites, social media, etc. are used to gather information about us and to target us with very specific, convincing communications in an attempt to extract further information to be used for financial gain or to take control of your devices or your credentials.

There are multiple steps recommended to help reduce your vulnerability to fall victim to these attacks:

DO

1. Create strong passwords, and use unique/distinct passwords for all of your online accounts
2. Where available, use Multi-Factor-Authentication (MFA) to add a layer of validation for your accounts. Hostos had made MFA available to all students, faculty and staff through its Single Sign On solution. For more information, click here: www.hostos.cuny.edu/SSO
3. Keep your operating system and anti-virus software up to date – this is a very simple way to keep your devices protected.
4. Always use a password/passcode for your devices
5. Log out of websites when you are done using the computer, especially if a public computer
6. Be wary of “free WiFi” – often times these open networks are setup by cyber criminals to collect your data
7. Watch out for imposter scams claiming to be from a family, friend or colleague including those offering “jobs” or requesting urgent financial assistance

DON’T

1. Click on any email links, open attachments or reply with personal information/login credentials, especially if unexpected. When in doubt – DON’T ENGAGE. Hostos tags External or Suspected Spam emails in the subject and body to give you an added indication that the email might be risky. Always forward suspicious e-mails to reportspam@hostos.cuny.edu

2. Share/Store/Upload sensitive information about yourself or others via e-mail or cloud storage platforms such as
3. Download “free” software/apps which may seem to address a personal/professional need but may have hidden spyware or might collect personal information and resell it.

The college’s IT Department continues to take the necessary steps to secure the data and computing environment and additional helpful information can be found on the CyberSecurity webpage. If you suspect you may have inadvertently clicked on a malicious link, please notify our IT Department immediately.

As we continue to work/learn/interact online, our need to exercise extreme caution on an ongoing basis cannot be overstated.

Thank you for your continued vigilance.

Office of the President
Eugenio María de Hostos Community College
475 Grand Concourse, A-Building, Room 341, Bronx, NY 10451
718-518-4300 | PRESIDENTSOFFICE@hostos.cuny.edu