From: CSI Technologyservices <Technologyservices@csi.cuny.edu>
Sent: Monday, June 2, 2025 5:03 PM
To: CSI-FacultyStaffBroadcast <FacultyStaffBroadcast@csi.cuny.edu>
Subject: CUNY Cybersecurity Training Course for Faculty and Staff 2025

CUNY Cybersecurity Training Course for Faculty and Staff

- The CUNY Cybersecurity Awareness Training Course 2024-25 is live and ready for all faculty and staff on Blackboard.
  - Access the College of Staten Island's Blackboard organization through this link: https://bbhosted.cuny.edu/webapps/blackboard/execute/courseMain?course_id=_2409463_1.
  - **CSI is currently only 22% compliant, and it is mandatory for all faculty and staff to complete this training.**
- Remember, our cybersecurity resilience is only as strong as our weakest link. Education is our best defense against cyber threats. Training and staying vigilant can break the "it won't happen to me" mindset. Let's not wait for a crisis to occur—let's be proactive in strengthening our cybersecurity.

Important Reminders:

***If you think** a security threat has already impacted you:*

- DO raise awareness of scams by reviewing the CUNY "How to Protect Yourself Against Secret Shopper, Personal Assistant, and Other Online Scams!" and Phishing advisories posted at security.cuny.edu under CUNY Issued Security Advisories.
- DO NOT reply to unexpected or unusual emails from any sender.
- DO be cautious when an "external source" warning banner is present.
- DO NOT reply to emails with any personal information or passwords. If you have reason to believe that the request is genuine, call the institution or company directly.
- Please don't click a link or open an attachment in an unsolicited email. If you believe the request is genuine, type the company or institution's web address directly into your browser.

- DO NOT use the same password for your work account, bank, Facebook, etc. If you fall victim to a phishing attempt, perpetrators attempt to use your compromised password to access many online services.
- DO change ALL your passwords if you suspect any account you access may be compromised.
- Be particularly cautious when reading emails on a mobile device. Reading emails on a smaller screen may make missing telltale signs of phishing attempts easier.
- Please remember that official communications should not solicit personal information by email.
- DO read the CUNY Personal Assistant Scam and Phishing Advisories posted at security.cuny.edu under CUNY Issued Security Advisories.
    - How to Mark Spam using Outlook 360 in Web Browser:
        - ****Do not forward any email that you believe to be spam to anyone at the College or within CUNY****
            - Right Click the email in your Inbox:
            -
- DO complete information security awareness training located at security.cuny.edu