KINGSBOROUGH COMMUNITY COLLEGE
★ DREAMS BEGIN HERE ★

OFFICE OF STUDENT AFFAIRS

September 16, 2019

Kingsborough Students,

A recent phishing email scam has been brought to our attention. An email announcing students were selected as a "***Kingsborough Community College Job Placement & Student Services as a secret shopper***" has been circulated from other Kingsborough email addresses. This email was not distributed by Kingsborough Community College. KCC will never ask or instruct any students to deposit checks, purchase gift cards, or solicit personal information via email. Please remain vigilant when responding to emails. Be aware of common scams:

- Copycat and fake websites pose as legitimate ones to capture personal and financial information
- E-cards, unexpected "gifts" and job offers ("secret shopper") from unknown senders may contain links that lead to malware
- Fake advertisements, coupons or shipping notifications may include infected attachments and/or contain links that lead to malware
- Phishing email messages and fraudulent posts on social networking sites may request support for phony causes or offer "too good to be true" deals on merchandise
- Security or "fix or tune up your PC" software offered as an unexpected pop-up ad
- "Secret Shopper" scam. This is something that is prevalent and has impacted a lot of students recently. The attachment from the Federal Trade Commission website provides an overview of how frauds involving the "secret shopper" MO are typically perpetrated.
-

To avoid such risks that could result in a security breach, identity theft or financial loss:

- Approach all unsolicited offers and communications with skepticism and caution
- Do not follow unsolicited links or download attachments from unknown sources
- Always compare a link in an email to the link you are actually directed to and determine if it matches and will lead you to a legitimate site
- Turn on enhanced account authentication features that use a companion mobile app to verify account activity or text unique verification codes to your mobile device
- View online shopping safety tips by the Department of Homeland Security, the National Cyber Security Alliance and the Federal Trade Commission

If you believe you are a victim of an online scam or malware campaign, please report it and consider the following actions:

2001 Oriental Boulevard | Brooklyn, NY 11235
T: (718) 368-5563 | F: (718) 368-4609 www.kbcc.cuny.edu
CUNY The City University of New York

- Advise your financial institution immediately of any account information that may have been compromised. Watch for unexplained charges to your account
- Immediately change any passwords that you might have revealed. If you used the same password for multiple websites make sure to change it for each account, and do not use that same password in the future

If you are a victim or have received a suspicious email, please contact Public Safety at 718-368-5069 or call the Office of Student Affairs at 718-368-5563. Thank you for your attention to this matter.

Sincerely,

Dr. Brian R. Mitra
Dean of Student Affairs