CUNY Security Alert: Phishing Campaigns

CUNY has recently experienced several instances of fraudulent, phishing attempts. The intent of this alert is to raise awareness of these types of campaigns. Please review the following information which can help you recognize phishing attempts should one be directed to you.

Security Threat Identification / Symptoms

- Phishing email in which COVID-19-related grant money / benefits or a stay-at-home job is offered.
- Emails may be entitled “Important/Urgent Message from the College Finance Department” “COVID-19 Benefits” or similar.
- The email or email attachment contains a link to “sign up” for the fraudulent offers. Please note that the sender of the phishing email could be from a CUNY email account that has been compromised.
  Samples of several such phishing emails are included at the bottom of this message.

If you think you have already been impacted by this security threat

If you believe you are a victim of an online scam or malware campaign, please report it to the CUNY CIS Service Desk (service.desk@cuny.edu, 646-664-2311) and consider the following actions:

- 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.
- Go to https://www.identitytheft.gov/ for information on reporting identity theft.

Recommended User Action

- DO NOT reply to unexpected or unusual email from any sender.
- DO be particularly cautious when the “external source” warning banner is present.
- DO NOT reply to email with, or provide any, personal information or passwords. If you have reason to believe that a request is real, call the department, institution or company directly.
- DO NOT click a link or open an attachment in an unsolicited email message. If you have reason to believe the request is real, type the web address for the company or institution directly into your web browser.
- DO NOT use the same password for your work account, bank, Facebook, etc. In the event you do fall victim to a phishing attempt, perpetrators attempt to use your compromised password to access many online services.
- DO change ALL of your passwords if you suspect any account you have access to may be compromised.

- DO be particularly cautious when reading email on a mobile device. It may be easier to miss telltale signs of phishing attempts when reading email on a smaller screen.
- DO remember that official communications should not solicit personal information by email.
- DO read the CUNY Phishing Advisory posted at security.cuny.edu under CUNY Issued Security Advisories.
- DO complete information security awareness training located at security.cuny.edu.

Security Threat Explained

Such phishing messages request that the recipient click on a link in the email or in an attachment that requests personal or login/password credential information to be entered. The associated website is fraudulent. Information entered in response to the phish is harvested by malicious actors to be used to conduct identity theft, account compromise, data theft, etc.

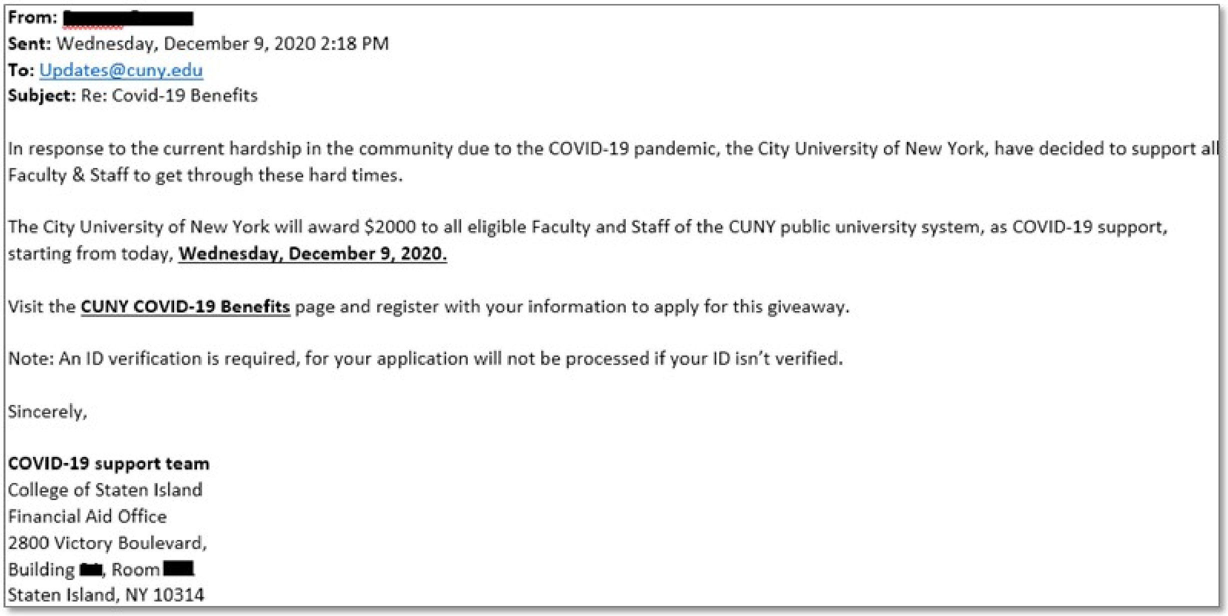
Security Alert Updates

CUNY/CIS will send an update if/when there is more information to share.

Cyber Security Questions

If you have any cyber security questions, please contact LaGuardia's Information Security.

Samples of Phishing Emails



From: [redacted]
Sent: Wednesday, December 9, 2020 2:18 PM
To: Updates@cuny.edu
Subject: Re: Covid-19 Benefits

In response to the current hardship in the community due to the COVID-19 pandemic, the City University of New York, have decided to support all Faculty & Staff to get through these hard times.

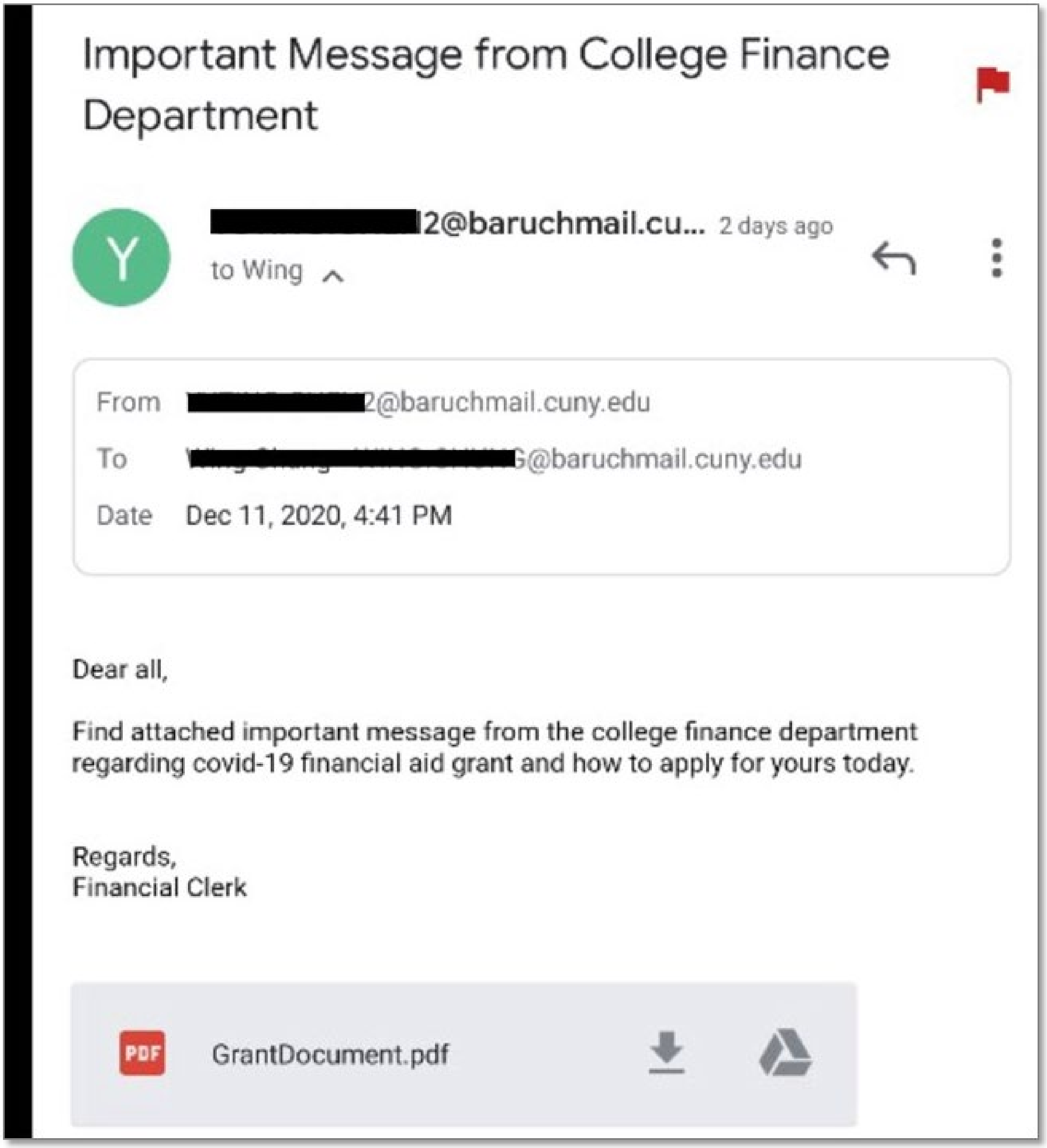
The City University of New York will award $2000 to all eligible Faculty and Staff of the CUNY public university system, as COVID-19 support, starting from today, **Wednesday, December 9, 2020.**

Visit the **CUNY COVID-19 Benefits** page and register with your information to apply for this giveaway.

Note: An ID verification is required, for your application will not be processed if your ID isn't verified.

Sincerely,

COVID-19 support team
College of Staten Island
Financial Aid Office
2800 Victory Boulevard,
Building [redacted], Room [redacted]
Staten Island, NY 10314



Important Message from College Finance Department

[redacted]2@baruchmail.cu... 2 days ago

to Wing

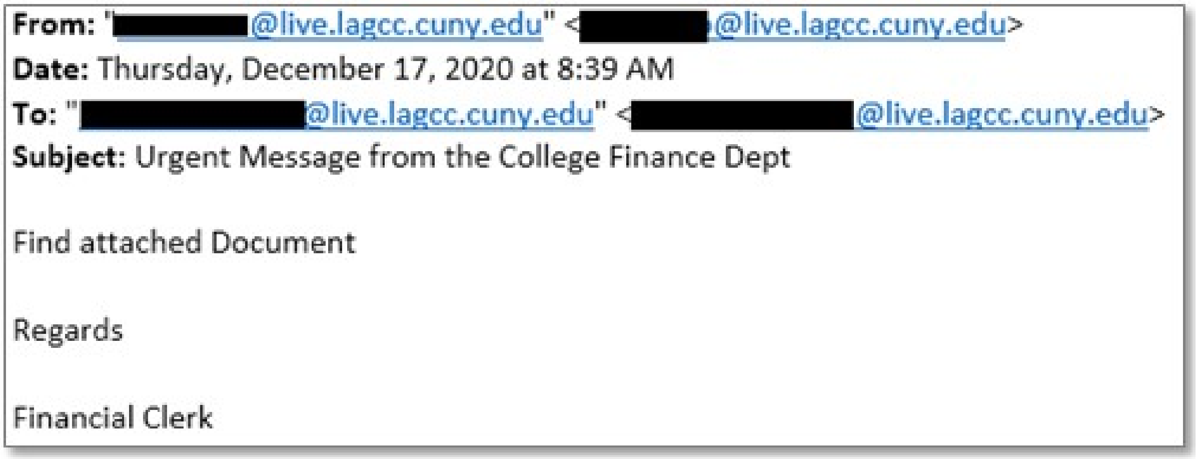
From	[redacted]2@baruchmail.cuny.edu
To	[redacted]@baruchmail.cuny.edu
Date	Dec 11, 2020, 4:41 PM

Dear all,

Find attached important message from the college finance department regarding covid-19 financial aid grant and how to apply for yours today.

Regards,
Financial Clerk

GrantDocument.pdf

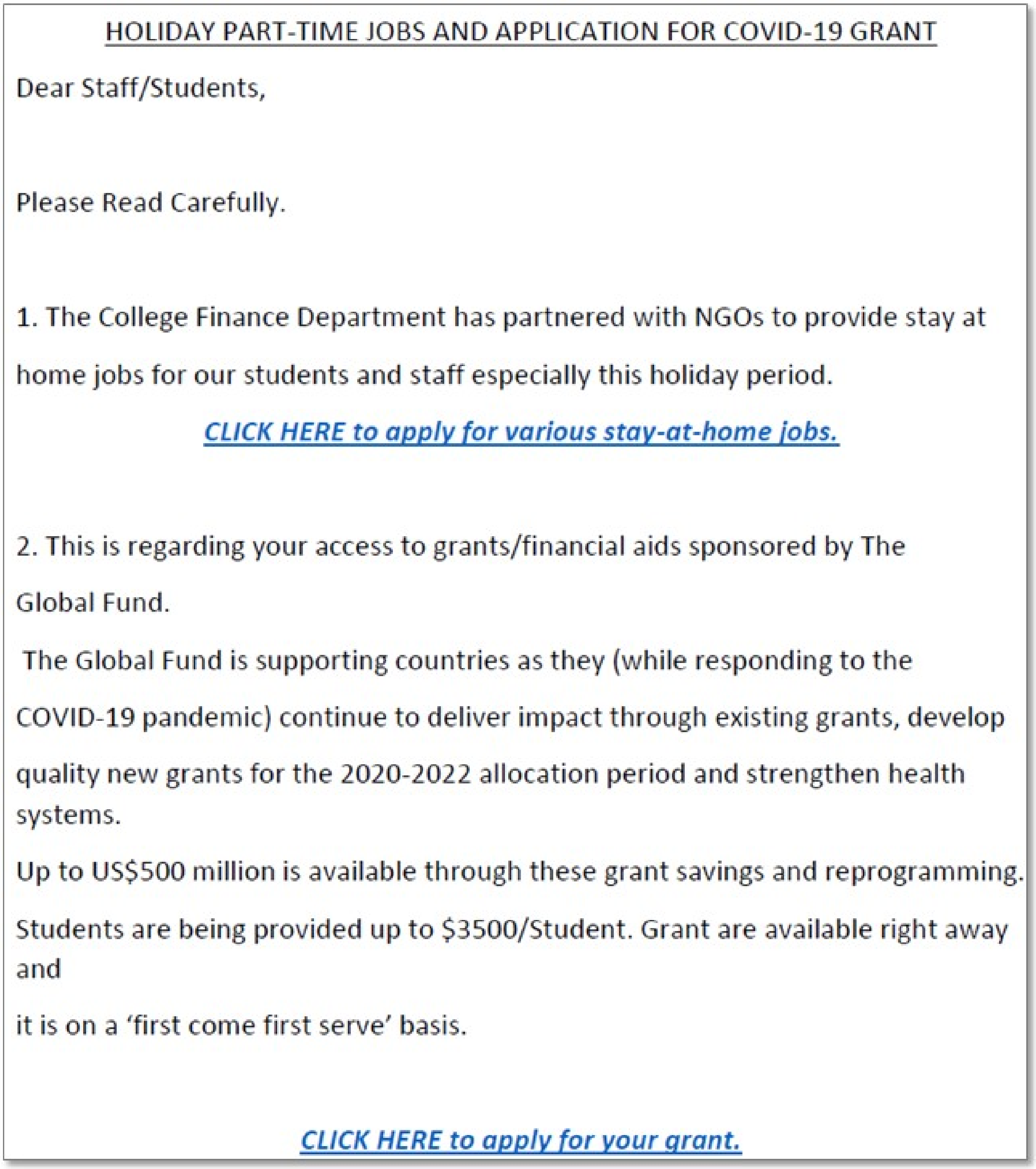


From: "[redacted]@live.lagcc.cuny.edu" <[redacted]@live.lagcc.cuny.edu>
Date: Thursday, December 17, 2020 at 8:39 AM
To: "[redacted]@live.lagcc.cuny.edu" <[redacted]@live.lagcc.cuny.edu>
Subject: Urgent Message from the College Finance Dept

Find attached Document

Regards

Financial Clerk



HOLIDAY PART-TIME JOBS AND APPLICATION FOR COVID-19 GRANT

Dear Staff/Students,

Please Read Carefully.

1. The College Finance Department has partnered with NGOs to provide stay at home jobs for our students and staff especially this holiday period.

CLICK HERE to apply for various stay-at-home jobs.

2. This is regarding your access to grants/financial aids sponsored by The Global Fund.

The Global Fund is supporting countries as they (while responding to the COVID-19 pandemic) continue to deliver impact through existing grants, develop quality new grants for the 2020-2022 allocation period and strengthen health systems.

Up to US$500 million is available through these grant savings and reprogramming.

Students are being provided up to $3500/Student. Grant are available right away and

it is on a 'first come first serve' basis.

CLICK HERE to apply for your grant.