

Subject: CIS Security Alert: Surge in phishing and other email scams 3/27/2019

CIS Information Security has observed a recent increase in targeted email-based scams and phishing emails, both at CUNY campuses and at the Central Office. Please review the following information to reinforce your awareness of such scams and what you should and should not do in response.

Security Threat Identification / Symptoms

Unsolicited email, sometimes appearing to have been sent by a familiar sender, including CUNY presidents, deans, department heads, etc. Some messages have included a signature block with the name and email address of a real CUNY staff member in a financial or human resources role.

The message may

- contain an unadorned link that leads to a site that attempts to infect malware
- contain an attachment that is claimed to be an invoice or similar
- request the purchase of gift cards on the requestor's behalf
- offer employment as a "secret shopper"
- request a change of direct deposit bank information, targeting human resources and finance staff
- plead for urgent or immediate action

Examples of such messages are included at the end of this message.

Recommended User Action

- DO NOT reply to email with any personal information or passwords. If you have reason to believe that a request is real, call the individual or company directly by independently looking up contact information.
- DO NOT click a link or open an attachment in an unsolicited email message. If you have reason to believe a request is real, type the web address for the company or institution directly into your web browser.
- BE SUSPICIOUS of any message requesting urgent action, particularly when the message appears to be sent by a VIP.
- 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 verify that the message sender address is a CUNY (cuny.edu) address. Be wary of non-CUNY addresses crafted to mislead, such as "dean.cuny.edu@gmail.com".
- 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 change ALL of your passwords if you suspect any account you have access to may be compromised.
- DO complete the 30 minute information security awareness training located at security.cuny.edu.

Annotated scam message examples are found below.

Robert N. Berlinger, CISSP

CHIEF INFORMATION SECURITY OFFICER
 CITY UNIVERSITY OF NEW YORK
 646-664-2511
 security.cuny.edu

Example of a message intended to infect finance staff computers with banking malware if the link is clicked. Message signs off with contact information for a real CUNY staff member:

The screenshot shows an email interface with the following elements:

- Sender:** Account Manager <Arquitectura@proyectosyestructuras.net> (Annotated as "Non-CUNY Address").
- Subject:** Aw: New Invoice / XW948642465 / SM# 60494
- To:** SFA, [redacted]
- Attachment:** digital_sign.txt (2 KB)
- Body:** Attached is the invoice copy you need.
- Link:** [http://\[redacted\]wp-content/dngj-25t_k-kS/](http://[redacted]wp-content/dngj-25t_k-kS/) (Annotated as "Unadorned and unfamiliar link").
- Signature:** Best regards, [redacted] @brooklyn.cuny.edu (Annotated as "Real CUNY staff member lends faux legitimacy").
- Footer:** -----Original Appointment-----
- Header (quoted):**
 - > *From:* "" <SFA [redacted]@cuny.edu>
 - > *Sent:* Monday, March 25, 2019 16:10
 - > *To:* [redacted]@brooklyn.cuny.edu>
 - > *Subject:* Re: [redacted] ACH Payment info

Example of direct deposit manipulation attempt of a CUNY college president.

Name of CUNY college president

From: [redacted] [mailto:ldpp134@aol.com]
Sent: Monday, March 25, 2019 8:47 AM
To: [redacted]
Subject: MAR 03/2019 Pay DD!

Good Day,
I want to change the deposit account for my pay . Do you need me to provide you my Details ?

Regards,
[redacted]

Example of a “secret shopper” fake job offer:

Hello,
This Job is currently recruiting. A Job that will not affect your present employment or studies, fun and rewarding. You get to make up to \$300 weekly, I tried it and i made cool cash. If You are interested you can visit their website at www.timecodeoutsourcing.com to apply and read more about the job.
Best Regards,

Job Placement & Student Services
City University of New York
University Offices
205 East 42nd Street
New York, NY 10017

From: [redacted]
Sent: Friday, October 26, 2018 7:25 AM
Subject: Part time Job

You have been selected as a Secret Shopper in your area A job that will not affect your present employment & no sign up fee. It's fun, rewarding and flexible. You can make up to \$1000 weekly also. To view details of the job and apply please visit our website [https://tinyurl.com/\[redacted\]](https://tinyurl.com/[redacted])

Regards

No such office exists

Lucrative potential earnings offer (fake) helps lure victims