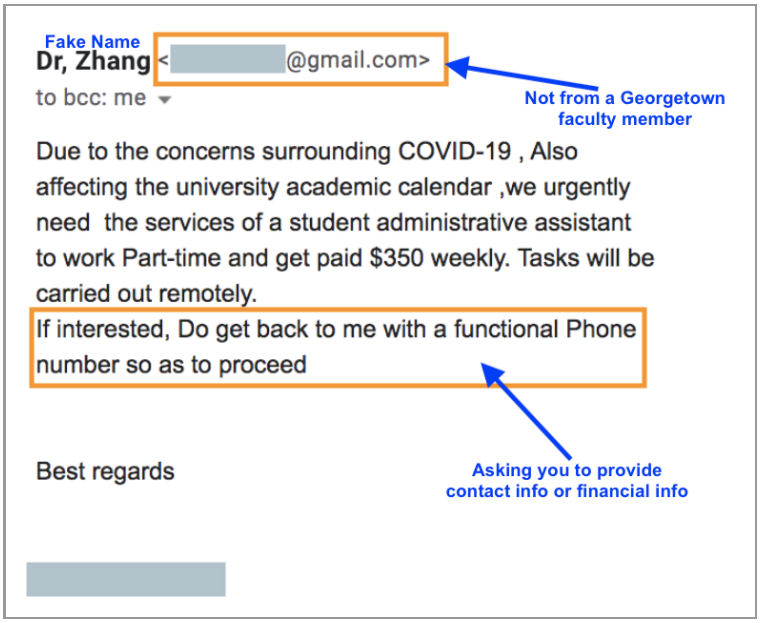
To: All Georgetown Students
From: Office of the CIO
Date: Tue, Sep 22, 2020 at 2:09 PM
Subject: **Phishing Scams Targeted at Georgetown Students**

Dear Georgetown Student,

Please be advised there are multiple fraudulent emails currently circulating which target Georgetown University students with job opportunities. **These messages are phishing attempts, and we ask that you do not respond to or interact with these emails.**



Please be aware:

- This email is **not** from a Georgetown faculty member.
- This email is not a legitimate job opportunity, as official university student employment opportunities are not advertised in this manner. To verify legitimate student employment opportunities, please visit the Georgetown University Student Employment Office website where positions are posted.
- The scammer will try to induce you into spending **thousands of dollars** on equipment claiming that Georgetown will reimburse you.
- Your banking, Paypal, Venmo or other financial account information should never be shared with anyone that you do not know.

If you receive this type of email, mark it as spam in Gmail and then immediately delete it. You can also report suspicious emails by forwarding them to CIRT@georgetown.edu. You can check current phishing scams at UIS's phishing examples website.

As we continue working and learning in virtual environments, phishing and other scams are on the rise, so we encourage you to improve your security by reviewing online best practices on the UIS Security website.

Sincerely,

Judd Nicholson
VP for Information Technology and CIO