Suffolk County Community College

College Brief

NO. 43 December 15, 2021

TO: The College Community

FROM: Information Technology Services

SUBJECT: Seasonal and Pandemic-related Malicious Email and Phone Scams

During significant times of stress, such as the COVID-19 pandemic, and during the holiday season and between semesters, bad actors are known to increase their phishing campaigns and scams through both email and phone. Criminals may reach out to administrative staff, impersonating a student, employee or vendor with the objective of stealing sensitive information or diverting college funds. Here are some indicators that the phone call or email you received is most likely a scam or attack:

- Communicates a tremendous sense of urgency, including a deadline where you will lose access to services. The criminals are trying to rush you into making a mistake.
- Pressures you into bypassing or ignoring the college's policies and procedures, including identity verification.
- Poses as a student, employee or vendor, reaching out from an email address or phone number not on file, asking you to:
    - change their account details on record for payroll, payments or other disbursements
    - provide other confidential information, including college credentials
- Watch out for an email, with an attachment or URL, that states it is providing COVID-19 test results, or critical information about a COVID-19 variant asking you to perform any task.
- Be wary of any phone call or message that pretends to be a representative of a government organization or health agency, or purporting to be a member of college leadership, urging you to take immediate action.

Additional steps you can take to remain safe online:

- Check the sender's email address to verify it is valid.
- Voice Verify: Pick up the phone and call vendors, students and employees with contact information on file to ensure the request is legitimate.
- Follow all process and procedures.
- Do not feel you must comply with urgency due to someone's title or standing at the college or within government, a health agency, or law enforcement, if the request seems suspicious in nature.

You must fully verify the identity of all requesters to avoid malicious activity that could be extremely harmful to the college community.

If you believe you may have fallen victim to a scam that matches the examples listed above, please change your password immediately and then report the incident immediately by forwarding the suspicious email to it-help@sunysuffolk.edu.

Thank you for supporting a cybersafe environment at the college.