Holiday Season Online Scams

CUNY CIS Information Security reminds the CUNY community to be alert to scams and other malicious activity during the holiday season. Common scams include:

- Unexpected requests from colleagues, superiors or executives to purchase gift or stored value cards on their behalf or soliciting personal information
- Advertisements, coupons and promotions that offer “too good to be true” deals on merchandise
- Unsolicited job offers (e.g., “secret shopper” or “personal assistant”) that are frequently financial scams
- Fake shopping websites posing as legitimate sites to capture personal and financial information
- Social networking posts requesting support for phony charitable causes

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

- Review online shopping safety tips by SANS OUCH!, and the Department of Homeland Security
- Approach all unsolicited offers and communications with skepticism and caution
- Always verify the authenticity of the sender. Be particularly cautious with messages that are marked as having been received from an external source
- Additional caution is necessary when responding to email from a mobile device where the sender’s full email address may not be displayed for verification
- Turn on “multi-factor” or “enhanced” authentication features that use a companion mobile app or text unique verification codes to your mobile device to verify sign-ins.
- Do not follow unsolicited links or download attachments from unknown sources
- Always compare a link in an email to the link you are directed to and determine if it matches and will lead you to a legitimate site
- Refer to advisories posted at security.cuny.edu under “CUNY Issued Security Advisories”

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

Wishing everyone a safe, healthy and enjoyable holiday season.

Updated: November 2021