Holiday Season Phishing Scams
and Malware Campaigns

CUNY/CIS Information Security advises the CUNY community to remain vigilant when browsing online during the holiday season. Please be aware of some prevailing scams:

- Copycat and fake websites—a fake website poses as a legitimate one to capture personal and financial information
- E-cards and unexpected “gifts” from unknown senders may contain malicious links
- Fake advertisements, coupons or shipping notifications may deliver infected attachments or contain malicious links
- Phishing email messages and fraudulent posts on social networking sites may request support for phony causes or offer “too good to be true” deals on merchandise

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

- Approach all unsolicited offers and communications with skepticism and caution
- Do not follow unsolicited links or download attachments from unknown sources
- Always compare a link in an email to the link you are actually 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”
- Visit the Federal Trade Commission’s Consumer Information page on Charity Scams for more information on this subject

If you believe you are a victim of an online scam or malware campaign, please report it to your campus helpdesk and consider the following actions:

- Contact your financial institution immediately to advise of any account information that may have been compromised. Watch for any unexplainable charges to your account
- Immediately change any passwords that you might have revealed. If you used the same password for multiple resources make sure to change it for each account, and do not use that password in the future

Wishing all a safe and enjoyable holiday season.

Published: November 2014