

COUNTY OF SUFFOLK



KATE BROWNING

County Legislator, 3rd District
Public Safety Committee, Chair

Media Release

November 25, 2014

COUNTY LEGISLATURE

1120 Montauk Hwy., Suite G
Mastic, NY 11950
Fax: (631) 852-1303

Contact: Joshua Slaughter

631-852-1300

631-456-1718

Beware: Holiday Phishing Scams and Malware Campaigns On the Rise

Mastic, NY – Legislator Kate Browning (WF-Shirley) has received information from the New York Electronic Crimes Task Force and the United States Computer Emergency Response Teams (US-CERT) US-CERT informing residents to remain vigilant when browsing online this holiday season. E-cards from unknown senders may contain malicious links, fake advertisements or shipping notifications may deliver infected attachments, and spoofed e-mail messages and fraudulent posts on social networking sites may request support for phony causes.

To avoid seasonal campaigns that could result in security breaches, identity theft, or financial loss, US-CERT encourages users to take the following action:

- Approach similar content with caution. Do not follow unsolicited links or download attachments from unknown sources.
- Refer to US-CERT's security tips to learn more about [Shopping Safely Online](#), [Avoiding Social Engineering and Phishing Attacks](#), and [Protecting Personal Internet-Enabled Devices](#).
- For information on charity scams, visit the [Federal Trade Commission website](#).

“While the holiday season is a time for everyone to be grateful for family and friends, and to give to those that are in need, some individuals are using the holidays as a guise to prey on victims and take advantage of vulnerable populations,” stated Legislator Browning. “Please be aware of the internet sites you are visiting, e-mails you receive, and make sure you do not click on anything that is unknown to you.”

If you believe you are a victim of a Holiday Phishing scam or Malware campaign, consider the following actions:

- File a complaint with the [FBI's Internet Crime Complaint Center \(IC3\)](#).
- Report the attack to the police, and file a report with the [Federal Trade Commission](#).
- Contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords 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.

###