TLP:WHITE

NCCIC

Holiday Scams and Malware Campaigns

Original release date: November 19, 2018

As the holidays approach, NCCIC reminds users to be aware of seasonal scams and malware campaigns. Users should be cautious of unsolicited emails that contain malicious links or attachments with malware, advertisements infected with malware, and requests for donations from fraudulent charitable organizations, which could result in security breaches, identify theft, or financial loss.

NCCIC recommends the following actions:

- Use caution when browsing the internet, shopping online, and using email.
- Avoid clicking on links or opening attachments in unsolicited emails. See Avoiding Social Engineering and Phishing Attacks for more information.
- Be wary of fraudulent social media pleas, calls, texts, websites, and door-to-door solicitations for donations to charities. See How to Donate Wisely and Avoid Charity Scams for more information.

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

- Contact your financial institution immediately, and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. See Preventing and Responding to Identity Theft for more information.
- Immediately change any passwords you might have revealed. Avoid reusing passwords. See Choosing and Protecting Passwords for more information.
- Report the attack to the police, and file reports with the Federal Trade Commission and the FBI's Internet Crime Complaint Center.

TLP:WHITE