Holiday Scams and Malware Campaigns

Original release date: November 16, 2017

US-CERT reminds users to remain vigilant when browsing or shopping online this holiday season. Emails and ecards from unknown senders may contain malicious links. Fake advertisements or shipping notifications may deliver attachments infected with malware. Spoofed email messages and phony posts on social networking sites may request support for fraudulent causes.

To avoid seasonal campaigns that could result in security breaches, identity theft, or financial loss, users are encouraged to take the following actions:

- Avoid following unsolicited links or downloading attachments from unknown sources.
- Refer to our Tips to learn more about Shopping Safely Online and Avoiding Social Engineering and Phishing Attacks.
- Read the Federal Trade Commission's blog: Holiday Shopping Tips from the FTC.
- Visit the Federal Trade Commission's Consumer Information page on Charity Scams.

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 and do not use that password in the future. Avoid reusing passwords on multiple sites. See Choosing and Protecting Passwords for more information.