



**Homeland  
Security**

**US-CERT** | United States  
Computer Emergency  
Readiness Team

## Potential Hurricane Harvey Phishing Scams

NJCCIC Members,

In the furtherance of public-private partnerships, the [DHS/US-CERT Advisory](#) is being provided in order to assist NJCCIC members in guarding against the persistent malicious actions of cyber criminals.

US-CERT warns users to remain vigilant for malicious cyber activity seeking to capitalize on interest in Hurricane Harvey. Users are advised to exercise caution in handling any email with subject line, attachments, or hyperlinks related to Hurricane Harvey, even if it appears to originate from a trusted source. Fraudulent emails will often contain links or attachments that direct users to phishing or malware-infected websites. Emails requesting donations from duplicitous charitable organizations commonly appear after major natural disasters.

US-CERT encourages users and administrators to use caution when encountering these types of email messages and take the following preventative measures to protect themselves from phishing scams and malware campaigns:

- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the US-CERT Tip [Using Caution with Email Attachments](#) for more information on safely handling email attachments.
- Keep antivirus and other computer software up-to-date.

Refer to the [Avoiding Social Engineering and Phishing Attacks](#) for more information on social engineering attacks.

- Review the Federal Trade Commission information on [Charity Scams](#).
- Verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number. You can find trusted contact information for many charities on the BBB [National Charity Report Index](#).

**Connect with us!**

