

US-CERT Current Activity

Mississippi Flooding Disaster Email Scams, Fake Antivirus, and Phishing Attack Warning

Original release date: May 16, 2011 at 10:15 am Last revised: May 16, 2011 at 10:15 am

Users should be aware of potential email scams, fake antivirus, and phishing attacks regarding the Mississippi flooding disaster. Email scams may contain links or attachments that may direct users to phishing or malicious websites. Fake antivirus attacks may come in the form of pop-ups that flash security warnings and ask the user for credit card information. Phishing emails and websites requesting donations for bogus charitable organizations commonly appear after these types of natural disasters.

US-CERT encourages users to take the following measures to protect

themselves:

- * Do not follow or open unsolicited web links or attachments in email messages. Maintain up-to-date antivirus software.
- * Review the Recognizing Fake Antivirus document for additional information on recognizing fake antivirus.
- * Refer to the Avoiding Social Engineering and Phishing Attacks document for additional information on social engineering attacks.
- * Refer to the Recognizing and Avoiding Email Scams (pdf) document for additional information on avoiding email scams.
- * Review the Federal Trade Commission's Charity Checklist.
- * Verify the legitimacy of the email by contacting the organization directly through a trusted contact number. Trusted contact information can be found on the Better Business Bureau National Charity Report Index.