Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

April 25, 2013

BEWARE OF POSSIBLE FRAUD ASSOCIATED WITH THE BOSTON MARATHON EXPLOSIONS

The FBI reminds the public there is the potential for fraud in the aftermath of the Boston Marathon bombings. The FBI's Internet Crime Complaint Center has received indications that individuals may be using e-mail and social networking sites to facilitate fraudulent activities.

The FBI is aware of a spam e-mail with the subject line "Boston Marathon Explosion" and similarly themed messages being circulated to lure potential victims to malicious software and exploits. Spam e-mails and Web sites to which they are linked use a wide variety of deceptions to trick a user into taking actions that put the user's computer at risk for infection. Common techniques include links to compromised Web sites and pop-up messages prompting users to download software to view pictures, videos or other files.

Social media is another avenue criminals use to solicit donations. The FBI is aware that an account on a popular social media service using the Boston Marathon name and official logo was created soon after the explosions. Communications from the account represented that $1 would be donated to the Boston Marathon victims for every communication other users sent to the account. Though the account was suspended by the social media service, others may use similar methods to commit fraud.

The FBI is also aware of numerous questionable domains registered within hours of the Boston Marathon explosions. Though the intentions of the registrants are unknown, domains have emerged following other disasters for fraudulent purposes.

Individuals should always exercise reasonable caution and vigilance when using e-mail and social networking Web sites. Based on experiences from previous times of tragedy, it is reasonable to believe that criminals will continue to exploit such events to solicit fraudulent donations, to obtain victims' personally identifiable information (PII), and to further other illegal activities.

Individuals can limit exposure to cyber criminals by taking the following preventative actions when using email and social networking Web sites:

- Do not agree to download software to view content. Messages may contain pictures, videos, and other attachments designed to infect your computer with malware.
- Do not follow a link you receive via e-mail to go to a website. Links appearing as legitimate sites (example: fbi.gov), could be hyperlinked to direct victims to another website when clicked. These sites may be designed to infect your computer with malware or solicit personal information.
- Verify the existence and legitimacy of organizations by conducting research and visiting official websites. Be skeptical of charity names similar to but not exactly the same as reputable charities.
- Do not allow others to make donations on your behalf. Donation-themed messages may also contain links to websites designed to solicit personal information, which can be routed to a cyber criminal.

	• Make donations securely by using a debit/credit card or write a check made out to the specific charity. Be wary of making donations via money transfer services; legitimate charities do not normally solicit donations using this method of payment. --- If you believe you have been the victim of fraud by someone soliciting funds on behalf of disaster victims or want to report suspicious e-mail solicitations or fraudulent Web sites, please file a complaint with the FBI's Internet Crime Complaint Center, https://www.ic3.gov/