Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 24, 2014

CYBER CRIMINALS USING FAKE GOVERNMENT E-MAIL TO PERPETRATE SCAM

Cyber criminals posing as Internet Crime Complaint Center (IC3) employees are defrauding the public. The IC3 has received complaints from victims who were receiving e-mails purported to be from the IC3. This advisory informs readers how the scheme works, offers measures to help mitigate the threat, and advises how to report incidents to law enforcement.

Victims report that the unsolicited e-mail sender is a representative of the IC3. The e-mails state that a criminal report was filed on the victim's name and social security number and legal papers are pending. Scammers impersonate an IC3 employee to increase credibility and use threats of legal action to create a sense of urgency. Victims are informed they have one to two days from the date of the complaint to contact the scammers. Failure to respond to the e-mail will result in an arrest warrant issued to the victim.

Some victims stated they were provided further details regarding the 'criminal charges' to include violations of federal banking regulations, collateral check fraud, and theft deception. Other victims claimed that their address was correct but their social security number was incorrect. Victims that requested additional information from the scammer were instructed to obtain prepaid money cards to avoid legal action. Victims have reported this scam in multiple states.

If you receive this type of e-mail:

- Resist the pressure to act quickly.
- Never wire money based on a telephone request or in an e-mail, especially to an overseas location.

The IC3 **never** charges the public for filing a complaint and will **never** threaten to have them arrested if they do not respond to an e-mail. Individuals who have fallen victim to this type of scam are encouraged to file a complaint with the IC3 at http://www.ic3.gov.