



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



October 16, 2008

FRAUDULENT SPAM E-MAIL PURPORTED FROM FBI DEPUTY DIRECTOR JOHN S. PISTOLE

A spam e-mail claiming to be from FBI Deputy Director John S. Pistole is currently being circulated. This attempt to defraud is the typical e-mail scam using the name and reputation of an FBI official to create an air of authenticity.

As with many scams, the e-mail advises the recipient that they are the beneficiary of a large sum of money which they will be permitted to access once fees are paid and personal banking information is provided. The appearance of the e-mail leads the reader to believe that it is from FBI Deputy Director John S. Pistole.

THIS E-MAIL IS A HOAX. DO NOT RESPOND.

The IC3 continues to receive and develop intelligence regarding fraud schemes misrepresenting the FBI and/or FBI officials. The scam e-mails give the appearance of legitimacy through the use of pictures of FBI officials, seal, letter head, and/or banners.

These fraud schemes claim to be from domestic as well as international FBI offices. The typical types of schemes utilizing the names of FBI officials and/or the FBI are lottery endorsements and inheritance notifications but can cover a range of scams from threats and malicious computer program attachments (malware) to online auction scams.

These scams use the social engineering technique of employing the FBI's name to intimidate and convince the recipient the e-mail is legitimate.

Please be cautious of any unsolicited e-mail referencing the FBI, Director Mueller, Deputy Director Pistole or any other FBI official claiming that the FBI is endorsing any type of Internet activity.

Always be cautious when responding to requests or special offers delivered through unsolicited e-mail:

- Guard your personal information as well as your account information carefully.
- You should never give any personal, credit, or banking information in response to unsolicited e-mails.

Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware. Providing your PII will compromise your identity!

If you have received this e-mail, or a similar e-mail, please file a complaint at www.IC3.gov.