U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

FBI NATIONAL PRESS OFFICE
(202) 324-3691
www.fbi.gov

FOR IMMEDIATE RELEASE
JULY 17, 2007

FBI WARNS PUBLIC OF E-MAIL SCAMS

Washington, D.C. — The FBI today warned the public against three separate Internet scams that continue to flourish through spam e-mails. The warning comes after the FBI's Internet Crime Complaint Center (IC3) received a rising number of complaints from citizens over the past few weeks.

In one scam, an e-mail recipient receives an electronic greeting card containing malware (malicious software). The cards, which are also referred to as e-cards or postcards, are being sent via spam. Like many other Internet fraud schemes, the perpetrators use social engineering tactics to entice the victim, claiming the card is from a family member or friend. Although there have been variations in the spam message and attached malware, generally the spam directs the recipient to click the link provided in the email to view their e-card. Upon clicking the link, the recipient is unknowingly taken to a malicious web page.

In another scam, fraudulent e-mails misrepresent the FBI and/or Director Robert S. Mueller III and give the appearance of legitimacy due to the usage of pictures of the FBI Director, seal, letter head, and/or banners. The types of schemes utilizing the Director's name and/or FBI are lottery endorsements and inheritance notifications.

The third is spam e-mail which claim to be from an official of the U.S. military sent on behalf of American soldiers stationed overseas. The scam e-mails vary in content; however, the general theme of each is to request personal information and/or funds from the individual receiving the e-mail.

These spam e-mail messages are hoaxes and should be immediately deleted. Consumers need to be wary of unsolicited e-mails that request them to take any action even if that means just clicking on an attachment. It is possible that by "double-clicking" on attachments to these messages, recipients will cause malicious software – e.g., viruses, keystroke loggers, or other Trojan horse programs – to be launched on their computers.

For further information on computer safety tips please visit the FBI website at www.fbi.gov and the IC3 website at www.ic3.gov.