Contact Information:
Cyber Criminal Intelligence Program
9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)
Fax: 703.805.2351 (DSN 655)
E-mail:
cybercrimintel.cciu@us.army.mil

CCIU Web Page:
www.cid.army.mil/cciu.html

CID Cyber Lookout
On Point for the Army

"DO WHAT HAS TO BE DONE"

2CAN 0021-09-CID221-9H **30 March 2009**

STIMULUS PROGRAM MAY LEAVE YOU LESS THAN STIMULATED

OVERVIEW:

Well they're at it again. Given the current economic downturn, cybercriminals are at it once again in an attempt to keep up with the current events. This time around you're likely to receive an e-mail, or see an online ad, or Web site claiming that you are eligible for an economic stimulus payment. All you have to do is complete the form and send it back or submit one online. This message may appear to have originated from a rebate company or have been sent directly by the Internal Revenue Service (IRS).

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

THE PHISHING THREAT:

There's more than one way to perpetuate a stimulus scam. Some scam artists might ask you to send a small processing fee, in order to get a bigger check in return. That's money you'll never see again. Others skip the fee, and instead, ask for your bank account number so they can "deposit" your check. Then, they use the information to clean out your account or open new ones using your personally identifiable information (PII). Some scams encourage you to click on links, open attached forms, or call phony toll-free numbers. But in doing so you could be installing harmful software, like spyware, on your computer, which allows identity thieves to steal your PII.

The so-called "phishing" e-mail, may also display photographs of President Barack Obama and Vice President Joe Biden and claim to offer people their portion of the recently approved stimulus bill. Recipients are instructed to click on an e-mail link and enter their personal financial information into a counterfeit Web site. The Better Business Bureau warns that the federal government does not award grants to help consumers pay general debt, and people who sought free advice from scam Web sites were ultimately charged as much as $69.95 every month on their credit or debit card.

The Internal Revenue Service Web site states:

"The IRS does not initiate taxpayer communications through e-mail. In addition, the IRS does not request detailed personal information through e-mail or ask taxpayers for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts."

Do not open any attachments to questionable e-mails, which may contain malicious code that will infect your computer. Please be advised that the IRS does not initiate contact with taxpayers via e-mails."

Cyber Crime Alert Notice

The United States Computer Emergency Readiness Team (US-CERT) offers the following general guidance to avoid falling victim to phishing schemes:

- Do not follow unsolicited Web links received in e-mails.
- Contact your financial institution immediately if you believe your account and/or financial information has been compromised.
- Verify the legitimacy of the e-mail by contacting the company directly through a trusted contact number.
- Visit the Anti-Phishing Working Group for more information on known phishing attacks.

For more information about key logging or phishing, we encourage Army Knowledge Online users to visit the On Cyber Patrol Web site at https://www.us.army.mil/suite/page/190357 and review previous 2CANs and other relevant information products.

PROTECTING YOUR HOME COMPUTER:

The Army Computer Emergency Response Team offers free antivirus software for Department of the Army personnel to use on home computers. You must access the following link from a .mil computer system and authenticate with your CAC and PIN:

https://www.acert.1stiocmd.army.mil/Antivirus

ADDITIONAL INFORMATION:

Federal Trade Commission
http://www.ftc.gov/opa/2009/03/stimulusscam.shtm

Better Business Bureau's Phishing Phacts:
http://www.bbbonline.org/idtheft/phishing.asp

Better Business Bureau's Stimulus Scam Warning:
http://www.bbb.org/us/article/9363

The Wall Street Journal
http://online.wsj.com/article/SB123803264428843907.html

ICE ***CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.***

CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.