Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cyber Crime Alert Notice

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.htm

"DO WHAT HAS TO BE DONE"

2CAN 0028-08-CID221-9H **24 April 2008**

IRS REBATE CHECK COULD LEAVE YOU BROKE

OVERVIEW:

Once again, unscrupulous cyber criminals have shown that they will use practically any means available to further their illicit schemes: Computer security experts are warning users to beware of phishing Web sites and spam e-mails targeting unsuspecting taxpayers as they anxiously await their economic stimulus rebate checks.

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

THE PHISHING THREAT:

The scam starts out like this: "Our records indicate that you are qualified to receive the 2008 Economic Stimulus Refund. The fastest and easiest way to receive your refund is by direct deposit to your checking/savings account. Please click on the link and fill out the form and submit before April 24th, 2008 to ensure that your refund will be processed as soon as possible."

Anyone clicking on the link is taken to a purported Internal Revenue Service (IRS) Web site, where individuals are asked for their bank routing number and checking account number. These phony Web sites usually have IRS logos and graphics and appear authentic to the untrained eye. In reality, cyber criminals use the sites to harvest bank account information and soon pillage funds from these accounts.

Another twist on these recent phishing e-mails involves a request for recipients to call a phone number and provide debit card information to facilitate the economic stimulus refund. This approach is known as "vishing" and was covered in 2CAN 0006-07 from January 2007.

IRS WARNING:

The IRS 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."

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.

Additional Reporting and Information:

MX Logic Security Blog:
http://www.mxlogic.com/itsecurityblog/entry.cfm?entry_id=77A9817C-802A-1088-12EAB4F9726C12F6

SANS Institute News Letter:
http://www.sans.org/newsletters/ouch/issue/20080206.php

Government Computer News:
http://www.gcn.com/online/vol1_no1/46153-1.html

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

Internal Revenue Service Tips for Avoiding Tax Scams:
http://www.irs.gov/newsroom/article/0,,id=180075,00.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.