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

DISTRIBUTION:
This document is authorized for wide release with no restrictions.

"DO WHAT HAS TO BE DONE"

2CAN 0010-09-CID221-9H **30 January 2009**

USAJOBS.GOV DATA COMPROMISED

OVERVIEW:

The U.S. Office of Personnel Management warned in a recent security alert that cyber criminals recently gained illegal access to USAJOBS.gov, the U.S. Government's official job listing web site. The hackers stole user IDs, passwords, email addresses, names, phone numbers, and some basic demographic data from the resume database run by Monster.com, the technology provider for USAJOBS.gov. The information accessed does not include resumes, social security numbers, or personal financial data.

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

ONLINE JOB SEEKERS BEWARE:

Current and former job seekers could find themselves targeted by so-called "phishing" e-mails, possibly disguised as Monster.com or USAJOBS.gov messages. Officials at Monster.com reported that immediately upon learning about the incident, they initiated an investigation and took corrective steps. Monster.com advises that it continually monitors for any illicit use of information in its database, and so far, they have not detected the misuse of this information.

Ms. Mary Volz-Peacock, Program Director, USAJOBS®, cautioned that "an email address could be used to target 'phishing' emails. USAJOBS® will never send an unsolicited email asking you to confirm your username and password, nor will Monster ask you to download any software, 'tool' or 'access agreement' in order to use your USAJOBS® account."

If you have received an e-mail that claims to be from Monster.com and clicked on an embedded link in the e-mail, Monster.com advises running an anti-virus application to remove anything that may have been maliciously installed in your computer. Users are encouraged to contact a Monster.com representative to have your Monster account password changed. Should you receive an e-mail purportedly from Monster.com instructing you to download a tool or update your account or access agreement, please contact Monster.com to verify its legitimacy.

For more information about key logging or phishing, we encourage you to visit the Army Knowledge Online website at https://www.us.army.mil/suite/authenticate.do to review previous 2CANs.

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. The ACERT website can be accessed from .mil networks or from home, and requires AKO authentication (username/password or CAC/PIN).

Army Computer Emergency Response Team
https://www.acert.1stiocmd.army.mil/Antivirus/

ADDITIONAL REPORTING AND INFORMATION MAY BE FOUND AT:

USAJOBS.com
http://www.usajobs.opm.gov/securityNotice.asp

Monster.com
http://help.monster.com/besafe/jobseeker/index.asp

Nextgov.com
http://www.nextgov.com/nextgov/ng_20090127_1299.php?zone=ngtoday

SANS.org
http://isc.sans.org/diary.html?storyid=5737

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.