United States Army

Criminal Investigation Command

Media contact: CID Public Affairs
703-806-0372
Christopher.Grey@us.army.mil

FOR IMMEDIATE RELEASE

CID Cyber Lookout
On Point for the Army

CID Warns Against Personal Computer Threat

‘Keylogging’ methods can steal Thrift Savings Plan account funds

FORT BELVOIR, Virginia, February 7, 2007 -- Soldiers, family members and Army civilians using their home computers to access Thrift Savings Plan (TSP) accounts online can be vulnerable to having their personal information stolen, according to a recent alert posted on TSP’s Web site.

According to the alert, TSP officials have identified customers who are victims of a computer crime known as “keylogging” or “keystroke logging.” Keylogging is a diagnostic tool used in software development that captures a user’s keystrokes, but in the wrong hands, it enables criminals to record all the typing on a keyboard without the user’s knowledge. The technique can capture a computer user’s TSP Personal Identification Number (PIN) or other personal account information such as a Social Security Number.

The Director of the U.S. Army Criminal Investigation Command’s Computer Crime Investigative Unit, Michael Milner, said personal information is increasingly available on ‘keylogger’ lists for sale through criminal networks and so far, all of the TSP cases involve the transfer of electronic funds, since criminals normally prefer the ‘paperless’ way to steal money.

“Computer users should protect themselves from keyloggers and other malicious software and should promptly close the Web browser after they have checked their TSP account information,” Milner explained. “Users must remember that logging off a Web site does not clear a browser’s

- more -

memory, and subsequent users might be able to access the TSP account information."

Milner said he is unaware of any Army victims at this point, but strongly recommends computer users review their home system's security effectiveness to reduce exposure to these types of attacks.

According to the TSP's notice, external penetration testing determined the TSP record keeping system was not breached, but concluded personal information was compromised when keyloggers monitored each individual keystroke of some victims when they used home computers to enter their TSP PIN and Social Security Number. TSP was also able to identify participants who had relatively small amounts withdrawn from their accounts. As an added security measure, TSP has discontinued making electronic payments for on-line transactions, according to TSP officials.

Milner also explained that the best advice for computer users is to follow general computer security principles at home and to download antivirus software. Army personnel can download free antivirus software for their home computers by visiting the Joint Task Force–Global Network Operations (JTF-GNO) Web site at: https://www.jtfgno.mil/antivirus/home_use.htm. They must access the JTF-GNO Web site from a ".mil," or military computer system and authenticate with their government Common Access Card (CAC) and PIN. After downloading the software, they can then install it on their home computers.

The U.S. Army Criminal Investigation Command, commonly known as CID, will continually release notices such as TSP alert through their *"CID Cyber Lookout"* program, an initiative aimed at helping Soldiers protect themselves and their families from becoming victims of cyber crime.

To view the TSP Alert, visit www.tsp.gov/account/login_security-news-ab.html.

To learn more about CID's Computer Crime Investigative Unit, visit www.cid.army.mil/cciu.htm.

-30-

Editor's note: To download high resolution versions of the CID Lookout logo visit www.cid.army.mil/lookout_logos.html

CID Lookout is a U.S. Army Criminal Investigation Command (USACIDC) initiative to partner with the Army community by providing a conduit for members of the Army family, to help prevent, reduce and report felony-level crime.

The USACIDC, commonly known as CID, is an independent criminal investigative organization that investigates serious, felony-level crime such as murder, rape, sexual assault, robbery, arson, fraud, and even cyber crime or intrusions into the Army networks (see CID Cyber Lookout).

Solving and preventing these types of crime cannot be achieved solely by CID Special Agents and the Military Police. Together, professional law enforcement officers and the Army community must work hand-in-hand to fight serious crime. As such, CID is *On Point for the Army* and depends heavily on Soldiers, family members and civilian employees to *Be On The Lookout* and provide assistance in keeping the *Army Strong* and safe.

CID Lookout provides the latest information to the Army community aimed at helping Soldiers protect themselves, their families and to reduce their chances of becoming crime victims.

For more information on CID or to report a felony-level crime or provide information concerning a crime, contact your local CID Office or the Military Police, or visit www.cid.army.mil.