Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571-305-4485 (DSN 240)
Fax: 571-305-4189 (DSN 240)
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 0013-13-CID361-9H 13 March 2013

The Not So Thrifty Apps

Overview:

The purpose of this Cyber Crime Alert Notice (2CAN) is to inform Department of the Army personnel of third party mobile applications that reference the Thrift Savings Plan (TSP) retirement savings and investment plan for federal employees and members of the uniformed services, but are not sponsored by the Federal Retirement Thrift Investment Board. Using non-sanctioned applications to access TSP accounts can potentially lead to the compromise of TSP account information and theft of funds. CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

Background:

An application called **TSP Funds** was initially released on 19 Feb 13 as a free application on Apple's iTunes App Store. The application provides general information about TSP funds and performance history. It also has a feature that allows users to enter their TSP login information to access individual account balances and other information. A broader review of mobile application sites disclosed several other TSP-related apps for Android and iPhone devices.

These apps are not sponsored or endorsed by the Federal Retirement Thrift Investment Board, which administers the TSP.

On 1 Mar 13, TSP issued a statement on the TSP.gov website cautioning participants not to use third party apps to access TSP accounts. Providing login information, TSP warned, could "result in a security risk to your account." TSP further cautions that it is not responsible for losses from individual accounts due to unsafe security practices by participants, including accessing TSP accounts from a compromised computer.

TSP participants who believe their account information may have been compromised should contact the TSP (see reverse).

Cyber Crime Alert Notice

General Tips About Mobile Apps:

- Before downloading, installing, or using an application, take a moment to review the "About the Developer" section. This will help you get an idea about other apps that specific developer has previously published. If available, visit the developer's website and assess its content for things like history, professional appearance, etc..
- Peruse the user ratings and try to get a sense from previous customers as to the veracity of the application's claim. Arguably no app is completely perfect from the perspective of all users, but complaints about security concerns should quickly stand out from other relatively benign issues.
- If you're still not sure and end up downloading an application, inspect your device's application permissions screen to determine what other applications or information will be accessed by the app. A video game, for example, is unlikely to have a legitimate need to access your contacts.

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review previous cyber crime alert notices and cyber crime prevention flyers.

Additional Information:

Thrift Savings Plan (TSP.gov)

- TSP Security Center: Online Security
- Contact TSP: Telephone 1-TSP-YOU-FRST (1-877-968-3778), international 404-233-4400

U.S. Computer Emergency Response Team

- Avoiding Social Engineering and Phishing Attacks
- Preventing and Responding to Identity Theft
- Protecting Portable Devices: Data Security
- Safeguarding Your Data