Cyber Crime Alert Notice

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.htm

CID Cyber Lookout
On Point for the Army

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

"Do What Has To Be Done"

2CAN 0029-13-CID361-9H **7 October 2013**

"MyPay" or No Pay 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 Defense Finance and Accounting Services (DFAS) myPay system for federal employees and members of the uniformed services, but are not sponsored by the Department of Defense or U.S. Government. DFAS processes pay for all DoD military and civilian personnel, retirees and annuitants, and also supports other government agencies. Using non-sanctioned applications to access your myPay account can potentially lead to the compromise of your myPay 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 "MyPay DFAS LES" was initially released on 13 Jul 13, as a free application on Google Play Android App Store. The App provides the user with the ability to control their military pay after the user enters their myPay login information to access their individual account. Additionally, it provides the ability for the user to update their security questions to reset their password. Google Play estimates that between 10,000-50,000 members have already installed this App. A broader review of mobile App sites disclosed several other myPay related Apps for Android and iPhone devices.

This App is not sponsored or endorsed by the Department of Defense or DFAS.

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…
- Apps that purport to allow access to military or government sites should only be installed if they are official Apps sponsored by the military or other government agency.
- Peruse the user ratings and reviews to 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 App, 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:

Defense Finance and Accounting Service (DFAS.mil)

- **DFAS: myPay Secure**
- **Contact DFAS: Telephone 888.332.7411**

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**

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this 2CAN.

CCIU uses 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.