

Attention Disbursing Officers and Supply Officers

NAVY CASH[®] FLASH!
Naval Supply Systems Command

Naval Supply Systems Command
Navy Family Support Mechanicsburg
Code 56
5450 Carlisle Pike
P.O. Box 2050
Mechanicsburg, PA 17055-0791

Navy Cash[®] Flash 09-007

21 May 2009

Subject: NAVY CASH SECURITY PROTECTIONS

The Navy and the Navy Cash Program Office enforce multiple security protections within the Navy Cash system, but security breaches can and do happen. In view of a recent unclassified network security violation on board a U.S. Navy ship, this Navy Cash Flash serves to remind Disbursing Officers and Supply Officers about the importance of our Navy Cash security policies, protections, and procedures.

The Internet is a powerful business and operational medium that is critical to DOD's Global Information Grid (GIG) and its role in supporting our warfighting capabilities. Our reliance on the Internet means Navy networks and systems are exposed to a complex and unrelenting threat environment. Over the past several years, DOD and the Navy have focused on a layered defense, or defense-in-depth, to protect our networks, systems and data. While policy and network-based security tools can mitigate much of the risk, each individual server and workstation on the network is an integral part of the defense against these threats.

One of the most prevalent ways in which a server or workstation can be compromised is the installation of unauthorized applications or executable files that contain malicious code, often downloaded off the Internet. Once compromised, a server or workstation on the network may be used for a variety of malicious purposes, e.g., to launch denial-of-service attacks; to gain access to other Navy systems; to alter, steal or disclose Navy information; or to install malicious software.

If any malicious software (virus, worm, Trojan horse, etc.) were to open a ship's network communications ports AND if someone gained access through the created vulnerability, several security levels will prevent serious impact to Navy Cash. First, the Navy Cash server requires both a user ID and password for access. Second, the Navy Cash data base requires an additional user ID and password for data access. Third, Navy Cash files are encrypted, and all data transported between ship and shore is encrypted on a file level. Fourth, data base fields for SSN and home banking information are individually encrypted. Thus, even if ports were maliciously opened and accessed, these security hurdles make malicious access into Navy Cash extremely unlikely.

Navy Cash security policy and procedures require that system operators safeguard Navy Cash related information and the Navy Cash system from unauthorized or inadvertent modification, disclosure, destruction or use. Like any Navy information system, the Navy Cash system is for official use and for authorized purposes only. Each individual operator is responsible for protecting the user ID and password that is required for system logon.

Please route immediately to the Supply Officer and Disbursing Officer

Attention Disbursing Officers and Supply Officers

Subject: NAVY CASH SECURITY PROTECTIONS

Reminder: If you notice any unusual activity on any Navy Cash equipment, please contact the Navy Cash Central Support Unit (CSU) through the Global Distance Support Center at 1-877-41TOUCH (418-6824) or via DSN at 510-42TOUCH (428-6824) or commercially at 1-866-3NAVYCASH (362-8922) or via e-mail at navycashcenter@ezpaymt.com.

POC: Beth Pollock, beth.pollock@navy.mil, (717) 605-6743, DSN 430


MARLENE HIGGINS
Director, Navy Disbursing

Please route immediately to the Supply Officer and Disbursing Officer