CLASSIFICATION: UNCLASSIFIED/
ROUTINE
R 171752Z APR 26 MID320018652807U
FM SECNAV WASHINGTON DC
TO ALNAV
INFO SECNAV WASHINGTON DC
CNO WASHINGTON DC
CMC WASHINGTON DC
BT
UNCLAS

ALNAV 017/26

MSGID/GENADMIN/SECNAV WASHINGTON DC/-/APR//

SUBJ/THREAT AWARENESS AND CYBER HYGIENE RECOMMENDATIONS DURING OPERATION EPIC FURY//

RMKS/1. In response to Operation EPIC FURY, adversary cyber actors are conducting a social engineering campaign actively targeting Department of the Navy (DON) personnel and their families via spear phishing and social media contacts.
These actors seek to psychologically influence DON personnel and their families, and also seek to trick personnel into clicking on/opening potentially malicious links and files.
The Naval Criminal Investigative Service provides the following recommendations to proactively secure electronic devices and personal information, in an effort to reduce the malicious actors' ability to identify and target DON personnel.

a. Remove your online personal identifiable information (PII) that is returned in a Google Search: https://support.google.com/websearch/answer/9673730/ or by utilizing an alternate search engine. Contact legitimate sites, if possible, and request your PII be removed.

b. Set social media privacy settings to the highest level; limit who can view your current and historical social media profiles, contacts, and who can contact you.
Periodically re-check these settings as application updates may void/change your settings or necessitate changes to new services.

c. Pause online posts if able; if unable, be mindful of what you post online. Does the background of your pictures include clues about you, your friends/family, your home, your location, your activities?

d. Request that personal contacts limit information/images they post about you or obtain your approval beforehand.

e. Be wary of and research strangers attempting to contact/friend/connect/link with you.

f. Change account passwords; make passwords complex/use passphrases or passkeys; do not reuse passwords; use different passwords for different sites; and consider using a reputable password manager.

g. Turn on multi-factor authentication for all accounts; consider using an authenticator app (i.e., Google Authenticator, Microsoft Authenticator, Authy, etc.).

h. Adjust device settings to turn off app access to location, cameras, microphones, texts, and other private information if not needed.

i. Regularly update your electronic devices and applications. These updates often fix bugs/vulnerabilities that cyber actors try to exploit.

j. Lock your electronic devices (e.g., passwords, fingerprints, Personal Identification Numbers) and turn off Wi-Fi and Bluetooth when not in use.

k. Research and verify that you are downloading software and applications from legitimate, trusted sources (not pop- ups, unsolicited emails, or knock-off products that may be malicious).

l. Beware of dating or other apps that encourage or require the use/sharing of personal information. Before using such apps, research reviews, company ownership, security practices, and data protection policies.

m. Avoid public Wi-Fi and use reputable virtual private network software when possible.

n. Read pop-ups and warnings carefully; be mindful of what you click.

o. Be on the look-out for spear phishing messages, which may stand out based on their use of urgency, flattery, or vague terms. Do not respond or click on anything in these emails.

2. Any DON personnel receiving suspicious email and/or text messages related to Operation EPIC FURY should NOT respond and should NOT click on any links/open any attachments.
Report suspicious messages to your unit's agency's Information Technology department.

3. Released by the Honorable John C. Phelan, Secretary of the Navy.//

BT
#0001
NNNN
CLASSIFICATION: UNCLASSIFIED/