Naval Criminal Investigative Service

Quantico, Va.

FOR IMMEDIATE RELEASE
JULY 26, 2021
www.ncis.navy.mil

CONTACT: JEFF HOUSTON
PHONE: (571)-302-2307

NCIS Urges Department of the Navy Personnel to Stay Safe on Social Media

Most of us have smartphones and use some form of social media everyday to express ourselves, monitor the news, and connect with friends, family, and coworkers. The ubiquity of social media in our lives, however useful, can leave us vulnerable to criminal threats posed by hackers, scammers, and other nefarious actors.

The novel coronavirus pandemic has notably presented an opportunity for malicious actors to conduct spearphishing campaigns, financial scams, and disinformation campaigns via social media to collect sensitive information, steal money via fake donation websites, spread false information, and deliver malware to victims. Even more disturbing, groups claiming to act on behalf of terrorist organizations have scoured social media and military websites in recent years to collect and publish the names, photographs, ranks, and addresses of military personnel online, encouraging their supporters to kill them.

NCIS urges all Department of the Navy personnel, including both service members and civilians, to remain cognizant of such online criminal threats. Remember that the information you post on social media is *not* private, and that criminals can use this information to target you. To stay safe while using social media, keep the following tips in mind:

- **Limit the amount of personal information you post.** Do not post information that would make you vulnerable, such as your address or information about your schedule or routine.
- **Remember the Internet is a public resource.** Post only information you are comfortable with everyone seeing, and be aware that other people may forward your information to others—including information and photos in your profile and in blogs and other forums.
- **Be wary of strangers.** Consider limiting the number of people who are allowed to contact you through these sites. Only “friend” people you know.
- **Evaluate your settings.** You can customize settings to restrict access to certain people. However, there is still a risk that even this information could be exposed, so don’t post anything that you wouldn’t want the public to see.
- **Use strong passwords.** Protect your account with passwords that cannot be easily guessed. Try to use a combination of at least eight letters, numbers, and symbols. Also, use different passwords for all your online accounts.
- **Use and update security software.** Install and regularly update firewalls and antivirus programs on your personal computing devices.

If you know or suspect you have been targeted with a crime via social media, please report it to NCIS using the NCIS Tips app or at www.ncis.navy.mil.

NCIS is a federal law enforcement agency that investigates felony crime, prevents terrorism, and protects secrets for the U.S. Department of the Navy. NCIS employs approximately 2,000 personnel, including 1,000 federal special agents, in 41 countries and 191 locations around the world. To learn more about NCIS, visit www.ncis.navy.mil and follow NCIS on Facebook, Twitter, and YouTube.

//////////////////////////