Naval District Washington

WEEKLY UPDATE | HPCON C

http://facebook.com/NavDistWash

*Protect our People | Maintain Mission Readiness | Support Whole-of-Government Effort*

# Mission First: Behind the Scenes at the NDW Regional Operations Center

By: Mass Communication Specialist 2nd Class Jason Amadi, Naval District Washington Public Affairs

WASHINGTON (NNS) – Naval District Washington (NDW) activates its Crisis Action Team (CAT) when an incident occurs on an installation in the region that requires a large-scale response.

Representatives of every N-code come together in the Regional Operations Center (ROC) and develop solutions to complex problems. The CAT's latest complex problem is how to continue the NDW mission during the current COVID 19 pandemic.

"We can't all come into the room together, nor should we at this time," said Jeff Sanford, NDW emergency management director. "If we did, we'd be violating the very same thing we're telling people not to do. We're not above getting sick and nobody is immune to getting COVID-19."

Current social distancing protocols dictate that no more than 10 people be grouped together at once. NDW's CAT has used modern technology to continue with their mission.

"We use bridge lines where everybody calls in from their homes.

*Continued on page 2*

*Senior Chief Religious Programs Specialist Montana Sor views the latest COVID-19 data on the coronavirus COVID-19 global cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU) on display at the Naval District Washington Regional Operations Center (ROC).*

DEFEATING COVID-19

March 31, 2020 | Vol 1 |Issue 3

# NCIS: Beware of Coronavirus-Themed Scams

By Naval Criminal Investigative Service Public Affairs

QUANTICO, Virginia (NNS) -- The novel coronavirus pandemic presents 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.

Several spearphishing campaigns since January have falsely represented various healthcare organizations, including the U.S. Centers for Disease Control and Prevention and the World Health Organization. In many cases, victims receive coronavirus-themed emails requesting the victim to open an attachment or click on a link to obtain details about the coronavirus. Once a victim clicks on the attachment or link, they are directed to a malicious website requesting the victim to enter login credentials.

Law enforcement agencies have observed campaigns wherein victims received hoax emails from what appear to be the CDC requesting donations via Bitcoin to fund an "incident management system" in response to the coronavirus pandemic.

Agencies also observed in February a spearphishing campaign targeting Japan-based Internet users with emails that appeared to provide information relating to coronavirus prevention. The emails included malicious Microsoft Office files that upon opening would initiate the download of a sophisticated Trojan known as Emotet.

U.S. officials have released statements advising Russia is likely behind coronavirus disinformation campaigns that are being spread via social media. Reports indicate thousands of Twitter, Facebook, and Instagram accounts have been used to spread false information about the coronavirus pandemic.

*Continued on page 2*


## In This Issue

*ROC from page 1*

The evolution of the learning curve is quick. You learn not to step on each other when you're talking over the phone line and you really learn to have patience with connectivity issues and things like that. But we've proven in other events like for state of the union addresses that we can operate in a virtual environment, but it's just never been every day. We're operating in this virtual environment seven days a week and it's working," said Sanford.

Using technology to communicate with more than a dozen people has its own set of challenges, but NDW's CAT continues to press on and carry out its mission.

"The biggest challenge I'm finding is losing the interactions you'd normally have," said Mike Hedrick, NDW deputy director of operations. "Email and phone conversations can cut in and out. There's a lot of side-bar conversations that go on in a normal environment where you have a room full of people. When you're only communicating via electronic means, you lose those side-bar conversations where some good ideas and solutions are generated."

"But with all of today's technologies and things like Defense Collaboration Services, we've been able to overcome some of the challenges we wouldn't have been able to overcome five or 10 years ago with just email. Our essential task is to keep the doors open so the tenant commands can do their essential functions to keep the Navy and military effective. We've been able to do so and will continue to be able to do so with these mitigation factors," said Hedrick.


## A Tip For Working At Home

Find the most quiet place you can to set up your home work area. Make sure you have good lighting, a comfortable chair and plenty of outlets to plug in your computer, monitor, phone charger, etc. Put everything you need nearby so that you don't need to constantly hop up to find a report, get supplies, etc. Maintain as much of an office-like demeanor as you can. If you are using video for meetings, remember, you're on camera too.

## Use Official News Sources

Monitor official news resources and public health updates regularly to stay informed. Navy Region Naval District Washington will continue to provide weekly (or more frequently as needed) updates.

See Navy-specific updates for the Navy family on the NDW FaceBook Page

*NCIS from page 1*

Although there is no evidence that the Department of the Navy has been targeted, NCIS urges DON personnel to remain vigilant and use the following best practices to identify and avoid online scams:

Use complex passwords, use different passwords for different services, and change passwords often.

Go directly to a trustworthy website for information rather than clicking on email attachments, links, or pop-ups.

Double-check a website address prior to typing it in as scammers typically slightly alter URLs so they closely resemble a legitimate URL.

Do not enter sensitive data such as username and password into websites that do not typically ask for it.

Use multi-factor authentication whenever possible.

Check for spelling and grammatical errors within the contents of emails or suspicious websites.

Keep systems updated and running antivirus software.

If you have been targeted with this scam, 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.