



## NCIS: BEWARE OF CORONAVIRUS-THEMED SCAMS

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.



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](http://www.ncis.navy.mil).