Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 04-24
Date: May 7, 2024
Phone: (202) 372-1218
E-Mail: portstatecontrol@uscg.mil

PHISHING EMAILS IMPERSONATING U.S. COAST GUARD

The Coast Guard, in conjunction with the maritime community and the UK Department for Transportation, has been made aware of several phishing attempts by nefarious actors impersonating Coast Guard port state control (PSC) authorities. These incidents range from unsophisticated attempts asking for vessels to urgently contact PSC teams at a malicious hyperlink, to more sophisticated and targeted "spear phishing" attempts, which include details such as the ship name and IMO number to appear legitimate.

Phishing is a common form of social engineering that uses email or malicious websites to solicit personal information or to get a victim to download malicious software by posing as a trustworthy entity. Email correspondence from the Coast Guard will always be from the "uscg.mil" domain, will NOT include links requesting information, and will typically copy the vessel's agent in the port of destination. Emails claiming to be from the Coast Guard or PSC teams that do not state the specific purpose of the correspondence and/or are not from the uscg.mil domain should be regarded with suspicion. If you have received correspondence that is suspicious or has left you unsure of its legitimacy, please contact your agent or call the Coast Guard Sector Command Center at your port of destination.

Additionally, the Coast Guard encourages vessel operators to keep the following in mind regarding correspondence that may be phishing attempts:

- Do not click on any links or attachments that may appear suspicious.
- Take time to evaluate a suspicious email or correspondence, as victims of phishing tend to be those who go through emails quickly.
- The Coast Guard will not request personal information via email.

Per 33 CFR § 101.305, an owner or operator that is required to have a security plan shall report activities that may result in a transportation security incident or is a breach of security to the National Response Center. A successful phishing attempt may result in a Transportation Security Incident or Breach of Security, as defined in 33 CFR § 101.105, and is a Cybersecurity Incident per the Coast Guard Navigation and Vessel Inspection Circular No.02-24. Accordingly, a Transportation Security Incident or Breach of Security resulting from Cybersecurity Incidents on MTSA-regulated vessels shall be reported to the National Response Center at 1-800-424-8802.

The Coast Guard strongly encourages vessel operators to provide regular phishing and cybersecurity awareness training to all employees to identify and report suspicious correspondences. Additionally, the Coast Guard encourages all international partners to pass on information relating to suspicious behavior observed in the Marine Transportation System to their respective regulatory organizations.