U.S. COAST GUARD

MARITIME CYBER BULLETIN

18 March 2026

MCB 01-26: Awareness for Increased Phishing

THREAT SUMMARY

Coast Guard Cyber Command (CGCYBER) has observed an increase in the prevalence and sophistication of phishing campaigns targeting the Marine Transportation System (MTS). In 2025, phishing techniques were leveraged for reconnaissance and initial access in 43% of reported MTS cyber incidents, an increase from 25% in calendar year 2024. Adversaries are employing advanced social engineering tactics, frequently exploiting intra-organizational trust by weaponizing compromised accounts to launch additional phishing attacks against internal users and external partners.

Threat actors are increasingly using impersonation techniques for financial exploitation, often posing as company executives or customers to solicit fraudulent transactions, such as invoice requests. Another commonly observed tactic is exploiting trust after compromising employee accounts through phishing with malicious hyperlinks and credential harvesting. In one notable 2025 case, nine employee accounts were compromised, enabling the attacker to send thousands of phishing emails to external contacts.

In July 2025, the Coast Guard codified new cybersecurity measures that establish training requirements under 33 CFR 101.650(d) which will be mandatory. This training requirement is specifically designed to counter threats, including phishing. Properly trained personnel are a critical line of defense, equipped to identify and report indicators of a phishing attempt.

Recommendations

CGCYBER strongly recommends that maritime stakeholders undertake a rigorous review of access control and user awareness protocols. Defensive measures should include:

- Use of Multi-Factor Authentication (MFA) across all user accounts.
- Recurring, scenario-based phishing awareness training that emphasizes exploitation of authority, urgency, and familiarity.
- Establishment of verification procedures for anomalous or high-value requests, including out-of-band confirmation with purported senders.
- Deployment of advanced email filtering and anti-phishing solutions.
- Regular assessment and refinement of incident response playbooks to address phishing and vishing contingencies.

Resources

- CISA: Phishing Guidance
- FBI: Business Email Compromise Advisory
- NIST: Phishing Fact Sheet

For more insights into evolving threats, the upcoming 2025 Coast Guard Cyber Threats in the Information Environment (CTIME) publication will provide additional analysis.

Resources

Facilities that observe any unusual or suspicious activity, breaches of security, or interruptions to their network should report those activities to:

Coast Guard's National Response Center:
1-800-424-8802

OR

Cybersecurity and Infrastructure Security Agency (CISA) Central:
1-888-282-0870

If you have any questions, please visit our website at:
https://www.uscg.mil/MaritimeCyber
or reach out to MCRB at:
maritimecyber@uscg.mil