



NAVY & MARINE CORPS PERSONNEL RECEIVE THREATENING MESSAGES FROM IRANIAN CYBER GROUP



Product created in joint coordination with the Naval Criminal Investigative Service (NCIS) and the United States Marine Corps (USMC).

Recent reporting indicates that Department of the Navy (DON) personnel—including service members, civilians, and family members—have been targeted by a coordinated messaging campaign linked to Iranian-affiliated cyber actors, including a hacktivist group known as “Handala.”

These activities are part of a broader effort to conduct psychological and information operations against U.S. military personnel. Rather than relying solely on technical cyber intrusions, these actors seek to influence perception, generate fear, and amplify the appearance of access or capability through coordinated messaging, public claims, and alleged data leaks.

Recent Activity

On April 27, 2026, DON-affiliated personnel began receiving threatening messages from a Bahrain-registered phone number. The messages claimed that recipients were under surveillance and included threats of kinetic targeting, referencing drones and missile strikes. The messages were signed “Handala” and directed recipients to a website associated with the group.

The following day, April 28, 2026, Handala posted to its Telegram channel claiming it had released the personal information of 2,379 U.S. Marines stationed in the Persian Gulf region.

This activity follows earlier incidents on March 2, 2026, when DON and Department of the Navy/Department of War personnel received threatening emails from unknown Iranian-affiliated cyber actors. These emails warned recipients they were “under close surveillance,” instructed them to “stop” and “go home,” and included threats directed at both the individuals and their families.

Threat Assessment

While the tone and content of these messages are designed to be alarming, current assessment indicates that these activities are primarily intended to intimidate and influence behavior, rather than signal credible, imminent physical threats.

Their operations typically combine:

- Direct messaging to individuals
- Public amplification through platforms such as Telegram
- Claims of data compromise or exposure

Together, these elements are designed to extend the psychological impact beyond the initial contact and generate broader concern within targeted communities.

Capabilities and Targeting

The group primarily relies on common techniques such as spear-phishing and the reuse of previously exposed data.

Targeting patterns indicate a preference for sectors where disruption or fear can generate significant visibility, including:

- Government and defense personnel
- Technology organizations
- Critical infrastructure entities

Outlook

NCIS assesses that this messaging campaign is likely to continue, particularly in the context of ongoing U.S. operations in the region. The release of personal data, where it occurs, is likely to involve legacy or publicly sourced information, rather than newly compromised Department of the Navy systems.

Guidance for Personnel

- Personnel who receive suspicious or threatening messages should treat them as part of a coordinated influence effort and take appropriate precautions.
- Recipients are advised not to engage with the sender, avoid clicking on links or downloading attachments, and preserve the message for reporting purposes.
- All such incidents should be reported through appropriate channels, including local security personnel, the nearest NCIS Field Office, or the NCIS Tips program.



REPORTING IS ANONYMOUS

SUBMIT A TIP AT
WWW.NCIS.NAVY.MIL

