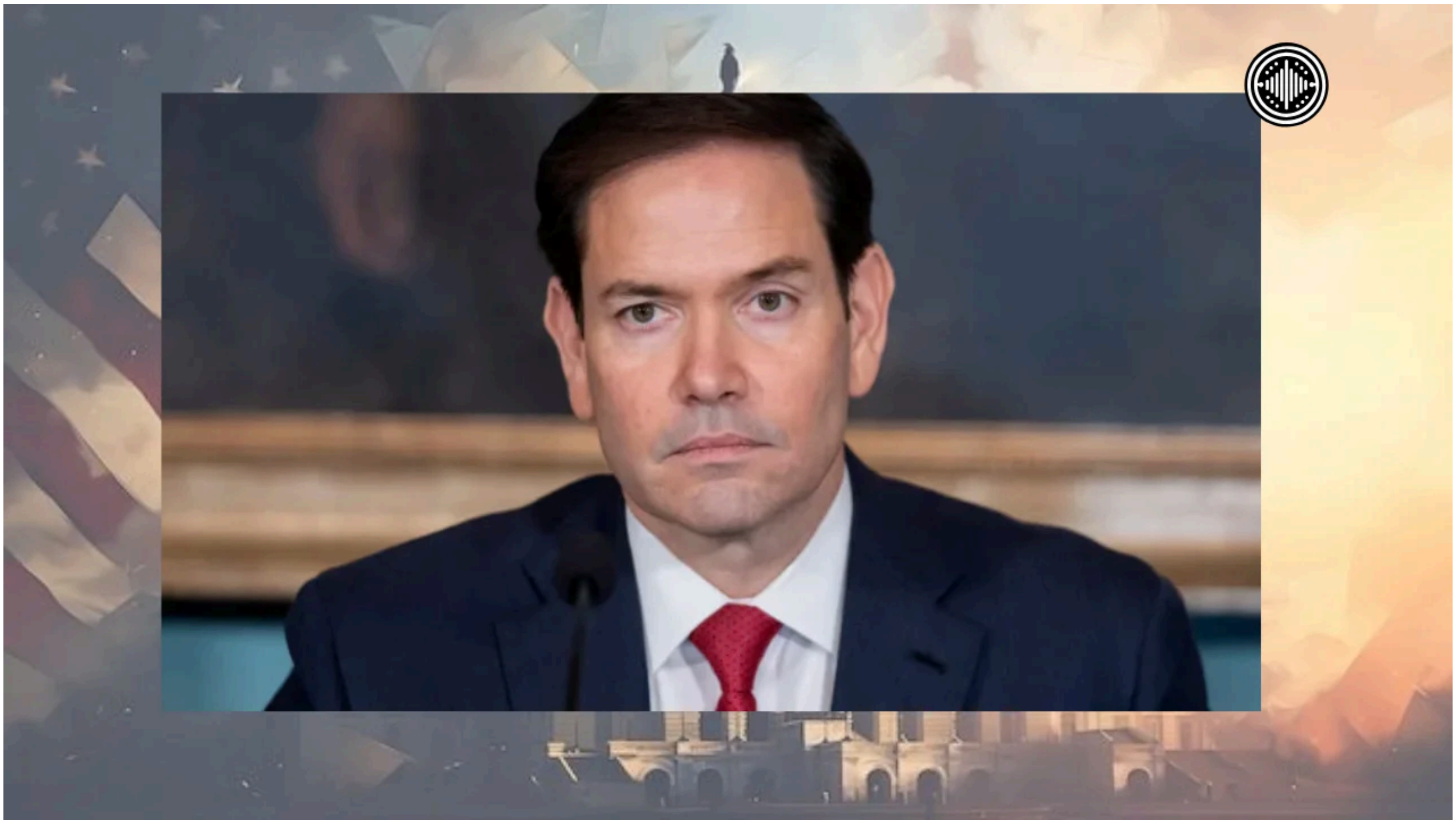
OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

AI Scam Targets U.S. Officials by Impersonating Rubio

July 9, 2025
— Categories: Politics & Government



The United States State Department has issued a new warning about an alarming attempt to use artificial intelligence to impersonate top American officials. According to senior officials and an internal cable sent to embassies and consulates worldwide, an impostor posing as Secretary of State Marco Rubio began contacting several prominent leaders in mid-June, prompting a global alert issued on July 3.

The scheme targeted exactly three foreign ministers, a United States senator, and a state governor. The fake messages arrived by text, Signal, and voicemail. While the specific recipients were not named, the department confirmed it had uncovered the effort and is now monitoring the situation closely.

“The State Department is aware of this incident and is currently addressing the matter,” said spokeswoman Tammy Bruce. She declined to provide further details, citing security reasons and an active investigation.

Officials described the impersonation as ‘not very sophisticated,’ yet serious enough to prompt a worldwide diplomatic warning. To warrant a global alert to U.S. diplomats and foreign governments. The department emphasized that while no direct cyber threat was detected, any information shared with a fraudulent account could be exploited.

This episode is the latest example of how quickly AI tools can be turned into weapons of deception. Earlier this year, scammers used AI-generated voice messages to impersonate President Donald Trump’s chief of staff, Susie Wiles, targeting U.S. officials.

Experts warn these incidents will only increase as deepfake technology improves. Siwei Lyu, a computer scientist at the University at Buffalo, noted that a few years ago, deepfakes were easier to spot because of obvious flaws like robotic voices or visual errors. Today, the technology has advanced to a point where realistic fake audio and video can fool even careful observers.

“It’s an arms race, and right now the generators are getting the upper hand,” Lyu said.

In the Rubio impersonation case, scammers attempted to sow confusion by creating fake communications that looked and sounded credible. Some of the messages referenced sensitive issues like U.S. policy in Ukraine. This follows a deepfake video released earlier this year that falsely depicted Rubio threatening to cut Ukraine’s access to Starlink internet services, a claim Ukrainian authorities quickly denied.

The Federal Bureau of Investigation has also issued warnings about malicious campaigns using AI-generated content to impersonate officials and spread false information.

As concerns mount, lawmakers and tech experts are exploring solutions, from stricter penalties for deepfake scams to better tools for verifying identities. The State Department stressed that employees should remain alert and verify any suspicious messages before responding.

Download IPFS