OpenVoiceNews Australia

Transparent. Unbiased. Yours.

UAP and Trumpet of Patriots Hit by Cyberattack

July 17, 2025

— Categories: Human Rights

The United Australia Party (UAP) and Trumpet of Patriots, both led by Clive Palmer, were targeted in a ransomware cyberattack on June 23, 2025, compromising sensitive data like emails, banking records, and personal details. This article explores the breach's impact, the parties' response, and the broader implications for cybersecurity, highlighting concerns about the Labour government's digital defenses.

On July 17, 2025, the UAP and Trumpet of Patriots announced a significant data breach, with hackers gaining unauthorized access to their servers. The attack, identified as a ransomware incident, potentially exposed all electronic records, including emails, attachments, phone numbers, identity documents, banking details, and employment histories. “We were the subject of a ransomware cyberattack,” the UAP stated, as reported by 9News, with a near-identical notice on the Trumpet of Patriots website. The breach, reported to the Office of the Australian Information Commissioner (OAIC) and the Australian Signals Directorate (ASD), has raised alarms about the vulnerability of political organizations, especially after the parties’ high-profile campaigns in the 2025 federal election.

The UAP, deregistered in 2022, and its successor, Trumpet of Patriots, failed to secure seats in the recent election despite heavy spending. The breach affects supporters who provided personal information, with the parties urging vigilance against scams. “We don’t know the full extent of the data compromised,” a UAP spokesperson told Crikey, noting that systems were restored from backups but individual notifications were impractical. X posts reflect public outrage, with users slamming the Labour government for weak cybersecurity policies, arguing that stronger measures could prevent such breaches. The Australian Electoral Commission (AEC) clarified that it does not supply phone numbers to parties, leaving questions about how data was sourced for past text campaigns.

This incident underscores the growing threat of cyberattacks on political entities, especially as Australia navigates tensions with foreign actors like China’s People’s Liberation Army (PLA) in the Indo-Pacific. Critics on X

question the Labour government's focus on diplomacy over robust digital infrastructure, citing the ASD's report of 121 ransomware incidents in 2023-2024. The breach serves as a wake-up call for stronger cybersecurity, ensuring Australia's political and personal data remains secure against opportunistic hackers.