Com-affiliated actors use vishing to hijack cloud accounts for data theft and extortion



Unit 42 reports repeated vishing waves since August 2026 by Com-affiliated actors, leading to data theft and extortion. Targets include financial services, healthcare and legal firms in the U.S., U.K. and Australia.

- Palo Alto Networks Unit 42 says it has tracked and responded to numerous vishing waves since August 2026.
- The activity is attributed to Com-affiliated threat actors.
- Reported outcomes are data theft and extortion attempts, with cloud accounts hijacked.
- Targets named are financial services, healthcare and legal services in the U.S., U.K. and Australia, plus other sectors such as construction.

Palo Alto Networks Unit 42 has disclosed that it is tracking, and has responded to, numerous waves of vishing (voice phishing) attacks carried out by threat actors affiliated with the Com since August 2026. The campaigns have resulted in data theft and extortion attempts, and the headline describes cloud accounts being hijacked.

Who has been targeted

According to the report, victims are in financial services, healthcare and legal services located in the U.S., the U.K. and Australia. Other targets include construction, among additional sectors. The source excerpt does not name specific victims or list Saudi targets.

Why it matters for Saudi institutions

Vishing relies on persuading a person by phone rather than exploiting a software flaw, so technical patching alone does not close the gap. Financial, healthcare and legal organisations in the Kingdom handle similar sensitive data and use similar cloud services, which makes the pattern relevant even though no regional activity is reported. The source excerpt does not describe the exact call scripts or technical steps used, so teams should avoid assuming details beyond what Unit 42 has published.

Practical next step

Treat this as a prompt to review how help desks and staff verify callers, and how cloud account recovery and access changes are approved. Check Unit 42's full publication for indicators and detailed guidance.

What to do now

1. Require call-back verification through a known number before a help desk resets credentials or MFA for any cloud account.
2. Brief staff, especially help desk, finance and legal teams, on vishing and on reporting suspicious calls immediately.
3. Review approval steps for cloud account recovery and privileged access changes, adding a second approver for high-risk requests.
4. Check cloud audit logs for unusual sign-ins, new MFA registrations or bulk data downloads.
5. Read Unit 42's full report and add its indicators to monitoring where applicable.