CAROUSEL

REAL-TIME ALERT:

Update: Friday, Nov. 29, 10:00 AM

Dear Client/Service Provider:

It seems that Hackers have taken a particular interest in monitoring the FCC's Robocall Mitigation Database — apparently in an effort to stay ahead of carrier-specific robocall mitigation plans and strategies.

Based on the best available evidence, a team of Hackers has gained access to the backend of some well-known systems and are reading the plans, in real time, as they are being created.

There is a confirmed case of unauthorized access to a professional instance of Microsoft OneDrive, allowing Hackers to view the plan, in real-time, as it is being created by the Service Provider's professional counsel.

This is a significant security flaw and vulnerability. The appropriate authorities have been contacted, but thus far it is unclear whether corrective measures have been implemented.

Caution is advised when preparing any network-level or security-related document for submission to the FCC – as it appears that Hackers, Robocallers, and AI-Enabled dialing systems, determined to stay ahead of any regulations that could apply to them, are *peering* into specific systems, hacking specific networks, and targeting specific professionals, in an effort to gain access to mitigation strategies – in advance – so that they can, in turn, design pathways to avoid software, Vendors, and analytics designed to detect them.

Updates, notes and commentary posted at: https://telepath.global/alerts