

Social Engineering Tactics

TACTICAL INTELLIGENCE REPORT // 2026

The Psychology of Deception

Adversaries are moving away from 'mass-spam' to 'Hyper-Personalized' lures. If a hacker knows the name of your child's daycare, they can craft a lure that bypasses 99% of traditional skepticism.

Case Study: The 2025 Kido International Incident

THE 'HEARTSTRING' LURE

In September 2025, attackers targeted a major childcare provider. They didn't send a fake invoice; they sent a fake 'Emergency Medical Update' to staff. The urgency caused a high-level administrator to bypass security protocols. The result: data on 8,000 children stolen, followed by a double-extortion demand that leveraged public outrage.

The Deepfake Frontier

Vishing 2.0

Using 3 seconds of high-quality audio from a YouTube interview, hackers can now clone a CEO's voice in real-time to authorize 'urgent' wire transfers during Friday afternoon chaos.

Operational Best Practices

Building Resilience

- **Out-of-Band Verification:** Establish a 'Secret Word' or a secondary platform (Signal/WhatsApp) for high-stakes approvals.

INTERNAL USE ONLY - SENSITIVE RESOURCE - NOT FOR PUBLIC REDISTRIBUTION

- **Simulation-as-Training:** Run 'Live-Fire' phishing that mirrors current news events.