Social Engineering & Physical Testing

Your employees and buildings are prime targets. We run realistic phishing campaigns, voice-based deception, and on-site intrusion attempts to gauge how well your staff and facilities stand up to manipulation. The results reveal gaps in training and access controls so you can fix them before criminals exploit them.

EMAIL PHISHING

Custom-crafted email campaigns that mirror real attacker tactics. We measure open rates, link clicks, credential submissions, and payload execution to benchmark staff vigilance.

VOICE & SMS ATTACKS

Phone calls and text messages using caller-ID spoofing, pretexting, and open-source research to coax employees into sharing sensitive details or taking risky actions.

ON-SITE PRETEXTING

In-person scenarios where our team poses as vendors, contractors, or employees to test badge policies, visitor procedures, and staff willingness to challenge strangers.

MALICIOUS MEDIA DROPS

Strategically placed USB drives, mailed packages, and QR-code flyers designed to see if employees will plug in unknown devices or follow suspicious instructions.

FACILITY BREACH ATTEMPTS

Controlled break-in exercises that probe locks, badge readers, and security guards. We document how far an intruder could get and what data or systems they could reach.

AWARENESS METRICS

Quantified results showing who clicked, who reported, and where policies broke down - giving leadership clear data to prioritize training and tighten controls.

WHY BARCODE SECURITY

People are often the easiest entry point for attackers. Our assessments replicate the manipulation techniques used in real breaches, revealing weaknesses in human behavior and physical safeguards so you can close the gaps.

PUT YOUR PEOPLE TO THE TEST. **Launch a social engineering assessment.**