Service Overview

SynAck Solutions' Phishing as a Service delivers managed phishing simulation campaigns that measure and strengthen your organisation's resilience against social engineering attacks. Each campaign replicates real-world threat actor TTPs, tracking granular metrics — open rates, click-throughs, credential submissions, and employee reporting rates. Results feed directly into targeted awareness training, creating a measurable feedback loop that drives behavioural change.

Business Value

- Quantify organisational phishing susceptibility with empirical, board-ready metrics
- Identify high-risk departments and roles for targeted awareness intervention
- Reduce credential compromise incidents through progressive testing
- Satisfy compliance requirements under APRA CPS 234 and ISO 27001
- Strengthen the human firewall without disrupting operations
- Benchmark performance against industry baselines and track improvement
- Accelerate incident reporting culture by measuring employee report rates

What's Included

- Dedicated campaign manager and phishing simulation specialist
- Threat intelligence-informed pretext development for your industry
- Custom landing pages replicating credential harvesting and MFA bypass scenarios
- Multi-vector execution across email, SMS (smishing), and voice (vishing)
- Granular tracking: delivery, open, click, credential submission, and report rates
- Segmented targeting by department, role, or custom groupings
- Post-campaign analytics dashboard with per-user and per-department drill-down
- Executive summary report with trend analysis and risk scoring
- Targeted micro-training modules for users who interact with simulated phishes
- Quarterly cadence with progressive difficulty escalation
- Benchmarking against Australian industry averages

Scope

Campaigns are scoped to your user base and communication channels, with parameters agreed during onboarding and refined quarterly:

- All employees, contractors, and third-party users with organisational email
- Email phishing with configurable complexity through to targeted spear-phishing
- Optional SMS-based smishing and voice-based vishing campaigns
- Credential harvesting simulations using realistic cloned portals
- Payload-based simulations (macro documents, HTML smuggling) where agreed
- Integration with existing awareness platforms (KnowBe4, Proofpoint, Mimecast)

What's Excluded

- Exploitation of submitted credentials against production systems
- Physical social engineering (available as a separate engagement)
- Modification of email gateway configurations beyond safe-listing
- Development of real malware or weaponised payloads
- Campaigns targeting personal email addresses or devices outside scope
- Awareness training platform licensing (integration included)

Methodology

Campaigns follow NIST SP 800-50 and MITRE ATT&CK initial access techniques (T1566 Spearphishing). Pretexts use current ACSC threat advisories and real-world patterns. Each wave increases in sophistication, progressing from generic lures through to highly targeted, context-aware spear-phishing.

Engagement Timeline

Onboarding — target list ingestion, safe-listing, and first campaign design — completes within two weeks. Each campaign wave runs five to ten business days, with real-time analytics and formal report within five business days. Standard engagements run quarterly on a twelve-month commitment.

Get Started

Contact SynAck Solutions to schedule a PhaaS onboarding consultation. We will assess your awareness posture, define campaign objectives, and launch your first simulation within weeks.

info@synack.au | https://www.synack.au

ABN 88 667 784 956