Service Overview

SynAck Solutions delivers targeted Phishing and Social Engineering Assessments that measure your organisation's human attack surface — the single most exploited entry point in modern breaches. Our certified operators design and execute realistic campaigns that replicate the tactics used by sophisticated threat actors, from mass credential harvesting to highly targeted spear-phishing and pretexting scenarios.

Every engagement is tailored to your organisation's threat profile and industry context. Campaigns are conducted under strict rules of engagement with full transparency to nominated stakeholders, providing measurable insights into employee security awareness and organisational resilience against social engineering attacks.

Business Value

- Measure employee susceptibility to phishing, vishing, and pretexting attacks with hard data
- Identify departments, roles, and user groups most vulnerable to social engineering
- Validate the effectiveness of email security controls, web proxies, and URL filtering
- Test incident reporting workflows — do employees report suspicious emails to the SOC?
- Meet compliance obligations: ISO 27001, PCI DSS, Essential Eight, APRA CPS 234
- Provide targeted, evidence-based input to security awareness training programs
- Benchmark your organisation's phishing resilience against industry baselines

What's Included

- Custom phishing campaign design: branded templates, realistic pretexts, and convincing lures
- Credential harvesting landing pages with pixel-perfect cloning of target portals
- Spear-phishing scenarios targeting high-value individuals (executives, finance, IT admins)
- Payload delivery testing: macro-enabled documents, HTML smuggling, QR code phishing
- MFA bypass simulation using reverse-proxy phishing techniques where scoped
- Vishing (voice phishing) and pretexting calls targeting help desk and support staff
- Real-time campaign tracking: open rates, click rates, credential submission, and reporting rates
- Employee response analysis: who reported, who clicked, who submitted credentials
- Branded report with campaign metrics, findings, and awareness recommendations
- Post-engagement debrief with actionable training recommendations

Campaign Types

SynAck offers multiple campaign types tailored to your objectives:

- Mass phishing: broad-scope credential harvesting across the organisation
- Spear-phishing: targeted attacks against specific individuals or teams
- Payload delivery: test endpoint controls with simulated malicious attachments
- QR code phishing (quishing): physical and digital QR-based lure campaigns
- Vishing: voice-based social engineering targeting help desk and staff
- Pretexting: scenario-based deception to elicit sensitive information or actions
- MFA bypass: advanced reverse-proxy phishing to test multi-factor resilience

Campaign complexity and target selection are agreed during pre-engagement scoping.

What's Excluded

- Actual malware deployment or persistent access to endpoints
- Physical security testing or facility access assessments (available separately)
- Internal or external network penetration testing (available separately)
- Attacks against personal email accounts or personal devices
- Campaigns targeting third-party staff without explicit written authorisation
- Denial-of-service or any destructive testing

Methodology

Our methodology aligns with the Social Engineering Penetration Testing Execution Standard and MITRE ATT&CK Initial Access techniques. Campaigns progress through reconnaissance, pretext development, infrastructure staging, execution, and analysis. All campaign infrastructure is purpose-built per engagement and decommissioned upon completion.

Engagement Timeline

A typical phishing assessment runs 2-4 weeks including campaign design, execution window, and reporting. Vishing engagements typically run 1-2 weeks. Final report delivery within 5 business days of campaign completion. Follow-up campaigns available to measure improvement after awareness training.

Get Started

Contact us to discuss your objectives and receive a tailored proposal. We will work with you to define campaign scope, target lists, pretexts, and success criteria aligned to your security awareness goals.

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

ABN 88 667 784 956