Service Overview

SynAck Solutions delivers practical, role-appropriate cybersecurity awareness training that transforms your workforce from a vulnerability into an active layer of defence. Our programs are built around real-world attack scenarios and current threat intelligence — not generic compliance slide decks — with content tailored to your industry and the specific risks facing different roles within your organisation.

Business Value

- Reduce the success rate of phishing, social engineering, and credential harvesting attacks
- Satisfy compliance requirements for security training (APRA CPS 234, ISO 27001, PCI DSS)
- Build a security-conscious culture where employees actively report suspicious activity
- Tailor content to role-specific risks, ensuring relevance across all staff levels
- Measure effectiveness with quantitative metrics: click rates, reporting rates, assessment scores
- Reduce incident response costs by preventing human-initiated security incidents
- Demonstrate due diligence to cyber insurers, auditors, and clients

What's Included

- Training needs analysis to identify role-specific risks and knowledge gaps
- Customised content aligned to your industry, threat profile, and policies
- Instructor-led sessions (on-site or virtual) covering core security awareness topics
- Executive briefing on targeted threats: BEC, whaling, and deepfake social engineering
- Developer-focused secure coding awareness covering OWASP Top 10
- Pre- and post-training knowledge assessments to measure learning outcomes
- Simulated phishing campaign (one round) to baseline employee susceptibility
- Training completion tracking and compliance reporting for HR and audit
- Incident reporting procedure training for recognising and escalating security events
- Post-training recommendations report with behavioural metrics

Scope

Programs cover all personnel or specific business units as agreed, with content developed for distinct audience segments:

- General staff — phishing recognition, password hygiene, safe browsing, data handling
- Executives — targeted attack awareness (BEC, whaling, deepfakes), incident escalation
- IT and security teams — privileged access risks, advanced social engineering techniques
- Software developers — secure coding, OWASP Top 10, input validation
- New starters — baseline security awareness as part of onboarding
- Contractors and third parties — data handling, acceptable use, and incident reporting

What's Excluded

- Ongoing managed phishing campaigns (available as Phishing as a Service)
- Development or hosting of a learning management system (LMS)
- Penetration testing, red team assessments, or technical security testing
- Policy development or ISMS documentation (available as separate engagements)
- Physical security assessments beyond the included phishing simulation
- Translation of materials into languages other than English (available on request)

Methodology

Our methodology aligns with NIST SP 800-50 and ACSC guidance on cyber security awareness. Content uses adult learning principles — scenario-based, interactive, and focused on behavioural change. Modules are mapped to ISO 27001 Annex A.6.3 and tailored using current ACSC and ASD threat intelligence.

Engagement Timeline

Training engagements are delivered over two to four weeks. Week one covers needs analysis, content customisation, and pre-assessments. Sessions are delivered over one to two weeks. Post-assessments and phishing simulation run in the final week, with a report within five business days.

Get Started

Contact SynAck Solutions to discuss your security awareness training needs. We will assess your current program maturity, identify role-specific gaps, and propose a tailored program that meets compliance and risk reduction objectives.

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

ABN 88 667 784 956