SERVICE BRIEF · 05

KnowBe4 Security Awareness Training.

Transform your users from security risk to human firewall.

THE PROBLEM & THE APPROACH

Technical security controls can't prevent users clicking malicious links, sharing credentials, or falling victim to social engineering. Human error remains the leading cause of security breaches and attackers know it.

CNNECT's KnowBe4 deployment implements the world's largest library of security awareness training combined with sophisticated simulated phishing campaigns. We establish baseline susceptibility, design training aligned to your risk profile and deliver measurable reduction in user vulnerability over time.

Key challenges addressed

EIGHT HUMAN-RISK GAPS

01 Users clicking phishing links despite technical email security controls.

02 No way to measure security awareness or identify high-risk individuals.

03 Generic "sheep-dip" training that doesn't engage users or change behaviour.

04 Inability to demonstrate security culture improvements to board or insurer.

05 Compliance requirements for regular security awareness training.

06 Reactive approach to security incidents rather than proactive prevention.

07 No visibility into which users or departments represent highest risk.

08 Training quickly forgotten with no reinforcement or ongoing engagement.

SERVICE OVERVIEW

Continuous training plus realistic phishing tests.

KnowBe4 combines continuous security awareness training with realistic simulated phishing attacks. Users receive engaging, relevant content matched to their role and risk level and campaigns identify users who need additional support.

Our deployment establishes baseline phishing susceptibility, implements automated training campaigns, configures ongoing phishing at frequencies aligned to your risk appetite, and provides dashboards showing measurable improvement over time.

PILLAR 01 · TRAIN

Continuous Training

Engaging, role-aware modules drawn from KnowBe4's library the largest of its kind automatically scheduled across the year and adjusted to each user's risk profile.

- Role-matched content library
- Automated annual scheduling
- Compliance evidence pack
- Reinforcement & refreshers

PILLAR 02 · TEST

Simulated Phishing

Realistic phishing campaigns measure real-world vulnerability, identify high-risk users, and feed automatically into targeted training closing the loop between awareness and behaviour.

- Baseline susceptibility test
- Frequency tuned to risk appetite
- Auto-targeted follow-up training
- Departmental risk dashboards

TYPICAL TIMELINE

2 weeks

Contract to first phishing campaign & training launch.

IMPLEMENTATION

From £4,750

Implementation fee on start; subscription invoiced annually.

WHAT'S INCLUDED — SIX DELIVERABLES · PLUS DEMO ON REQUEST

01 Platform access 02 Baseline phishing 03 Year-1 campaigns 04 Quarterly reviews 05 Ongoing support

NEXT STEPS · REQUEST A DEMO

Book a 30-minute scoping call or request a live platform walk-through.

hello@cnnect.com

+44 20 7173 5320

CNNECT.COM