SERVICE DEFINITION
SOCIAL ENGINEERING TESTING

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- **to reduce the risk of significant security incidents**
- **to speed up the detection and containment of threats, and**
- **to demonstrate robust governance to stakeholders such as boards, auditors, and insurers**

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Central government department — MFA reset verification gaps

We conducted a vishing pretext targeting the service desk, making a plausible request to reset MFA for a senior official. Our call flows showed that agents relied on basic biographical checks and visible directory data. While several agents followed procedure, one agent reset credentials after we used persuasive urgency cues. During the same window, our email campaigns prompted mixed reporting and led to delayed triage.

JUMPSEC tightened verification by requiring out-of-band checks and ticket linkage, implemented step-up approval for privileged principals, and introduced a concise agent script for refusal and escalation. We focused awareness materials on urgency manipulation and authority bias. In a short retest, we evidenced consistent refusal and clear escalation paths.

NHS Trust — Finance process manipulation via supplier change

We crafted email pretexts as a known supplier requesting bank-detail changes. JUMPSEC observed that established controls routed requests through shared mailboxes, but verification processes depended on replying to the same thread. Several recipients forwarded our emails to finance without challenge, and one individual initiated a change without independent confirmation.

We mandated that staff use verified contact channels outside the originating request, enforced dual approval for changes, and blocked risky domains from appearing in auto-complete lists. JUMPSEC delivered targeted micro-lessons to coach staff on recognising supplier-change fraud patterns. In our retest, we saw that recipients performed out-of-band verification correctly and reported incidents within minutes.

Local authority — Contractor onboarding and badge collection

We executed physical pretexts by attempting access using contractor language and timing our deliveries to coincide with busy periods. JUMPSEC observed that reception processes varied across sites; at one location, staff issued a temporary pass without requiring a sponsor to be present. In parallel, we sent an email pretext requesting Wi-Fi guest credentials, citing the urgency of an impending audit.

JUMPSEC standardised visitor policies across all sites, mandated the presence of a sponsor or verified contact, and transitioned to QR-based guest onboarding with built-in expiration and logging. We conducted follow-up checks and confirmed that sites consistently maintained access control and that all passes were auditable upon issuance.

National charity — Password capture via branded landing and SMS

We sent smishing messages that mimicked a familiar collaboration tool using a look-alike domain. JUMPSEC observed that recipients who clicked the links were redirected to a safe landing page, where we recorded only their intent. Staff reported incidents to security, but we noted that the process lacked a one-click reporting option and that the SOC did not initiate automatic domain takedown.

JUMPSEC introduced a single-click report button for all clients, automated domain takedown requests, and applied banners to external emails from near-match domains. Through our follow-up verification campaign, we saw quicker reporting, automated domain takedown, and a reduction in click-through rates.

Service Overview

JUMPSEC conduct an independent assessment of human and process resilience against social engineering. The engagement designs realistic pretexts, runs controlled campaigns across agreed channels, and measures susceptibility, detection, and reporting. Delivery emphasises non-destructive techniques, clear safety gates, and evidence that links human behaviour to business risk. Outputs focus on actionable improvements to identity, process, and culture, with measurable acceptance criteria.

Objectives

- Measure susceptibility to targeted phishing, vishing, and smishing in agreed populations
- Test verification processes for high-risk requests such as MFA reset and payment changes
- Assess reporting behaviour, response workflows, and containment steps during live attempts
- Provide practical, testable improvements to policies, controls, and staff guidance

Approach

Work begins with scenario design that reflects attacker tradecraft, business context, and peak-risk processes. Campaigns run in defined windows with opt-out rules, harm minimisation, and regulator-aware communications. Evidence collection avoids real data capture; benign artefacts and safe landing pages demonstrate risk without processing personal content. Stakeholders usually include Security, Service Desk, HR, Finance, and Communications.

Method

- **Plan** — define objectives, targets, channels, safety gates, escalation, harm-minimisation, and evidence handling
- **Prepare** — build pretexts, benign payloads, voice scripts, and tracking with privacy-preserving analytics
- **Execute** — run campaigns in windows, adapt to live responses, and observe verification steps
- **Analyse** — map behaviours to control gaps, training needs, and process weaknesses
- **Debrief** — present outcomes, owners, acceptance tests, and retest options for sustained improvement

Deliverables

- Executive briefing describing key behaviours observed, material risks, and priority actions
- Social Engineering Assessment Report covering campaign design, participation, susceptibility rates, reporting patterns, verification failures, and control/process gaps with precise improvements
- Issue register (CSV/XLSX) listing actions, owners, due dates, and acceptance criteria

- Optional awareness pack containing comms templates, quick-reference guides, and targeted micro-lessons aligned to observed behaviours
- Optional verification letter confirming improvement after targeted retests
- Standards and alignment embedded in reporting, referencing NCSC phishing guidance, NIST SP 800-53 control families for awareness and identity processes, and applicable regulator expectations where payroll, payments, or citizen communications are affected

Outcomes and benefits

- Lower likelihood of credential theft, payment fraud, and malicious changes
- Clearer verification procedures and stronger response to suspicious activity
- Targeted awareness materials that address observed behaviours, not generic risks
- Evidence suitable for governance, audit, and insurer dialogue

Pricing model

Fixed price per application or domain set and ingress mix, or time-and-materials aligned to SFIA. Price drivers include ingress diversity, API coverage, custom rule volume, and verification depth.

Timelines

- Planning and artefact preparation in 1–2 weeks
- Execution windows as agreed for each channel
- Report issue in 5–10 working days after testing completion
- Optional retest by agreement

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement Lead** — scope, governance, quality management, stakeholder alignment
- **Social Engineering Specialist(s)** responsible for campaign design and execution
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Approve target groups, pretexts, and safety gates
- Provide routing for reports and hotlines, and coordinate supplier participation where service desks are outsourced

JUMPSEC responsibilities

- Operate within agreed rules of engagement and ethics criteria
- Avoid real data capture; use benign artefacts and safe destinations
- Handle metrics securely and retain only for agreed periods

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- Non-destructive techniques; no malware, no real credential collection
- Voice calls recorded only with prior written consent and in line with policy and law
- Third-party/service-desk participation requires written approval
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Phishing and Vishing Simulation
- Threat-Led Penetration Testing
- Cyber Incident Exercising (NCSC Assured)

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com