SERVICE DEFINITION
PHISHING AND VISHING SIMULATION

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

Corporate advisory firm — Deal-team phishing and data room impersonation

We ran a campaign that mirrored M&A workflows, with JUMPSEC creating look-alike domains for data rooms and lenders. We crafted lures that referenced live project code names, which JUMPSEC sourced from public filings and advisory announcements. Our targets followed links to a benign portal that JUMPSEC built to imitate SSO prompts and watermark notices. In parallel, we used vishing scripts to press for urgent MFA resets ahead of a board pack deadline. During the engagement, the service desk relied on directory data and caller assertiveness rather than ticket linkage or call-back verification.

For remediation, JUMPSEC enforced publisher trust for OAuth applications, blocked consumer IdPs on enterprise tenants, and added step-up verification for data-room and SSO resets. We introduced playbooks that required out-of-band call-backs to verified numbers, issued rapid firm-wide advisories for active lures, and implemented mailbox banners for near-match domains. After a short retest, we evidenced prompt reporting from deal teams, consistent refusal of reset requests, and earlier suppression of look-alike domains across ongoing transactions.

National retailer — Store support desk vishing during promotion launch

During a national promotion, JUMPSEC called the store support desk, posing as a regional manager and requested a temporary bypass on POS updates. At the same time, we sent parallel emails from a look-alike domain to request SSO resets for merchandising accounts. Most agents followed procedure on these calls, but one agent processed a reset without linking it to a ticket. Several stores forwarded our email to a shared inbox, but did not tag it as suspicious. We updated runbooks to require roster and ticket checks before any reset and initiated call-backs to verified contacts. JUMPSEC mandated that POS changes needed a change ID and dual approval. We configured SIEM rules to correlate look-alike domains, promotion terms, and reset attempts. Over a short verification window, we recorded prompt refusals, clean escalations, and earlier advisories to stores, which reduced risk during peak trading.

Local authority — MFA reset and removal under meeting pressure

JUMPSEC ran a campaign that directly contacted the IT service desk just before a cabinet briefing. We used councillor details sourced from public minutes and posed as a caller claiming a lost device, urgently requesting an MFA reset and temporary removal “to avoid missing the vote”. The agent verified the name and department only, then issued a reset link within the same email thread. In parallel, JUMPSEC sent emails from a near-match domain referencing genuine agenda items and requested SSO re-enrolment, thereby increasing urgency and plausibility. Our logs showed that agents didn’t link requests to tickets, failed to call back to a verified number, and didn’t obtain step-up approval for privileged accounts.

For remediation, we enforced ticket-first handling, required mandatory call-backs to verified directory numbers, and mandated step-up approval for MFA resets involving councillors, executives, and administrators. JUMPSEC updated service desk scripts to include firm refusal wording and escalation triggers for authority and urgency cues. We revised identity policies to block MFA removal except under break-glass criteria with dual approval. JUMPSEC detected sequences of reset attempts and mailbox rule creation. During a short verification window, we recorded consistent refusals without ticket linkage, prompt escalations to Information Governance, and clean re-enrolment flows before the next cabinet cycle.

Service Overview

JUMPSEC conduct controlled simulations of real-world phishing and voice pretexts to measure susceptibility, reporting behaviour, and control effectiveness. Campaigns mirror credible attacker tradecraft and run in defined windows with clear safety gates. Evidence demonstrates risk using benign artefacts rather than collecting real credentials or sensitive data. Outputs prioritise measurable improvements to identity controls, service-desk verification, training, and communications.

Objectives

- Quantify susceptibility and reporting rates across agreed populations
- Exercise verification steps for high-risk requests such as MFA resets and payment changes
- Surface process gaps, escalation friction, and tooling limitations
- Deliver specific, testable improvements with owners and acceptance criteria

Approach

Work begins with scenario design aligned to business processes and peak-risk periods. Campaigns use privacy-preserving landing pages, unique tokens, and consented call handling where voice is in scope. Operations adapt to live responses and maintain an authority matrix for pauses, messaging, and escalation. Stakeholders include Security, Service Desk, HR, Finance, and Communications.

Method

- **Plan** — confirm objectives, target cohorts, channels, safety gates, escalation, and evidence handling
- **Prepare** — craft pretexts, benign landing pages, tracking, and voice scripts with harm minimisation
- **Execute** — run campaigns in agreed windows, observe verification steps, and capture response timing
- **Analyse** — map behaviours to control gaps, training needs, and process weaknesses
- **Debrief** — present outcomes, owners, acceptance tests, and a retest path

Deliverables

- Executive briefing summarising susceptibility, reporting latency, and material risks by cohort
- Phishing and Vishing Assessment Report covering scenario design, artefacts, behaviour metrics, verification outcomes, and precise improvements for identity, process, and comms
- Issue register (CSV/XLSX) assigning actions, owners, due dates, and acceptance criteria
- Optional awareness and enablement pack including targeted micro-lessons, mailbox banners, service-desk scripts, and supplier-change verification templates

- Optional verification confirming improvement after focused retests
- Standards and alignment embedded in reporting, referencing NCSC guidance on phishing and suspicious email reporting, NIST control families for awareness and identity processes, and relevant regulatory expectations where payments or citizen communications are affected

Outcomes and benefits

- Lower risk of credential theft, payment redirection, and malicious account changes
- Clear verification steps and faster escalation for high-risk requests
- Targeted training that addresses observed behaviours rather than generic advice
- Assurance artefacts suitable for governance, audit, and insurer dialogue

Pricing model

Fixed price per campaign package or time-and-materials for bespoke programmes. Price drivers include target count, channel mix, language variants, pretext complexity, and retest depth.

Timelines

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

Team and roles

- Engagement Lead for governance, ethics, and quality
- Social Engineering Specialist(s) for scenario design and execution
- Coordinator for logistics, inbox routing, hotline monitoring, and action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Approve targets, pretexts, comms, and safety gates
- Provide routing for staff reports and hotlines and coordinate supplier

JUMPSEC responsibilities

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

participation where service desks are outsourced

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 simulations; no malware and no collection of real credentials
- Call recording only with prior written consent and in line with policy and law
- Third-party and service-desk participation requires written approval
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Social Engineering Testing
- Cyber Incident Exercising (NCSC Assured)
- Incident Response Retainers

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com