
# Social Engineering

## Service Definition Document

January 2026

HM Government
G-Cloud
Supplier

# Document Control

| | | | |
|---|---|---|---|
| **Document Type** | Confidential - Customer Facing | | |
| **Company** | Maple Networks | | |
| **Address** | The Print Rooms<br>164/180 Union Street<br>London<br>SE1 0LH | | |
| **Primary Contact** | Graham Tetley | **Role** | CTO/Lead Consultant |
| **Phone Number** | 020 3858 0048 | **Email address** | gt@maple-networks.com |



# Revision History

| Issue Date | Author | Version | Revision Description |
|---|---|---|---|
| 24/06/2025 | Jonny Zammer | 0.1 | Initial Draft |
| 29/01/2026 | Tim Luck | 0.2 | Updates for G-Cloud 15 |

HM Government
G-Cloud
Supplier

# Table of Contents

## Contents

HM Government
G-Cloud
Supplier

# Services Overview

Maple Networks are next generation Digital and IT service provider in the UK, with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks' Social Engineering services.

HM Government
G-Cloud
Supplier

# Service Description

## Maple Networks Social Engineering

Modern attacks typically don't start with exploits, they start with people. Our Social Engineering services simulate real-world adversary behaviour to test whether your organisation can be manipulated into granting access, disclosing sensitive information, or bypassing security controls.

We assess technology, people, and processes using realistic, intelligence-led attack scenarios, helping organisations understand real risk and strengthen their security posture.

Different types of Maple's Social Engineering services are outlined below:

### Cyber Social Engineering

Cyber Social Engineering uses electronic communication channels to influence staff and test organisational resilience against phishing and impersonation attacks. Engagements are tailored using open-source intelligence (OSINT) to replicate realistic threat actor techniques.

**What We Test**

- Email
- SMS (text messaging)
- Voice / telephone
- Collaboration platforms (e.g. Microsoft Teams, Slack)

**Core Techniques**

- Email Phishing (mass, spear, and whaling)
- SMS Phishing (Smishing)
- Voice Phishing (Vishing)
- Direct Message Phishing (DMishing)
- Phishing Susceptibility Audits (technology-focused)

### Phishing Susceptibility Audit (Technology-Focused)

The Phishing Susceptibility Audit assesses whether your technical controls can prevent or detect modern phishing techniques without relying on user behaviour.

**Scope Includes**

- Domain spoofing
- Third-party and supply chain impersonation
- Abuse of trusted email infrastructure
- Attachments, links, OAuth abuse, and session token theft
- Proxy and web filtering effectiveness

### Physical Social Engineering

Physical Social Engineering tests whether attackers can bypass physical controls and manipulate staff to gain access to restricted areas, sensitive information, or critical assets.

Engagements are often combined with cyber assessments to demonstrate end-to-end compromise.

HM Government
G-Cloud
Supplier

**Service Options**

- Covert Intrusion Assessments
- Overt Intrusion Assessments
- Physical Security Audits

**What We Test**

- Access controls, badges, and visitor processes
- Staff responses to social engineering and impersonation
- Physical security technologies and procedures
- Detection, response, and escalation capability

**Physical Security Audits**

An open review of physical security controls, conducted either as a walkthrough or following an intrusion assessment.

**Focus Areas**

- Policy enforcement (e.g. clear desk, visitor handling)
- Access control and surveillance effectiveness
- Everyday security behaviours and oversight gaps

## *Service Package*

| | |
|---|---|
| **Objective** | To assess an organisation's resilience to social engineering attacks by simulating realistic cyber and physical threat scenarios, identifying weaknesses across people, processes, and technology, and providing actionable remediation guidance. |
| **Description** | Social Engineering testing replicates real-world attacker techniques to evaluate whether staff can be manipulated into disclosing sensitive information, granting access, or bypassing security controls. Engagements are intelligence-led, using OSINT and realistic pretexts across digital and physical channels, and can be conducted as standalone or chained assessments. |
| **Hosted In** | Customer environment (remote and/or on-site), using controlled infrastructure and tooling operated by Maple Networks. No customer data or systems are permanently hosted by Maple Networks as part of testing. |
| **Supported from** | Primarily UK-based delivery, with remote support available globally. Physical testing subject to location, legal, and regulatory considerations. |
| **Testing Areas** | Scenarios would include (but not limited to):<br>• Email phishing (mass, spear, whaling)<br>• SMS phishing (smishing)<br>• Voice phishing (vishing)<br>• Direct message phishing (e.g. Teams, Slack)<br>• Phishing susceptibility (technology-focused)<br>• Physical intrusion and impersonation<br>• Physical security controls and procedures<br>• Staff awareness and response behaviours |

HM Government
G-Cloud
Supplier

| | |
|---|---|
| **Process** | • Scoping & Objectives: Define goals, constraints, and success criteria<br>• Intelligence Gathering: OSINT and reconnaissance to develop realistic pretexts<br>• Attack Simulation: Controlled execution of agreed cyber and/or physical scenarios<br>• Observation & Evidence: Document access paths, responses, and control failures<br>• Reporting & Debrief: Clear findings, impact assessment, and prioritised remediation recommendations |
| **Output** | A structured report outlining tested scenarios, identified vulnerabilities, demonstrated impact, and prioritised remediation actions, supported by executive and technical debriefs. |