

The UK SMB Security Benchmark

Anonymised insights from 531 public-passive scans across 16 UK sectors. Per-cohort medians, score distributions, and the most prevalent issues per sector.

531 **16** **0** **28 May 2026**
TOTAL SCANS SECTORS COMPOSITE SIGNALS GENERATED

Headline findings

- 100%** 100% of UK general sites scanned have "Does not meet bulk-sender email requirements"
- 96%** 96% of UK manufacturing sites scanned have "Email authentication grade: F (0/100)"
- 96%** 96% of UK legal sites scanned have "UK GDPR: 4 UK GDPR gaps detected — Article 32 requires "appropriate technical measures""
- 91%** 91% of UK general sites scanned have "Content Security Policy missing"
- 85%** 85% of UK general sites scanned have "Missing HSTS header"
- 60%** 60% of UK charity-non-profit sites scanned have "Hidden iframe injection (1x1 or display:none)"
- 49%** 49% of UK general sites scanned have "Homepage unreachable"
- 46%** 46% of UK media-publishing sites scanned have "EU NIS2: Sector suggests NIS2 may apply — 3 baseline cybersecurity gaps"

Sector cohorts

Median score, cohort size, top three issues per sector. SOURCE Anonymous SiteIntel Mode 1 scans.

Sector	Median Score	Cohort Size	Issue	Prevalence
General	61 _{/100}	n=138	Homepage unreachable	49%
			No modern TLS protocol supported	25%
			No TLS certificate	24%
			TLS certificate expired	1%
			Possible Generic API Key in rendered page	1%
			Does not meet bulk-sender email requirements	1%
E-commerce	70 _{/100}	n=138	Homepage unreachable	49%
			No TLS certificate	25%
			next@unknown — CVE-2025-29927 (CVSS 9.1)	24%
			No modern TLS protocol supported	1%
			Does not meet bulk-sender email requirements	1%
			Does not meet bulk-sender email requirements	1%
Healthcare	74 _{/100}	n=58	next@unknown — CVE-2025-29927 (CVSS 9.1)	9%
			Homepage unreachable	5%
			CVE-2024-45440: 87.5% exploitation probability	3%
			No modern TLS protocol supported	2%
			Does not meet bulk-sender email requirements	95%
			Does not meet bulk-sender email requirements	95%
Financial services	75 _{/100}	n=58	next@unknown — CVE-2025-29927 (CVSS 9.1)	9%
			No modern TLS protocol supported	5%
			CVE-2024-45440: 87.5% exploitation probability	3%
			Homepage unreachable	2%
			Does not meet bulk-sender email requirements	95%
			Does not meet bulk-sender email requirements	95%
Legal	73 _{/100}	n=51	next@unknown — CVE-2025-29927 (CVSS 9.1)	8%
			Public bucket listing: azure-blob — feaasstatic/assets	6%
			No modern TLS protocol supported	4%
			Login form uses GET method (credentials in URL)	4%
			No TLS certificate	4%
			Does not meet bulk-sender email requirements	95%
Media & Publishing	72 _{/100}	n=51	Possible Generic API Key in rendered page	8%
			Homepage unreachable	6%
			next@unknown — CVE-2025-29927 (CVSS 9.1)	4%
			CVE-2024-45440: 87.5% exploitation probability	4%
			Does not meet bulk-sender email requirements	4%
			Does not meet bulk-sender email requirements	95%

SaaS / Technology n=40

77_{/100}

median · p25 72 · p75 78

CRITICAL	next@unknown — CVE-2025-29927 (CVSS 9.1)	5%
CRITICAL	CVE-2024-45440: 87.5% exploitation probability	3%
CRITICAL	Possible Generic API Key in rendered page	3%
HIGH	Does not meet bulk-sender email requirements	100%
HIGH	Hidden iframe injection (1x1 or display:none)	43%

Manufacturing

71_{/100}

median · p25 65 · p75 77

CRITICAL	No modern TLS protocol supported	
CRITICAL	Homepage unreachable	
CRITICAL	No TLS certificate	
CRITICAL	CVE-2024-45440: 87.5% exploitation probability	
CRITICAL	.git/config exposed (full source code recoverable)	

charity-non-profit n=15

74_{/100}

median · p25 70 · p75 76

CRITICAL	No modern TLS protocol supported	7%
CRITICAL	No TLS certificate	7%
CRITICAL	Homepage unreachable	7%
CRITICAL	CVE-2024-45440: 87.5% exploitation probability	7%
HIGH	Does not meet bulk-sender email requirements	100%

public-sector

68_{/100}

median · p25 64 · p75 70

CRITICAL	OpenAI API key exposed in page source	
HIGH	Does not meet bulk-sender email requirements	
HIGH	Missing HSTS header	
HIGH	Content Security Policy missing	
HIGH	Homepage returned HTTP 403	

retail n=7

59_{/100}

median · p25 59 · p75 63

CRITICAL	Homepage unreachable	57%
HIGH	Content Security Policy missing	100%
HIGH	Missing HSTS header	100%
HIGH	Does not meet bulk-sender email requirements	100%
HIGH	No SPF record	29%

education

75_{/100}

median · p25 70 · p75 75

CRITICAL	lodash@unknown — CVE-2019-10744 (CVSS 9.1)	
HIGH	Does not meet bulk-sender email requirements	
HIGH	No DKIM records found	
HIGH	Missing HSTS header	
HIGH	Content Security Policy missing	

technology n=3

64_{/100}

median · p25 54 · p75 64

CRITICAL	No modern TLS protocol supported	67%
CRITICAL	Homepage unreachable	33%
HIGH	Does not meet bulk-sender email requirements	100%
HIGH	Missing HSTS header	67%
HIGH	Content Security Policy missing	67%

media

59_{/100}

median · p25 59 · p75 59

CRITICAL	Homepage unreachable	
HIGH	Content Security Policy missing	
HIGH	Missing HSTS header	
HIGH	Does not meet bulk-sender email requirements	
HIGH	No DKIM records found	

hospitality n=2

67_{/100}

median · p25 67 · p75 67

HIGH	Does not meet bulk-sender email requirements	100%
HIGH	Missing HSTS header	100%
HIGH	Content Security Policy missing	50%
HIGH	No DKIM records found	50%
MEDIUM	UK GDPR: 3 UK GDPR gaps detected — Article 32 requires "appropriate technical measures"	100%

real-estate

75_{/100}

median · p25 75 · p75 75

HIGH	UK GDPR: 4 UK GDPR gaps detected — Article 32 requires "appropriate technical measures"	
HIGH	Content Security Policy missing	
HIGH	Does not meet bulk-sender email requirements	
MEDIUM	Missing Content-Security-Policy	
MEDIUM	No cookie consent banner detected	

Methodology

- **Scope.** SiteIntel Mode 1 (Public Passive) — 46 checks across DNS, TLS, headers, supply-chain, breach exposure, threat intel. No active testing or login attempts.
- **Corpus.** Public UK sites from FCA register, IMRG Top 500, ABPI member list, The Lawyer 200, Make UK members, Press Gazette Top 50. Anonymised at ingest (domain hashed, no identifying metadata persisted).
- **Score.** Composite 0-100; weighted across security, performance, SEO, accessibility, tech-debt.
- **Composite signals.** Pairs of finding codes with $\geq 5\%$ co-occurrence (support) and $\geq 1.5\times$ score-drop lift versus sector baseline. Information-severity findings excluded.
- **Cohort floor.** Sectors with < 5 scans excluded from percentile reporting.
- **Refresh.** Aggregate cached 1 hour; corpus grows continuously as new scans land.
- **Identification.** No individual sites named in this report. Cohort sizes published; underlying scan IDs and domain hashes are not.

© 2026 SiteIntel - siteintel.luk - Generated 28 May 2026