How UK Councils Look to an External Security and Privacy Scan

A September 2026 baseline of 379 council websites across England, Wales, Scotland and Northern Ireland, written for people who do not work in cyber security

Second edition, 15 September 2026. The exposed-service and software-weakness findings have been re-examined and corrected; see overleaf.

> **What this report is**
>
> We looked at every council website in our tracked estate from the outside, the way any member of the public could, and recorded what was visible. We did not log in anywhere, try any password, or touch anything inside a council's systems. This report says what we saw, what it means in plain English, and what is worth doing about it.

Sources	Four separately tracked national estates, reported separately: **England 314 websites**, **Wales 22**, **Scotland 32** and **Northern Ireland 11**.
Combined	No website appears in more than one estate, so the four together represent **379 distinct websites**. This was checked rather than assumed.
Evidence	One assessment, 9 September 2026. **All 379 completed and none failed.** 293 produced an exact score and 57 a floor score, so 350 carry a published figure. 29 produced no score but still produced findings, which are counted throughout.
This edition	On 15 September 2026 we re-read the same evidence to establish **who each exposed service actually belongs to**. No count changed and no score changed. What changed is the reading: **ten of the seventeen exposed services turned out to be a hosting provider's own equipment, not a council's.** This edition supersedes the first at the same address.
Limits	Nothing here says any council has been broken into. Nothing here is a legal or compliance judgement. Everything here is what was visible from outside on one day.
Prepared by	Huro Data Technologies Ltd / MyDomainRisk
Date	Assessed 9 September 2026 | this edition 15 September 2026

Research and external assessment: MyDomainRisk | Huro Data Technologies Ltd

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Executive summary

The four things that need attention

1. Stolen staff passwords are circulating for a third of councils. 122 websites, 501 records. These are keys to the council's own systems and the council can take them back today.

2. Sixty-three councils do not force visitors onto a secure connection. Anything typed into those pages can be read or altered on the way. This is the largest concrete job in the report.

3. Two councils run software with a weakness criminals are known to be using now, listed in the public catalogue of weaknesses being exploited in the real world rather than merely recorded somewhere. One sits on an address registered to the council itself, on web server software past the end of its supported life.

4. Seven councils have a service answering the internet that probably should not be, three of them a database. The first edition of this report said seventeen and thirteen. Re-reading the same evidence to establish whose equipment answers, ten turn out to be a hosting provider's own machinery, replying on dozens of ports for every customer behind it, all ten in England. No score or average changed; section 11 sets out the working.

Everything above is small in count and serious in kind. None of it means a council has been broken into, and every item needs checking privately first. Together they involve fewer than 200 of the 379 websites, which makes them finishable. **Five councils have a confirmed lowest-band score**, all in England.

What we found, worst first

What it is, in plain English	Why it matters	Websites
Software weakness known to be exploited now	In the public catalogue of weaknesses criminals are using. 11 more were read from version numbers only.	**2**
A database answering the internet, on council hosting	Databases hold records. They belong behind the website, not beside it.	3
Any risky service reachable, on council hosting	Remote access, file transfer, admin tools. The 3 databases are inside this 7.	7
Cannot stop email being forged in the council's name	Residents act on council emails fast. The cheapest item here to fix.	17
Visitors not forced onto a secure connection	The largest concrete job here, and the one a resident could notice.	63
Staff passwords in criminal collections	Harvested by viruses on individual computers. 501 records.	122
Staff identities exposed on other companies' platforms	Work email addresses used to sign in elsewhere. 929 records.	216
No cookie consent mechanism detected	The regulator actively tests this. Needs checking in a browser.	243

Rows overlap and must never be added. Residents' own account details circulate for 358 councils, 46,137 records, covered in section 9. A further 22 councils have a certificate or outdated-encryption problem, and **10 cases are deliberately absent**: ports answering on a hosting provider's own equipment, corrected in this edition.

Executive summary, continued

Stolen passwords, and why this is the finding to read twice

What a criminal collection actually is

When a virus infects somebody's computer it copies every username and password saved in the browser, and those get bundled up and traded. If a member of staff ever saved a work login on an infected machine, their council address and password can end up on a list anyone can buy. We never see or try those passwords, only that records exist against a council's domain and how many. **We cannot tell whether any still works**, only that the material is out there.

122	4	0
councils with staff passwords circulating, 501 records	records on a typical affected council: wide, not deep	ransomware listings, breach records or browser warnings anywhere

The shape matters. Four records on an affected council, 501 across UK local government, is modest for a sector employing over a million people. Broad and shallow: many councils with a handful each, not a few with hundreds. **That makes it finishable.** A reset, a multi-factor check and an ended session deals with most of it.

Why some councils have a floor score rather than an exact one

The change that matters for reading every table in this report

Some council websites answer an automated visitor with a protection page rather than the real homepage. That is a security control working, not a fault, but it means we cannot read the instructions the site sends to a browser, and those form part of the score. For **57 councils** that was the only gap, so we publish a **floor score**: every unread instruction counted as absent, "at least this much", so **the true figure can only be the same or higher**. For **29** a second piece was missing too, so no score is published, though their other findings still count throughout.

Scores	Websites	Average
Exact scores	293	75.6
Floor scores, counted at their floor	57	59.3
All published figures, 350 of 379	**350**	**72.9**

Use 75.6 for the sector's measured position and 72.9 for the most cautious one. Were every unread instruction in place, those 57 councils would average 80.4 rather than 59.3. The truth sits between. The remaining 29 have no published figure at all.

What is going well, and it is worth saying

227 councils, six in ten, instruct other mail systems to refuse email forged in their name, and only 17 have not started. Getting there means listing every system that sends mail in a council's name and testing before enforcing, or genuine letters to residents bounce. Councils have largely done it, with no law requiring it, and **378 of 379 publish the record identifying their own mail servers.**

Exact-score averages sit within two points of each other, 74.5 in Wales to 76.7 in Scotland, but **will not carry a league table**: the evidence behind each differs and only Northern Ireland needed no floor scores.

Why this matters for a council in particular

A council is the organisation a resident cannot choose not to deal with. Council tax, housing, school places, planning, benefits, bin collections, parking, social care: every one of those leaves personal information with an authority the resident has no realistic option to take elsewhere. That is a different relationship from the one a customer has with a shop, and it changes what a failure means.

It also changes what impersonation means. A message that appears to come from a council carries the weight of an institution with legal powers. A demand for council tax, a notice about a benefits claim or a parking penalty gets acted on quickly, and often by the people least able to absorb the loss.

A way of picturing what we did

> **Somebody walking down your street**
>
> They never go inside any building and never try a door. They walk past and notice what is visible from the pavement: a window left open, a side gate unlatched, a spare key under the mat where everyone knows to look.
>
> None of that means the house has been burgled. It means somebody passing by can see opportunities, and most of them take a minute to put right.

That is exactly this assessment. We looked at each council from the public internet, the way any resident or anyone with worse intentions would see it. When this report says staff passwords are circulating, that is the spare key under the mat: it does not mean anyone has used it, but somebody else knows where it is. When it says a service is reachable that need not be, that is the side gate nobody remembers leaving unlatched. And when a council's website turns our scanner away, that is a locked gate doing its job, which is why those councils get a floor score rather than a mark against them.

> **What we could not see, which is most of it**
>
> Standing in the street tells you nothing about the alarm, the safe or the locks on the internal doors. Many of these councils will have good protections we simply cannot observe: staff training, backups, monitoring, incident plans, internal access controls, everything inside the building.
>
> So nothing in this report is a verdict on any council's security. It is an account of what is showing from outside, which is a useful thing to know precisely because it is what a criminal sees too.

Three cautions that apply to every number in this report

A finding is not a break-in. Nothing here establishes that any council has been compromised, and every serious item needs the council to check it privately before anyone treats it as fact.

A floor score is not a bad score. Fifty-seven councils carry one, and each could sit substantially higher. They should never be compared with exact scores or ranked against them.

Nothing here is a compliance judgement. We observe technical settings. We cannot see contracts, retention, staff training or how personal information is actually handled, and this report never pretends otherwise.

1. The words used in this report

This section exists so that nothing later needs a specialist to interpret. Each term is given the way it is used here, not as a formal definition.

Term	What it means in this report
Cyber posture	The condition of an organisation's defences at a point in time, as seen from outside. If a stranger looked at your council from the public internet, what could they learn?
Criminal credential collection	A traded list of usernames and passwords, mostly harvested by viruses from the browsers of infected computers. Also called infostealer data.
Floor score	A score published as "at least this much" where one part of the check could not be read. Every unread item is counted as missing, so the true figure can only be the same or higher.
Forged email, and the setting that stops it	Anyone can put a council's name on an email. A published instruction called a **DMARC policy** tells receiving mail systems to refuse those forgeries. It can be set to refuse, to send to spam, or to do nothing.
Secure connection	The padlock. A page served over HTTPS is encrypted in transit; one served over plain HTTP can be read or altered on the way. Forcing every visitor onto the secure version is a setting.
Exposed service	Something answering the public internet that normally faces inwards: a database, a remote-access tool, a file-transfer or admin console.
Known-vulnerability evidence	A public source records a documented weakness against software the website appears to be running. It may already be patched; it needs checking.
Cookie consent mechanism	The banner that asks permission before storing things on a visitor's device. The law governs what may be stored before a choice is made.
Website instructions to the browser	Settings a website sends telling the browser how to treat the page. Their absence is a review point, not a hole. These are the items a floor score counts as missing.
Certificate	The credential that proves a website is who it claims to be and enables the padlock. It can expire or be misconfigured.

> **Security is cumulative, which is why there is no single fix**
>
> A strong position is rarely one product. It is the combined effect of many ordinary settings done properly: strong sign-in, sensible configuration, secure email, patched software, limited exposure to the internet, knowing what suppliers hold, a clear route for someone to report a problem, and a plan for when something goes wrong.
>
> That is also why a good score can sit alongside a real finding, and why one serious item can hold an otherwise well-run website down a band.

2. Where councils sit in the rules

Councils occupy an unusual position, and it explains a good deal of what this report found.

Security: no legal duty specific to councils

Councils hold some of the most sensitive personal information in the public sector and run services residents cannot get anywhere else. Yet **they are not designated as operators of essential services** under the main UK cyber security regulations, and there is no dedicated regulator for council cyber security the way there is for aviation or energy.

What exists instead is help rather than obligation. The government adapted the National Cyber Security Centre's Cyber Assessment Framework for local government, working with councils, and published it as a tool authorities can use to assess themselves.[2] The Cyber Security and Resilience Bill, currently before Parliament, largely leaves councils outside its scope: it targets essential service operators, digital providers, data centres, managed service providers and designated critical suppliers. The Local Government Association supports the supply chain and incident reporting parts while pressing for clarity, support and realistic timescales, noting legacy systems and limited in-house expertise.[3]

> **A result worth sitting with**
>
> On the one control this assessment measures that most directly protects residents from being defrauded in a council's name, local government performs strongly, and it does so with no law compelling it. That is an argument about what shared support and central guidance achieve, and the evidence makes it rather than us.

Data protection: a duty that does apply, directly

Where the security regime is voluntary, data protection is not. Councils are legally responsible for the personal information they hold about residents under the UK GDPR, and separate rules govern what may be stored on a resident's device when they visit a website. The Information Commissioner's Office regulates both and publishes the guidance that decides whether a particular arrangement is lawful.[4]

> **What this report can and cannot say about that**
>
> We can see whether a website forces a secure connection, whether a privacy policy can be found, whether a cookie banner is present in the page as delivered, and what the website stores. **None of that establishes whether a council is complying with anything.**
>
> We cannot see the lawful basis for any processing, how long information is kept, what contracts are in place with suppliers, whether information leaves the country, how requests from residents are handled, or any of the training and internal controls that make up most of the regime. Those are the substance. We observe the shop window.

How this differs from the statistics you may have seen

Most sector cyber figures come from surveys, which ask organisations what happened to them and what they have in place. This study asked nobody anything. Every number is an observation taken from outside using the same checks on every website. A survey tells you what a sector believes about itself; this tells you what it is showing to the world.

3. What we measured, and how to read the numbers

Each website was checked against the same set of external tests and given a score out of 100 where enough evidence came back. **Good** is 75 or more, **needs improvement** is 50 to 74, and **at risk** is below 50.

Coverage	England	Wales	Scotland	N Ireland	UK
Tracked websites	314	22	32	11	379
Completed a scan	314	22	32	11	379
Exact score	241	19	22	11	293
Floor score	47	3	7	0	57
No score published	26	0	3	0	29
Any published figure	**288**	**22**	**29**	**11**	**350**

Why different numbers here have different denominators

Not every test could answer for every website, so a percentage in this report always states what it is a percentage of. The main groups are:

379 tracked websites, all of which completed a scan, used for stolen-password findings, exposed services and most technical checks. **293 exact scores**, used for the measured average and bands. **350 published figures**, used for the cautious average. And **narrower groups** for individual tests: 315 websites returned a readable page for the browser-instruction checks, 370 gave cookie evidence, 305 could be checked for tracking technology.

Every table shows the count and its denominator together, in the form 200 / 253 readable, with the rate beside it. Where a test returned an unknown for some websites, the denominator is the number that actually answered, because an unknown is not a pass.

Three rules this report follows throughout

Counts are of websites, not of problems. A website with five instances of the same issue counts once. One unpatched piece of software can generate dozens of technical observations, which is why we report the number of councils affected and not the number of observations.

Rows in a table overlap and must never be added. The clearest case: 17 websites have a risky service and 13 have a database exposed, but the 13 are inside the 17. The total is 17 councils, not 30.

Stolen passwords come in three separate populations, covering different people and fixed by different parties. Section 9 sets them out. They are quoted independently and never combined into one headline number.

4. Source one: England, 314 websites

England is 83% of the estate, so its result largely determines the UK figure. All 314 completed a scan. 241 produced an exact score, 47 a floor score and 26 no score. **All five confirmed lowest-band results in the UK are here.**

Band	On exact scores 241 websites	Including floor scores 288 websites
Good, 75 and above	101 (42%)	101 (35%)
Needs improvement, 50 to 74	135 (56%)	179 (62%)
At risk, below 50	5 (2.1%)	8 (2.8%)

Exact average **75.5**, median **74**. Counting the 47 floor scores at their floor gives **72.8**. Those floors average 58.9 and would average 80.2 if every unread instruction turned out to be in place, so the three extra At risk results in the right-hand column may all sit higher.

Observation	Websites	Rate
No cookie consent mechanism detected	200 / 253 readable	79%
Tracking technology present	177 / 253 verified	70%
No privacy policy route found	49 / 243 answered	20%
Visitors not forced onto a secure connection	53 / 294 answered	18%
Risky service reachable, on the council's own hosting	4 / 314 tracked	1.3%
Cannot refuse forged email in the council's name	14 / 314 tracked	4%
Database answering the internet, on the council's own hosting	1 / 314 tracked	0.3%
Outdated encryption still accepted	12 / 297 answered	4%
Software with a publicly listed weakness	9 / 314 tracked	3%
Secure page loading insecure content	7 / 253 readable	3%
Invalid certificate	2 / 308 answered	0.6%
Ransomware, breach or browser-safety findings	**0 / 314 tracked**	**0%**

England carries the whole of this edition's correction. Fourteen websites showed a risky service, but **ten answer from a protection service or shared platform with nothing identified**, so they describe the provider's equipment and are excluded above. Four remain to validate: two with a product identified, one a database, and two with nothing identified. All 227 software-weakness observations were read from version numbers, two websites holding 171 of them, and one carries an actively-exploited catalogue entry on a hosting provider's address.

5. Source two: Wales, 22 websites

Every Welsh website now carries a published figure: 19 exact scores and 3 floor scores, with none left unscored. The exact average is **74.5**, median **74**, the lowest of the four estates, and no website is in the lowest band on either basis.

> **Wales holds both extremes in this study**
>
> **Not one of the 18 readable Welsh homepages showed a cookie consent mechanism.** That is the only estate with a complete absence, and the strongest single prompt for browser testing in the report.
>
> **Every Welsh council can refuse forged email in its name**, 14 set to refuse and 8 to send to spam, with none doing nothing. Wales is the only estate with no gap at all on that control.

Band	On exact scores 19 websites	Including floor scores 22 websites
Good, 75 and above	9 (47%)	9 (41%)
Needs improvement, 50 to 74	10 (53%)	13 (59%)
At risk, below 50	0	0

Counting the three floors at their floor gives **72.8**. Those floors average 62.3 and would average 74.0 with every unread instruction in place, the narrowest gap of any estate.

Observation	Websites	Rate
No cookie consent mechanism detected	18 / 18 readable	100%
Tracking technology present	8 / 18 verified	44%
No privacy policy route found	6 / 17 answered	35%
Mail signing record missing on the names we sampled	5 / 22 tracked	23%
Visitors not forced onto a secure connection	4 / 22 tracked	18%
Outdated encryption still accepted	2 / 21 answered	10%
Risky service, database, listed software weakness	1 each / 22	5%
Forged email, invalid certificate, insecure content, ransomware, breach, browser safety	**0 / 22 tracked**	**0%**

Wales's risky service, exposed database and software weakness are **the same single website**, on ordinary shared hosting where a file-transfer and a database service were both identified by name. Unlike most English cases this is real, not a provider's equipment answering on many ports. Its 32 software observations were all read from version numbers and **none appears in the actively-exploited catalogue**.

6. Source three: Scotland, 32 websites

Scotland has the highest exact average and median of the four, **76.7** and **77.5**, on 22 websites. Seven carry a floor score and three have none, so the exact average describes two thirds of the estate.

Band	On exact scores 22 websites	Including floor scores 29 websites
Good, 75 and above	12 (55%)	12 (41%)
Needs improvement, 50 to 74	10 (45%)	17 (59%)
At risk, below 50	0	0

Counting the seven floors at their floor gives **72.8**. **Scotland has the widest floor-to-ceiling gap of any estate**, 60.6 against 84.6, so those seven websites are the least well understood in the study.

Observation	Websites	Rate
No cookie consent mechanism detected	20 / 23 readable	87%
Tracking technology present, all one product	14 / 23 verified	61%
No privacy policy route found	9 / 22 answered	41%
Mail signing record missing on the names we sampled	6 / 32 tracked	19%
Visitors not forced onto a secure connection	6 / 32 tracked	19%
Outdated encryption still accepted	2 / 31 answered	6%
Secure page loading insecure content	1 / 23 readable	4%
Software weakness in the actively-exploited catalogue	**1 / 32 tracked**	**3%**
Risky service reachable, forged email gap	1 each / 32	3%
Database exposed, invalid certificate, ransomware, breach, browser safety	**0 / 32 tracked**	**0%**

The single most specific finding in the whole study is in Scotland

Scotland's one risky-service case is ordinary hosting with nothing identified on the flagged port, so the first question there is whether anything is listening. The software weakness is a different website, and a different order of concern. **It runs web server software with two recorded weaknesses. One appears in the public catalogue of weaknesses criminals are known to be exploiting now**, a far shorter and more serious list than "recorded somewhere", and the product is marked past the end of its supported life, so no more fixes are coming. What makes it stand out is the address: most exposure evidence here points back at a hosting company, but **this one is registered to the local authority itself**, so there is no ambiguity about who owns it. Both observations were read from a version number rather than confirmed, so check the running version first, quietly and directly with the council. **If one thing in this report is acted on this week, it is this.**

Council identities on other companies' platforms reach 78% of Scottish websites, against 55% in England and the widest footprint in the study: work email addresses used to sign in elsewhere, not anything on a council system. Credential figures for all four estates are compared in section 9.

7. Source four: Northern Ireland, 11 websites

Northern Ireland is the only estate where every website produced an exact score. No floor scores were needed anywhere, which means it is also the only estate whose figures are fully comparable within themselves. The average is **76.5**, median **76**.

> **Complete evidence is not the same as a good result**
>
> Full coverage means the information was collectable, not that the estate is in good order. Northern Ireland has the highest rate of certificate and encryption findings of any estate, 4 of 11, the highest rate of councils unable to refuse forged email, 2 of 11, and the lowest payment-surface score of the four. Those things are easy to confuse and this is the clearest illustration of the difference in the study.

Band	Websites	Share of 11
Good, 75 and above	6	55%
Needs improvement, 50 to 74	5	45%
At risk, below 50	0	0%

Observation	Websites	Rate
Tracking technology present	10 / 11 verified	91%
No published route to report a security problem	7 / 9 answered	78%
No cookie consent mechanism detected	5 / 11 readable	45%
Outdated encryption still accepted	**4 / 11 tracked**	**36%**
No privacy policy route found	2 / 10 answered	20%
Cannot refuse forged email in the council's name	2 / 11 tracked	18%
Risky service and exposed database on one website, insecure content on another	1 each / 11	9%
Listed weakness, invalid certificate, insecure connection, ransomware, breach, browser safety	**0 / 11 tracked**	**0%**

Its single exposed service is genuine: ordinary hosting with a database identified by name, one of only three identified council databases in the UK. There was no software-weakness evidence at all here. **Northern Ireland also has the lowest credential exposure in the study on all three populations.** On an estate of eleven a single council moves any percentage by nine points, so nothing on this page is a rate that would hold at larger scale.

8. The four estates compared, and the UK total

All four were assessed the same day with the same checks. **This is not a league table.** Northern Ireland needed no floor scores while Scotland needed seven on 32 websites, so the estates do not carry equal evidence and their averages should not be ranked.

Measure	England	Wales	Scotland	N Ireland	UK
Websites, all completed	314	22	32	11	379
Exact / floor / no score	241/47/26	19/3/0	22/7/3	11/0/0	293/57/29
Exact average / median	75.5 / 74	74.5 / 74	76.7 / 77.5	76.5 / 76	75.6
Cautious average, floors at floor	72.8	72.8	72.8	76.5	72.9
Confirmed lowest band	5	0	0	0	5
Risky service, all cases	14	1	1	1	17
of which on the council's own hosting identified databases: 1 / 1 / 0 / 1, UK 3	**4**	**1**	**1**	**1**	**7**
Software weakness read from a version	9	1	1	0	11
Weakness in the actively-exploited catalogue	**1**	**0**	**1**	**0**	**2**
Staff passwords in criminal lists	33%	36%	28%	18%	32%
Identities on other platforms	55%	59%	78%	36%	57%
Cannot refuse forged email	4%	0%	3%	18%	4.5%
Certificate or encryption finding	4%	9%	6%	36%	5.8%
No consent mechanism detected	79%	100%	87%	45%	80%

Wales at 22 and Northern Ireland at 11 are small populations where one council moves a percentage by several points.

What is national, and what is local

Four findings hold everywhere. Forged email is refused or filed to spam almost universally. Genuinely exposed services are rare, seven websites in 379. Consent mechanisms are weakly detected everywhere. And every estate returned nothing on ransomware, breach records and browser safety warnings.

Three findings are local and should not be generalised. Certificate and encryption problems are 4% in England against 36% in Northern Ireland, identities on other companies' platforms 78% in Scotland against 36% in Northern Ireland, and all five confirmed lowest-band results are English.

One pattern appears only once you ask who owns the equipment. All ten provider-infrastructure cases are English, while each smaller estate has exactly one risky-service case and all three are genuine.

The UK total

No website appears in two estates, so the four can be added: **379 distinct websites**, all completed. On exact scores the average is **75.6** across 293, banding 128 Good, 160 needing improvement and 5 at risk. Counting the 57 floor scores at their floor gives **72.9** across 350, banding 128, 214 and 8. **The three extra at-risk results are floor figures and may sit higher.**

9. Stolen credentials: three different problems

This is the largest and most misunderstood body of evidence in the report. The provider returns three separate populations, they concern different people, they are fixed by different parties, and **they must never be added into one number**. Counts were returned and reconciled for all 379 websites.

Population	Who it concerns, and who can act	Websites	Rate	Records
1. Staff	Accounts on the council's own domain. **The council can fix these today** by resetting the password, ending active sessions and confirming multi-factor sign-in.	122 / 379	32.2%	501
2. Identities elsewhere	Council email addresses used to sign in to other companies' platforms. The council can act, but the reset happens on the other company's system.	216 / 379	57.0%	929
3. Residents	Members of the public with an account on a council service, whose own device was infected. **Nobody at the council can reset these.** Only the resident can.	358 / 379	94.5%	46,137
1 or 2	**Deduplicated. Not 122 plus 216.**	**229 / 379**	**60.4%**	**n/a**

Why the order matters more than the size

The staff population is the one that matters and it is the smallest. It is a key to the council's own systems, the council issued it, and the council can take it back this afternoon.

The identities-elsewhere population follows closely, because a work address reused across several platforms is how one compromise becomes several.

The residents population is ninety times larger and ranks last. It is not access to anything the council runs. It is a resident's own laptop that caught a virus. It carries no weight in the score and nobody at the council can reset it. It is a duty-of-care and communication question, not a security hole.

Reported as one total of 47,567 this would describe a sector in serious trouble. Reported as three populations it describes a manageable job, a wider hygiene question, and a public-protection issue belonging to a different team.

What 'identities elsewhere' does not mean

It counts **the council's own email addresses appearing on somebody else's platform**. It is **not** a count of suppliers holding access into the council, which is close to the opposite. Described that way it would claim something this study has not measured, so we never call it a supplier figure.

9 continued: the four estates side by side

Websites carrying records	England of 314	Wales of 22	Scotland of 32	N Ireland of 11	UK of 379
1. Staff	103 (33%)	8 (36%)	9 (28%)	2 (18%)	122 (32%)
2. Identities elsewhere	174 (55%)	13 (59%)	25 (78%)	4 (36%)	216 (57%)
3. Residents	303 (96%)	19 (86%)	29 (91%)	7 (64%)	358 (94%)
1 or 2, deduplicated	**184 (59%)**	**14 (64%)**	**26 (81%)**	**5 (46%)**	**229 (60%)**

Records, and how many per affected website	England	Wales	Scotland	N Ireland	UK
1. Staff	438	14	46	3	501
per affected website	4.3	1.8	5.1	1.5	4.1
2. Identities elsewhere	789	28	105	7	929
per affected website	4.5	2.2	4.2	1.8	4.3
3. Residents	42,372	2,007	1,707	51	46,137
per affected website	**140**	**106**	**59**	**7.3**	**129**

Three things only the aggregated view shows

The two populations that matter are wide and shallow. Both sit at roughly four records per affected council across the UK. Many councils with a handful each, not a few councils with hundreds. That is the shape that makes this finishable.

Scotland is the outlier on reach and England on volume. Scotland has the widest footprint, 81% of its websites carrying something the council can act on. England holds 86% of the actionable records, a little ahead of its 83% share of the estate.

The residents population behaves like a different measurement entirely, from 7.3 records per affected website in Northern Ireland to 140 in England. That twentyfold spread tracks population served and how many residents hold online accounts, not security. It is the clearest reason never to fold it in with the other two.

What these records establish, and what they do not

They are public-source records tied to a council's domain, mostly harvested by viruses on individual computers. **We cannot see whether any password still works, whether the account still exists, or when the infection happened.** The source does not tell us how completely it has collected, so we make no claim that this is fresh or complete.

None of it is evidence that a council has been broken into. It is a reason for each council to check its own accounts privately against its own records, and never by trying a recovered password.

10. Cookies, consent and tracking

This is the largest body of evidence in the report and the one that concerns what happens on a resident's own device. It also sits in the regime that applies to councils directly.

> **Read this before the number**
>
> Our privacy check scored **61.8% of the points it was able to assess**. **That is not 62% compliant with anything.** It scores a handful of visible technical settings and nothing about how a council actually handles personal information.

What we looked for	Yes	No	Could not tell	Why it matters
Visitors forced onto a secure connection	296	63	20	Anything typed into an insecure page can be read on the way.
No insecure content on a secure page	296	9	74	A padlock is weakened if parts of the page arrive unprotected.
Privacy policy route found	226	66	87	People should be able to find out what happens to their data.
Cookie consent mechanism found	**62**	**243**	**74**	The law governs what may be stored before a person chooses.
Route to report a security problem	40	247	92	Someone who spots a flaw needs a way to tell the council privately.

243 of the 305 websites we could read showed no consent mechanism, 80%. The national picture varies more here than on any other measure: 53 detections in England, six in Northern Ireland, three in Scotland and none at all in Wales.

> **An absent banner is a reason to look, not a finding**
>
> There are innocent explanations. The site may store only what is strictly necessary, for which no permission is needed. It may use a system our check does not recognise. It may load the banner later than a single page request sees. **And a banner being present proves just as little**: it does not show that refusing is as easy as accepting, or that nothing was stored before the visitor chose.
>
> The only way to settle any of it is to open the site in a browser and watch. That takes about ten minutes per site and needs no specialist.

10 continued: the regulator is testing this

In December 2025 the Information Commissioner's Office reported the result of testing the **top 1,000 websites used in the UK**. It checked three things: whether advertising cookies were stored before consent, whether refusing was as easy as accepting, and whether cookies were placed without permission at all.

564	17	21
of the 1,000 only became compliant after the ICO contacted them	received preliminary enforcement notices	were still non-compliant when the ICO reported

The ICO said it will keep testing the top 1,000 periodically.[5] Two things follow for councils. An absent consent mechanism is not unusual, since more than half of the UK's most-visited websites needed prompting. And more importantly, **the regulator tests precisely the behaviours this scan cannot see**, so our signal is a prompt to look rather than an answer.

> **What a browser check should establish, in order**
>
> **1.** What is stored on the device before any choice is made, and is any of it not strictly necessary. **2.** Is there a refuse option, is it on the first screen, and does it take no more effort than accepting. **3.** Does refusing actually stop the storage, or just record a preference. **4.** Does the same hold on service pages and forms, not just the homepage. **5.** What does each piece of tracking code load, and what leaves the browser when it does.

Tracking technology, and one vendor's dominance

Tracking technology was present on **209 of the 305 websites we could check, 69%**. One product accounts for almost all of it: Google Tag Manager appears on 202 of those 209, so a single company's code sits on roughly two thirds of the readable council web estate. Microsoft Clarity appears on 27, Google Analytics on 3 and Facebook Pixel on 2, and these overlap.

The presence of tracking code proves nothing on its own. It does not show that personal data was sent, that permission was needed, that permission was missing, or what legal role the vendor plays. A tag manager is a container: what it loads and when has to be watched, not assumed. Microsoft Clarity is worth separate attention because it records sessions rather than counting pages, which raises sharper questions about what is captured and whether form fields are masked.

What the websites store

Cookie evidence came back for 370 websites. **164 stored something during the first page visit, 306 items in total.** Of those 164, 65 stored at least one item without the setting that limits it being sent from other websites, 43 without the setting that keeps it off insecure connections, and 21 without the setting that hides it from page scripts.

This only sees what the first page request returns, so the real numbers are higher. Not every item needs every setting, so this is a review list rather than a defect list: each one needs its purpose, lifetime and necessity looked at together, and that same review answers the consent question above.

11. Card payments and the concrete technical work

Councils take card payments at scale: council tax, business rates, parking, licensing, garden waste, leisure, school meals, rents. The card industry's security standard applies wherever an organisation handles card data or runs something connected to a system that does. Most councils will have arranged their payment pages to send the payer to a specialist provider, which keeps as much as possible out of scope.

> **Two things this report is not**
>
> Our payment-surface check scored **89.6% of the points it could assess**. Controls we could not verify were removed from the calculation rather than counted as passes, which is exactly why that number is high. **It does not mean 89.6% compliant.** Three controls could not be answered for a single council in the estate.
>
> And **this is not the scan the card standard requires.** That standard requires quarterly scans by a company specifically approved by the card industry. We are not one, and nothing here can be submitted as evidence of compliance.[6]

One point makes this newly relevant. Under the current version of the standard, quarterly approved scanning now applies even to the lightest category, the one most councils will be in, following a change that became mandatory in March 2025. The reasoning was that sending a payer off to a provider still leaves the council's own page exposed to code injected before the payer ever gets there.[6] **That is the same page carrying the tracking code in section 10.**

Where the concrete work actually is

63	7	2
councils do not force visitors onto a secure connection	have a risky service on their own hosting, 3 of them a database	run software with a weakness known to be actively exploited

Sixty-three is the largest single number of this kind in the report, and the one a resident could notice. A page reached without the padlock can be read and altered on the way, and so can anything typed into it. A further 63 do not tell the browser to stop trying the insecure version at all, which means the first request of every visit is exposed even where a redirect exists. The two belong in one piece of work.

11 continued: who is actually answering

What is answering on the flagged port	England	Wales	Scotland	N Ireland	UK	Databases
A website-protection service sitting in front of many sites answers on dozens of ports for every site behind it	4	0	0	0	4	4
A shared platform address used by several councils no database or other service ever identified	6	0	0	0	6	6
Ordinary hosting, a service identified by name	**2**	**1**	**0**	**1**	**4**	**3**
Ordinary hosting, nothing identified answering	**2**	**0**	**1**	**0**	**3**	**0**
All risky-service cases	**14**	**1**	**1**	**1**	**17**	**13**

Rows are exclusive and sum to the totals. The classification uses only evidence we already held: which company the answering address is registered to, whether more than one council's flagged address sits in the same small block, and whether a named product actually answered. **The top two rows are a question for the provider, not work for a council.** The bottom two rows, seven websites, are the ones to check.

The eleven software-weakness cases produced 261 technical observations between them, 227 on nine English websites, 32 on one in Wales and two on one in Scotland. **Report the eleven, not the 261**, and treat even the eleven carefully: every one of the 261 was read from a version number and **not one was confirmed by the provider running it**. Two websites alone hold 171 of them, both on a widely used web server where suppliers routinely apply fixes without changing the version number, which makes version-read matches overstate the position. Two entries, on two websites, appear in the catalogue of weaknesses known to be actively exploited. **Those two are the ones that matter**, and the Scottish one described in section 6 is the more specific of them.

The 22 certificate and encryption findings split into **20 councils still accepting outdated encryption and 2 with an invalid certificate**. These are different jobs: an invalid certificate is visible to every resident who visits, while outdated encryption is invisible and matters only to an attacker already in a position to use it.

12. Forged email: the sector's best result

Anyone can put a council's name on an email. What stops it reaching the inbox is a published instruction telling receiving mail systems what to do with a message that fails the checks. It can say refuse, send to spam, or do nothing.

What the council publishes	England	Wales	Scotland	N Ireland	UK	Share
Refuse the forgery	193	14	15	5	227	60%
Send it to spam	107	8	16	4	135	36%
Do nothing, monitoring only	12	0	1	2	15	4%
Nothing published, or unclear	**2**	**0**	**0**	**0**	**2**	**0.5%**

Two figures, both true, and they answer different questions. Only 17 councils, 4.5%, publish nothing or monitoring-only, and those are the ones with work to start. But 135 more ask only for spam filing rather than refusal, so 152 do not ask for outright refusal. **The 4.5% identifies who needs to begin; the 60% describes how far the sector has actually got.**

The work behind this is harder than the result suggests. Publishing the instruction takes minutes. Doing it safely does not: a council has to know every system that sends mail in its name, the customer system, the payments provider, the schools mailer, the parking contractor, the consultation platform, the recruitment system, and watch for long enough to be confident, or genuine letters to residents start being refused.

> **Spam filing is a staging post, not a destination**
>
> The right sequence is watch, then file to spam, then refuse. A council already filing to spam has done most of the work and should finish. A council doing nothing should not jump straight to refusal: list the legitimate senders first, or it will stop its own benefits notifications reaching the people who need them.

This describes what a council asks other mail systems to do. It does not prove a forgery would in fact be refused, because receiving systems apply their own judgement, and it does not prove every genuine sender is set up correctly. Supporting records are strong: 378 of 379 councils publish the basic record identifying their mail servers, and 347 had a signing record under the names we sampled, with 31 not found. A name we did not sample may still exist.

13. Two settings almost nobody has, and one dependency nobody records

Setting	Have it	Do not	What it does
Mail server record	378	1	Names which servers may send mail for the council. Near universal.
Mail signing record	347	31	Signs outgoing mail so it can be verified. Sampled, so absence is not conclusive.
Encryption reporting	234	145	Asks other systems to report failures in protecting mail in transit.
Security contact route	53	237	A published file telling a researcher where to report a problem privately.
Certificate authority record	42	337	Names which companies may issue certificates for the domain, so a rogue one is refused.
Signed domain records	**8**	**371**	**Stops someone forging the answer to 'where is this council's website'.**

Eight councils out of 379 have signed domain records, 2%. Seven in England and one in Northern Ireland, none at all in Wales or Scotland. The certificate authority record sits at 11%. **A gap shared by nine councils in ten is a sector fact, not 371 individual failures**, and it is a natural candidate for central guidance rather than 379 separate projects.

The security contact route deserves its own note. 53 councils publish one and 237 do not, with 89 we could not determine. Someone who finds a problem at one of those 237 has no obvious way to tell them privately, which is how problems end up made public instead.[1]

The dependency that is on nobody's risk register

Observation	England	Wales	Scotland	N Ireland	UK
Some form of network concentration	250	21	28	9	308
All address records with one provider	249	9	24	10	292
Mail transport policy finding	184	15	16	9	224
Address flagged on public reputation sources	**6**	**1**	**2**	**0**	**9**

These overlap and must not be added. A flagged address can belong to another organisation sharing the same infrastructure, so ownership needs confirming first.

292 councils, 77%, depend entirely on one company to answer the question 'where is this council's website'. That is not a fault. Concentration is usually the better-resourced and better-run choice, and splitting the job across providers brings its own problems. **The question is whether anyone has written it down.** A council that has consciously accepted a single provider and knows what happens if it fails is in a different position from one that has never considered it, and on this evidence the arrangement is close to universal and unlikely to appear on many risk registers.

Domain expiry and transfer-lock observations are deliberately excluded from this report. The public evidence does not show whether automatic renewal is switched on and is not reliable enough to support a finding either way.

14. The 86 websites we could not fully read

Fifty-seven councils carry a floor score and 29 have no score at all. Together that is 86 websites, 23% of the estate, and the reason is the same for all of them: **their website answers an automated visitor with a protection page rather than the real homepage.**

> **This is a locked gate, not a hole in the fence**
>
> A site that refuses an unknown automated visitor is exercising a security control. It is doing something sensible. The consequence for us is simply that we cannot read the instructions that site sends to a browser, and those are one of the things the score is built from.
>
> Where that was the only gap we publish a floor: every unread instruction counted as missing, so the true figure can only be higher. Where a second piece was also missing, usually the certificate or the connection to the homepage itself, no score is published at all.
>
> **This cannot be fixed from our side.** No amount of rescanning will change it without the council or its provider choosing to let the scanner through. It is not evidence of a problem and should never be reported as one.

Outcome	England	Wales	Scotland	N Ireland	UK
Floor score published	47	3	7	0	57
No score published	26	0	3	0	29
Combined	**73**	**3**	**10**	**0**	**86**

Every one of the 86 was scanned and produced findings, and those findings are counted in every table in this report. Do not put off a real finding because its website has a floor score or none. That is the single most important handling instruction in this document.

What else we could not see

Evidence type, of 379 scanned	Got it	Partly	Could not
Domain registration details	375	0	4
Encryption and certificates	371	0	8
What the website stores on a device	370	0	9
Website instructions to the browser	315	0	64
Other systems on the same infrastructure	143	96	140
Direct mail server test	42	0	337
Cloud storage discovery	**0**	**379**	**0**

These limits apply to scored websites too, so a score does not mean complete evidence and this report never treats it as if it did. Cloud storage could only be partly checked everywhere, which is why that control appears as unknown throughout rather than as a pass. Direct mail server testing ran on 42 websites and still produced no definitive answer.

15. What to do, in order

Ordered by consequence, not ease. These groups overlap and are not a count of separate councils.

1	**Deal with the two actively-exploited weaknesses this week** Start with the Scottish case: an address registered to the council itself, web server software past the end of its supported life, and an entry in the catalogue of weaknesses criminals are using now. The other is on a hosting provider's address and needs the provider brought in. Confirm the running version before anything else, and go to the council privately first.
2	**Check the seven real exposed services, three of them databases** Seven, not seventeen. Four have a service identified by name, one each in England, Wales and Northern Ireland being a database, and three have nothing identified at all on the flagged port, so the first question there is whether anything is listening. Confirm who owns the address and whether the hosting is shared with other customers.
3	**Send the other ten to the provider, not to a council** Ten English cases answer from a website-protection service or a shared platform address. Those ports belong to the provider's equipment, which answers the same way for every customer behind it. Ask the provider to confirm it; do not raise it as a council database, and correct anything already published that did.
4	**Check the five confirmed lowest-band results privately** All five are in England. Confirm each is real and belongs to the council before it is treated as fact. The three further at-risk results are floor scores: resolve them by reading the missing evidence, not by treating them as findings.
5	**Reset the staff passwords** 122 councils, 501 records, roughly four each. Reset, end sessions, confirm multi-factor sign-in, never test a recovered password. Then the 216 councils with identities on other platforms, where the reset happens elsewhere.
6	**Force every visitor onto a secure connection** 63 councils. Pair it with the instruction that stops the browser trying the insecure version first, and test for compatibility before switching it on.
7	**Open the 243 websites in a browser and watch what happens** The largest group in the report and the one that cannot be settled from outside. Ten minutes per site, Wales first, where nothing was detected anywhere.

15 continued: what to do, in order

8	**Finish the email work, carefully** 17 councils publish nothing or monitoring-only: list every legitimate sender, watch, then enforce, never jumping straight to refusal. The 135 filing to spam have done most of it and should complete.
9	**Split the certificate and encryption work** 20 councils accepting outdated encryption and 2 with an invalid certificate are different jobs with different urgency. Verify each before changing anything live.
10	**Publish a route for reporting problems, and look at the near-universal gaps** 237 councils have no security contact route. Signed domain records sit at 2% and certificate authority records at 11% sector-wide, making both a job for central guidance rather than 379 separate projects.
11	**Write down the provider dependency, and handle residents' records proportionately** 292 councils rely on one company for their address records: know the failure route and who owns it, rather than change it. 46,137 resident records need proportionate protection, and no council should be called breached because of them.
12	**Decide whether to let a known scanner through** 86 websites cannot be fully read because their protection turns automated visitors away, which is a legitimate control. The choice is whether a complete external picture is worth letting a known scanner through.

Conclusion

Councils are strong where an attacker would come at them directly, and weak where a regulator would look. Six in ten refuse forged email outright and only 17 have not started. Genuinely exposed services are rarer than we first reported: seven websites in 379, three of them an identified database. There is not one ransomware listing, breach record or browser safety warning anywhere in 379 scans. None of that is required by law, because councils sit outside the main cyber regulations and largely outside the Bill going through Parliament.

The privacy picture runs the other way. **243 websites showed no consent mechanism and tracking code was found on 209**, in the one regime that does apply to councils directly and has a regulator actively testing it. The security rules councils are outside are the ones they are handling well; the data protection rules they are firmly inside hold the largest body of unresolved evidence.

> ### Where the work actually is
>
> **Fewer than 200 websites carry the genuinely serious items.** Two actively-exploited software weaknesses, seven exposed services, five confirmed lowest-band results, 63 without a forced secure connection and 122 with staff passwords circulating. That is a finishable list, not a sector in crisis, and the sharpest items number two.
>
> **243 need ten minutes in a browser.** Cheap to investigate, and the regulator is already testing it elsewhere.
>
> **86 websites need a decision rather than a fix.** Their protection turns our scanner away, which is a control working. Each council can choose whether a complete external picture of itself is worth letting a known scanner through.

Three things this report does not claim. It does not say any council has been broken into: we could not see inside one and did not try. It does not rank the four nations, because the amount of evidence behind each average differs and one estate needed no floor scores at all. And it makes no compliance judgement of any kind, because we observe settings, not lawfulness.

One thing it does claim. Where a finding is concrete, a floor score or a missing score is not a reason to wait. Two actively-exploited weaknesses, seven exposed services, 229 credential cases, 63 insecure connections and 243 consent cases can be worked today, and every one should be checked privately before it is acted on or disclosed.

And one correction it insists on. This edition reports seven exposed services and three council databases where the first reported seventeen and thirteen. No number in the underlying scan changed; we simply established who owned the equipment. Anyone who quoted the earlier figures should use these instead.

About this report

Produced with MyDomainRisk, a tool developed by Huro Data Technologies Ltd, which has a commercial interest in this analysis and declares it here so readers can weigh it. Every observation was made from outside using public websites, domain records, certificates, cookies and public threat intelligence. Nothing was logged into, no password was tried and nothing was exploited. It is not certification, an audit, legal advice or regulatory advice.

How to read the figures

Bands, and what a score is

Good is 75 and above, **needs improvement** is 50 to 74, **at risk** is below 50. One serious finding can hold a website below a band however much else is right. **A score is a floor, not a verdict**: it records what was visible from outside on one day, not internal controls, patching, training, incident readiness or legal compliance.

Exact scores and floor scores

293 websites have an exact score and 57 a floor score, published as "at least this much" where the browser instructions could not be read. **Floor scores count every unread item as missing**, so the true figure can only be the same or higher, and the bands they fall into may be understated. They are never compared with exact scores or used to rank a council. Two averages are given throughout: **75.6** on exact scores alone and **72.9** counting floors at their floor.

Which population each number comes from

Credential findings and exposed services are shares of **379 tracked websites**; bands and averages are shares of the **293 exact** or **350 published** figures as stated. Individual checks use narrower groups, stated in each table. Where a check returned an unknown, the denominator is the number that answered.

Counting

Every figure counts **websites, not problems**. One unpatched service can produce dozens of observations, which is why councils are counted and observations given only as context. Rows overlap and must never be added: the 3 databases sit inside the 7 exposed services, and the 2 actively-exploited weaknesses inside the 11 read from version numbers. The four estates share no websites, so UK totals are true sums.

Exposure figures are reported by owner. Where a flagged port answers from a protection service or shared platform serving many customers, it describes the provider's equipment, not council exposure. Of 17 cases observed, **7 are council exposure and 10 provider infrastructure.**

The two percentage scores are not compliance rates

The privacy check scored 61.8% and the payment-surface check 89.6% **of the points each was able to assess**. Controls that could not be verified from outside were removed from the calculation rather than counted as passes, which is why the payment figure is high. Neither may be described as a percentage of compliance with anything.

> **Publication rule**
>
> Do not describe an individual council as 'at risk', as non-compliant, or as having a consent failure on this evidence alone. Everything serious needs the council to check it privately first. A website that refuses an automated scanner is exercising a security control, not showing a weakness. And do not attribute a provider's infrastructure to a council.

Notes

- Every figure describes the 9 September 2026 assessment; the exposure provenance reading is dated 15 September 2026. No trend is reported and none should be inferred. Resident account records are unscored and concern the public, not council systems. The population is tracked websites, not legal authorities, and shared websites count once; a zero means a check ran and found nothing.

Sources and notes

[1] National Cyber Security Centre

10 Steps to Cyber Security; *Email security and anti-spoofing*, including the staged move from monitoring, through spam filing, to refusal; *Vulnerability disclosure toolkit*; *Using TLS to protect data*; *Multi-factor authentication for corporate online services*. Free plain-English guidance requiring no specialist team. ncsc.gov.uk

[2] Cyber Assessment Framework for local government, Ministry of Housing, Communities and Local Government

The NCSC framework adapted for councils by MHCLG working with local authorities, structured around managing risk, protecting against attack, detecting events and minimising impact. Published as a self-assessment tool, not a statutory duty. Page last updated 15 January 2026. security.gov.uk and localdigital.gov.uk

[3] Local Government Association, *Cyber Security and Resilience Bill: policy briefing*

Councils are largely outside the Bill's direct scope, which targets operators of essential services, digital providers, data centres, managed service providers and designated critical suppliers. The LGA welcomes the supply chain, incident reporting and threat intelligence provisions while pressing for clarity, support, realistic timelines and a unified approach to supplier assurance. Future regulations could introduce duties for councils themselves. At committee stage. local.gov.uk

[4] Information Commissioner's Office

Guide to PECR: cookies and similar technologies, governing what may be stored on a person's device and the permission needed, and *A guide to data security* under the UK GDPR. These decide whether an arrangement is lawful; the signals in sections 10 and 11 of this report are technical observations and are not such an assessment. ICO cookie guidance and ICO data security guidance

[5] Information Commissioner's Office, *ICO action secures increased cookie compliance*, December 2025

The ICO tested the top 1,000 websites used in the UK against three requirements: no non-essential advertising cookies before consent, refusing as easy as accepting, and no cookies placed without permission. 415 passed without intervention, 564 improved after ICO engagement, 17 received preliminary enforcement notices and 21 remained non-compliant at the point of reporting. The ICO will continue testing periodically. ico.org.uk

[6] PCI Security Standards Council

The PCI DSS standard (v4.x) and the Council's applicability guidance determine actual scope; payment flows, redirection arrangements, call-centre processes and supplier relationships cannot be scoped from an external scan. Requirement 11.3.2 requires passing external scans by an Approved Scanning Vendor at least every three months and after any significant change. Under version 4 that extends to the lightest e-commerce self-assessment category, mandatory from 31 March 2025, having not applied to it under version 3.2.1. An Approved Scanning Vendor is one specifically qualified by the Council. PCI DSS standard, applicability guidance, ASV resource guide

[7] MyDomainRisk / Huro Data Technologies Ltd, four national estate baselines and one comparative baseline, extraction 13:39 UTC on 9 September 2026, exposure provenance revised 15 September 2026

England 314 tracked and completed, 241 exact scores (sum 18,194) and 47 floor scores (sum 2,770), 26 unscored, medians 74. Wales 22 / 19 exact (1,415) / 3 floors (187) / 0 unscored, median 74. Scotland 32 / 22 exact (1,687) / 7 floors (424) / 3 unscored, median 77.5. Northern Ireland 11 / 11 exact (842) / no floors, median 76. Membership reconciles as 314 + 22 + 32 + 11 = 379 distinct websites with no cross-estate overlap. Exact scores 241 + 19 + 22 + 11 = 293, sum 22,138. Floor scores 47 + 3 + 7 + 0 = 57, sum 3,381. Published 350, sum 25,519. Averages are calculated from those underlying scores, not from rounded national averages. The 15 September rerun was read-only against the same snapshot: latest attempts were still dated 8 and 9 September, and every score count and sum above reproduced exactly. Exposure provenance reconciles as 4 + 6 + 4 + 3 = 17 risky-service websites and 4 + 6 + 3 + 0 = 13 database-port websites, of which 7 and 3 respectively are reported as council exposure.

Provenance and handling

The source is a read-only production snapshot taken at 13:39 UTC on 9 September 2026, selecting the latest attempt for each tracked website. Latest attempts are dated 8 and 9 September 2026. The extraction date does not refresh an observation, and a source date should be checked before operational use.

Correction notice, second edition

The first edition of this report, published from the same 9 September assessment, described **17 councils with a risky service reachable from the internet and 13 with an exposed database**. A provenance re-reading of the same retained evidence on 15 September 2026 established that ten of those cases answer from a website-protection service or a shared platform address range serving many customers, with no database or other service identified. **This edition reports 7 and 3.**

The first edition also described the software-weakness evidence in terms that conflated weaknesses recorded in a catalogue with weaknesses known to be actively exploited. All 261 observations were read from software version numbers and none was confirmed by a provider; **2 entries on 2 websites appear in the actively-exploited catalogue**. That wording is corrected here.

No count, score, average or band changed. Only the reading of who owns the equipment behind an observation. Any article, briefing or derivative quoting 17 risky services or 13 council databases from the first edition should be corrected to these figures.

No council is named in this report. The findings are aggregate by design: a named council beside its weakness is a document that cannot safely be circulated, and the value here is the sector pattern. Per-council detail exists and is available privately to the council concerned, or to anyone it authorises.

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Every named finding should be rechecked immediately before responsible disclosure, because public-facing settings change constantly. Aggregate figures may be used with the cautions in this report. This document contains counts only: no passwords, no personal records, no raw provider data, no exploit instructions and no named council detail. A finding is not evidence that any council has been compromised or is in breach of any obligation.