PERIMETRY RESEARCH

Baromètre de la sécurité des councils britanniques

Les councils britanniques protègent-ils bien leurs sites et leur messagerie ? Mesures passives des domaines des councils d'Angleterre, du pays de Galles, d'Écosse et d'Irlande du Nord.

Édition de novembre 2026

359
domaines avec un site à eux, notés

95,5 %
appliquent DMARC (quarantine ou reject)

35,9 %
ont A ou B

Perimetry Cloud
perimetry.cloud · Publiée le 14 novembre 2026

À propos de ce rapport

Perimetry Research publie des études sur la façon dont les organisations protègent leurs sites et leur messagerie, mesurée avec les mêmes contrôles passifs que Perimetry Cloud. Cette édition porte sur 366 domaines des councils du Royaume-Uni ; 366 sont actifs, et les 359 qui ont un site à eux sont notés. Elle ne nomme que les collectivités qui font bien ; tous les autres chiffres sont des moyennes, et les problèmes graves ont été signalés en privé aux collectivités avant la publication.

Sommaire

01 Synthèse 3

02 Principaux constats 4

03 Notes 5

04 Contrôle par contrôle 6

05 Par catégorie 8

06 Les domaines sans site à eux 9

07 Comparaison avec nos autres études 10

08 Les collectivités qui font bien 11

09 Problèmes graves 12

10 Recommandations 13

11 Méthodologie 14

12 À propos de Perimetry 16

01

Synthèse

359	69	95,5 %	35,9 %
domaines avec un site à eux, notés	note moyenne sur 100	appliquent DMARC (quarantine ou reject)	ont A ou B

Note moyenne des 359 domaines notés : 69 sur 100 ; médiane 67.

1. 99,4 % des domaines notés publient une politique DMARC et 95,5 % l'appliquent (collectivités françaises : 32,8 % ; collectivités allemandes : 41,1 %).
2. Côté sites : 98,1 % ont un certificat valide, 85,5 % renvoient vers HTTPS, 57 % utilisent HSTS d'au moins six mois.
3. 1,9 % des domaines notés sont signés avec DNSSEC ; 11,4 % publient un enregistrement CAA.
4. 7 domaines actifs n'ont pas de site à eux ; 0 % d'entre eux n'appliquent pas DMARC.

02

Principaux constats

99,4 % des domaines notés publient une politique DMARC et 95,5 % l'appliquent (collectivités françaises : 32,8 % ; collectivités allemandes : 41,1 %).

Côté sites : 98,1 % ont un certificat valide, 85,5 % renvoient vers HTTPS, 57 % utilisent HSTS d'au moins six mois.

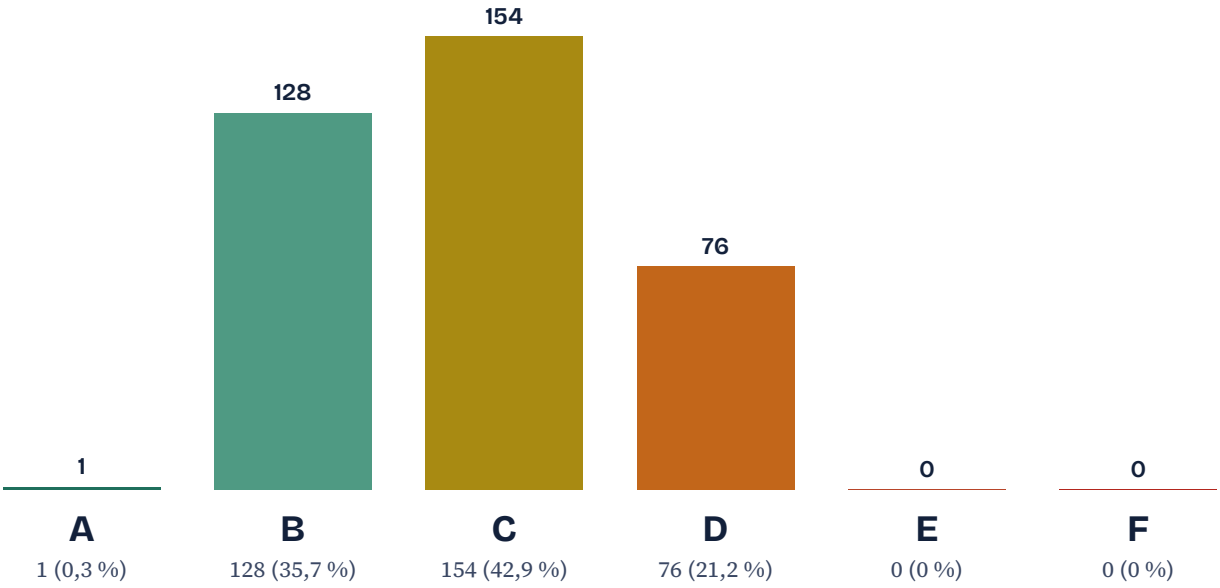
1,9 % des domaines notés sont signés avec DNSSEC ; 11,4 % publient un enregistrement CAA.

7 domaines actifs n'ont pas de site à eux ; 0 % d'entre eux n'appliquent pas DMARC.

03

Notes

Chaque domaine qui a un site à lui reçoit une note : la part des neuf contrôles qu'il réussit, parmi ceux qui le concernent (la note de nos autres études, sans le contrôle de l'adresse de contact, que les listes ne donnent pas). A à partir de 90, B de 75, C de 60, D de 40, E de 20, F en dessous.

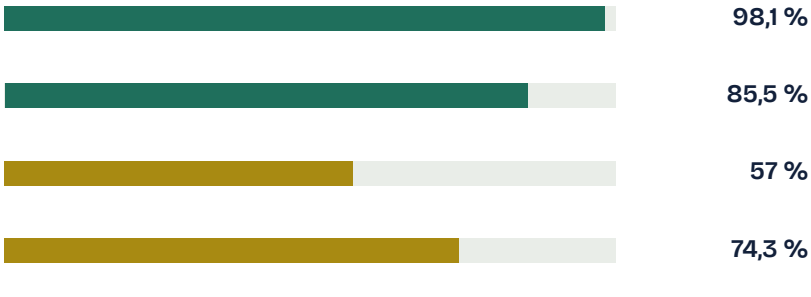


04

Contrôle par contrôle

Part des domaines notés qui réussissent chaque contrôle, parmi ceux qu'il concerne.

Site web



DNS



E-mail



Les neuf contrôles	
Site web · Certificat HTTPS valide	Le site répond en HTTPS avec un certificat en cours de validité, émis pour son nom et reconnu par les navigateurs.
Site web · HTTP renvoie vers HTTPS	Quelqu'un qui tape l'adresse arrive sur le site chiffré, et non sur une page que n'importe qui sur le réseau peut lire ou modifier.
Site web · HSTS d'au moins six mois	Les navigateurs retiennent qu'il faut utiliser HTTPS : la première requête non chiffrée ne peut pas être détournée.
Site web · En-têtes de protection de base	X-Content-Type-Options: nosniff, et une protection contre l'affichage du site dans le cadre d'un autre site (X-Frame-Options ou frame-ancestors dans la CSP).
DNS · DNSSEC	Les réponses DNS du domaine sont signées : on ne peut pas faire croire à un résolveur que le site ou la messagerie de l'administration sont ailleurs.
DNS · Enregistrement CAA	Le domaine désigne les autorités de certification autorisées à émettre des certificats à son nom.
E-mail · SPF strict	Le domaine liste les serveurs autorisés à envoyer son courrier et demande de rejeter ou de signaler les autres (-all ou ~all).

Les neuf contrôles	
E-mail · Enregistrement DMARC	Le domaine publie une politique DMARC, la norme qui relie SPF et DKIM à l'expéditeur affiché.
E-mail · DMARC appliqué	La politique est quarantine ou reject : un message falsifié au nom de l'administration, adressé à des usagers par exemple, part en indésirables ou est refusé, au lieu d'être distribué.

05

Par catégorie

Les catégories de moins de dix domaines notés ne sont pas détaillées.

Groupe	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
Comtés (Angleterre)	21	71	38,1 %	95,2 %	–
Districts (Angleterre)	154	69	33,8 %	94,8 %	67
Districts métropolitains	35	69	28,6 %	97,1 %	67
Autorités unitaires (Angleterre)	53	69	39,6 %	96,2 %	67
Arrondissements de Londres et City de Londres	33	73	51,5 %	100 %	78
Conseils du pays de Galles	21	66	23,8 %	95,2 %	–
Conseils écossais	31	69	32,3 %	96,8 %	67
Conseils d'Irlande du Nord	11	75	54,5 %	81,8 %	–

Moyenne



06

Les domaines sans site à eux

7 domaines actifs n'ont pas de site à eux : 0 renvoient vers un autre site, 7 ne servent qu'à la messagerie. Ils peuvent quand même servir à falsifier des e-mails au nom de la collectivité, et sont jugés sur leur DNS et leur messagerie seulement.



Note moyenne sur le DNS et la messagerie seulement : 60 sur 100.

07

Comparaison avec nos autres études

Les mêmes contrôles dans nos autres études (dernières éditions) : part des domaines notés qui réussissent chacun. Les collectivités françaises comptent dix contrôles, les autres neuf.

	Councils	Allemagne	Collectivités FR	État britannique
Note moyenne	69	62	60	54
Certificat HTTPS valide	98,1 %	96,4 %	98,7 %	67,4 %
HTTP renvoie vers HTTPS	85,5 %	92 %	90,9 %	75 %
HSTS d'au moins six mois	57 %	74,3 %	38,8 %	42,1 %
En-têtes de protection de base	74,3 %	68,6 %	40,7 %	47,8 %
DNSSEC	1,9 %	15 %	25,9 %	3,8 %
Enregistrement CAA	11,4 %	12,4 %	2,6 %	4,7 %
SPF strict	100 %	88,6 %	97,1 %	85,6 %
Enregistrement DMARC	99,4 %	73,6 %	77,8 %	84,3 %
DMARC appliqué	95,5 %	41,1 %	32,8 %	74,6 %

08

Les collectivités qui font bien

1 collectivités réussissent les neuf contrôles et n’ont aucun problème grave.

Collectivité	Catégorie
Newry, Mourne and Down District Council	Conseils d’Irlande du Nord

09

Problèmes graves

2 domaines ont un problème grave qui pourrait être utilisé contre eux. Ils ne sont nommés ni dans ce rapport ni ailleurs : les collectivités ont été prévenues en privé avant la publication.

Certificats expirés	2

10

Recommandations

1 **Appliquer DMARC**
La plupart des councils le font déjà : les autres devraient suivre, en commençant par les domaines qui n'envoient pas de courrier.

2 **Activer HSTS et les en-têtes de protection**
HSTS fait retenir aux navigateurs de n'utiliser que HTTPS ; deux en-têtes empêchent une autre page d'afficher le site dans un cadre et le navigateur de mal lire ses fichiers.

3 **Signer les domaines avec DNSSEC**
Presque aucun council ne le fait ; le registre du .gov.uk le permet.

4 **Vérifier l'adresse sans « www »**
Plusieurs certificats expirés ont été trouvés sur le domaine nu alors que le site en www allait bien : un visiteur qui tape l'adresse courte reçoit un avertissement.

5 **Surveiller dans la durée**
Les certificats expirent, les prestataires changent, des enregistrements se perdent lors d'une migration. Un contrôle régulier le voit avant les habitants.

11

Méthodologie

Des contrôles passifs uniquement

Nous lisons ce que n'importe quel visiteur ou serveur de messagerie peut voir : les enregistrements DNS publics, l'enregistrement du domaine (RDAP), le certificat TLS, une requête sur la page d'accueil en HTTP (sa redirection est lue, pas suivie), et la page d'accueil en HTTPS (en suivant ses redirections, comme un navigateur). Rien d'autre n'est demandé au site. Quand un domaine publie une politique MTA-STS, son fichier de politique est lu aussi, comme le font les serveurs de messagerie.

Pas de balayage de ports, pas de recherche de sous-domaines, pas de tentative de connexion, pas de formulaire, pas de test de vulnérabilité. Le robot est lent exprès et répartit ses requêtes sur plusieurs heures.

Le robot

Il se présente comme PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). Si vous gérez un site qu'il a visité et préférez qu'il ne le fasse plus, écrivez à hello@perimetry.cloud : nous retirerons le domaine des prochaines éditions.

L'étude des councils britanniques

Population étudiée : les councils en place de la liste des noms et codes des autorités locales britanniques de mySociety (CC BY 4.0) : comtés, districts, districts métropolitains, autorités unitaires et arrondissements de Londres en Angleterre, la City de Londres, et les conseils du pays de Galles, d'Écosse et d'Irlande du Nord. Les conseils de paroisse et de ville, les autorités combinées et stratégiques sont écartés. Le site de chaque council est celui que donne sa fiche d'autorité locale sur GOV.UK (Open Government Licence v3.0) ; deux councils qui partagent un domaine (services communs) ne font qu'un domaine dans l'étude.

Catégories : le type du council dans la liste de mySociety. Le reste suit l'étude de l'État français : domaines inactifs comptés et écartés, chiffres principaux sur les domaines qui ont un site à eux, neuf contrôles, groupes de dix domaines notés ou plus, seuls les councils qui réussissent les neuf contrôles nommés. Un site qui répond à notre robot par une page d'erreur (souvent un filtre qui écarte les réseaux de centres de données) garde ses contrôles de certificat et de redirection mais n'est pas noté sur ses en-têtes. Les problèmes graves sont signalés en privé au council avant la publication ; l'étude n'en donne que le nombre.

Uniquement les bons élèves

Nous nommons les communes qui font bien (le tableau d'honneur et les meilleures de chaque tranche de population), jamais celles qui font mal, et jamais une commune qui a un problème grave, quelle que soit sa note. Tout le reste est publié en moyennes : par taille de commune et par département, où un département de moins de dix communes notées n'est pas détaillé, pour qu'aucune d'elles ne puisse être reconnue.

Les plateformes de sites sont notées sur un échantillon de cinq sites de communes au plus : un contrôle compte comme réussi quand la majorité de l'échantillon le réussit.

Les problèmes graves sont signalés en privé

Certains constats pourraient servir tout de suite contre une commune : un domaine inscrit dans l'annuaire officiel qui n'existe plus (n'importe qui pourrait l'enregistrer), un domaine que le registre est en train de supprimer, un certificat expiré, un enregistrement SPF qui permet à n'importe qui d'envoyer du courrier en son nom. Ils ne sont jamais publiés. Nous prévenons d'abord la commune, discrètement, et nous les comptons dans l'étude sans nommer personne.

Limites

Chaque édition est une photographie prise en quelques heures. L'annuaire peut être en retard ou erroné ; nous l'utilisons tel qu'il est publié. Les clés DKIM ne sont cherchées que sur les sélecteurs courants : elles ne sont donc pas notées. Un site derrière un service de protection peut répondre à un robot autrement qu'à un visiteur. Les serveurs de messagerie ne sont pas testés (STARTTLS demande le port 25, que l'infrastructure de l'étude ne peut pas joindre).

12

À propos de Perimetry

Perimetry est un outil libre qui audite l'extérieur d'un domaine comme n'importe qui sur Internet le voit : authentification des e-mails, DNS, certificats, serveurs de messagerie, sites. Perimetry Cloud en est la version hébergée, avec surveillance continue, alertes et rapports, pour les organisations et les agences qui s'en occupent.

Citer : Perimetry Research, Baromètre de la sécurité des councils britanniques, novembre 2026. https://perimetry.cloud/fr/research/uk-councils/

Vous pouvez réutiliser les chiffres de ce rapport avec un lien vers l'étude. Contient des données de mySociety (CC BY 4.0) et des informations du secteur public britannique sous Open Government Licence v3.0.

Contact : hello@perimetry.cloud

`https://perimetry.cloud/fr/research/uk-councils/`