PERIMETRY RESEARCH

Baromètre de la sécurité des domaines de l'État britannique

L'État britannique protège-t-il bien ses sites et sa messagerie ? Mesures passives des domaines de GOV.UK, des ministères, agences, organismes publics et gouvernements dévolus de listes ouvertes, comparées à l'État français.

Édition de novembre 2026

236
domaines avec un site à eux, notés

74,6 %
appliquent DMARC (quarantine ou reject)

30,1 %
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 les 497 domaines de l'administration centrale britannique de la liste des noms de domaine en .gov.uk du Cabinet Office et des organisations de GOV.UK ; 463 sont actifs, et les 236 qui ont un site à eux sont notés. Elle ne nomme que les domaines qui font bien ; tous les autres chiffres sont des moyennes, et les problèmes graves sont signalés au NCSC 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 l'État français et nos autres études 10

08 Les domaines qui font bien 11

09 Problèmes graves 12

10 Recommandations 13

11 Méthodologie 14

12 À propos de Perimetry 16

01

Synthèse

236
domaines avec un site à eux, notés

54
note moyenne sur 100

74,6 %
appliquent DMARC (quarantine ou reject)

30,1 %
ont A ou B

Note moyenne des 236 domaines notés : 54 sur 100 ; médiane 56.

1. 84,3 % des domaines notés publient une politique DMARC et 74,6 % l'appliquent (l'État français : 43,3 %).
2. Côté sites : 67,4 % ont un certificat valide, 75 % renvoient vers HTTPS, 42,1 % utilisent HSTS d'au moins six mois.
3. 3,8 % des domaines notés sont signés avec DNSSEC (l'État français : 3,8 %).
4. 227 domaines actifs n'ont pas de site à eux ; 33,9 % d'entre eux n'appliquent pas DMARC.
5. Sur les mêmes neuf contrôles, l'État britannique a en moyenne 54 sur 100, l'État français 46.

02

Principaux constats

Les indicateurs propres à l'État

25,5 % des domaines actifs sont hors du .gov.uk.

0,2 % des domaines inscrits sont absents du DNS.

84,3 % des domaines notés publient une politique DMARC et 74,6 % l'appliquent (l'État français : 43,3 %).

Côté sites : 67,4 % ont un certificat valide, 75 % renvoient vers HTTPS, 42,1 % utilisent HSTS d'au moins six mois.

3,8 % des domaines notés sont signés avec DNSSEC (l'État français : 3,8 %).

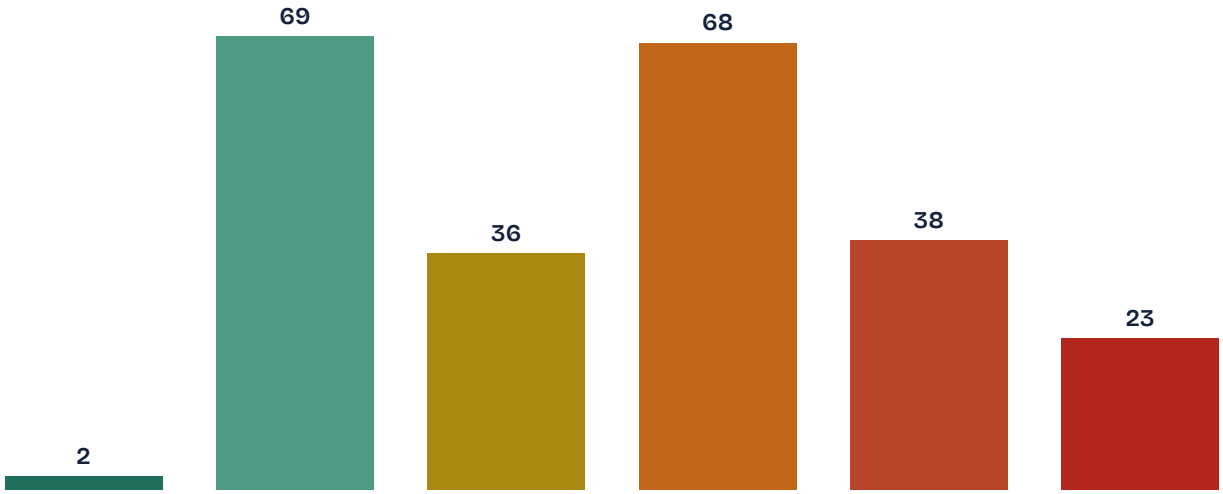
227 domaines actifs n'ont pas de site à eux ; 33,9 % d'entre eux n'appliquent pas DMARC.

Sur les mêmes neuf contrôles, l'État britannique a en moyenne 54 sur 100, l'État français 46.

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.

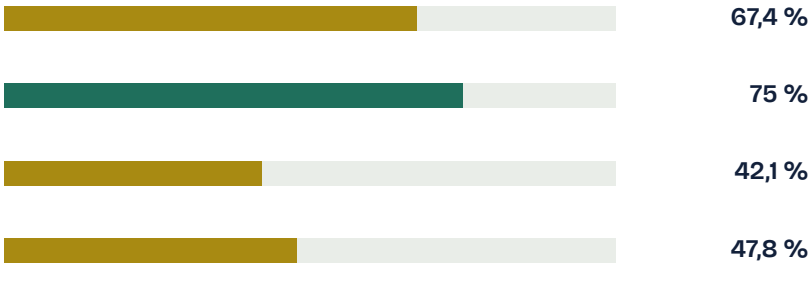


04

Contrôle par contrôle

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

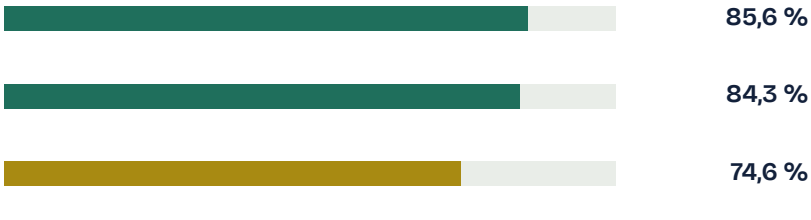
Site web



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.

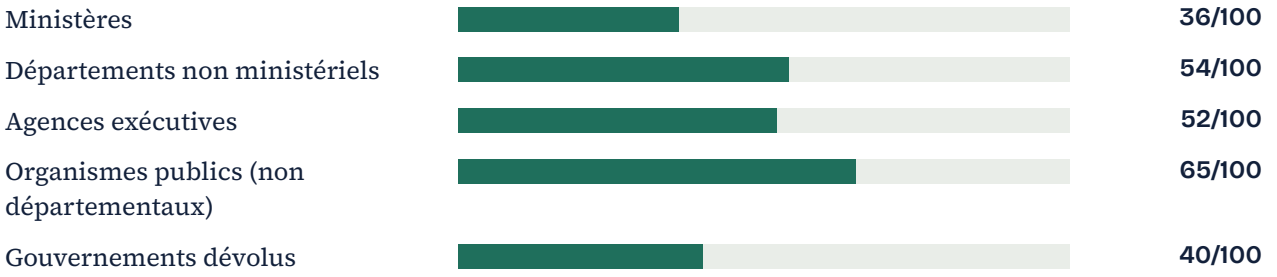
05

Par catégorie

La classification des organisations de GOV.UK. Les catégories de moins de dix domaines notés ne sont pas détaillées.

Groupe	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
GOV.UK	1	·	·	·	·
Ministères	61	36	6,6 %	70,5 %	33
Départements non ministériels	15	54	46,7 %	73,3 %	–
Agences exécutives	22	52	27,3 %	77,3 %	–
Organismes publics (non départementaux)	116	65	42,2 %	83,6 %	67
Cours et tribunaux	2	·	·	·	·
Gouvernements dévolus	12	40	25 %	33,3 %	–
Autres organismes centraux	7	·	·	·	·

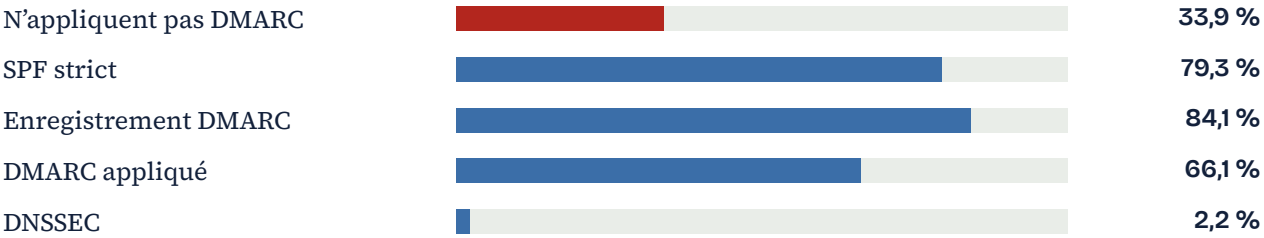
Moyenne



06

Les domaines sans site à eux

227 domaines actifs n'ont pas de site à eux : 129 renvoient vers un autre site, 98 ne servent qu'à la messagerie. Ils peuvent quand même servir à falsifier des e-mails au nom de l'administration, et sont jugés sur leur DNS et leur messagerie seulement.



Note moyenne sur le DNS et la messagerie seulement : 47 sur 100.

07

Comparaison avec l'État français et nos autres études

Les mêmes contrôles dans nos études de l'État français, des communes, des collectivités, de l'enseignement supérieur et des domaines .fr (dernières éditions) : part des domaines notés qui réussissent chacun. Les communes et les collectivités comptent dix contrôles, les autres neuf.

	Royaume-Uni	État français	Communes	Collectivités	Enseignement supérieur	Domaines .fr
Note moyenne	54	46	47	60	64	32
Certificat HTTPS valide	67,4 %	63,8 %	93,4 %	98,7 %	100 %	59,1 %
HTTP renvoie vers HTTPS	75 %	77,3 %	86,4 %	90,9 %	95,2 %	53,4 %
HSTS d'au moins six mois	42,1 %	33,3 %	28,3 %	38,8 %	46,1 %	17,3 %
En-têtes de protection de base	47,8 %	51,9 %	26,1 %	40,7 %	57,5 %	14,1 %
DNSSEC	3,8 %	3,8 %	22,1 %	25,9 %	12,7 %	25,9 %
Enregistrement CAA	4,7 %	18,5 %	2,8 %	2,6 %	41 %	1,2 %
SPF strict	85,6 %	56,2 %	85,9 %	97,1 %	93 %	71,6 %
Enregistrement DMARC	84,3 %	56,7 %	45,2 %	77,8 %	86,9 %	38,6 %
DMARC appliqué	74,6 %	43,3 %	19,2 %	32,8 %	45,4 %	11,7 %

08

Les domaines qui font bien

2 domaines réussissent les neuf contrôles et n'ont aucun problème grave.

Domaine	Catégorie
officeforstudents.org.uk	Organismes publics (non départementaux)
thenational.academy	Organismes publics (non départementaux)

09

Problèmes graves

5 domaines ont un problème grave qui pourrait être utilisé contre eux. Ils ne sont nommés ni dans ce rapport ni ailleurs : ils sont signalés au NCSC avant la publication.



10

Recommandations

1 **Appliquer DMARC sur chaque domaine, y compris ceux sans site**
Un domaine qui ne fait que renvoyer vers GOV.UK, ou n'envoie que du courrier, peut servir à falsifier des e-mails au nom de l'administration. Chaque domaine qui n'envoie pas de courrier devrait publier un SPF qui n'autorise rien et une politique DMARC reject.

2 **Activer HSTS partout**
GOV.UK le fait ; beaucoup de sites propres d'organismes non. HSTS fait retenir aux navigateurs de n'utiliser que HTTPS.

3 **Signer les domaines avec DNSSEC**
Le registre du .gov.uk le permet ; peu de domaines l'utilisent.

4 **Retirer les domaines qui ne servent plus**
Les domaines inscrits sans site ni messagerie devraient publier une politique qui refuse le courrier, ou sortir de la liste.

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 usagers.

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 domaines de l'État britannique

Population étudiée : les domaines de l'administration centrale britannique de listes ouvertes sous Open Government Licence v3.0. GOV.UK lui-même, le site unique des ministères et de la plupart de leurs organismes. Les domaines de la liste des noms de domaine en .gov.uk du Cabinet Office enregistrés pour une organisation de l'administration centrale : les dernières éditions de la liste ne donnent que les noms de domaine ; pour qui un domaine est enregistré est donc lu dans l'édition du 30 mars 2023, la dernière à l'indiquer, rapproché par son nom des organisations de GOV.UK, et le domaine n'est gardé que s'il figure encore dans la dernière édition (31 mars 2026). Et les sites des organisations de GOV.UK qui en gardent un à elles. Les collectivités locales (conseils, conseils de paroisse et de ville), la police et les pompiers sont écartés, comme l'étude française écarte communes et collectivités ; de même les entreprises publiques (la BBC, Channel 4…) et les organismes que GOV.UK classe en « autres » (la Banque d'Angleterre…).

Catégories : la classification des organisations de GOV.UK (ministères et départements non ministériels, agences exécutives, organismes publics non départementaux, cours et tribunaux, gouvernements dévolus, autres organismes centraux). Un domaine enregistré après mars 2023, ou pour un nom différent de celui de l'organisation sur GOV.UK, ne peut pas être classé et n'est pas dans l'étude : la liste est complète pour les sites propres des organismes, pas pour chaque domaine en .gov.uk de l'administration centrale.

Tout 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, domaines sans site présentés à part, neuf contrôles, trois applicables pour être noté, groupes d'au moins dix domaines notés, seuls les domaines qui réussissent les neuf contrôles nommés. Les problèmes graves sont signalés au NCSC 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 domaines de l'État britannique, novembre 2026. https://perimetry.cloud/fr/research/uk-government/

Vous pouvez réutiliser les chiffres de ce rapport avec un lien vers l'étude. Contient des informations du secteur public britannique sous Open Government Licence v3.0.

Contact : hello@perimetry.cloud

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