Defensive domain registrations

# Defensive domain registrations

The Ministry of Justice (MoJ) and associated organisations (Executive agencies, non-departmental public bodies and so on) maintain varying levels of 'online presence' using domain registrations. This are a fundamental part of the organisation's identity on the public internet. An example is the justice.gov.uk email domain used for contacting other government organisations, partners and members of the public.

Each MoJ organisation **must** identify a core set of internet domains it considers critical to its internet identity. Each MoJ organisation must then defensively register a small number of obvious variations (for example, justice.gov.uk may justify justicegov.uk, justice.co.uk and justice.uk where already not used for legitimate purposes).

These registrations will help protect the organisation, as well as its partners and members of the public, from illegitimate parties pretending to be the organisation when they are not. Failing to register these domains can cause problems, such as phishing emails using what seem to be plausible domains.

## Limiting the permutations to register

Domain permutations for defensive registration should be limited to the organisation's core identity, as opposed to tertiary campaigns/identities, in order to keep costs and management overheads down.

Some domain registrars have methods to detect malicious registrations of overtly government-associated domains through the use of misspellings and so on. Unless there are strong justifications as to why misspellings must be covered, organisations should only defensively register .uk and .co.uk top-level domain variants and visual manipulations. For example, the removal of one dot from justice.gov.uk leads to justicegov.uk which could be a registerable domain and one that looks a lot like justice.gov.uk during a casual inspection.

## Mandatory features for defensively registered domains

The following features are required when registering a defensive domain:

### Functional nameservers

The defensively registered domain must have a functional nameserver configuration.

### Sender Policy Framework (SPF)

There must be an [SPF record](https://en.wikipedia.org/wiki/Sender_Policy_Framework) which uses *strict* configurations to indicate whether the domain is expected by the owner to send emails, or not.

Example 'no permitted sender' record:

v=spf1 -all

Additional [SPF implementation guidance](https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf) is available on GOV.UK.

### Domain-based Message Authentication, Reporting and Conformance (DMARC)

There must be a [DMARC record](https://en.wikipedia.org/wiki/DMARC) configured in line with [published DMARC guidance](https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc) on GOV.UK.

Example 'reject' policy record:

v=DMARC1;p=reject;rua=mailto:dmarc-rua@dmarc.service.gov.uk;

### Mail Exchanger (MX)

There must be a nullified [MX record](https://en.wikipedia.org/wiki/MX_record) in order to ensure any attempt to send emails to the defensive domain to instantly failed.

Example nullified record:

MX priority 0 with host name .

### DomainKeys Identified Mail (DKIM)

There must be a nullified [DKIM record](https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail) in explicitly highlight that any outbound email attempts are likely invalid.

Example nullified record:

v=DKIM1; p=

### DNS Certification Authority Authorization (CAA)

There must be a [DNS CAA](https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization) record(s) to indicate restrictions so that certificate authorities that certificates should not be issued for these domains.

Example nullified record:

issue ";"

Example iodef notification record:

iodef "mailto:certificates@digital.justice.gov.uk"

### Automated renewals

Defensively registered domains should be configured to automatically renew by default.

### Web services/redirects

Web services/redirects must **not** be functional or available for defensively registered domains.

The www. should *not* be created. The apex @ record, if required and created, should not respond to TCP/80 (HTTP) or TCP/443 (HTTPS).

### Mail services/redirects

Mail services/redirects must **not** be functional or available for defensively registered domains.

## Registering and maintaining a defensive domain

MoJ organisations should contact [domains@digital.justice.gov.uk](mailto://domains@digital.justice.gov.uk) for assistance with defensive doman registrations and operations.