



NOMINET

TACKLING ONLINE CRIMINAL ACTIVITY

1ST NOVEMBER 2019 - 31ST OCTOBER 2020

Nominet operates at the heart of the UK internet infrastructure, responsible for running the .UK domain. We work with law enforcement agencies to help protect internet users from criminality online.

CRIMINAL ACTIVITY

When alerted by law enforcement agencies, we work quickly with our registrars to suspend domains in accordance with our [Criminal Practices Policy](#).



- 1 Counter Terrorism Internet Referral Unit (CTIRU)
- 2 Environment Agency
- 3 Financial Conduct Authority (FCA)
- 4 Medicines and Healthcare Products Regulatory Agency (MHRA)
- 5 Metropolitan Police – Central Specialist Crime
- 6 Ministry of Defence Police
- 7 National Crime Agency (NCA)
- 8 National Food Crime Unit (NFCU)
- 9 National Fraud Intelligence Bureau (NFIB)
- 10 Office of Communications (Ofcom)
- 11 Police Intellectual Property Crime Unit (PIPCU)
- 12 Trading Standards
- 13 Veterinary Medicines Directorate (VMD)

RANGE OF LEGISLATION CITED FOR SUSPENSION REQUESTS INCLUDED:

- Fraud Act 2006
- Trade Marks Act 1994
- Copyright, Designs and Patents Act 1988
- Human Medicines Regulations 2012
- Medical Device Regulations 2002
- Consumer Protection from Unfair Trading Regulations 2008
- The Electronic Commerce Regulations 2002
- The Consumer Contracts Regulations 2013
- Financial Services and Markets Act 2000
- Regulation 38(1)(a) Environmental
- Permitting Act 2016
- Radio Equipment Regulations 2017



22,158 domains suspended for criminal activity (compared to 28,937 in the previous year)

BREAKDOWN BY REQUESTING AGENCY

Total number of requests - 22,205
22158 (suspensions) plus 47 (requests that did not result in a suspension)



21,632 (-6,974 yoy*)

Police Intellectual Property Crime Unit (PIPCU)



266 (+88 yoy*)

National Fraud Intelligence Bureau (NFIB)



232 (+184 yoy*)

Financial Conduct Authority (FCA)



7 (-83 yoy*)

Trading Standards (TS)



13 (-18 yoy*)

Medicines and Healthcare Products Regulatory Agency (MHRA)



3

National Crime Agency (NCA)



3

Environment Agency



2

Ofcom

*Year-on-year (yoy)

HOW IT WORKS



Law enforcement agency notifies Nominet that a domain is being used for criminal activity

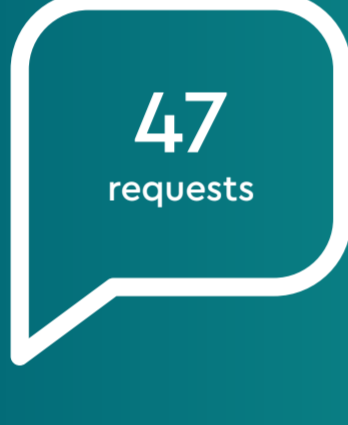


Nominet makes administrative checks



Nominet notifies the registrant and works with the registrar to suspend the domain

REQUESTS NOT RESULTING IN SUSPENSIONS



received in the specified 12 months that didn't result in suspensions

A suspension request may not result in a suspension for a number of reasons – for example, the domain may have already been suspended due to a parallel process, the domain may have already been transferred on a court order, or the registrant may have modified the website following notification and is now compliant.

REVERSALS



Data refers to domains suspended due to requests received during the specified period

A suspension is reversed if the offending behaviour has stopped and the enforcing agency has since confirmed that the suspension can be lifted.

PROSCRIBED TERMS

Nominet prohibits the registration of domain names that promote or incite serious sexual offences (where there is no reasonable or legitimate use for that domain) under our proscribed terms policy.

HOW IT WORKS



NEW REGISTRATIONS
New domain registrations are run through an automated process where potential breaches are flagged



EXISTING REGISTRATIONS
If Nominet receives a complaint about an existing domain name



Each flagged domain name is manually checked to ensure no false positives go through. If a domain name is in breach, the registrant and registrar are notified and the domain suspended and blocked so that no one can register that domain in the future. Registrants have 30 days to request a review of this assessment.



We advise that any complaints about website content and not the domain name should be referred directly to law enforcement

1060

potential breaches flagged (new registrations)

0

domains suspended and blocked

0

reviews

0 suspension requests from the Internet Watch Foundation on Child Sexual Abuse Images (CSAM) on .UK domains

DOMAIN WATCH

Nominet's anti-phishing initiative to further increase the security of the .UK zone is designed to quickly identify and suspend newly registered domains that are obvious phishing attempts. If a domain is suspended, the registrant will receive an email informing them what has happened, together with the next steps required if they feel the suspension was not correctly applied.



5,006

suspensions pending additional checks



558

successfully passed additional due diligence and completed the registration process

EXAMPLES OF DOMAINS SUSPENDED THROUGH DOMAIN WATCH:

Private Sector:

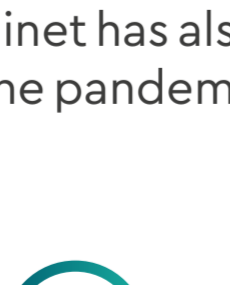
- netflixbilling.org.uk
- tesco.me.uk
- canada-goose.me.uk
- supportbarclays.co.uk
- halifax-login.co.uk

Public Sector:

- rebate-govuk-return.co.uk
- uhl-nhs.uk
- hertsmeregov.uk
- hmcr.gov.co.uk
- tax-claim-gov.uk

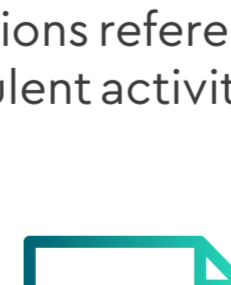
COVID-19

Nominet has also stepped up checks on new domain registrations referencing the pandemic and related terms to mitigate against fraudulent activity.



3,811

suspensions pending additional checks



1,568

successfully passed additional due diligence and completed the registration process

To understand more about Nominet's collaboration with UK law enforcement, read our [Criminal Practices Policy](#), available at [nominet.uk/policies](#)

For rights holders who wish to seek control of a domain name they believe should be theirs Nominet offers an award winning Dispute Resolution Service (DRS). The DRS offers an efficient and transparent method of resolving disputes relating to .UK domain names. The DRS seeks to settle disputes through mediation and, where this is not possible, through an independent expert decision.

More information about the DRS is available at [nominet.uk/disputes](#)

ABOUT NOMINET

Nominet is driven by a commitment to use technology to improve connectivity, security and inclusivity online. For over 20 years, Nominet has run the UK internet infrastructure, developing an expertise in the Domain Name System (DNS) that now underpins sophisticated threat monitoring, detection, prevention, and analytics that is used by governments and enterprises to mitigate cyber threats. Our [public benefit programme](#) aims to improve the lives of one million people, providing support and opportunities to tackle some of the most important digital issues facing young people in the UK today.