

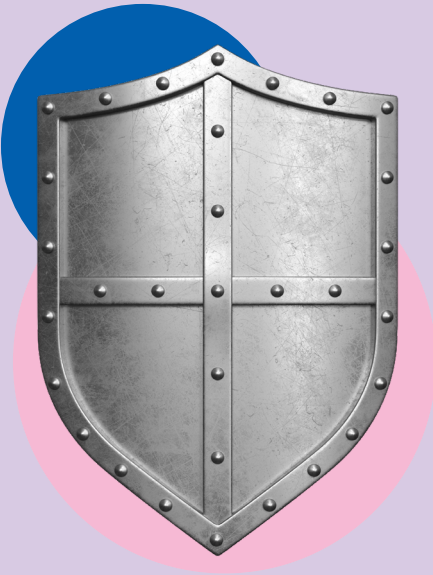
TACKLING ONLINE CRIMINAL ACTIVITY

1 November 2023 - 31 October 2024

Nominet operates at the heart of the UK’s internet infrastructure, responsible for running the .UK domain.

We work with law enforcement agencies to help protect internet users from criminality online.

To understand more about Nominet’s collaboration with UK law enforcement, read our Criminal Practices Policy, available at nominet.uk/policies



913 Domains suspended for criminal activity under our Criminal Practices policy



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



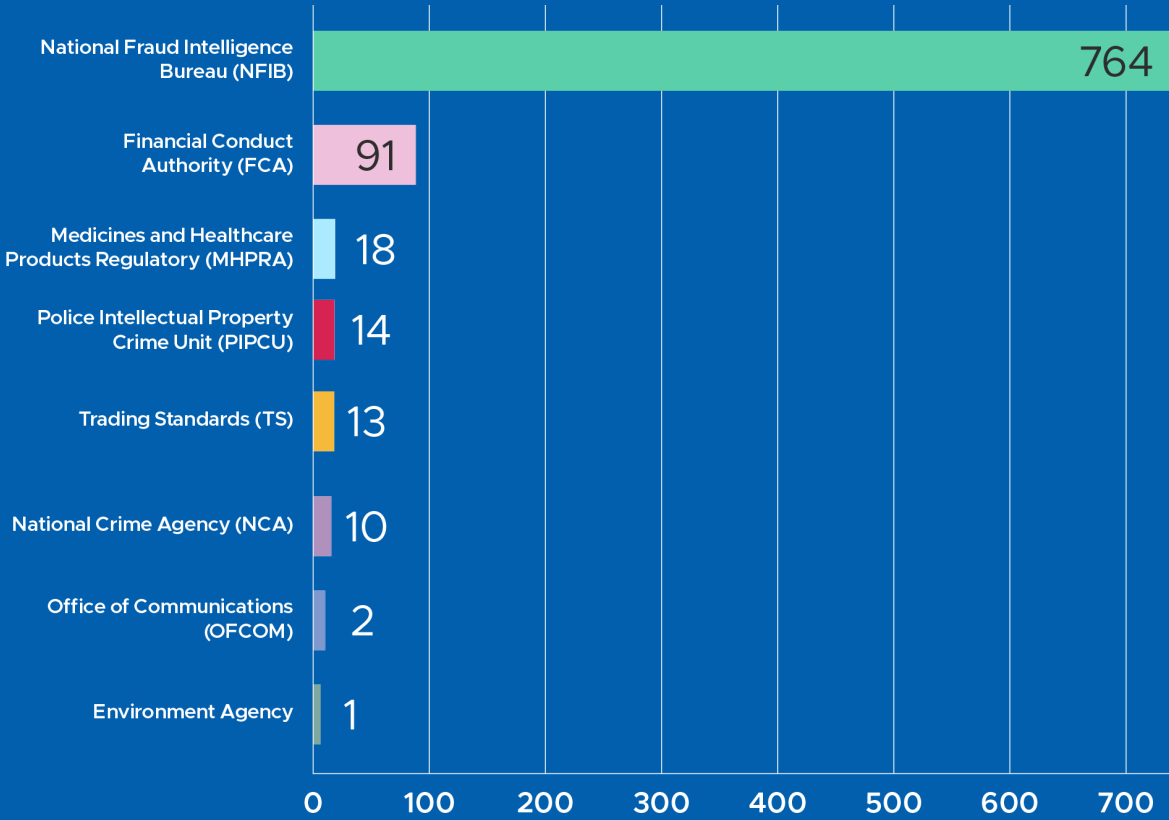
Nominet makes administrative checks



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

Breakdown of suspensions by reporting agency

When alerted by law enforcement agencies, we work quickly with our registrars to suspend domain in accordance with our Criminal Practices Policy.



Criminal activity

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



14 Enforcement Agencies

CTIRU - Counter Terrorism Internet Referral Unit

EA - Environment Agency

FCA - Financial Conduct Authority

MHRA - Medicines and Healthcare Products Regulatory Agency

MPCSC - Metropolitan Police – Central Specialist Crime

MOD - Ministry of Defence Police

NCA - National Crime Agency

NFCU - National Food Crime Unit

NFIB - National Fraud Intelligence Bureau

OFCOM - Office of Communications

OPSS - Office for Product Safety and Standards

PIPCU - Police Intellectual Property Crime Unit

TS - Trading Standards

VMD - Veterinary Medicines Directorate

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) as part of our terms and conditions of domain registration.

While 1,012 potential breaches were flagged, no domains were suspended.



2 Suspension requests

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

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



Domain Abuse Activity Reporting

6,315 Domains suspended

This year we continued our efforts to tackle abuse in .UK to include existing domain registrations that appear on threat feeds.

Using third party data we have investigated 8,820 reports on .UK domains, which were flagged as potential phishing, malware, fake webshops, command and controls or cryptocurrency scams. Of these threat reports, 6,315 led to domain suspensions.



Domain Watch

Nominet’s anti-phishing initiative is designed to quickly identify and suspend newly registered domains that are potential phishing attempts. The domains listed are examples of the domains identified through Domain Watch.

Public Sector

- cabinet-officegov[.]uk
- thegov[.]uk
- tax-gov[.]uk

Private Sector

- account-o2[.]uk
- vodafone.co[.]uk
- paypal.org[.]uk
- alert-santander.co[.]uk
- hotmailmail.co[.]uk
- bbcbc.co[.]uk,
- barclays-notify.co[.]uk
- hsbcukbank[.]uk
- fcamail-org.co[.]uk

4,349 Domains suspended