Resilience highlights this year

2.1 million
cyber-enabled commodity campaigns removed

6.5 million
suspicious email reports received & 62k scam URLs removed

34 million
Early Warning alerts about attacks, compromises, vulnerabilities or open ports

90%
increase in signups to Early Warning service.

Expansion
of counter-ransomware services

Support to Ukraine
in bolstering their cyber resilience in the face of Russian invasion

Bolstered UK resilience
in light of heightened cyber risk from the conflict

UK-wide Cyber Aware campaign
to change citizen behaviour around personal email security

CYBER ESSENTIALS

15% rise in certificates awarded (28,989)

5,799 businesses achieved "Plus" status – a **15%** increase on last year

Now over **300** cyber security companies licensed as certification bodies for Cyber Essentials

Cyber Essentials-certified SMEs **60%** less likely to need to make a cyber insurance claim

100,000th Cyber Essentials certificate issued (since launch)

Active Cyber Defence

Protective Domain Name Service (PDNS) - prevents users from accessing malicious domains or IP addresses.

> Organisations using PDNS rose **23%** (from 928 to 1,140)

Mail Check helps public and third sector assess and improve email security compliance to prevent criminals spoofing email domains.

> New users increased by 43% (from 1,386 to 2,448)

> **Domain-based Message Authentication, Reporting and Conformance** (DMARC) protection in place has increased:

- From 58% to 68% of public sector organisations
- From 21% to 29% Universities
- From 21% to 27% further education colleges
- From 11% to 16% of the top 3,000 charities

Exercise in a Box (EiaB) - a toolkit of scenarios for organisations to refine their response to cyber security incidents.

> New users increased by 42% (from 11,851 to **16,808**)

Early Warning Service - a free service to notify members about potential attacks , compromises, vulnerabilities or open ports on their networks.

> Over 90% increase in signups this year (from 3,924 to 7,523)

> 34 million notifications issued about potential threats, risks, vulnerabilities or open ports in user's networks

Email Security Check - free for all UK organisations to check for correctly applied standards like DMARC and Transport Layer Security (TLS)

> Since launch in April 2022 the service has been used for **32,000 checks**

Vulnerability Disclosure Services - to report, manage and remediate vulnerabilities in government and other key services

> **Over 750 reported** vulnerabilities across the UK government remediated

Suspicious Email Reporting Service (SERS) allows the public to report potential scam messages for removal.

> Reports increased by 20% going from 5.4m to 6.5m

> Total number of reports reached 13.7m (since April 2020)

> 62k scam URLs removed, bringing total takedowns since SERS started to 174k
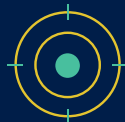
Takedown Service - works with hosts to remove malicious sites and infrastructure from the internet.

> Share of global phishing remained at 2%, in 2016 the figure was over 5%

> Number of fake UK government phishing scams decreased by 46% (from 13,000 to 6,000)

> 2.1 million cyber-enabled commodity campaigns removed

Web Check - helps users find and fix common security vulnerabilities in their websites.

> New users increased by 37% (from 3,539 to 4,849)

> 43% increase in unique URLs scanned using Web Check

> 12.5% increase in urgent findings reported to users, along with remediation advice